INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Papel desempenhado pela Gestão de Recursos Humanos na Cibersegurança Organizacional

Alexandrina Raquel Gouveia Ferreira

Mestrado em Políticas de Desenvolvimento dos Recursos Humanos

Orientador:
Doutor Henrique Duarte, Professor Associado com Agregação do Departamento de Recursos Humanos e Comportamento Organizacional de ISCTE-IUL

Outubro, 2024

CIÊNCIAS SOCIAIS
E HUMANAS

Departamento de Economia Política

Papel desempenhado pela Gestão de Recursos Humanos na Cibersegurança das Organizações

Alexandrina Raquel Gouveia Ferreira

Mestrado em Políticas de Desenvolvimento dos Recursos Humanos

Orientador:
Doutor Henrique Duarte, Professor Associado com Agregação do Departamento de Recursos
Humanos e Comportamento Organizacional de ISCTE-IUL

ISCTE – Instituto Universitário de Lisboa

Outubro, 2024

Agradecimentos

Dedico todo este trabalho à minha família, que mesmo estando a 967km de distância, fizeram sempre questão de demonstrar o seu apoio incondicional para continuar a correr atrás dos meus sonhos.

Abstract

The digital world is constantly evolving, offering many benefits across sectors but also presenting challenges that compel organizations to adopt strategies to mitigate risks. Numerous recent studies highlight organizational vulnerabilities tied to end-user negligence, putting organizational cybersecurity at risk. The need to mitigate these risks has prompted researchers to explore strategies, positioning HRM as central to stronger cybersecurity due to its connection with individuals.

Through a qualitative methodology, structured interviews were conducted with HR, IT, and other professionals to gauge HRM's role. Analysis following Bardin (2014) and Esteves (2006) principles revealed that while IT views HR as 'translators', HR seeks a central role in cybersecurity training. There is also a consensus on the importance of HR-IT collaboration for end-user awareness. Lastly, the participants were questioned about the importance of implementing practices related to CS in the Recruitment and Selection process and the HR denoted to be the professionals placing high value on integrating this practice. Findings allowed to verify all the Hypotheses formulated *a priori* and to prove that the role of HRM continues to be undervalued and to exist a necessity of explore more about this HRM role. In the other hand, it was found a growing appreciation for HRM's role in building a cybersecurity culture (CC) within organizations, reflecting a notable evolution from existing literature

Keywords: Human Resources Management; Information Technology; Cybersecurity; Cybersecurity Culture; Training; Recruitment and Selection process; *Awareness*;

Resumo

O mundo digital está em constante evolução e, apesar de acarretar diversas vantagens para os demais setores, traz também diversos desafios que obrigam as organizações a evoluir e adotarem estratégias para mitigar os riscos. A existência de diversos estudos elaborados nos últimos anos mostram a fragilidade as organizações relacionadas com o descuido dos *end-users* que estão a colocar a CS organizacional das mesmas em risco. A necessidade de mitigar estes riscos, levou estudiosos a pensar sobre que estratégias poderiam ser utilizadas internamente e, é desta forma que a GRH é colocada no centro da questão e percecionada, por estes estudiosos, como a possível solução para uma CS mais forte devido à sua ligação com os indivíduos.

Assim, através de uma metodologia qualitativa, com recurso a um guião de entrevistas estruturadas, foram elaboradas onze entrevistas a profissionais de Recursos Humanos, Tecnologias da Informação e de Outras Áreas de maneira a explorar as opiniões existentes sobre o papel da GRH nesta temática. Com a análise de conteúdo feita com base nos princípios de Bardin (2014) e Esteves (2006), constatou-se que em questões de formação os profissionais de TI consideram os RH meros 'tradutores' e que os RH consideram importante ter um papel mais central nestas formações. Aquando da exploração sobre a Consciencialização dos *end-users*, constatamos uma valorização de uma colaboração entre os RH e os IT como opinião geral a todos os envolvidos. Por último, foi igualmente explorada a opinião sobre a exploração de questões de CS nos processos de Recrutamento e Seleção e concluiu-se que os RH foram os profissionais que maior importância atribuiu a esta prática. Os resultados obtidos permitiram verificar todas as hipóteses elaboradas à priori e que o papel da GRH ainda se encontra desvalorizado em questões de CS nas organizações e há uma necessidade de explorar mais sobre esta questão. Por outro lado, constatou-se uma crescente valorização do papel da GRH no estabelecimento de uma CC nas organizações, o que representa uma evolução significativa em relação ao encontrado na literatura explorada.

Palavras-chave: Gestão de Recursos Humanos; Tecnologias da Informação; Cibersegurança; Cultura de Cibersegurança; Formação; Recrutamento e Seleção; Consciencialização

Indice de Tabelas

2.1 - Características dos Participantes 14

3.1 - Definição de Categorias 15

3.2 – Tabela de Categorias: Familiarização com o conceito 16

3.3 – Tabela de Categorias: Importância atribuída à Cibersegurança no contexto Organizacional 17

3.4 – Tabela de Categorias: Perceção dos Riscos cibernéticos no contexto organizacional 17

3.5 – Tabela de Categorias: Estabelecimento de uma Cultura de Cibersegurança numa Organização .19

3.6 – Tabela de Categorias: Práticas para estabelecer uma Cultura de Cibersegurança.....21

3.7 – Tabela de Categorias: Proximidade dos RH com os colaboradores internos 22

3.8 – Tabela de Categorias: Formação dos colaboradores (TI).....23

3.9 – Tabela de Categorias: Formação dos colaboradores (RH) 24

3.10 – Tabela de Categorias: Consciencialização dos colaboradores 25

3.11 – Tabela de Categorias: Consciencialização dos colaboradores (Colaboração RH e TI).....26

3.11 – Tabela de Categorias: Consciencialização dos colaboradores (Colaboração RH e TI).....27

3.13 – Tabela de Frequências 29

Glossário de Siglas

CS - Cibersegurança

TI – Tecnologias da Informação

GRH – Gestão de Recursos Humanos

RH – Recursos Humanos

CC – Cultura de Cibersegurança

IOT – *Internet of Things*

CO – Cultura Organizacional

PRH – Profissionais de Recursos Humanos

PTI – Profissionais de Tecnologias da Informação

POA – Profissionais de Outras Áreas

Introdução

O mundo globalizado e cada vez mais tecnológico em que vivemos traz inúmeras vantagens para o nosso quotidiano, tais como o acesso fácil a todo o tipo de informação, ferramentas e plataformas, mas acarreta também novos perigos, tais como o acesso indevido a informações pessoais e organizacionais. Esta crescente evolução tecnológica fez com as organizações ficassem cada vez mais expostas a perigos cibernéticos, o que as obrigou a colocarem a sua segurança cibernética como prioridade e investir na Cibersegurança (CS) interna. A CS, que pode ser brevemente definida como um conjunto de políticas, ferramentas, ações e tecnologias utilizadas para proteger o ciberespaço, e as suas estratégias convencionais, que se focavam essencialmente na componente técnica por detrás dos ataques cibernéticos, estratégias estas que aparentam já não ser suficientes, uma vez que à medida que a tecnologia avança, a complexidade destes ataques também evolui. Um relatório realizado pelo Willis Towers Watson em 2020, concluiu que cerca de 90% destes ciberataques acontecem devido a algum tipo de erro ou comportamento humano dentro das organizações (in Chief Executive, 2020). Desta forma, é cada vez mais importante que as organizações percecionem os seus membros como cruciais para assegurar a CS Organizacional e explorem maneiras de mitigar as fugas de informação causadas por indivíduos internos. A problemática em torno da Cibersegurança é tradicionalmente atribuída ao departamento de Tecnologia da Informação (TI) das organizações, no entanto, sendo complexo e dispendioso acompanhar a evolução técnica destes ataques cibernéticos, torna-se crucial trabalhar diretamente na falha humana existente por detrás destes e não apenas na parte técnica do problema, uma vez que os '*end-users'* são o alvo mais acessível dos cibercriminosos nas organizações.

A necessidade de trazer para a problemática da CS uma componente mais humana fez com que a Gestão de Recursos Humanos (GRH) começasse a ser percecionada como uma solução para mitigar estas fragilidades organizacionais cibernéticas relacionadas com os *end-users*. Assim, através de novas práticas e políticas direcionadas para a CS, a GRH, como vamos explorar ao longo desta dissertação, começou a ser vista como um elemento estratégico nesta temática. No entanto, este departamento na maioria das empresas não é o primeiro ponto de contacto ou quem gere a questão cibernética: estima-se que 88% das empresas continuam a

delegar estas questões para os departamentos de TI, o que faz com que o problema humano por detrás das brechas de informação não seja atribuído a importância devida (Marsh and Microsoft's Global Cyber Risk Perception Survey, 2019). Esta falta de integração direta dos Recursos Humanos (RH) pode originar numa fragmentação da abordagem de CS numa organização, onde os RH não estão familiarizados com o assunto e com a estratégia cibernética organizacional. Torna-se, por esta razão, essencial incluir todos os departamentos em assuntos de CS e garantir um envolvimento central dos RH (Hussin and Graepel, 2024). As práticas levadas a cabo pela GRH para a CS podem contribuir para o estabelecimento de um sentimento de responsabilidade geral, criar um ambiente onde a CS é percecionada como uma preocupação central e comum a todos os membros da organização e contribuir assim para o estabelecimento de uma Cultura de Cibersegurança (CC). Este tipo de cultura, que é definido como as atitudes, assunções, crenças e conhecimentos que os indivíduos internos às organizações utilizam para interagir com os sistemas e procedimentos organizacionais, é única a cada organização, deve estar ligada à cultura organizacional e não deve ser imposta aos colaboradores, mas sim criada em conjunto com os mesmos (Veiga, 2016). O conceito de CS, por ser um conceito muito atual e de extrema relevância nos dias de hoje, tende a ter diferentes perspetivas sobre a sua importância, os seus riscos associados e sobre por quem deve ser gerido organizacionalmente. Tendo em conta que, na maioria das empresas, este problema continua a ser atribuído apenas aos TI e à componente mais técnica da questão, esta investigação tem como objetivo explorar a importância que o departamento de RH e a GRH podem ter nestas questões e pretende responder à seguinte questão: Qual o papel da GRH na Cibersegurança Organizacional e de que maneira contribui para o estabelecimento de uma Cultura de Cibersegurança?

De modo a responder à questão, numa primeira fase será explorada a literatura existente sobre o tema, onde serão exploradas as possíveis práticas da GRH e como estas contribuem para o estabelecimento de uma CC. Após a análise teórica, será levada a cabo uma abordagem qualitativa recorrendo a entrevistas estruturadas onde serão exploradas as opiniões de Profissionais de RH, Profissionais de TI e Profissionais de Outras Áreas. Para além de responder à pergunta de investigação, tem também o objetivo de explorar as seguintes questões/objetivos: (1) Qual a importância da Cibersegurança Organizacional e quais os riscos associados à ausência de uma Cibersegurança estável? (2) Qual o papel da GRH na Formação e Awareness dos colaboradores na CS organizacional? (3) De que maneira estas práticas contribuem para o estabelecimento de um Cultura de Cibersegurança nas organizações?

Capítulo 1

Revisão de Literatura

1.1 Cibersegurança e a sua importância no contexto organizacional

A digitalização está em constante evolução e esta tem vindo a facilitar todas as tarefas outrora executadas manualmente, o que por sua vez aumentou a eficiência e rapidez dessas mesmas tarefas. As mais beneficiadas dentro da evolução foram as organizações, que através da implementação de ferramentas e plataformas digitais, viram a sua produtividade e eficiência aumentar. As empresas tornaram-se, em grande medida, dependentes da utilização da tecnologia. A interconectividade a nível mundial com a *Internet of Things* (IOT) trouxe consigo grande potenciais e um fácil acesso a todo o tipo de informação em segundos, mas trouxe também muitos riscos associados ao ciberespaço. É então necessário explorar em primeiro lugar em que consiste o ciberespaço, ligado ao prefixo de 'ciber' no termo Cibersegurança, para um melhor entendimento sobre este conceito central nesta investigação.

O ciberespaço é definido como um conjunto de sistemas de informação interconectados de evolução dinâmica, onde as pessoas se interligam e têm contacto com estes sistemas. O ciberespaço está em constante evolução e é, simplificando, um conjunto de softwares, ideias, interações e inovações que são influenciadas por aqueles que contribuem para o desenvolvimento e evolução deste. O ciberespaço é, nos dias de hoje, utilizado por milhares de indivíduos e organizações, que através de uma ligação têm acesso a todo o tipo de informação. A evolução constante do ciberespaço veio também facilitar o acesso indevido a informações pessoais e organizacionais, denominado de cibercrime, que representa hoje uma das maiores ameaças à integridade pessoal e sobrevivência organizacional. O cibercrime pode ser definido como um crime organizado no contexto do ciberespaço, onde cibercriminosos forçam o acesso a dados pessoais e organizacionais (Veiga, 2016). Estes acessos indevidos podem acarretar para as organizações vastas perdas financeiras, declínio da reputação das mesmas ou até mesmo violação de diretos humanos, quando dados pessoais são roubados e utilizados indevidamente.

Desta forma, a integridade do ciberespaço tornou-se fundamental tanto para as organizações públicas e privadas como para os indivíduos, sendo esta a razão pela qual a Cibersegurança se apresenta como tópico central nas organizações nos dias de hoje. Pouca importância foi atribuída a este conceito até ao início do século 21, no entanto, na última década tornou-se um tópico estratégico e de investimento para as empresas, uma vez que as ameaças cibernéticas têm vindo a crescer exponencialmente (Ciolan, 2014). O conceito de Cibersegurança não se foca exclusivamente na proteção do ciberespaço, mas também em proteger quem o utiliza, sendo definido como um conjunto de políticas, ferramentas, ações e formações tecnologias que podem ser utilizadas para proteger o ciberespaço, as organizações e os indivíduos (International Telecommunications Union, 2011). São então um conjunto de processos, práticas e medidas de mitigação desenhadas para proteger as redes de acesso indevido, destruição ou roubo de forma a garantir a confidencialidade, integridade e disponibilidade das mesmas (Public Safety Canada, 2014). Os modelos mais tradicionais de CS focavam-se essencialmente no investimento, evolução e proteção tecnológica dos seus sistemas, como a restrição de sites e alterações frequentes de palavras-chave (Beyer and Brummel, 2015). No entanto cada vez mais estudiosos chegam à conclusão de que a CS de uma organização é mais que uma preocupação tecnológica e que é essencial dar enfase à componente social e humana por detrás desta (Asiltürk, 2022). Uma organização só é capaz de ter políticas de CS eficazes quando esta é percecionada como um problema comum a todos os elementos da organização.

1.2 Cultura de Cibersegurança

De maneira que uma organização consiga garantir a eficácia das suas políticas e procedimentos relacionados com a CS, é necessário que todos os seus membros estejam aptos e motivados para reduzir o risco de ataques cibernéticos (Huang and Pearlson, 2019). É, portanto, necessário monitorizar e moldar os comportamentos dos *end-users* organizacionais para garantir uma CS estável e eficaz. No entanto, estes comportamentos são influenciados por diversos fatores tais como normas, pontos de vista e hábitos diferentes, o que dificulta a moldagem destes (Joison and Steen, 2018). Torna-se importante para as organizações criarem hábitos e uma Cultura Organizacional (CO) – Cultura de

Cibersegurança - onde a norma é respeitar as políticas de Cibersegurança e ter em atenção estes aspetos no seu dia a dia. A CO pode ser definida como um sistema de assunções, valores e crenças partilhadas que influenciam a forma como os indivíduos se comportam nas organizações (Pavlova, 2020). A CC é uma subcultura da CO e começou a ser mais explorada com o *boom* da tecnologia e das ameaças cibernéticas. Esta apresenta-se, não só como o cumprimento e respeito pelas políticas internas, mas também com o envolvimento pessoal dos indivíduos na segurança cibernética da sua organização (Huang and Pearlson, 2019). Este tipo de cultura pode ser definido como as atitudes, assunções, crenças e conhecimentos que os membros internos utilizam para interagir com os sistemas e procedimentos das suas organizações, interação esta que resulta em bons e maus comportamentos cibernéticos (Da Veiga, 2016). A CC é única a cada organização e esta diz muito sobre a CS da mesma, quanto mais eficiente, robusta e transversal esta cultura for, melhor será a resistência organizacional a qualquer tipo de ameaça cibernética externa. Para que esta cultura seja forte, é necessário estar diretamente ligada à CO e estar adaptada às necessidades e práticas dos seus colaboradores (ENISA, 2017)

1.3 A Gestão dos Recursos Humanos e Cultura de Cibersegurança

A proteção de dados tem sido uma preocupação central na agenda das organizações, no entanto algumas pequenas e médias empresas continuam a funcionar de forma tradicional, onde as questões relacionadas com a CS encontram-se ainda muito concentradas, ou apenas no departamento de TI ou nos altos quadros das mesmas, representando apenas uma preocupação para a gestão de topo e para uma pequena percentagem de indivíduos dentro de uma organização (Pace, 2016). Desta forma, e como supramencionado, a CS ainda é frequentemente percecionada como um problema maioritariamente tecnológico, o que faz com que a gestão de topo atribua esta responsabilidade ao departamento de TI, se foquem essencialmente no investimento de novos sistemas e na contratação de profissionais de TI altamente qualificados como solução para a ameaça cibernética (Asiltürk, 2022). No entanto, as estratégias utilizadas pelos cibercriminosos são cada mais complexas, o que torna impossível às organizações

monitorizarem os padrões de comportamento e as novas técnicas utilizadas por estes, assim como investir em novas tecnologias com o intuito de se salvaguardarem.

De acordo com estudo levado a cabo em 2021, concluiu-se que o erro humano é a causa de 95% das fugas de informação nas organizações (Forbes, 2021). Assim, os colaboradores internos, através de comportamentos negligentes maliciosos ou não maliciosos, são considerados uma das principais ameaças à integridade da CS organizacional (Pace, 2016). Num artigo publicado em 2022, a Forbes explora alguns dos hábitos mais comuns dos *end-users* que podem colocar em causa todo o investimento feito na CS de uma organização, tais como adiar a atualização de *softwares*, visitar sites desconhecidos e não terem em atenção o nível de segurança das suas palavras-chave de acesso. Os *end-users* ao levarem a cabo, consciente ou inconscientemente, alguma destas simples práticas, podem estar a comprometer a segurança cibernética da sua organização, facilitando o acesso indevido a informações internas, dados pessoais ou financeiros, assim como a utilização não autorizada destas informações (Kweon et al., 2019). Desta forma, a estratégia tradicional e dispendiosa de investir em tecnologia mais avançada para mitigar estes ataques torna-se ineficiente, uma vez que o grande problema poderá ter início nos indivíduos internos às organizações. Os indivíduos nem sempre são a porta de entrada destas ameaças, mas são, de facto, onde a organização pode ter cuidados acrescidos (Choi, 2017).

São com estes argumentos que tem sido explorada a necessidade de trazer a esta problemática uma componente mais humana e de gestão direcionada aos end-users das organizações. É defendida uma abordagem holística, onde o departamento de TI trataria da parte mais técnica da CS organizacional, através da implementação dos sistemas adequados para garantir a segurança da informação e a Gestão de Recursos Humanos ficaria responsável por pôr em prática, diretamente com os end-users, as políticas, práticas e procedimentos adequados e que criassem nas organizações uma cultura direcionada para tal (Pace, 2016). Os RH sendo o departamento de uma empresa com mais ligação e mais impacto nos membros internos, podem detetar padrões de comportamento dos indivíduos, e vir a ser a solução, em conjunto com os TI, para mitigar os ataques cibernéticos que usam os indivíduos internos das empresas como meio para os executar (ENISA, 2017). Para que a CS de uma organização seja assegurada é necessário que todos os seus membros tenham conhecimento de todas as práticas, políticas, cuidados e procedimentos relacionadas com o tema (Kweon et al. 2019). É, portanto,

necessário que os indivíduos tenham o conhecimento suficiente sobre o conceito de CS e a importância de assegurar a estabilidade da CS da sua organização, assim como saberem de que maneira devem agir quando estão em situações de risco. A CS organizacional e a importância que os indivíduos atribuem a esta está diretamente relacionada com a forma como estes vêm e se sentem em relação à sua organização (Choi, 2017). Isto é, quando os indivíduos se sentem mais envolvidos e próximos da sua empresa, tendem a zelar pelo bem-estar da mesma, o que por sua vez os faz ter mais consciência e um cuidado acrescido com as questões de CS interna (Choi, 2017).

É inegável a importância do papel dos TI no que concerne à componente técnica da CS, uma vez que será sempre necessária uma constante manutenção técnica para que o risco de fugas de informação seja menor. No entanto, a vulnerabilidade dos *end-users* numa organização em relação aos cibercriminosos, e como defendem os estudiosos aqui mencionados, poderá ser mitigada com a GRH e a sua relação próxima com estes *end-users* organizacionais, que com o seu conhecimento transversal de todas as áreas e funções dentro da organização podem fazer chegar aos colaboradores um apoio e formação mais personalizada e eficaz (ENISA, 2017). Assim, a GRH pode também ter um papel preponderante na mudança de comportamentos e de visão dos indivíduos no que concerne a questões relacionadas com a CS, assim como contribuir em grande medida para o estabelecimento de uma CC. A forma como a CC é percecionada pela gestão de topo e pela GRH é essencial para assegurar a credibilidade e estabilidade da mesma. É necessário que a CS e a sua integridade sejam percecionadas como prioridade para todos os membros de uma organização, sendo por isto importante que a GRH demonstre a importância que atribui ao tópico e providenciem um acompanhamento continuo sobre o mesmo (Reegård et al, 2019). É aqui que entram as práticas da GRH e a forma como estas podem contribuir para o estabelecimento de uma CC numa organização.

1.4 As práticas da Gestão dos Recursos Humanos no estabelecimento de uma Cultura de Cibersegurança:

1.4.1 Recrutamento e Seleção

O Recrutamento e Seleção é, em grande parte das organizações, o primeiro contacto que os RH estabelecem com possíveis futuros colaboradores. Sendo esta a porta de entrada para qualquer organização, é possível serem adotadas práticas e medidas desde esta fase incipiente do processo de entrada de novos membros com o objetivo de mitigar o risco associado à fuga de informação a longo prazo e contribuir para a implementação de uma CS robusta **(**Wipawayangkool, 2010). Numa fase embrionária do processo de seleção é possível explorar a importância que os indivíduos atribuem à proteção de dados, através de verificações de antecedentes, avaliar os candidatos quanto ao seu conhecimento sobre a CS e perceber se estão alinhados com a organização nessa matéria (Mizrak, 2023). Práticas como verificação de registo criminal, elaboração de questionários sobre a perceção pessoal da proteção de dados e CS para avaliar a postura dos candidatos quanto a esta problemática, incluindo conceitos como o *phising*, senhas de acesso e uso seguro da internet, podem contribuir para o estabelecimento de uma CC desde cedo na organização.

Aquando da seleção de candidatos e efetiva entrada na organização, é também importante fornecer-lhes apenas o acesso à informação necessária para a sua função na empresa (Mizrak, 2023). Esta prática da GRH torna-se essencial para garantir que apenas as pessoas indicadas têm acesso a determinada informação da organização, contribuindo assim para um menor risco da fuga, acesso e utilização indevida desta informação (Menaka, 2022). Para além disto, é possível implementar desde esta fase sessões iniciais de formação e de esclarecimento onde são apresentadas as iniciativas e políticas da organização sobre a CS. Uma vez que o Recrutamento e Seleção apresenta-se na literatura como uma das práticas possíveis da GRH para contribuir ativamente para a CS Organizacional e para o estabelecimento de uma CC, considerou-se essencial explorar a importância atribuída pelos profissionais entrevistados de serem exploradas questões relacionadas com a CS numa fase de Recrutamento e Seleção. No entanto, tendo em conta que esta prática diz respeito aos profissionais de RH, prevê-se que estes profissionais

atribuirão uma maior importância a esta prática, tendo sido sendo por esta razão elaborada a Hipótese nº1:

H1: Os profissionais de RH, em relação aos restantes profissionais, atribuem uma maior importância à implementação de práticas relacionadas com a Cibersegurança durante os processos de Recrutamento e Seleção.

1.4.2 Awareness (Conciêncialização)

Uma vez que se tem vindo a verificar que os colaboradores internos das empresas são frequentemente a porta de entrada de ameaças externa nas organizações, torna-se importante resolver o problema de dentro para fora. Como já mencionado anteriormente, grande parte das empresas tendem a apostar em novas tecnologias para mitigar estes ataques cibernéticos em vez de investir na formação e consciencialização dos seus colaboradores através dos RH (Kweon et al., 2019). A consciencialização é diferente de formação, esta é utilizada para moldar comportamentos ou reforçar algumas práticas de CS (National Institute of Standards and Technology, 2003). O propósito desta prática da GRH é trazer a atenção dos indivíduos para as questões relacionadas com a CS e a proteção de dados, através da qual os colaboradores são capazes de percecionar o grau de importância desta questão para a sua organização e as consequências que o descuido nestes tópicos podem trazer para o colaborador e para a própria organização (Wipawayangkool, 2010). Uma organização que tenha boas práticas e políticas de CS, mas que não as faz chegar aos seus colaboradores, está a contribuir para o enfraquecimento e ineficácia das mesmas, sendo por isto de extrema importância existirem sessões de consciencialização frequentes para os *end-user* internos (Kweon et al., 2019). Práticas como workshops e palestras educacionais ministradas pelo departamento de TI, simulações de *phising*, onde são partilhados métodos de identificação de possíveis emails maliciosos, simular situações de manipulação, realizar sessões sobre como criar palavras-chave seguras e que cuidados a ter, como identificar possíveis ameaças e como agir em tais situações poderão ter um impacto significativo na perceção e sentimento de responsabilidade geral dos colaboradores. Para além disto, poderão também ser feitos concursos e desafios de maneira a

promover um maior dinamismo e interação por parte dos colaboradores, assim como exposição e partilha de panfletos informativos nos espaços comuns.

Uma vez que os colaboradores representam a maior ameaça no que concerne à CS organizacional devido, na maioria das vezes, à sua falta de conhecimento sobre o assunto, é essencial promover o interesse deste em saber mais sobre o ciberespaço, cibercrime e CS, assim como garantir a motivação em serem orientados e formados no assunto.

Desta forma, a *Awareness* dos *end-users* poderá ser mais eficaz se os RH e os TI trabalharem em conjunto. Os TI, com o seu conhecimento mais aprofundado sobre Cibersegurança e sobre os riscos associados a esta podem colaborar com os RH na passagem da informação, onde estes últimos, com o seu conhecimento de cada função e facilidade de comunicação podem ser fator chave para o sucesso de uma CS organizacional.

H1: Tanto os profissionais de RH como os profissionais de TI vêm uma colaboração entre si como vantajosa na consciencialização dos colaboradores em questões de Cibersegurança.

1.4.3 Formação

A GRH ao promover a consciencialização dos *end-users* leva-os a estar mais recetivos à formação, que se apresenta como uma das práticas mais importante no que concerne à CS organizacional. Esta prática difere, em grande medida, da prática de consciencialização, uma vez que a formação tem como objetivo desenvolver e adquirir competências técnicas para garantir a segurança da informação (National Institute od Standards and Technology, 2003). Fornecer formação em assuntos de CS dá a capacidade aos colaboradores, que são a primeira linha de defesa contra as ameaças externas, de identificar e responder a potenciais ataques cibernéticos (Mizrak, 2023), como por exemplo, detetar possíveis emails de *phising*, como partilhar dados de forma segura ou como enviar informação confidencial utilizando encriptação (Joison and Steen, 2018). Um estudo levado a cabo em 2017 concluiu que a existência de formações e exercícios práticos que evidenciem o porquê da adoção e existência de certas políticas internas traz maior credibilidade para as mesmas (Ramakrishna & Figueroa, 2017) Desta forma, a existência de formações contínuas sobre esta temática faz com que os

colaboradores adiram e respeitem mais as políticas e práticas relacionadas com as informações às quais têm acesso (Kumah *et al*., 2018).

Desta forma, estudos de caso reais de incidentes, exercícios e simulações de situações de risco e de crise contribuem para uma maior sensibilização dos colaboradores com estas situações, uma maior confiança quando deparados com certas situações, assim como para a mitigação destes riscos (Zafar, 2013). Para além disto, demonstrar como funcionam as ferramentas e aplicativos utilizados para a deteção, tais como *firewalls* e antivírus, faz com que os colaboradores entendam como cada ferramenta e aplicativo ajuda na proteção dos sistemas. É essencial conhecer claramente as tarefas, comportamentos e o ambiente de cada função para que os programas de formações consigam ser desenhados para cada função e consigam responder aos objetivos institucionais (Beyer and Bummer, 2015). A GRH, através de uma equipa de *Learning and Development,* equipa esta que tem como objetivo central monitorizar as necessidades de desenvolvimento e formação interna, através do seu conhecimento sobre as funções de cada membro de uma organização, em conjunto com o departamento de TI, podem tornar estas sessões mais personalizadas ao criar formações adaptadas às diferentes funções e necessidades dos seus colaboradores (Reegård et al., 2019). As organizações não devem assumir que os seus colaboradores já têm o conhecimento suficiente sobre a segurança da informação associada às suas tarefas diárias e sistemas de informação aos quais têm acesso diariamente nas suas funções, e deve promover assim sessões de esclarecimento sobre as políticas e leis de proteção de dados e de como reconhecer e agir perante ameaças cibernéticas (Jameel and Ramazan, 2024).

H3: Os RH, em relação aos restantes profissionais, consideram ter um papel ativo no levantamento de necessidades e desenho de formação relacionados com a CS, enquanto os profissionais de TI os consideram meros 'tradutores'

Capítulo 2

Enquadramento e Metodologia da Investigação

2.1 Abordagem Qualitativa

Neste capítulo apresentamos as linhas metodológicas que guiaram esta investigação. Considerando a temática e os objetivos propostos para esta investigação, considera-se que a metodologia qualitativa será a metodologia mais adequada para a recolha de dados. A abordagem qualitativa investiga ideais e centra-se na análise de casos concretos, o que se aplica a esta investigação, e cujo objetivo é explorar as opiniões e ideais dos envolvidos. A escolha dos profissionais em questão passou por uma estratégia de comparação de perspetivas individuais sobre o assunto e comparar com a informação explorada na literatura.

2.2 Técnicas de Recolha de Dados

Considerando os objetivos definidos e a metodologia escolhida, recorremos a entrevistas estruturadas como técnica de recolha de dados (anexo C, D e E). As questões colocadas aos participantes foram estruturadas *à priori* tendo em conta a literatura recolhida e os objetivos estabelecidos para a investigação, de maneira a garantir similaridade de conteúdo e recolher dados comparáveis entre os participantes. Estas questões tinham, em todos os tipos de participantes, o mesmo objetivo, mas foram adaptadas à realidade de cada profissional.

De modo a garantir uma experiência igual a todos os participantes, as entrevistas foram feitas através da plataforma *Zoom*, onde foram criadas as reuniões e enviados os links de acesso aos participantes aquando da sua confirmação de interesse e disponibilidade. Os convites de participação nas entrevistas foram enviados através de correio eletrónico (anexo A) onde foi explicado o objetivo das entrevistas, o tema e para que fins seriam utilizados os dados recolhidos. Para além disto, no convite enviado e durante as entrevistas os participantes foram informados que as mesmas seriam gravadas e que as gravações seriam ocultadas e eliminadas assim que concluída a investigação, assim como confirmado o consentimento dos envolvidos com as mesmas. As entrevistas levadas a cabo tiveram uma duração média de 20 a 25 minutos.

2.3 Participantes

O público-alvo definido para esta investigação teve por base a informação recolhida na revisão literária. Foram entrevistados onze profissionais de diferentes sector e áreas: Profissionais de Recursos Humanos, Profissionais de Tecnologias e Informação e Cibersegurança e Profissionais de Outras Áreas. A escolha dos tipos de profissionais em questão passou pela estratégia de comparação supramencionada que vai de encontro aos objetivos desta investigação: explorar as opiniões e perspetivas destes profissionais em relação ao tema. Os profissionais de RH considerou-se fazer todo o sentido incluir, de maneira a explorar as perspetivas dos próprios profissionais em relação ao tema, os profissionais de TI de maneira a explorar as suas opiniões sobre o assunto e se vão de encontro com o foi explorado na literatura e os profissionais de outras áreas com o intuito de explorar as opiniões de profissionais não relacionados com o tema. De maneira a garantir a confidencialidade prometida aos envolvidos e facilitar a análise e exploração dos dados, cada profissional foi identificado como: Profissional de RH de 1 a 5, Profissional de TI de 1 a 4 e Profissional de Outras Áreas 1 e 2:

Participantes	**Género**	**Idade**
PRH1	F	24
PRH2	F	25
PRH3	F	31
PRH4	F	30
PRH5	M	27
PTI1	M	24
PTI 2	M	26
PTI 3	M	27
PTI 4	M	46
POA1	F	25
POA2	M	40

Tabela 2.1 - Características dos Participantes

Capítulo 3

Análise de Conteúdo e Definição de categorias

3.1 Análise de Contéudo

A análise de conteúdo é definida como a interpretação e redução de longas comunicações em categorias de conteúdo guiando-se por regras de codificação (Stemler, 2001). Para proceder a esta análise seguimo-nos por três fases distintas: A pré-análise (1), que consiste em organizar e sistematizar as ideias a partir da leitura de documentos e da criação de hipóteses e indicadores, a exploração do material (2), que representa a fase de análise propriamente dita, e o tratamento de os resultados, a inferência e a interpretação (3), que tem como objetivo a organização e interpretação dos dados de maneira a torná-los significativos (Bardin, 2014). Após a análise e leitura de toda a informação recolhida das entrevistas, procedeu-se a uma análise categorial, análise central numa análise de conteúdo e que é definida como a classificação e redução dos dados pertinentes para a investigação (Esteves, 2006). Assim, através da categorização, é possível simplificar e classificar os dados recolhidos de maneira a facilitar a sua interpretação. Numa fase inicial foi feita uma análise do conteúdo obtido e definidas as categorias e sub-categorias, tento em conta as regras de categorização de Bardin: Exclusividade, Homogeneidade, Objetividade, Fidelidade e Pertinência:

Categoria	Subcategoria	Código
A. O Conhecimento geral do Conceito da Cibersegurança	A.1 Familiarização com o conceito	**FC**
	A.2 Importância atribuída à Cibersegurança no contexto Organizacional	**IC**
	A.3 Perceção dos Riscos cibernéticos no contexto organizacional	**PR**
B. Cultura de Cibersegurança	B.1 Responsáveis pelo estabelecimento de uma Cultura de Cibersegurança numa Organização	**RCC**
	B.2 Práticas para estabelecer uma Cultura de Cibersegurança	**PCC**
C. A Cibersegurança Organizacional	C.1 Proximidade dos RH com os colaboradores internos	**PC**
	C.2 Formação dos colaboradores	**PF**
	C.3 Consciencialização dos colaboradores	**CC**
	C.4 Práticas levadas a cabo no processo de Recrutamento e Seleção	**PRS**

Tabela 3.1 - Definição de Categorias

3.1 Apresentação, Análise e Discussão dos Resultados

Neste capítulo serão apresentados e discutidos os resultados obtidos com as análises das entrevistas dos onze participantes. Primeiramente será apresentada descritivamente cada categoria e as suas sub-categorias, de maneira a facilitar a apresentação e leitura da informação recolhida e posteriormente, a discussão de resultados, recorrendo a excertos dos participantes e à revisão de literatura.

Categoria A – O conhecimento geral do Conceito de Cibersegurança

Esta categoria foi dividida em três subcategorias: Familiarização com o conceito, Importância atribuída à Cibersegurança no contexto Organizacional e Perceção dos Riscos cibernéticos no contexto organizacional. Uma vez que o conceito de Cibersegurança é um conceito relativamente recente no contexto organizacional, consideramos importante explorar o conhecimento de cada profissional sobre o conceito a nível organizacional. Com a análise das entrevistas, constatamos que todos os participantes estavam familiarizados com o conceito:

Categoria	Subcategoria	Excertos mais relevantes
Categoria A – O conhecimento geral do Conceito de Cibersegurança	A.1 Familiarização com o conceito	"'Apesar de não ser especialista, Cibersegurança está, tal como o nome indica, associada à segurança do espaço cibernético" (PRH1) "Ok, portanto, o que eu entendo por Cibersegurança é no fundo todas as práticas levadas a cabo para proteger todas as informações confidenciais dentro de uma empresa." (PRH2) "A Cibersegurança é a prática de proteger tudo o que seja hardwares e softwares numa empresa, neste caso computadores, dispositivos móveis, a rede..." (PTI2)

Tabela 3.2 – Tabela de Categorias: Familiarização com o conceito

Para além da familiarização com o conceito, considerou-se importante explorar a importância atribuída pelos profissionais em questão, principalmente aos da área de RH e de Outras Áreas, uma vez que são áreas que por norma não estão diretamente relacionadas com o

conceito. Constatou-se que todos os profissionais entrevistados consideram a Cibersegurança importante para as organizações:

Categoria	Subcategoria	Excertos mais relevantes
Categoria A – O conhecimento geral do Conceito de Cibersegurança	A.2 Importância atribuída à Cibersegurança no contexto Organizacional	"Acho que é super importante nas organizações, principalmente aquelas que lidam com clientes, pessoas externas e muitos dados e informações confidenciais" (PRH2) "A importância é enorme porque caso aconteça algum incidente podemos sofrer, quer na nossa imagem quer monetariamente e estamos numa era digital, a informação vale dinheiro e se essa informação é partilhada de forma ilegal ou se usa essa informação de forma ilegal podem ter vantagens com isso" (PIT3) "É cada vez mais importante que haja todo uma preocupação com o domínio da Ciberseguranca" (POA2)

Tabela 3.3 – Tabela de Categorias: Importância atribuída à Cibersegurança no contexto Organizacional

Para além da exploração do conceito e da sua importância a nível organizacional, considerou-se pertinente explorar a perceção individual dos riscos da ausência de uma Cibersegurança Organizacional. Os riscos mais mencionados foram os riscos financeiros e fuga ou utilização não autorizada de dados internos:

Categoria	Subcategoria	Excertos mais relevantes
Categoria A – O conhecimento geral do Conceito de Cibersegurança	A.3 Perceção dos Riscos cibernéticos no contexto organizacional	"Os riscos podem ser muito variados desde o roubo de informações confidenciais mais relacionada com os RH, com os colaboradores para outros fins, ou então também temos aqui riscos muito graves a nível financeiro." (PRH5) "Podem ir desde o simples acesso ao computador e perda de toda a informação ou cópia dessa informação, que pode ser informação banal como pode ser informação sensível..." (POA2) "Risco de reputação, risco monetário, acabam por ser estes os principais" (PIT3)

Tabela 3.4 – Tabela de Categorias: Perceção dos Riscos cibernéticos no contexto organizacional

Nestas duas primeiras questões, que foram utilizadas para enquadrar os participantes no tema, conclui-se que tanto os profissionais de RH, como os de TI e Outras Áreas estão familiarizados com o conceito, consideram este importante para a sobrevivência organizacional e estão a par dos riscos que a ausência de uma Cibersegurança pode ter numa organização. No entanto, e como era esperado, os profissionais de TI utilizaram termos mais técnicos como 'ataques maliciosos' (PTI2), 'base de dados' (PTI4), 'estrutura' (PTI1), 'rede' (PTI4) aquando destas questões, o que demonstra uma maior *expertise* sobre o assunto. Apesar da CS ser um assunto relativamente recente no contexto organizacional de muitas empresas, a amostra recolhida nas entrevistas demonstra que tanto os profissionais diretamente relacionados com a área da tecnologia como os outros profissionais de outras áreas, estão minimamente a par sobre a CS, sobre a sua importância no contexto organizacional e os riscos da sua ausência.

Categoria B - Cultura de Cibersegurança

Esta segunda categoria inclui duas sub-categoria: Responsáveis pelo Estabelecimento de uma Cultura de Cibersegurança numa Organização e Práticas para estabelecer uma Cultura de Cibersegurança. O conceito de Cultura de Cibersegurança é, como explorado no Capítulo 1, uma subcultura da Cultura Organizacional e surgiu com o *boom* da digitalização e com a crescente necessidade das organizações de se adaptarem às novas realidades. Uma vez que este tipo de cultura está diretamente relacionado com todas as práticas organizacionais levadas a cabo para fortalecer a CS organizacional, considerou-se importante explorar a perceção individual de cada um dos profissionais sobre este tipo de Cultura e sobre quem consideram ser os responsáveis por a implementar a nível organizacional. Nesta questão as opiniões foram diversas: denotamos que os profissionais de TI mencionaram, em todas as suas respostas a esta questão, a importância central dos RH nesta temática, ou seja, consideram os RH como um dos principais departamentos dentro de uma empresa que contribui ou deve contribuir para o estabelecimento deste tipo de Cultura numa organização. Esta profissionais consideram os RH como o departamento responsável pela implementação deste tipo de cultura, uma vez que são os 'tradutores', 'porta-voz' e quem implementa as ideias nos colaboradores. No entanto, observamos as respostas dos profissionais de RH e de AO, conseguimos constatar que consideram existir não só um papel dos RH nesta temática, mas também o papel do

departamento de TI. Na tabela seguinte é possível comparar as respostas dadas diferentes grupos de profissionais

Categoria	Subcategoria	Excertos mais relevantes
B. Cultura de Cibersegurança	B.1 Estabelecimento de uma Cultura de Cibersegurança numa Organização	"Os Recursos Humanos têm o nosso contacto direto, sempre que é necessário é com eles que tratamos, mesmo a nível pessoal. Posso afirmar que os Recursos Humanos fazem parte dessa questão." (PTI1) "(…) temos outras equipas como por exemplo de Recursos Humanos que têm um papel fundamental na implementação de ideias da Cibersegurança nos colaboradores" (PTI2) "Eles, os RH, por norma são os porta-voz. São os nossos "tradutores"… por isso sim, contribuem." (PTI3) "Os RH têm de informar as pessoas do que devem e não devem fazer, é esse o papel e a maneira que contribuem para esta cultura." (PTI4) "por isso cabe aos RH e os IT a darem todas as ferramentas e conhecimentos necessários para que os colaboradores tenham um papel fundamental na proteção dos dados." (PRH5) "Portanto a nível de formação, serem os Recursos Humanos a dar a formação, obviamente em conjunto com o departamento de Sistemas de Informação." (PRH2) "…o departamento de IT, juntamente com um departamento de RH ou de formação, dependendo da existência do departamento ou não na entidade, e terá de existir uma definição de procedimentos muito bem desenvolvida pelo departamento de TI" (POA2)

Tabela 3.5 – Tabela de Categorias: Estabelecimento de uma Cultura de Cibersegurança numa Organização

Estes três profissionais, PRH5, PRH2 e POA2 mencionaram a importância de existir influência dos dois departamentos, em conjunto ou não, no estabelecimento deste tipo de cultura dentro de uma organização. Dos cinco profissionais de RH entrevistados, três (60%) mencionam apenas os RH como principal responsável pelo estabelecimento desta cultura e, por

outro lado, os profissionais de AO, a opinião dividiu-se pelos dois profissionais entrevistados. Desta forma, em questões de implementar uma Cultura de Cibersegurança, os profissionais de TI atribuem a responsabilidade também aos RH, isto é, consideram que os RH são também responsáveis por passar para o resto da organização, como Huang e Pearlson (2019) defendem, o respeito e o envolvimento nas questões cibernéticas. Uma vez que este tipo de cultura é definido como as crenças, assunções e conhecimentos que os colaboradores internos têm sobre a CS e sobre a proteção de dados (Da Veiga 2016), conclui-se que o departamento de TI considera que os RH são quem deve trabalhar para passar o *mindset* correto aos colaboradores nestas questões. Em grande parte das temáticas organizacionais, a passagem de informação é na maioria das vezes uma responsabilidade atribuída aos RH, por terem esse *know how* e por serem o departamento dedicado aos colaboradores, no entanto, em temáticas de CS organizacional e como constatado com a literatura explorada, por ser um tema tão recente e muitas vezes atribuído apenas aos TI e não ser percecionado com uma responsabilidade geral de uma organização, o papel dos RH nestes casos torna-se menor ou até inexistente. Assim, e como defendido pelos estudiosos mencionados ao longo desta dissertação, considera-se estratégico a GRH ter cada vez mais um papel central e ativo nestas questões, uma vez que se têm concluído que os *end users*/colaboradores estão no centro de grande parte das fugas da informação e que o envolvimento crescente da GRH nestas questões pode ser uma estratégia eficaz na mitigação dessas fugas. As opiniões recolhidas demonstram que a tradicional responsabilização em questões mais tecnológicas que eram atribuídas apenas ao departamento de TI pode estar a evoluir e a existir uma crescente contribuição de outros departamentos, tal como o dos RH. Para além disto, alguns dos entrevistados deram alguns exemplos de práticas que podem contribuir para a implementação deste tipo de cultura:

Categoria	Subcategoria	Excertos mais relevantes
B. Cultura de Cibersegurança	B.2 Práticas para estabelecer uma Cultura de Cibersegurança	"Se dentro do próprio departamento/equipa tiverem focada em ter mais cuidado e um melhor comportamento com segurança dos dados/informação, acaba por passar esse tipo de cultura e maneira de ver a cibersegurança para os colaboradores. " (PRH1) " (…) o departamento de RH deve sempre agir como dando o melhor exemplo a restante população da empresa..." (PRH4) "Isto também ser um passo importante na integração dos colaboradores para ficarem a conhecer a importância da cibersegurança e a importância de respeitá-la e irem esporadicamente relembrando essa importância" (PRH2) "(…) onde é explicado no *onboarding* o que têm acesso e o que podem ou não fazer." (PRH3) "Eu acho que isto tem de começar desde o primeiro momento, desde o processo de recrutamento, com o reforço da importância da proteção dos dados." (PRH5)

Tabela 3.6 – Tabela de Categorias: Práticas para estabelecer uma Cultura de Cibersegurança

Consideram importante dar o exemplo, ou seja, "*Se dentro do próprio departamento/equipa tiverem focada em ter mais cuidado e um melhor comportamento com segurança dos dados/informação, acaba por passar esse tipo de cultura e maneira de ver a cibersegurança para os colaboradores. "* (PRH1*).* Como defende Reegård et al (2019), e como explorado no Capítulo 2, é importante que seja passado aos colaboradores a importância que o próprio departamento atribui à CS e à CC para garantir a estabilidade e credibilidade da mesma. Numa empresa onde os RH não demonstrem responsabilidade na gestão da informação, mais difícil se torna implementar este tipo de cultura. Para além disto, mencionaram também a importância de dar a conhecer a importância atribuída à CS no processo de recrutamento e *onboarding*, pois pode ser *"…um passo importante na integração dos colaboradores para ficarem a conhecer a importância da Cibersegurança e a importância de respeitá-la…"* (PRH2). Três dos onze profissionais entrevistados partilharam considerar essencial partilhar, numa fase incipiente do processo de seleção e recrutamento, a importância que a própria organização atribui à CS. Para

além disto, poderá ser também essencial, e como defendido por Mizarak (2023), explorar a própria importância atribuída pelos candidatos a esta temática, de maneira a perceber se estão alinhados com a própria organização.

Categoria C - Cibersegurança Organizacional

Esta categoria divide-se em quatro sub-categorias: Proximidade com os colaboradores internos, Formação dos colaboradores, Consciencialização dos colaboradores e Práticas levadas a cabo no processo de Recrutamento e Seleção. A proximidade dos colaboradores internos foi mencionada por dez dos onze entrevistados e mais que uma vez em algumas das entrevistas, alguns exemplos:

Categoria	Subcategoria	Excertos mais relevantes
C. A Cibersegurança Organizacional	C.1 Proximidade dos RH com os colaboradores internos	"Como estava a dizer, o primeiro passo somos sempre nós, como profissionais de RH, uma vez que lidam com informações pessoais e são o contacto mais próximo dos colaboradores" (PRH1) "E claro que, os Recursos Humanos deveriam de ter um papel muito importante nisso porque são o departamento mais próximo das pessoas na empresa." (PRH2) "(…) temos de trabalhar em conjunto para chegarmos a todos numa empresa, os Recursos Humanos conseguem muito mais facilmente que eu. "(PTI1) "São os que estão mais próximos dos end-users" (PTI3) "Acho que essencialmente RH até porque são o departamento mais próximo dos colaboradores que à partida conhece melhor as condições dos colaborares e o espaço da empresa." (POA1)

Tabela 3.7 – Tabela de Categorias: Proximidade dos RH com os colaboradores internos

Tal como a European Network and Information Secutiry Agency (ENISA) defende no seu relatório de 2017, os RH são, por norma, o departamento com mais ligação e maior impacto nos membros internos de uma organização. O departamento de RH tem, tendencionalmente, uma relação mais próxima com os colaboradores, no entanto, devido aos diversos fatores mencionados ao longo desta dissertação, em questões de CS organizacional não é atribuída tanta importância a esta proximidade. Por esta razão, e por ter sido mencionada diversas vezes pelos participantes, considerou-se essencial explorar esta subcategoria, uma vez que, e como já explorado, esta proximidade dos RH com os colaboradores em questões de CS pode apresentar-se como uma solução para a vulnerabilidade dos *end-users.*

Quanto à sub-categoria da Formação dos colaboradores, denotou-se uma opinião geral nos profissionais de TI envolvidos: necessidade de tradução e clareza na passagem da informação através dos RH:

Categoria	Subcategoria	Excertos mais relevantes
C. A Cibersegurança Organizacional	C.2 Formação dos colaboradores	"(…) temos sempre o apoio dos Recursos Humanos porque podem fazer o encaminhamento principal das formações desenhas e pensadas por nós e nós já só estamos no back office. Passam a mensagem mais simplificada." (PTI1) "É por isso que muitas das vezes estamos ligados aos Recursos Humanos, damos formação para isso também. Eles são os nossos tradutores." (PTI2) "(…) reunimos com eles e os RH traduziram e adaptaram a formação para os colaboradores e teve um papel fundamental de modo a conseguirmos transmitir a mensagem da melhor forma. São os nossos tradutores." (PTI3) "Neste caso considero importante que sejam os RH a validar as formações que são importantes para cada área. Todos têm de ter formação, mas têm de ter formações adequadas e só os RH é que têm mais noção das necessidades de cada função. No entanto conheço a realidade de algumas empresas e os RH não têm muito voto nesta matéria" (PTI4).

Tabela 3.8 – Tabela de Categorias: Formação dos colaboradores (TI)

No entanto, a opinião dos profissionais de RH entrevistados centra-se não só na importância do seu papel na passagem e simplificação de informação, mas também no levantamento de necessidade e desenho das mesmas:

Categoria	Subcategoria	Excertos mais relevantes
C. A Cibersegurança Organizacional	C.2 Formação dos colaboradores	"(…) algumas denominações e conceitos e os RH são aqui o departamento facilitador para que toda a gente perceba, daí a ser crucial os Recursos Humanos terem um papel central neste tema. Não só como mensageiros, mas também terem uma contribuição no levantamento de necessidade e planeamento das formações" (PRH2) "(…) porque todas estas iniciativas têm de ser passadas numa forma de formação e, portanto, isso é uma responsabilidade dos RH. Acredito que os RH têm de estar envolvidos em toda a fase desde o levantamento de necessidades, no desenho e na passagem de informação. " (PRH4) "Sim, eu acho que os RH têm de tentar fazer sempre um levantamento de necessidades de formação, até porque nós temos um número de horas anuais a cumprir e cabe também perceber quais as necessidades mais urgentes por parte dos colaboradores. Na minha carreira profissional já constatei a desvalorização do nosso papel em questões de CS" (PRH5)

Tabela 3.9 – Tabela de Categorias: Formação dos colaboradores (RH)

O objetivo com esta questão era perceber a perspetiva de cada profissional sobre a formação de CS e sobre quem deve estar envolvido nessas formações. A função dos RH no geral passa também pela formação dos colaboradores, no entanto, com a literatura explorada constatou-se que em questões de CS seria atribuída tradicionalmente uma maior importância ao departamento de TI em todo o processo relacionado com a CS organizacional. Com os excertos recolhidos nas entrevistas, é possível constatar que os profissionais de TI consideram o papel dos RH como tradutores da informação das formações desenhadas e postas em prática por eles. Assim, todo o levantamento de necessidades, desenho e planeamento de formações passam essencialmente pelo departamento de TI, na visão dos profissionais envolvidos. Por outro lado, os profissionais de RH mencionam até uma "*desvalorização do nosso papel em questões de CS"* (PRH5) e defendem uma participação ativa no levantamento de necessidades, desenho e planeamento de formações em questões de CS.

Quanto à importância atribuída ao levantamento de necessidades e adequação destas formações de CS consoante cada função, estas opiniões vão de encontro às ideias de Beyer and Bummer (2015), que defendem que é necessário conhecer cada área, cada função e perceber quais as necessidades de formação dessa função, de maneira que essa formação seja a mais direcionada possível e consiga atingir os objetivos pretendidos. Esta responsabilidade de monitorizar as necessidades e adaptar as formações desenhadas é atribuída aos RH por terem um conhecimento geral das empresas (Reegård et al. 2019). No entanto, os profissionais de TI entrevistados consideram ser quem deve levar a cabo este levantamento de necessidades. Assim, conclui-se que os profissionais de TI entrevistados mantém uma perspetiva de que em questões de formação a função dos RH é apenas de uma passagem de informação clara e de simplificar termos mais complexos da CS para os colaboradores. Tendo em consideração a premissa defendida pelos estudiosos explorados ao longo desta dissertação, de que a GRH pode contribuir para a mitigação dos ataques cibernéticos através da sua relação próxima com os *end-users* se tiver um papel central na formação dos mesmos, conclui-se que em questões de formação, os profissionais de TI envolvidos apenas consideram este papel necessário na simplificação e clareza da formação passada.

No que concerne à Consciencialização dos indivíduos, terceira sub-categoria, os participantes também atribuíram uma crescente importância à existência desta prática nas organizações:

Categoria	Subcategoria	Excertos mais relevantes
C. A Cibersegurança Organizacional	C.3 Consciencialização dos colaboradores	"(…) até porque sempre a prevenção em primeiro, portanto instruir as pessoas e passar lhe esse conhecimento." (PRH4) "Se estivermos a falar sempre do mesmo assunto diversas vezes numa organização e apelar à sensibilização dos colaboradores, há sempre resultados." (PTI2) ""(…) por ser muito importante o trabalho continuo e conjunto destes departamentos para essa haver sempre essa consciencialização, sensibilização e atualização de informação para que depois nada falhe." (POA1)

Tabela 3.10 – Tabela de Categorias: Consciencialização dos colaboradores

Como explorado no Capítulo 2, a Consciencialização/Awareness apresenta-se como uma prática diferente da formação. A Consciencialização tem como objetivo trazer a atenção dos indivíduos para estes tópicos, fazendo-os percecionar a importância atribuída pela sua organização à Cibersegurança, o que por sua vez os torna mais conscientes e mais cuidadosos com os sistemas de informação com o qual trabalham (Wipawayangkool, 2010). Aquando da exploração desta temática junto dos entrevistados, a maioria dos profissionais mencionaram uma colaboração entre o departamento de TI e os RH como essencial para a consciencialização dos colaboradores, alguns exemplos:

Categoria	Subcategoria	Excertos mais relevantes
C. A Cibersegurança Organizacional	C.3 Consciencialização dos colaboradores	"Sim, acredito que não parte apenas dos RH até porque para que isso aconteça acredito que devam ter mais informação e formação nesse aspeto. Aqui devem trabalhar com os TI" (PRH3) "Sempre que recebemos alertas de colaboradores tentamos falar sempre com os Recursos Humanos para passarem a mensagem e o Awareness relacionado com os emails e links em que acedem. (...)Se estivermos a falar sempre do mesmo assunto diversas vezes numa organização e apelar à sensibilização dos colaboradores, há sempre resultados." (PTI2) "(…) por ser muito importante o trabalho continuo e conjunto destes departamentos para essa haver sempre essa consciencialização, sensibilização e atualização de informação para que depois nada falhe." (POA1)

Tabela 3.11 – Tabela de Categorias: Consciencialização dos colaboradores (Colaboração RH e TI)

Como explorado no Capítulo 2, a *Awareness* apresenta-se como uma das possíveis práticas da GRH na CS organizacional. O departamento de RH, com o *know how* de motivar os colaboradores em certas questões e capacidade de passagem de informação mais clara, pode apresentar-se como estratégico nesta prática. No entanto, este conhecimento não é suficiente e precisam de um departamento de TI, com o seu conhecimento técnico, para que esta *Awareness* seja eficaz (Klipfel, 2019). Com esta prática, estes dois departamentos conseguem passar para o resto de uma organização a importância que é atribuía ao assunto, os riscos associados a simples descuidos nas suas funções e as políticas internas relacionadas com a CS, o que por sua

vez leva a um maior sentimento de envolvimento e um consequente cuidado acrescido nas suas funções (Wipawayangkool, 2010).

Por fim, a última sub-categoria: Recrutamento e Seleção. Para além de práticas relacionadas com a Formação e *Awareness*, o RS também é considerado umas das possíveis práticas da GRH em questões de CS. Aquando questionada a opinião individual de cada profissional sobre este tipo de prática dos RH, as opiniões foram diversificadas. No entanto, com as análises das entrevistas foi possível concluir que os profissionais de RH atribuem uma maior importância à implementação de práticas direcionadas para a CS organizacional numa fase inicial de seleção e entrada de novos membros, como podemos analisar nos excertos destes profissionais na tabela Por outro lado, dos quatro profissionais de IT, apenas um mencionou considerar importante explorar questões relacionadas com a CS numa fase de RS: *"...são os RH que dão a entrada ou não dessas pessoas é neste sentido que os RH devem ter mais consciencialização ou mais métodos no processo de seleção de modo a mitigar o risco porque na CS não há eliminar o risco, mas sim mitigá-lo*." (PTI3).

Categoria	Subcategoria	Excertos mais relevantes
C. A Cibersegurança Organizacional	C.4 Práticas levadas a cabo no processo de Recrutamento e Seleção	"É sempre importante passar aos candidatos esta importância que atribuímos à cibersegurança e também termos a certeza de que são pessoas de confiança dentro do possível e que vão cumprir os próprios códigos da empresa." (PRH1) " (...) acho que na parte de integração é fundamental já passar essa ideia da cibersegurança, portanto acho que sim. Provavelmente não terá de ser algo tão exaustivo como uma formação, mas claro que passar sempre a ideia que naquela empresa leva-se a sério a Cibersegurança" (PRH2) "Todos esses pequenas ações, considero que tem um papel importante na consciencialização dos colaboradores desde o início." (PRH5) "...são os RH que dão a entrada ou não dessas pessoas é neste sentido que os RH devem ter mais consciencialização ou mais métodos no processo de seleção de modo a mitigar o risco porque na CS não há eliminar o risco, mas sim mitigá-lo." (PTI3)

Tabela 3.12 – Tabela de Categorias: Práticas levadas a cabo no processo de Recrutamento e Seleção

Os restantes profissionais partilharam não considerar *"que seja o mais importante"* (PTI1) e que consideram mais importante explorar estas questões *"quando o colaborador já se encontra a exercer funções"* (PTI2). Quanto aos profissionais de Outras Áreas, a opinião dividiu-se, onde um considera *"mais relevante a implementação de práticas noutras fases"* (POA2) sem ser a do RS e o outro que considera apenas importante existir estes cuidados *"...para departamentos mais especializados."* (POA1). Assim, com a análise dos excertos das entrevistas, é possível concluir que os profissionais de RH atribuem, em relação aos restantes profissionais, uma maior importância à implementação de práticas numa fase inicial de entrada de novos membros numa organização, tais como verificação de antecedentes, o conhecimento e importância individual atribuída à CS, de modo a percecionar o quão alinhados se encontram os candidatos com os valores das organizações nestas questões.

3.2 Frequências e Exploração de Hipóteses

Nesta secção serão exploradas as frequências em que foram mencionados dos RH e os TI em cada sub-categoria. A tabela elaborada inclui apenas as sub-categorias que, tendo em conta as respostas e o objetivo de cada pergunta, fez sentido calcular a quantidade de vezes que cada 'tipo' de profissional foi mencionado, uma vez que algumas das restantes sub-categorias serviram para enquadrar os profissionais na temática e tirar conclusões extra. Esta tabela de frequências e de comparação surge no contexto da literatura explorada, onde constatou-se que os profissionais de RH, tradicionalmente, não são tão frequentemente mencionados aquando das temáticas de Cibersegurança Organizacional e onde é atribuído um papel central e quase exclusivo do TI nesta temática a nível organizacional. Com o cálculo das frequências, obtivemos os seguintes resultados:

Categoria	Subcategoria	Profissionais que mencionam RH	%	Profissionais que mencionam IT	%
B. Cultura de Cibersegurança	B.1 Estabelecimento de uma Cultura de Cibersegurança numa Organização	11	100%	3	27%
C. A Cibersegurança Organizacional	C.1 Proximidade com os colaboradores internos	10	91%	2	18%
	C.2 Formação dos colaboradores	11	100%	7	63%
	C.3 Consciencialização dos colaboradores	9	82%	10	91%
	C.4 Práticas levadas a cabo no processo de Recrutamento e Seleção	11	100%	0	0%

Tabela 3.13 – Tabela de Frequências

Como explorado na secção anterior, na sub-categoria Estabelecimento de uma Cultura de Cibersegurança numa Organização as opiniões dividiram-se. Os profissionais de TI partilharam considerar os RH os principais responsáveis pelo estabelecimento de uma CC nas organizações, outros profissionais mencionaram apenas os RH nestas questões e outros defenderam a

colaboração entre os dois departamentos em questões de CC. Assim, e como verificado na tabela acima, 100% dos participantes mencionaram os RH e apenas 27% mencionaram os TI aquando desta questão. Não foi elaborada uma Hipótese dedicada à CC mas é-nos possível tirar algumas conclusões. O papel da GRH é transversal a toda a organização, e como constatado com a exploração da literatura existente sobre o assunto, em questões de CS este papel ainda é muito desvalorizado. Aquando das entrevistas, era esperada alguma desvalorização do papel dos RH nesta temática por parte dos profissionais de TI e de AO, no entanto, todos os participantes mencionaram a importância do papel da GRH no que concerne ao estabelecimento deste tipo de cultura, o que demonstra existir alguma evolução e valorização do papel da GRH nesta temática.

A Proximidade com os colaboradores internos surgiu como sub-categoria devido à constante menção dos participantes. Com a tabela de frequências conclui-se que 91% dos participantes mencionaram a proximidade dos RH dos colaboradores como um fator importante em questões de CS e outros 18% mencionaram também a proximidade dos TI como importante nestas questões.

Quanto à Formação dos colaboradores em questões de CS, questão central nesta investigação, constatamos que 100% dos participantes mencionaram os RH e 63% mencionaram os TI aquando desta questão, no entanto foram mencionados por razões distintas. Como explorado no capítulo anterior, os TI partilharam entre si a mesma opinião: As formações são essencialmente desenhadas e pensadas por eles e os RH são apenas os 'tradutores' destas formações. Por outro lado, os profissionais de RH defenderam não apenas esta facilidade de 'tradução' inerente à função dos RH, mas também a participação ativa destes profissionais no levantamento de necessidades e desenho das mesmas. Esta conclusão leva-nos à *Hipótese nº3: Os RH, em relação aos restantes profissionais, consideram ter um papel ativo no levantamento de necessidades e desenho de formação relacionados com a CS, enquanto os profissionais de TI os consideram meros 'tradutores'*. Os RH, em relação aos restantes profissionais, atribuem uma maior importância à sua participação direta e ativa no levantamento de necessidades, enquanto os restantes profissionais, principalmente de TI, consideram os RH como meros *'tradutores'*. Esta hipótese foi elaborada devido à desvalorização do papel dos RH em questões de formação de CS encontrada na literatura explorada e esta verifica-se com os excertos recolhidos nas entrevistas realizadas.

Quanto à sub-categoria da Consciencialização constatamos que a diferença de percentagem é menor entre os profissionais de RH e TI do que nas restantes sub-categorias, o que nos leva à *Hipótese nº2: Tanto os profissionais de RH como os profissionais de TI vêm uma colaboração entre si como vantajosa na consciencialização dos colaboradores em questões de Cibersegurança.* A Consciencialização apresenta-se como uma prática diferente da formação e que parece ser uma prática que une os depois departamentos na opinião dos profissionais envolvidos. Tantos os profissionais de RH e de TI como os profissionais de OA consideram essencial e vantajoso existir uma colaboração entre os RH e TI de maneira a promover a Consciencialização entre os colaboradores de uma organização em questões de CS, o que leva à verificação desta segunda hipótese.

Quanto à última sub-categoria e última hipótese, os RH foram os únicos profissionais mencionados nesta última categoria por serem, por norma, o único departamento diretamente envolvido num processo de recrutamento e seleção. Aquando desta questão nas entrevistas as opiniões dos diferentes grupos de profissionais foram diversificadas como verificado no capítulo anterior. Concluiu-se que os profissionais de RH atribuem uma maior importância à implementação de práticas numa fase inicial do processo de entradas de novos membros em relação aos restantes profissionais, uma vez que os restantes profissionais partilharam não considerar *''que seja o mais importante"* (PTI1). Os excertos recolhidos das onze entrevistas permitem verificar a *Hipótese nº1: Os profissionais de RH, em relação aos restantes profissionais, atribuem uma maior importância à implementação de práticas relacionadas com a Cibersegurança durante os processos de Recrutamento e Seleção*. Desta forma, tendo por base os excertos recolhidos das entrevistas realizadas, foi-nos possível verificar todas as hipóteses formuladas à priori em função da literatura encontrada e explorada.

Capítulo 5

Conclusão

Esta dissertação teve como principal objetivo explorar o papel da Gestão de Recursos Humanos (GRH) na Cibersegurança organizacional e de que forma este pode contribuir para o estabelecimento de uma Cultura de Cibersegurança a nível organizacional. Foram feitas entrevistas estruturadas a onze profissionais com o objetivo de explorar as opiniões individuais sobre o tema. Aquando da exploração da literatura existente deparamo-nos com uma desvalorização do papel da Gestão de Recursos Humanos em questões de Cibersegurança organizacional e um papel centrado, em grande parte das organizações, no departamento de Tecnologias da Informação (TI) nestas matérias, tendo sido por esta razão elaboradas hipóteses e objetivos de modo a explorar as opiniões dos profissionais envolvidos sobre este papel. Com as entrevistas efetuadas e a análise de conteúdo feita posteriormente, foi possível constatar que os profissionais de Recursos Humanos (RH), em relação aos restantes, atribuem uma maior importância a estarem mais envolvidos nas questões de Cibersegurança organizacional: Em questões de formação, consideram essencial estar envolvidos em todo o processo desde o levantamento de necessidades até à passagem de informação, por outro lado, os profissionais de TI demonstraram uma certa desvalorização na inclusão dos RH nesta temática, atribuído apenas importância à facilidade de tradução e passagem de formação inerente à função de RH. Para além disto, nas práticas de Recrutamento e Seleção relacionadas com a Cibersegurança, os profissionais de RH atribuíram grande importância a esta aplicação, enquanto os restantes profissionais, principalmente os TI, mencionaram não considerar “que seja o mais importante" (PTI1). Por outro lado, os três grupos de profissionais atribuíram grande importância ao trabalho conjunto dos RH e dos TI na consciencialização dos colaboradores em questões de Cibersegurança, o que vai de encontro com as ideais defendidas na literatura estudada. Desta forma, e tendo em conta as restantes perguntas colocadas ao longo das entrevistas, é notória a valorização da proximidade dos RH com os end-users e a forma como esta proximidade pode ser útil em questões de Cibersegurança organizacional e para o estabelecimento de uma Cultura de Cibersegurança. No entanto, está também visível que grande parte dos profissionais de TI ainda desvalorizam o papel destes nas questões mais práticas da questão e que os consideram meros ‘tradutores’.

Os problemas organizacionais relacionados com a Cibersegurança não pararão por aqui e considera-se essencial estudar e possivelmente investir numa aproximação dos RH com o departamento de TI nestas questões e trabalhar na formação dos profissionais de RH sobre a matéria par que lhes seja possível acompanhar as evoluções constantes dos riscos cibernéticos organizacionais. Assim, este estudo veio demonstrar que ainda persiste uma mentalidade tradicional nos profissionais de TI e que é importante explorar mais a utilidade do papel da Gestão dos Recursos Humanos nestas questões, uma vez que poderá ser uma maneira de mitigar consideravelmente as brechas de informação organizacional associadas aos *end-users*. Esta dissertação explorou a opinião de apenas onze profissionais, o que representa uma amostra pequena do mundo corporativo e poderá não representar exatamente a opinião geral dos grupos de profissionais. Assim, para estudos futuros nesta temática, seria essencial explorar a opinião de um grupo significativo de profissionais, assim como as práticas concretas levadas a cabo nas suas organizações nesta temática, desde as práticas da GRH até ao tipo de colaboração que existe entre os departamentos de TI e RH em questões de CS organizacional.

A Cibersegurança organizacional continuará a ser um tema muito presente nas organizações, assim como uma fonte de investimento estratégico das mesmas e, uma vez que se tem chegado à conclusão que muitos dos ciberataques ocorrem por descuidos de indivíduos internos, será essencial repensar sobre que tipo de investimento e práticas terão de ser postas em prática. Esta dissertação foca-se no papel da GRH por este se apresentar como um departamento estratégico nestas questões aos olhos de muitos estudiosos. A GRH, como explorado nos capítulos anteriores, por ser um departamento com uma relação próxima com os *end-users*, por ter o *know how* da passagem da informação, por conhecer todas as funções e ter consciência das necessidades e fragilidades das mesmas, poderá apresentar-se como uma das soluções para mitigar as fugas de informação e os ciberataques que utilizam os *end-users* como intermediários para executar estes ataques. É por estas razões que este estudo se centrou na importância do papel destes profissionais e que apela a uma maior aposta em estudos futuros sobre o tema.

Capítulo 6

Referências Bibliográficas

Asiltürk, A. 2022, 'The role of Management and IT Team interaction on the Success of Cyber Security Strategies', in Serap, S. (Ed), *Advances in Social Sciences*, pp 267-286.

Ayyagari, R. & Figueroa, N. 2017. 'Issue 2 Is Seeing Believing? Training Users on Information Security: Evidence from Java Applets Is Seeing Believing? Training Users on Information Security: Evidence from Java Applets.' *Journal of Information Systems Education*, 28(2), pp. 115-112.

Bardin, L. 2014. Análise de Conteúdo. Lisboa: Edições Setenta

Beyer, R. E., & Brummel, B. 2015. Implementing effective cyber security training for end users of computer networks. Society for Human Resource Management and Society for Industrial and Organizational Psychology.

Choi, Y. 2017. 'Human Resource Management and Security Policy Compliance.', *International Journal of Human Capital and Information Technology Professionals*, 8(3), pp. 68-81.

Ciolan, I. M. 2014. 'Defining Cybersecurity as the Security Issue of the Twenty-First Century: A Constructivist Approach.', *Revista de Administratie Publica si Politici Sociale*, 12(1), pp. 40-43

Da Veiga, A.,0 2016. *A Cybersecurity Culture Research: Philosophy and Approach to Develop a Valid and Reliable Measuring Instrument*. In: *SAI Computing Conference 2016*. pp. 1006-1015.

Esteves, M, 2006. *Análise de conteúdo. In J. Á Lima & J.A. Pacheco (Orgs), Fazer Investigação (pp. 105-126). Porto: Porto Editora*

European Union Agency for Network and Information Security, 2017. *Cyber Security Culture in Organisations*. European Union Agency for Network and Information Security.

Forbes Technology Council, 2022. *14 Bad Tech Habits IT Leaders Want Their Teammates to Break*. [online] Available at: https://www.forbes.com/councils/forbestechcouncil/2022/10/25/14-bad-tech-habits-it-leaders-want-their-teammates-to-break/

Fung, A. 2017. 'Human Resource Management and Security Policy Compliance', Journal of Network and Computer Applications, vol. 84, pp 25-37

Forbes, 2019. *A culture of safety: How HR can partner with IT to improve cybersecurity*. Forbes Human Resources Council. [online] Available at: https://www.forbes.com/councils/forbeshumanresourcescouncil/2019/02/28/a-culture-of-safety-how-hr-can-partner-with-it-to-improve-cybersecurity/

Huang, K., & Pearlson, K. 2019. For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture. Cybersecurity Interdisciplinary Systems Laboratory Massachusetts Institute of Technology

Hussin, N. and Graepel, T., 2024. *Cybersecurity Awareness in HR: Examining the Gap Between Theoretical Knowledge and Practical Application*. DOI: http://dx.doi.org/10.13140/RG.2.2.34342.13123.

International Telecommunications Union (ITU), 2011. *ITU National Cybersecurity Strategy Guide*. [pdf] Available at: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf

Jameel, T. and Ramazan, A., 2024. *Cybersecurity Knowledge Among Human Resources (HR) Employees: Effects on HR Laws and Practices*. [online] ResearchGate. Available at:https://www.researchgate.net/publication/382589790_Cybersecurity_Knowledge_Among_Human_Resources_HR_Employees_Effects_on_HR_Laws_and_Practices

Joinson, A., & van Steen, T. 2018. ‘Human aspects of cyber security: Behaviour or culture change?.’, Cyber Security: A Peer-Reviewed Journal, 4 (1), pp. 351–360

Kearney, E., & Williamson, K. 2016. ‘Information security culture: a cross-organizational perspective.’, *Strategic HR Review*, 4(15), pp. 204-209

Kelly, R., 2020. *Almost 90% of cyber attacks are caused by human error or behavior*. [online] Chief Executive. Available at: https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/

Kweon, E., Lee, H., Chai, S. et al. 2021. ‘The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence.’, *Information Systems Frontiers*, 2(23), pp. 361–373

Marsh and Microsoft, 2019. *2019 Global Cyber Risk Perception Survey*. [pdf] Microsoft Security Blog. Available at: https://www.microsoft.com/en-us/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf

Menaka, R. 2022. ‘A Study On Role of Human Resources in Cyber Security in India-with special reference to Cyber Risk Management’ , Journal of Positive School Psychology, 6(2), pp.4495- 44501

Mizrak, F. 2024. ‘Enhancing Cybersecurity Risk Management Through Conceptual Analysis of HRM Integration’, *Journal of Administrative Sciences*, 51(22)

Neirotti, P., Raguseo, E., & Paolucci, E. 2020. ‘Defining Cybersecurity as the Security Issue of the Twenty-First Century: A Constructivist Approach.’, *Journal of Cybersecurity*, 1(6), pp. 1-18.

Ottis, R. and Lorents, P., 2010. *Cyberspace: Definition and implications*. ICIW, Cooperative Cyber Defence Centre of Excellence, pp. 267–270.

Pace, C. 2016. ‘Why HR and IT departments should talk.’, *Strategic HR Review*, 3(15), pp. 118-122

Pavlova, E.2020. ‘Enhancing the Organizational Culture related to Cyber Security during the University Digital Transformation.’, *Information & Security: An International Journal*, 3(46), pp. 239–249.

Public Safety Canada.2014. Terminology Bulletin 281: Emergency Management Vocabulary. Ottawa: Translation Bureau, Government of Canada.

Reegård, K., Blackett, C. and Katta, V., 2019. The Concept of Cybersecurity Culture. In: Proceedings of the 29th European Safety and Reliability Conference, Singapore, September 2019. [online] Available at: https://www.researchgate.net/publication/336149766_The_Concept_of_Cybersecurity_Culture

Stemler, S. 2001. ‘An Overview of Content Analysis’. *An overview of content analysis. Practical Assessment, Research & Evaluation*, 7(17), pp. 1-11

Tuorinsky, E., 2021. Compliance Score Alone Won’t Keep Your Company Safe From Data Breaches. Forbes Business Council. [online] Available at: https://www.forbes.com/sites/forbesbusinesscouncil/2021/10/08/compliance-score-alone-wont-keep-your-company-safe-from-data-breaches/?sh=72bc0f6b47a9

Wipawayangkool, K., 2010. *Strategic Role of Human Resource Management in Information Security Management*. [online] Semantic Scholar. Available at: https://www.semanticscholar.org/paper/Strategic-Role-of-Human-Resource-Management-in-Wipawayangkool/d7be082a8137e00b58f0d4e904906fa5a156f193

Zafar, H. 2013. ‘Human resource information systems: Information security concerns for organizations.’ *Human Resource Management Review*, 1(23), pp. 105–113.

Anexos

Anexo A - Email de convocatória:

“Boa Tarde,

Espero que se encontre bem!

Meu nome é Alexandrina Ferreira e estou atualmente a realizar uma investigação de Mestrado no Instituto Superior de Ciências do Trabalho e da Empresa (ISCTE), com o tema "O Papel da Gestão de Recursos Humanos na Cibersegurança Organizacional". Este estudo tem como principal objetivo estudar as diferentes perspetivas de profissionais de Recursos Humanos, Tecnologias de Informação e de outras áreas sobre o papel da Gestão dos Recursos Humanos nesta temática nas organizações.

Gostaria de convidá-lo para participar numa entrevista como parte desta pesquisa. Esta entrevista, por questões de tratamento de dados e análise de conteúdo, será online e gravada, e todos os conteúdos serão eliminados assim que terminada a investigação. Para além disto, ao longo da tese de mestrado serão apenas mencionadas as seguintes informações sobre os entrevistados: Profissão, Idade e Género, assegurando assim a confidencialidade de todas as informações pessoais.

Saliento também que o objetivo do estudo é estudar as perspetivas pessoais, como profissionais das áreas supramencionadas, sobre o papel da Gestão dos Recursos Humanos na Cibersegurança Organizacional, não o de explorar práticas especificas levadas a cabo pelas empresas das quais fazem parte.

Acredito que a sua experiência e conhecimento seriam de imenso valor para este estudo e gostaria de contar com a sua participação. A entrevista será realizada online e agendada tendo em conta a sua disponibilidade e preferência.

Caso esteja interessada em ser entrevistada e contribuir para o meu estudo, indique por favor se estaria disponível para realizar uma entrevista, com uma duração prevista de 30 minutos, numa data e hora mais conveniente para si.

Estou à disposição para quaisquer dúvidas ou esclarecimentos adicionais que possa ter.

Muito obrigada desde já pela colaboração!

Atenciosamente,"

Anexo B – Introdução no tema durante as entrevistas

Antes de mais obrigada pela disponibilidade para participar nesta entrevista e contribuir para a minha investigação de mestrado.

Como expliquei de forma breve no email enviado, a minha tese de mestrado tem como tema o papel da Gestão dos Recursos Humanos na Cibersegurança organizacional.

A escolha deste tema deve-se ao aumento dos riscos cibernéticos para as organizações e a crescente importância atribuída à Cibersegurança organizacional.

Diversos estudos feitos atualmente concluíram que cerca de 90% dos ataques cibernéticos nas organizações acontecem por algum tipo de erro ou comportamento humano, e por esta razão, tem sido atribuída cada vez mais importância ao conceito de Cibersegurança Organizacional.

O objetivo desta investigação é perceber as diferentes perspetivas existentes entre os próprios profissionais de Recursos Humanos, profissionais de Tecnologias da Informação e Profissionais de outras áreas sobre o papel da Gestão dos Recursos Humanos na Cibersegurança Organizacional.

Como também mencionado no email enviado, o objetivo desta entrevista é explorar a sua perspetiva como profissional de RH/TI/OA sobre o assunto e não sobre práticas levadas a cabo por alguma empresa em específico.

Toda a informação partilhada durante esta entrevista será apenas utilizada para fins desta investigação e será eliminada assim que concluída. Para além disto, não serão mencionadas informações pessoais sobre os entrevistados ao longo da minha investigação e serão apenas utilizados dados como Profissão, Género e Idade, assegurando assim a confidencialidade dos envolvidos.

Deste modo, gostaria de perceber se compreendeu e se consente a utilização das suas respostas apenas para fins de investigação científica, tendo em conta a confidencialidade descrita?

Anexo C – Guião para as entrevistas de Profissionais de RH

1 - O que entende por Cibersegurança e que importância atribui a este conceito dentro de uma organização?

2-Sabe quais os riscos associados à ausência de uma Cibersegurança e as consequências que podem ter numa organização?

Uma vez que a minha próxima questão está relacionada com a Cultura de Cibersegurança, considero importante partilhar uma breve definição do conceito:

Este tipo de cultura pode ser definido como um sistema, valores e crenças partilhadas que influenciam a forma como os indivíduos se comportam nas organizações e como estes interagem com os sistemas e procedimentos das suas organizações relacionados com a Cibersegurança. É, resumidamente, uma norma que se instala numa organização em que prevalece o respeito e comprometimento com as políticas e práticas de Cibersegurança.

3- De que maneira considera que o departamento de Recursos Humanos pode promover uma Cultura de Cibersegurança nos colaboradores internos de uma organização?

4- De que forma considera que os Recursos Humanos e o departamento de Tecnologias de Informação deveriam colaborar no sentido de fortalecer a Cibersegurança organizacional?

5- Considera que os Recursos Humanos têm ou deveria ter um papel central na Formação dos colaboradores e no planeamento das mesmas em questões de Cibersegurança?

6- Considera que os Recursos Humanos têm ou deveriam ter um papel central na Consciencialização (ou *Awareness* termo em inglês) dos colaboradores em questões de Cibersegurança?

7 - Aquando do processo de seleção e contratação de novos membros, considera que os Recursos Humanos devem ter em conta questões relacionadas com a Cibersegurança?

8 - De maneira geral, de que forma considera que os Recursos Humanos contribuem/pode contribuir para assegurar a Cibersegurança organizacional?

Anexo D – Guião para as entrevistas dos Profissionais de Cibersegurança/Tecnologias da Informação

1 - O que entende por Cibersegurança e que importância atribui a este conceito dentro de uma organização?

2 - Sabe quais os riscos associados à ausência de uma Cibersegurança e as consequências que podem ter numa organização?

Uma vez que a minha próxima questão está relacionada com a Cultura de Cibersegurança, considero importante partilhar uma breve definição do conceito:

Este tipo de cultura pode ser definido como um sistema, valores e crenças partilhadas que influenciam a forma como os indivíduos se comportam nas organizações e como estes interagem com os sistemas e procedimentos das suas organizações relacionados com a Cibersegurança. É, resumidamente, uma norma que se instala numa organização em que prevalece o respeito e comprometimento com as políticas e práticas de Cibersegurança.

3 - Considera que o seu departamento é o departamento que mais contribui para o estabelecimento deste tipo de cultura?

3.1 Considera que os Recursos Humanos contribuem para este tipo de Cultura de alguma forma?

4 - Considera importante existir uma colaboração entre o seu departamento e o departamento de Recursos Humanos em questões de Cibersegurança e proteção de dados?

5 - Considera que o seu departamento lidera as questões de Formação interna sobre a Cibersegurança? Considera pertinente algum tipo de colaboração com os Recursos Humanos neste assunto?

6 - Considera que o seu departamento lidera as questões de Consciencialização interna sobre a Cibersegurança? Considera pertinente algum tipo de colaboração com os Recursos Humanos neste assunto?

7 - Aquando do processo de seleção e contratação de novos membros, considera que os Recursos Humanos devem ter em conta questões relacionadas com a Cibersegurança?

8 - De forma geral, de que maneira considera que o seu departamento contribui/pode contribuir para assegurar a Cibersegurança organizacional.

9 - Como vê o papel dos Recursos Humanos na Cibersegurança organizacional?

Anexo E – Guião das entrevistas aos Profissionais de Outras Áreas.

1 - O que entende por Cibersegurança e que importância lhe atribui?

2 - Sabe quais os riscos associados à ausência de uma Cibersegurança e as consequências que podem ter numa organização?

Uma vez que a minha próxima questão está relacionada com a Cultura de Cibersegurança, considero importante partilhar uma breve definição do conceito:

Este tipo de cultura pode ser definido como um sistema, valores e crenças partilhadas que influenciam a forma como os indivíduos se comportam nas organizações e como estes interagem com os sistemas e procedimentos das suas organizações relacionados com a

Cibersegurança. É, resumidamente, uma norma que se instala numa organização em que prevalece o respeito e comprometimento com as políticas e práticas de Cibersegurança.

3 - Que departamentos dentro de uma empresa considera responsáveis pelo estabelecimento deste tipo de cultura? Considera que os Recursos Humanos devem ter algum tipo de responsabilidade no estabelecimento de uma Cultura de Cibersegurança?

4 - Considera importante existir colaboração entre o departamento de Tecnologias da Informação e os Recursos Humanos nestas questões? Se sim, de que maneira?

5 -Quais departamentos dentro de uma empresa considera os responsáveis pela Formação dos colaboradores em questões de Cibersegurança?

5.1 Considera que os RH têm/deveriam de ter algum tipo de papel na formação dos indivíduos sobre CS?

6 - Quais departamentos dentro de uma empresa considera os responsáveis pela Consciencialização (ou *Awareness* termo em inglês) dos colaboradores em questões de Cibersegurança?

6.1 Considera que os RH têm/deveriam de ter algum tipo de papel na consciencialização dos indivíduos sobre CS?

7 - Aquando do processo de seleção e contratação de novos membros, considera que os Recursos Humanos devem ter em conta questões relacionadas com a Cibersegurança?

8 - Quando pensa em Cibersegurança Organizacional, pensa em que departamentos?

9 - Como vê o papel dos RH, sendo o departamento mais próximo dos colaboradores, na Cibersegurança de uma empresa?