DEPARTAMENTO DE RELAÇÕES INTERNACIONAIS
MESTRADO EM RELAÇÕES INTERNACIONAIS
UNIVERSIDADE AUTÓNOMA DE LISBOA
"LUÍS DE CAMÕES"

AMEAÇAS CIBERNÉTICAS E OS SEUS IMPACTOS NA SEGURANÇA HUMANA

Dissertação para a obtenção do grau de Mestre em Relações Internacionais

Autora: Inês Gil Costa da Conceição
Orientador: Professor Luís Vasco Valença Pinto
Número da candidata: 30000813

Maio de 2023
Lisboa

DEDICATÓRIA

“A segurança humana está intrinsecamente ligada à segurança digital. Precisamos de investir em tecnologias e estratégias para enfrentar as ciberameaças.” - Angela Merkel

AGRADECIMENTOS

Quero expressar a minha profunda gratidão a todos os que me acompanharam nesta dissertação, pelo inestimável apoio. Sem cada um de vocês, esta conquista não teria sido possível.

À minha irmã, ao meu cunhado e ao meu namorado, pelo apoio constante e incondicional.

À família do meu namorado, pelo acolhimento carinhoso.

Aos meus pais, pela motivação em superar este desafio.

À minha avozinha, pelas palavras de força.

Ao meu padrinho, madrinha e prima, pela inspiração na luta contra as dificuldades.

À Lilienne e aos seus familiares, por me impulsionarem e fazerem-me acreditar nas minhas capacidades.

Aos docentes e aos meus colegas da UAL, pelo apoio e colaboração ao longo desta jornada académica. O conhecimento, a orientação e o companheirismo foram essenciais para o meu crescimento e desenvolvimento tanto a nível pessoal como profissional.

Aos locais onde trabalhei, por me terem permitido adquirir as ferramentas e o conhecimento para completar esta etapa.

Aos meus animais de estimação, pela alegria e amor inesgotáveis.

Ao meu orientador, Professor Luís Vasco Valença Pinto, pelos conselhos, pela orientação e pelos conhecimentos partilhados.

RESUMO

As Relações Internacionais desempenham um papel fundamental no contexto da segurança humana e da cibersegurança. À medida que a sociedade se torna cada vez mais dependente do mundo digital, surgem novos desafios e riscos para os Estados e para os indivíduos. Nesse sentido, esta dissertação procura explorar a interseção entre a segurança humana e a cibersegurança, considerando as diferentes dimensões da segurança humana (segurança física, segurança económica, segurança alimentar, segurança sanitária, segurança ambiental e segurança comunitária).

A primeira parte da pesquisa introduzirá o tema do espaço digital, de forma a destacar a sua importância e os debates atuais relacionados aos danos potenciais que podem afetar tanto os Estados quanto os indivíduos. Serão apresentados estudos académicos e opiniões de especialistas que contribuem para uma compreensão mais abrangente.

Na segunda parte, serão abordadas as ciberameaças existentes, sob a perspetiva dos indivíduos. Isso permitirá uma análise mais aprofundada dos riscos e impactos dessas ameaças, fornecendo uma base sólida para a pesquisa. Através da análise de documentos e dados relevantes, a dissertação irá explorar diferentes aspetos das ciberameaças e dos cibercrimes, evidenciando as implicações para a segurança humana.

Por fim, a dissertação estabelecerá a ligação entre o conceito de segurança humana e a cibersegurança, reconhecendo a importância central desta análise. Serão realizadas leituras críticas e uma revisão bibliográfica para definir os conceitos estruturantes que apoiarão a pesquisa. O objetivo é fornecer uma compreensão mais profunda das ciberameaças e dos cibercrimes, avaliando os impactos na segurança humana.

Além disso, a dissertação procurará analisar como é que o cibercrime pode ser considerado perturbador da segurança humana e investigar como é que o aumento da consciencialização em cibersegurança pode contribuir para a redução dos riscos e das ciberameaças. Essa análise contribuirá para gerar novas pesquisas, fornecendo dados e análises que complementam o conhecimento académico existente sobre a segurança humana e a cibersegurança.

Desta forma, a dissertação terá como objetivo principal compreender a complexidade das ciberameaças, explorar a sua relação com a segurança humana e contribuir para o avanço do conhecimento nesta área, fornecendo informações relevantes para pesquisadores e profissionais envolvidos nas Relações Internacionais.

PALAVRAS-CHAVE

Relações Internacionais; Segurança Humana; Dimensões da Segurança Humana; Cibersegurança; Consciencialização.

ABSTRACT

International Relations play a key role in the context of human security and cybersecurity. As society becomes increasingly dependent on the digital world, new challenges and risks emerge for states and individuals. In this sense, this dissertation seeks to explore the intersection between human security and cybersecurity by considering the different dimensions of human security (physical security, economic security, food security, health security, environmental security, community security).

The first part of the survey will introduce the topic of digital space to highlight its importance and the current debates related to the potential harms that can affect both states and individuals. Academic studies and expert opinions that contribute to a more comprehensive understanding will be presented.

In the second part, existing cyberthreats will be addressed from the perspective of individuals. This will allow a more in-depth analysis of the risks and impacts of these threats, providing a solid basis for research. Through the analysis of relevant documents and data, the dissertation will explore different aspects of cyber threats and cybercrimes, highlighting the implications for human security.

Finally, the dissertation will establish the link between the concept of human security and cybersecurity, recognizing the central importance of this analysis. Critical readings and a literature review will be conducted to define the structuring concepts that will support the research. The goal is to provide a deeper understanding of cyberthreats and cybercrimes by assessing the impacts on human security.

In addition, the dissertation will seek to analyze how cybercrime can be considered disruptive to human security and investigate how increased cybersecurity awareness can contribute to the reduction of risks and cyberthreats.

This analysis will contribute to the generation of new research by providing data and analysis that complements existing academic knowledge on human security and cybersecurity. Thus, the main objective of the dissertation will be to understand the complexity of cyber threats, explore their relationship with human security, and contribute to the advancement of knowledge in this area by providing relevant information for researchers and professionals involved in International Relations.

KEYWORDS

International Relations; Human Security; Dimensions of Human Security; Cybersecurity; Awareness.

Índice

ÍNDICE DE FIGURAS

1. Introdução

As Relações Internacionais têm um papel crucial na atualidade, tendo em conta que vivemos num mundo cada vez mais globalizado e interconectado. Neste contexto, a segurança humana e a cibersegurança têm sido temas de extrema importância para a estabilidade e o bem-estar das sociedades no mundo todo. As ameaças cibernéticas, também correntemente designadas ciberameaças, têm vindo a tornar-se uma preocupação crescente na era digital. Com o avanço da tecnologia e com a interconexão global, a segurança cibernética tornou-se um desafio significativo para as organizações, para os governos e para os indivíduos. Essas ciberameaças representam um conjunto diversificado de ciberataques e atividades maliciosas que visam comprometer os sistemas informáticos, as redes e as informações sensíveis. Neste contexto, compreender a natureza e a evolução das ameaças cibernéticas tornou-se fundamental para a implementação de estratégias eficazes de proteção cibernética.

No âmbito das Relações Internacionais, a segurança humana é reconhecida como uma abordagem ampla que visa garantir a proteção e o bem-estar das pessoas. Ela abrange diferentes dimensões. Cada uma dessas dimensões desempenha um papel essencial na vida das pessoas e está intrinsecamente ligada à segurança global. E, em todas elas, há riscos informáticos com impactos potencialmente consideráveis.

A segurança física refere-se à proteção contra ameaças que colocam em risco a integridade física das pessoas, como conflitos armados, terrorismo e violência. Num mundo digitalizado, a cibersegurança é uma extensão dessa dimensão, uma vez que os ciberataques podem ter consequências diretas na segurança física das pessoas. Por exemplo, um ciberataque direcionado a uma infraestrutura crítica, como centrais nucleares ou sistemas de transporte, pode colocar vidas em perigo.

A segurança económica é crucial para o desenvolvimento e a prosperidade das nações. Ela envolve a proteção contra ameaças que afetam a estabilidade económica, como crimes financeiros, roubo de propriedade intelectual e ciberespionagem a empresas e instituições financeiras. Os ciberataques podem resultar em perdas financeiras significativas, interrupção de operações e danos à reputação, o que por sua vez, pode afetar diretamente a segurança económica dos países e das pessoas.

A segurança alimentar está relacionada ao acesso adequado e sustentável aos alimentos. A cibersegurança desempenha um papel importante nessa dimensão, uma vez que a digitalização do setor agrícola e o aumento da interconetividade dos sistemas de produção e de distribuição de alimentos criam vulnerabilidades que podem ser exploradas por atores maliciosos. Um ciberataque direcionado a infraestruturas agrícolas ou sistemas de abastecimento de alimentos pode comprometer a segurança alimentar de uma nação e afetar milhões de pessoas.

A segurança sanitária tornou-se uma preocupação central no contexto da pandemia do COVID-19. A cibersegurança desempenha um papel fundamental na proteção dos sistemas de saúde contra ciberataques que visam comprometer a integridade dos dados médicos, a infraestrutura hospitalar e as pesquisas científicas. Além disso, a disseminação de desinformação e *fake news* relacionadas à saúde representa um desafio significativo que requer estratégias eficazes de cibersegurança e cooperação internacional.

A segurança ambiental está relacionada à proteção do meio ambiente e à mitigação das alterações climáticas. A infraestrutura digital está cada vez mais presente na monitorização e no controle de processos ambientais, como sistemas de gestão de recursos naturais, redes inteligentes de energia e monitorização da qualidade do ar. A cibersegurança é essencial para garantir a integridade e a confiabilidade desses sistemas, de forma a evitar ciberataques que possam comprometer a segurança ambiental. Por exemplo, um ataque direcionado a uma central de energia renovável poderia resultar em danos ambientais significativos, que afetariam negativamente a sustentabilidade e a segurança ambiental.

A segurança comunitária está relacionada à proteção e ao bem-estar das comunidades locais. No contexto da cibersegurança, envolve a proteção dos indivíduos e das comunidades contra ameaças online, como cibercrimes, *bullying* e assédio virtual. A segurança comunitária digital é fundamental para garantir que as pessoas possam participar ativamente na sociedade digital de forma segura e confiável.

A interconexão das dimensões da segurança humana com a cibersegurança destaca a importância de uma abordagem abrangente e integrada para a proteção das pessoas no mundo digital. A segurança humana não pode ser alcançada sem uma atenção adequada à cibersegurança, uma vez que as ciberameaças têm o potencial de afetar negativamente todas as dimensões da segurança humana.

Além disso, a natureza transnacional das ciberameaças exige uma cooperação internacional eficaz e o fortalecimento das Relações Internacionais. A partilha de boas práticas e a colaboração na resposta a ciberincidentes são fundamentais para enfrentar os desafios atuais e futuros.

Em síntese, as Relações Internacionais, a segurança humana e a cibersegurança são elementos interligados e de extrema importância na atualidade. A proteção das pessoas em todas as dimensões da segurança humana no mundo digital requer uma abordagem holística, que tenha em consideração os desafios emergentes da cibersegurança. A cooperação internacional e o fortalecimento das relações entre os atores internacionais são essenciais para garantir um ambiente seguro e confiável no mundo digital, promovendo a estabilidade, o desenvolvimento e o bem-estar das sociedades globais.

Tudo isto, faz-nos perceber que a cibersegurança é uma questão crucial nos dias de hoje, uma vez que, estamos cada vez mais dependentes da *internet* nas nossas atividades diárias. No entanto, nem sempre dedicamos a mesma atenção e proteção ao mundo digital em comparação com o mundo físico. O cibercrime não conhece fronteiras geográficas ou temporais e pode afetar indivíduos e organizações em qualquer lugar do mundo. Embora os principais alvos sejam os Estados e as empresas, os indivíduos também podem tornar-se vítimas indiretas desses ataques.
Para compreender melhor esta dinâmica e os seus impactos na segurança humana, esta dissertação tem como objetivo geral investigar os impactos das ciberameaças na segurança humana e analisar como é que a consciencialização em cibersegurança pode contribuir para mitigar esses impactos.

Os objetivos específicos desta dissertação são avaliar o impacto da consciencialização em cibersegurança e da cibercriminalidade na segurança humana, de forma a investigar como é que a falta de consciencialização ou conhecimento em cibersegurança pode resultar em perturbações na segurança das pessoas no ambiente digital. Analisar como é que as ciberameaças podem comprometer a segurança física, a estabilidade económica, o acesso adequado à alimentação e à saúde, a proteção do meio ambiente e a segurança nas comunidades, de forma a destacar a interseção entre a segurança humana e a cibersegurança, e para compreender como é que a proteção no mundo digital afeta diretamente o bem-estar e a qualidade de vida das pessoas. E para além do que já foi referido, propor métodos e estratégias para garantir a segurança no ambiente digital, indicar boas práticas em cibersegurança e apresentar recomendações para fortalecer a segurança no ambiente digital.

Ao alcançar estes objetivos, a dissertação pretende contribuir para uma melhor compreensão dos desafios que as ciberameaças impõem e destacar a importância da consciencialização em cibersegurança na proteção da segurança humana no mundo digital.

Ao abordar estas questões, espera-se fornecer perspetivas relevantes para promover um ambiente seguro no mundo digital, tendo em consideração a proteção das pessoas em todas as dimensões da segurança humana. A pesquisa será baseada em evidências, utilizando metodologias adequadas, como a recolha de dados empíricos e a revisão de literatura especializada, para responder às questões levantadas e alcançar os objetivos estabelecidos.

A dissertação será dividida em duas partes principais. Na primeira parte, será apresentado o enquadramento teórico da problemática da cibersegurança, abordando tópicos como a importância da cibersegurança na atualidade, as principais ciberameaças, e a relação entre a segurança humana e a cibersegurança. Além disso, serão exploradas as diferentes dimensões da segurança humana no contexto das Relações Internacionais. Será feita a análise da relação entre as ciberatividades e as abordagens de Segurança Nacional e de Segurança Humana nas Relações Internacionais, a ciber-resiliência será analisada e serão apresentados dados do aumento do cibercrime em Portugal. A estrutura da investigação e a metodologia utilizada também serão detalhadas, assim como os resultados esperados da investigação. Na segunda parte da dissertação, será realizada uma análise dos dados recolhidos, com foco na consciencialização sobre a cibersegurança entre os inquiridos. Será analisado como é que a educação em cibersegurança pode prevenir o cibercrime e promover a segurança humana. Serão analisadas as experiências dos inquiridos com a cibercriminalidade e será debatida a importância da consciencialização em cibersegurança para a segurança humana, tendo em consideração o contexto do espaço digital. Será destacada a necessidade de educação em cibersegurança, a importância da literacia digital e do fator humano na promoção da segurança no ambiente digital.

Com esta estrutura, a dissertação abordará de forma abrangente os principais aspetos relacionados à cibersegurança, à segurança humana e às Relações Internacionais, de forma a analisar de forma aprofundada e contribuir para o avanço do conhecimento nestas áreas.

Em resumo, a dissertação tem como objetivo principal compreender os impactos da cibersegurança na segurança humana e a importância da consciencialização. Através da análise de estudos académicos, dados empíricos e a consideração das diferentes dimensões da segurança humana, espera-se contribuir para promover um ambiente mais seguro no mundo digital.

2. Enquadramento teórico da problemática da cibersegurança

O surgimento da era digital trouxe consigo uma infinidade de oportunidades e progressos tecnológicos que revolucionaram profundamente as nossas formas de comunicação, de trabalho e de interação com o mundo ao nosso redor. No entanto, juntamente com essas transformações positivas, surgiram também novas ameaças e desafios que colocam em risco a segurança dos Estados e dos indivíduos.

Na primeira parte do enquadramento teórico, será introduzido o tema do espaço digital, abordando a sua expansão e influência em diferentes setores da sociedade moderna. Serão destacadas as características distintivas do mundo digital, como a conectividade global, a disseminação rápida de informações e o acesso generalizado a dispositivos eletrónicos. Será enfatizado que, embora o espaço digital ofereça benefícios significativos, ele também apresenta uma série de desafios relacionados à cibersegurança. Os cibercriminosos e atores mal-intencionados aproveitam as vulnerabilidades tecnológicas e as falhas de segurança para realizar uma variedade de ciberataques, como roubo de dados, violações de privacidade, fraudes *online* e ciberespionagem de infraestruturas críticas.

Na segunda parte do enquadramento teórico, será realizada uma análise detalhada das ciberameaças existentes, com base nas perspetivas dos indivíduos que participaram no questionário. Essa abordagem permitirá compreender melhor as preocupações e perceções dos utilizadores da *internet* em relação à sua segurança digital. Serão explorados diferentes tipos de ciberameaças, incluindo o *malware*, o *phishing*, a engenharia social, o *ransomware* e os ataques de negação de serviço (DoS). Cada uma dessas ameaças será descrita em termos da sua natureza, do impacto potencial e dos métodos utilizados pelos ciberatacantes. Além disso, serão discutidas medidas de proteção e as melhores práticas que os utilizadores podem adotar para mitigar os riscos.

A metodologia adotada para a elaboração do questionário foi concebida com o objetivo de abordar a temática da segurança no contexto digital, priorizando a análise das perceções e experiências dos inquiridos. Embora o termo "segurança humana" não tenha sido mencionado explicitamente no questionário, as questões foram cuidadosamente formuladas para captar informações relevantes que permitissem uma análise posterior alinhada com esse conceito.

Ao analisar as perspetivas dos indivíduos, será possível desenvolver estratégias mais eficazes para lidar com as ciberameaças emergentes. A compreensão das perceções e preocupações dos utilizadores da *internet* é fundamental para a formulação de medidas de proteção adequadas.

Por fim, neste enquadramento teórico, será estabelecida uma conexão entre o conceito de segurança humana e a esfera digital. A segurança humana refere-se à proteção e promoção das pessoas e das suas liberdades fundamentais, em contrapartida à segurança do Estado.

No contexto digital, a segurança humana ganha ainda mais relevância, uma vez que as ciberameaças afetam diretamente a vida das pessoas, as suas identidades digitais, a sua privacidade, o seu bem-estar psicológico e as suas oportunidades socioeconómicas. Portanto, é essencial abordar a segurança digital não apenas como uma questão técnica ou governamental, mas também como uma questão de segurança humana.

A segurança humana na esfera digital envolve proteger os indivíduos e as suas interações no espaço digital, garantindo a integridade, confidencialidade, disponibilidade e autenticidade dos seus dados pessoais, bem como promover a consciencialização e a educação em cibersegurança. Isso incluí a proteção contra os cibercrimes, as violações de privacidade, a manipulação de informações e outras formas de exploração digital.

A abordagem da segurança humana na esfera digital reconhece que as ciberameaças podem afetar todos os aspetos da vida das pessoas, desde a sua segurança pessoal até à sua participação em atividades sociais, políticas e económicas. Portanto, é necessário desenvolver estratégias de cibersegurança que coloquem os direitos e interesses dos indivíduos no centro das preocupações.

Ao estabelecer-se a ligação entre a segurança humana e a cibersegurança, será possível analisar de forma mais abrangente os impactos das ciberameaças na sociedade e nas Relações Internacionais.

A segurança digital tornou-se numa questão transnacional, por causa de ciberataques que podem originar-se num país, mas afetar alvos em todo o mundo. Portanto, é fundamental promover a cooperação internacional e o diálogo entre os Estados para enfrentar os desafios da cibersegurança.

O enquadramento teórico proposto neste capítulo da dissertação aborda a problemática da cibersegurança sob a perspetiva da segurança humana e das Relações internacionais. Ao compreender as ciberameaças, as perspetivas dos indivíduos e a importância da segurança humana na esfera digital, será possível desenvolver uma análise mais completa dos desafios e oportunidades apresentadas pela cibersegurança.

Dentro do contexto das Relações Internacionais, a cibersegurança tornou-se um tema crucial nas agendas políticas e de segurança. Os ciberataques podem ter implicações significativas nas relações entre os Estados, e por sua vez, afetar a estabilidade política, a segurança económica e até mesmo a soberania nacional.

As divergências de interesses, a falta de consenso sobre normas e responsabilidades, as questões de soberania e a dificuldade de atribuição de ciberataques são apenas alguns dos obstáculos a serem enfrentados. Portanto, é fundamental analisar todas essas complexidades e explorar estratégias para superá-las e fortalecer a cibersegurança a nível global.

A abordagem multidimensional permite uma compreensão abrangente dos desafios e oportunidades associados à cibersegurança, bem como a formulação de estratégias mais eficazes para enfrentar as ameaças emergentes. Ao considerar a segurança digital como parte integrante da segurança humana e ao analisar as dinâmicas internacionais relacionadas à cibersegurança, é possível promover uma abordagem mais colaborativa e abrangente para lidar com os desafios do mundo digital.

2.1. A cibersegurança na atualidade

A cibersegurança é um tema de extrema relevância na atualidade, à medida que as atividades informáticas maliciosas continuam a expandir-se tanto em escala como em sofisticação. Tanto os Estados quanto as organizações têm reconhecido a necessidade de desenvolver novas estratégias para abordar estas questões e proteger os seus sistemas e informações sensíveis.

Neste contexto, os Sistemas de Gestão de Segurança da Informação devem ser tratados com a atenção e os cuidados adequados[1].

Um dos principais debates em torno da cibersegurança está relacionado à perceção do ciberespaço e ao nível crescente das ciberameaças. Alguns especialistas argumentam que os ciberincidentes estão a tornar-se em instrumentos para demonstrar força no mundo *online*, chegam mesmo a ser considerados representações de um novo tipo de guerra.

[1] Tikk, E. (2011). *Ten Rules for Cyber Security* (Vol. 53). Survival.

Existem duas perspetivas principais nessa argumentação: alguns autores acreditam que as guerras futuras ocorrerão no ciberespaço, enquanto outros defendem que as ciberguerras não existem atualmente e não surgirão no futuro. Até o presente momento, houve poucos ciberataques que causaram danos graves e nenhum deles resultou em vítimas fatais.[2]

No entanto, é importante destacar que ocorreram ciberataques significativos que marcaram a história, como os direcionados à Estónia (2007), à Geórgia (2008), à Ucrânia (2015 e 2016) e ao Irão (2010).

Em abril de 2007, a Estónia enfrentou vários ciberataques em larga escala, conhecidos como os "Ciberataques da Estónia". Esses ciberataques surgiram como resposta a uma disputa política entre a Estónia e a Rússia relacionada à remoção de um monumento soviético em Tallinn. Os ataques envolveram o compromisso de um elevado número de sistemas, o que resultou em perturbações nos serviços governamentais, nas instituições financeiras, nos meios de comunicação e nas empresas. Entre os ciberataques estavam incluídos ataques de negação de serviço (DDoS), invasão de *sites*, roubo de dados e intrusões em sistemas. As investigações subsequentes apontaram que esses ciberataques foram da responsabilidade da Rússia.[3]

Durante o conflito entre a Geórgia e a Rússia em agosto de 2008, a Geórgia foi alvo de múltiplos ciberataques. Estes ciberataques ocorreram antes, durante e após os confrontos militares entre os dois países. Os ciberataques incluíram ataques de negação de serviço (DDoS) a *sites* governamentais e privados, assim como ataques de engenharia social e de *malware*.

Os sistemas de comunicação, os bancos, os meios de comunicação e também outros serviços foram afetados por esses ataques. Após minuciosas investigações, chegou-se à conclusão de que a autoria desses ciberataques recaía sobre a Rússia.[4]

Nos últimos anos, a Ucrânia tem sido alvo de vários ciberataques significativos. Em 2015 e 2016, ocorreram ciberataques que resultaram na interrupção do fornecimento de energia em determinadas regiões do país. Esses ciberataques foram atribuídos a um grupo de *hackers* conhecido como "*SandWorm*" (ou *Telebots*) com ligações à Rússia.

---

[2] Baylis, J., Wirtz, J. J., & Johnson, J. L. (2015). *Strategy in the Contemporary World*. Oxford University Press.
[3] Rid, T. (2012). *Cyber War Will Not Take Place* (Vol. 35). Journal of Strategic Studies.
[4] Rid, T. (2012). *Cyber War Will Not Take Place* (Vol. 35). Journal of Strategic Studies.

Os apagões prolongados resultantes desses ciberataques afetaram a infraestrutura crítica do país. As evidências apontaram de forma inequívoca para a implicação russa nos referidos ciberataques.[5]

Em 2010, o Irão foi alvo de um ciberataque em grande escala, conhecido como *Stuxnet*. Este ciberataque foi um dos primeiros exemplos conhecidos de um ciberataque direcionado a um sistema industrial, especificamente ao programa nuclear do Irão. O ataque foi atribuído a uma operação conjunta dos Estados Unidos e de Israel.[6]

Estes ciberataques destacam a crescente importância da cibersegurança e os desafios enfrentados pelas nações na proteção das suas infraestruturas críticas e dos seus recursos digitais contra ciberameaças cada vez mais sofisticadas.

No debate sobre a cibersegurança e a ocorrência de ciberguerras, há diferentes perspetivas que refletem interpretações distintas da definição de ciberguerra e das características dos ciberataques.

Thomas Rid (2012), um proponente contrário à ideia de ciberguerras, argumenta que, segundo a visão de Clausewitz (1831), a guerra está tradicionalmente associada à violência e é organizada politicamente entre Estados. Na sua opinião, os cenários de ciberataques letais ainda são fictícios.[7]

Por outro lado, um autor que defende que os ciberataques podem ser letais é Richard A. Clarke (2001). Clarke é um especialista em segurança informática e autor do livro "*Cyber War: The Next Threat to National Security and What to Do About It*"[8].

Nesse livro[9], ele argumenta que os ciberataques têm o potencial de causar danos significativos e até mesmo mortes, especialmente quando direcionados a infraestruturas críticas, como redes elétricas, sistemas de transporte e/ou serviços de saúde. Clarke enfatiza que as consequências dos ciberataques podem ser tão graves quanto as de um conflito militar convencional.

---

[5] Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers.* Doubleday.
[6] Zetter, K. (2015*). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown.
[7] Rid, T. (2012). *Cyber War Will Not Take Place (Vol. 35)*. Journal of Strategic Studies.
[8] *Ciberguerra: A Próxima Ameaça à Segurança Nacional e o Que Fazer a Respeito*, tradução livre.
[9] Clarke, R. A., & Knake, R. (2011). *Cyber War: The Next Threat to National Security and What to Do About It.* Paperback.

Ele destaca casos históricos, como o ciberataque que interrompeu o fornecimento de energia numa parte do território ucraniano em 2015, como um exemplo da forma como os ciberataques podem ter impactos tangíveis na vida das pessoas. A guerra na Ucrânia que começou na madrugada de 24 de fevereiro de 2022 evidencia de forma inequívoca a importância das dimensões da segurança humana no contexto dos ciberataques.

Os ciberataques direcionados às infraestruturas críticas, como redes elétricas e sistemas de transporte, tiveram um impacto direto na vida quotidiana da população ucraniana. Interrupções no fornecimento de energia elétrica, por exemplo, comprometeram a segurança das pessoas ao afetar serviços essenciais, como o aquecimento em condições climáticas adversas e o acesso a cuidados de saúde adequados. Além disso, a infraestrutura digital do país também foi alvo de ciberataques, acarretando implicações na segurança informática tanto para os indivíduos quanto para as instituições.

No contexto da guerra na Ucrânia, é importante destacar a relação das ciberameaças com as diferentes dimensões da segurança humana mencionadas no texto. As ciberameaças podem ampliar os impactos negativos em cada uma destas áreas:

- **Segurança Económica:** As ciberameaças direcionadas a infraestruturas económicas, como redes de energia e sistemas financeiros, podem agravar os danos causados pela guerra, resultando em perdas económicas ainda maiores e instabilidade financeira adicional.
- **Segurança Alimentar:** A interrupção das atividades agrícolas devido às ciberameaças pode agravar a insegurança alimentar, dificultando a produção, distribuição e acesso a alimentos básicos em áreas afetadas pelo conflito.
- **Segurança Sanitária:** As ciberameaças direcionadas a instalações médicas e sistemas de saúde podem comprometer ainda mais o acesso a cuidados de saúde adequados, colocando em risco a segurança sanitária da população no meio de um conflito.
- **Segurança Ambiental:** A contaminação ambiental resultante dos ciberataques, como o derramamento de produtos químicos ou a sabotagem de infraestruturas ambientais, pode ter impactos significativos na saúde das pessoas e na sustentabilidade do ecossistema local.
- **Segurança Pessoal:** Ações informáticas, como a utilização de *malware* para espionagem ou para obter informações pessoais sensíveis, podem comprometer a segurança pessoal das pessoas afetadas pelo conflito.

- **Segurança Comunitária:** A desinformação, a propaganda ou os ciberataques que visam criar divisões e minar a coesão comunitária podem agravar os efeitos negativos do conflito, afetando a segurança e o bem-estar das comunidades.
- **Segurança Política:** As ciberameaças direcionadas a sistemas políticos e de governação podem aprofundar a instabilidade política, minando a confiança nas instituições e dificultando a procura por soluções pacíficas e estáveis.

Assim sendo, a cibersegurança desempenha um papel crucial na proteção das dimensões da segurança humana durante conflitos armados, garantindo a integridade e a resiliência dos sistemas digitais. A interligação entre a segurança humana e a segurança digital reforça a necessidade de abordagens holísticas para enfrentar os desafios digitais e para proteger a população em conflitos e crises.

A cooperação internacional e o desenvolvimento de medidas de proteção coletiva são essenciais para mitigar os impactos dos ciberataques e garantir um ambiente mais seguro no espaço digital. Um debate relevante no campo da cibersegurança é a questão da atribuição. Thomas Rid (2012) argumenta que a atribuição na esfera digital é uma questão complexa e em constante evolução. Segundo ele, os Estados têm a capacidade de moldar a atribuição de ciberataques de acordo com os seus interesses políticos e estratégicos.

Rid destaca que a atribuição de um ciberataque é fundamental para evitar que os agressores se sintam impunes, agindo sob o véu do anonimato. Por outro lado, Randall W. Stone (2013) contesta a interpretação de Rid, baseando-se na definição de guerra de Clausewitz (1831). Stone argumenta que a definição de guerra como um ato de força física implica que ciberguerras futuras podem, de facto, causar violência e letalidade.[10]

Para Stone, a ideia de que a letalidade é necessária para que um ato seja considerado uma guerra não se mantém necessariamente válida no contexto dos ciberataques[11]. No entanto, é importante reconhecer que os ciberataques têm a capacidade de causar danos significativos, mesmo sem a utilização direta da força física. Ben Buchanan (2015) complementa o debate ao destacar que os ciberataques têm se tornado cada vez mais subtis e comuns.[12]

[10] Stone, J. (2013). *Cyber War Will Take Place* (Vol. 36). Journal of Strategic Studies.
[11] Stone, J. (2013). *Cyber War Will Take Place* (Vol. 36). Journal of Strategic Studies.
[12] Thomas Rid, B. B. (2015). *Attributing Cyber Attacks* (Vol. 38). The Journal of Strategic Studies.

Os agressores podem explorar vulnerabilidades nos sistemas de comunicação, infraestruturas críticas e até mesmo interferir em processos políticos, sem necessariamente causar danos letais. Assim, a atribuição torna-se ainda mais relevante para responsabilizar os agressores e evitar a impunidade.[13]

Na perspetiva das Relações Internacionais, os ciberataques apresentam desafios únicos. As fronteiras físicas perdem importância no ciberespaço, permitindo que os agressores realizem ataques a partir de qualquer lugar do mundo, desafiando os conceitos tradicionais de soberania e a territorialidade. Além disso, os ciberataques podem ser conduzidos de forma encoberta, dificultando a identificação clara do agressor e tornando as respostas políticas e diplomáticas mais complexas.

Diante destas questões, é crucial que os Estados invistam em estratégias de cibersegurança robustas, promovam a cooperação internacional e fortaleçam os mecanismos de atribuição de ciberataques. A atribuição efetiva permitirá responsabilizar os agressores, dissuadir futuros ataques e contribuir para a estabilidade e segurança no ciberespaço.

Para enfrentar esses desafios, os Estados devem fortalecer as suas capacidades de investigação e de atribuição digital. Isso envolve o desenvolvimento de tecnologias avançadas de monitorização e análise de tráfego de dados, bem como a cooperação internacional na troca de informações e partilha de boas práticas.

Além disso, os Estados devem procurar adotar mecanismos legais e acordos internacionais que promovam a responsabilização dos ciberatacantes e estabeleçam normas claras de comportamento no ciberespaço.

É essencial promover o diálogo e a cooperação entre os Estados para desenvolver estratégias conjuntas de ciberdefesa, de partilha de informações sobre ameaças emergentes e fortalecer a resiliência dos sistemas de tecnologia da informação e comunicação.

A atribuição de ciberataques é um tema complexo e em constante evolução, exige uma abordagem multifacetada e colaborativa. Para lidar efetivamente com os desafios da cibersegurança, é necessário um esforço conjunto de governos, do setor privado, das organizações internacionais e da sociedade civil.

[13] Thomas Rid, B. B. (2015). *Attributing Cyber Attacks* (Vol. 38). The Journal of Strategic Studies.

A consciencialização sobre as ciberameaças deve ser ampliada, de forma a promover a educação e a formação de profissionais especializados em segurança informática. As empresas devem implementar medidas robustas de proteção de dados e de infraestruturas de Tecnologias da Informação, enquanto os utilizadores finais devem adotar boas práticas de segurança digital.

É importante realçar a necessidade de uma abordagem holística na cibersegurança, tendo em consideração não apenas os aspetos técnicos e tecnológicos, mas também os aspetos legais, éticos, políticos e sociais. A cibersegurança não é apenas uma questão de proteção de dados e sistemas, é também uma questão de proteção dos direitos humanos, da privacidade, da liberdade de expressão e da estabilidade global. Somente por meio de uma abordagem abrangente e colaborativa é que podemos garantir um ambiente digital mais seguro e resiliente.

Eneken Tikk (2011) observa que as ciberatividades testam os limites do quadro jurídico existente, o que destaca a necessidade de medidas eficazes para proteger as pessoas no mundo digital.[14] Um marco significativo no campo da cibersegurança é o *Manual Tallinn 2.0*, elaborado por Michael N. Schmitt (2017) em colaboração com um grupo de especialistas jurídicos. O manual explora a aplicabilidade do Direito Internacional ao espaço digital e às operações de cibersegurança. Ele fornece uma visão abrangente das leis, regulamentos e tratados que visam proteger os civis e garantir a segurança global.[15]

Desde 2009, o *Cooperative Cyber Defense Center of Excellence* da NATO tem defendido e promovido o *Manual de Tallinn* como uma referência crucial para a aplicação do Direito Internacional no ciberespaço.[16] O *Manual Tallinn* não terá base legal até que seja reconhecido internacionalmente.

Atualmente, não existe um Tratado de cibersegurança universalmente aplicável que seja reconhecido internacionalmente. Os problemas jurídicos envolvidos em ciberataques são complexos devido ao conflito de leis no ciberespaço e à dificuldade de atribuir a autoria dos ciberataques.

---

[14] E Tikk, E., Kaska, K., & Vihul, L. (2011). *International Cyber Incidents: Legal Considerations.* Cooperative Cyber Defense Centre of Excellence.

[15] Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.

[16] Bustelo, R. V. (2019). *O Processo do Manual de Tallin e a Evolução da Estratégia de Dissuasão no Ciberespaço.* Obtido de https://comum.rcaap.pt/bitstream/10400.26/29895/3/O%20processo%20do%20Manual%20de%20Tallinn%20e%20a%20evolu%c3%a7%c3%a3o%20da%20estrat%c3%a9gia%20de%20dissuas%c3%a3o%20no%20ciberespa%c3%a7o_BUSTELO.pdf

Essa falta de consenso legal e normativo destaca a necessidade urgente de um tratado de cibersegurança globalmente reconhecido. Acredita-se que um Tratado de cibersegurança seja extremamente necessário para abordar as lacunas legais existentes e estabelecer diretrizes claras para a prevenção, a mitigação e a resposta a ciberataques. Esse Tratado poderia estabelecer normas de comportamento responsável no ciberespaço, definir as responsabilidades dos Estados na proteção dos seus cidadãos e infraestruturas digitais, assim como promover a cooperação internacional no combate às ciberameaças. A elaboração de um Tratado de cibersegurança não é uma tarefa fácil, uma vez que, envolve a participação de diversos atores e a superação de desafios técnicos, políticos e jurídicos. Para além disto, a tremenda rapidez da evolução no domínio digital gera o risco de sistematicamente desatualizar ou enfraquecer os Tratados a que se chegue. No entanto, a crescente importância da cibersegurança e a necessidade de proteger os indivíduos e as infraestruturas críticas exigem esforços conjuntos para estabelecer um marco legal robusto e eficaz.

Enquanto um Tratado de cibersegurança globalmente reconhecido não é estabelecido, é importante que os países continuem a desenvolver legislações nacionais e acordos bilaterais ou multilaterais para promover a cooperação e combater as ciberameaças. Além disso, organizações internacionais, como a NATO, a ONU e a União Europeia, podem desempenhar um papel importante na promoção de diretrizes e boas práticas de cibersegurança, na facilitação do diálogo e na promoção da cooperação entre os países.

A proteção dos indivíduos e das suas informações pessoais é essencial para garantir a sua segurança e bem-estar no mundo digital. Isso envolve medidas que vão além da segurança técnica, como a consciencialização dos utilizadores sobre os riscos digitais, a educação em cibersegurança e a promoção de boas práticas de proteção de dados.

As regras do *Manual de Tallinn* são um conjunto de princípios e orientações desenvolvidos por especialistas em Direito Internacional para lidar com questões relacionadas à cibersegurança.

Essas regras foram compiladas no *Manual de Direito Internacional Aplicável a Ciberoperações*, também conhecido como *Manual de Tallinn*, publicado pela primeira vez em 2013 pela organização sem fins lucrativos *Cooperative Cyber Defense Center of Excellence* da NATO em Tallinn, Estónia.

O *Manual de Tallinn* aborda uma variedade de questões legais e éticas relacionadas à cibersegurança e às ciberoperações, e foi desenvolvido com o objetivo de fornecer orientação a governos, militares, especialistas jurídicos e outros atores envolvidos nessa área.

Os ciberataques têm sido uma preocupação crescente. De acordo com a regra 92 do Manual Tallinn, esses ataques podem resultar em "danos físicos ou morte a pessoas" e também em "danos ou destruição a objetos."[17] Essa definição ampla abrange tanto os ataques direcionados a indivíduos como aqueles que visam perturbar ou destruir objetos de propriedade privada.

As regras 93 e 94 do *Manual Tallinn* estabelecem que os ciberataques contra civis ou objetos civis são proibidos e considerados ilegais quando a intenção é causar danos deliberadamente.[18] Essas regras visam proteger a segurança humana e garantir que os ciberataques não colocam em risco a vida e o bem-estar das pessoas.

É importante destacar que a regra 33 do *Manual Tallinn* estipula que o Direito Internacional não regula os ciberataques perpetrados por atores não estatais. Isso significa que, do ponto de vista legal, esses ataques não violam a soberania dos Estados, não são considerados intervenções nem são definidos como atos de força.[19]

No entanto, é essencial reconhecer que os ciberataques não estão restritos apenas a atores estatais, uma vez que, a atribuição dessas ações é complexa e muitas vezes difícil de determinar com certeza. Portanto, esta dissertação não se concentrará exclusivamente na questão da atribuição dos ciberataques nem se limitará aos atores estatais. Em vez disso, procurará analisar as ameaças e os ciberataques em que os civis e a sua segurança estejam em perigo.

A evolução tecnológica proporcionada pela *internet* trouxe uma série de benefícios para a sociedade, mas também resultou num aumento significativo das ciberameaças. Os *hackers* e os cibercriminosos estão constantemente a desenvolver novas técnicas e estratégias para explorar vulnerabilidades em sistemas, em redes e em dispositivos. O que por sua vez, cria uma série de desafios para as economias, para as infraestruturas estatais, para as organizações e para os indivíduos.

---

[17]Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.
[18] Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.
[19] Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge University Press.

Com o aumento das ciberameaças, a consciencialização sobre a importância da cibersegurança tem-se tornado cada vez mais relevante. As pessoas estão a tornar-se mais conscientes de como é que os seus dados pessoais podem ser utilizados para fins maliciosos, o que tem impulsionado a procura por soluções de segurança mais eficazes.[20]

Embora os estudos existentes tenham se concentrado principalmente nas políticas dos Estados em relação à cibersegurança, é igualmente importante compreender o impacto da cibersegurança no indivíduo. W. Alexander, no seu estudo, argumenta que a moral desempenha um papel crucial no domínio da cibersegurança, por estar diretamente relacionada ao comportamento emocional do público em geral.

Um exemplo disso é o ataque de engenharia social, uma forma de ciberameaça em que as pessoas são influenciadas através da manipulação psicológica com a finalidade de cumprirem as exigências de um ciberatacante ou a revelar informações pessoais.[21]

Os autores Peter W. Singer e Allan Friedman (2014) destacam a relação entre a cibersegurança e o comportamento humano. Eles argumentam que os ciberatacantes exploram a confiança das pessoas para obter acesso não autorizado a sistemas e a dados sensíveis.

Muitas vezes, as próprias pessoas, de forma inconsciente ou confiante, contribuem para a disseminação de vírus e *malware*, ao clicarem em *links* ou anexos infetados, ou ao conectarem dispositivos externos aos seus computadores.[22] Essa vulnerabilidade humana faz com que as pessoas sejam o elo mais fraco na luta contra a cibercriminalidade.

É importante ressaltar que não se trata apenas de falta de conhecimento ou de habilidades técnicas, mas também de questões comportamentais e psicológicas. Os ciberataques muitas vezes baseiam-se em técnicas de engenharia social, exploram a confiança, o medo, a curiosidade ou a falta de atenção das pessoas.

Em síntese, a cibersegurança na atualidade requer uma abordagem que considere o papel central do comportamento humano. As pessoas, muitas vezes inconscientemente, podem ser exploradas pelos ciberatacantes, tornando-se, como já vimos, o elo mais fraco na defesa contra as ciberameaças.

---

[20] Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge University Press.
[21] Mouton, F., Leenen, L., & Venter, H. (2016). *Social Engineering Attack Examples, Templates and Scenarios* (Vol. 59). Computers & Security, Elsevier.
[22] Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press.

As pessoas devem ser informadas sobre os riscos e as boas práticas para protegerem os seus dispositivos, os seus dados e as suas informações pessoais. Para enfrentar esse desafio, é necessário investir na consciencialização e na educação em cibersegurança, tanto a nível individual quanto coletivo.

Embora não seja necessário que todas as pessoas sejam especialistas em *internet* e em tecnologia, é crucial que elas estejam cientes das ameaças que podem comprometer a sua segurança pessoal. A consciencialização em cibersegurança refere-se à compreensão dos riscos de segurança no mundo digital, contemplando o conhecimento individual das pessoas sobre as diversas ciberameaças existentes e as suas capacidades de identificação e reação a essas ameaças."[23]

No próximo sub-capítulo desta dissertação, serão explorados os potenciais ciber-riscos que podem afetar a cibersegurança. Essa análise abrangerá diversas ciberameaças, tendo em consideração a diversidade de ataques e abordagens utilizadas pelos cibercriminosos.

2.2. As ciberameaças

Nos últimos anos, tem havido um impulso significativo na discussão sobre as ciberameaças. Os países estão a adotar posições e a desenvolver estratégias para prever essas ameaças, bem como para protegerem e prepararem o público em geral para os potenciais riscos.[24]

As ciberameaças são frequentemente associadas ao cibercrime, que é definido como "um termo utilizado para descrever a violência abaixo do nível de conflito armado entre os Estados, que incluí atores não estatais e pode envolver perturbações de infraestruturas críticas ou atos politicamente perturbadores."[25]

Neste sub-capítulo, será apresentada uma visão geral das ciberameaças e dos cibercrimes na esfera digital, de forma a destacar os riscos enfrentados pelos utilizadores individuais da *internet*. Além disso, serão exploradas as medidas de consciencialização das pessoas em relação à segurança digital, que podem ser consideradas como medidas de "higiene" digital para proteger a segurança humana. Um utilizador da *internet* geralmente enfrenta três tipos diferentes de riscos de segurança da informação. O primeiro é o roubo de dados, que pode revelar informações pessoais ou planos estratégicos.

[23] Amoroso, E. G. (2011). *Cyber Attacks: Protecting National Infrastructure*. Burlington: Butterworth-Heinemann.
[24] Lewis, J. A. (2014). *National Perceptions of Cyber Threats. Strategic Analysis,* (Vol. 38). Strategic Analysis.
[25] Lewis, J. A. (2014). *National Perceptions of Cyber Threats. Strategic Analysis,* (Vol. 38). Strategic Analysis.

O segundo é o uso indevido de credenciais, que pode levar à destruição ou alteração de dados pessoais. E o terceiro é o desvio de recursos, como assumir o controlo das finanças de um indivíduo.[26] Para identificar as ameaças específicas que serão discutidas e analisadas nesta dissertação, utilizámos o Relatório de Ciberameaças elaborado pela Agência Europeia para a Segurança das Redes e da Informação (ENISA)[27]. Esse Relatório abrange as 15 principais ciberameaças que afetaram os utilizadores da *internet* em 2015 e 2016.

Ele fornece uma visão geral das ciberameaças mais comuns e as suas tendências, incluindo uma breve explicação de cada ameaça. É importante ressaltar que muitas vezes essas ameaças não ocorrem isoladamente, podem ser um pré-requisito para outras ameaças.

Essas 15 principais ciberameaças são:

1. *Malware* - Refere-se a *software* malicioso que pode propagar-se pela rede, agir como um vírus e instruir as vítimas sobre os passos a seguir após a infeção. O *malware* pode resultar em perda de dados e/ou mau funcionamento dos dispositivos.[28]

2. Os ataques baseados na *web* - Exploram vulnerabilidades nos componentes e complementos da *web*, utilizando-os como pontos de entrada para comprometer servidores ou *websites*. Os utilizadores da *internet* podem ser alvo em *websites* infetados ou manipulados, com grupos específicos a serem frequentemente visados.[29]

3. Os ataques a aplicações *web* - Têm sobreposições com ataques baseados na *web*, mas as suas principais fontes são aplicações baseadas na *web* ou aplicações móveis. As aplicações públicas são um alvo fácil, e criam os chamados agentes de ameaça que continuam a transferir e a partilhar vulnerabilidades.[30]

---

[26] Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press.
[27] ENISA. (2017). *ENISA Threat Landscape Report 2016*. Obtido de The European Union Agency for Cybersecurity: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016
[28] Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press.
[29] Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press.
[30] ENISA. (2017). *ENISA Threat Landscape Report 2016.* Obtido de The European Union Agency for Cybersecurity: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

4. Os ataques de negação de serviço (DoS) - Têm como alvo servidores *web* ou outros subsistemas envolvidos em conexões à *internet*. Através da utilização de múltiplos computadores, os atacantes sobrecarregam a conexão do alvo, inundando-o com uma grande quantidade de dados e, desativam o sistema.[31]

5. Os *botnets* - Também conhecidos como "computadores *zombies*", tomam conta dos dispositivos dos utilizadores da *internet* de forma que estes possam nunca se aperceber de que os seus computadores são ou fizeram parte de *botnets*.[32] Os *botnets* cometem outros cibercrimes que afetam a segurança da informação e são capazes de enganar os controlos de segurança, como filtros de *spam*, por exemplo.[33]

6. O *Phishing* - É uma das formas mais sofisticadas de engenharia social, utilizam-se *e-mail's* que parecem ter sido enviados por uma fonte de confiança. Os *e-mail's* em si não causam danos, mas convidam a abrir páginas *web* maliciosas, a inserir credenciais ou a transferir dinheiro.[34]

7. O *Spam* - Semelhante ao *phishing*, não cria danos apenas por existir e pode até ser difícil de reconhecer como uma ciberameaça. No entanto, o *spam* é a forma mais comum de disseminação de *malware*, pode levar as vítimas a abrir anexos suspeitos, clicar em *URL's* maliciosos e realizar outras ações que comprometem a sua segurança.[35]

8. O *Ransomware* - É um tipo de *malware*, cujo objetivo principal é extorquir dinheiro através do bloqueio dos dispositivos do alvo ou da encriptação dos seus dados. As vítimas ficam com duas opções; pagar o resgate (geralmente em criptomoedas) ou tentar recuperar os dados através da desencriptação.[36]

---

[31] Buchanan, B. (2016). *The Life Cycles of Cyber Threats* (Vol. 58). Routledge, part of the Taylor & Francis Group.
[32] Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press.
[33] ENISA. (2017). *ENISA Threat Landscape Report 2016.* Obtido de The European Union Agency for Cybersecurity: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016
[34] Junger, M., Montoya, L., & Overink, F. (2017). *Priming and warnings are not effective to prevent social engineering attacks*. Computers in Human Behavior.
[35] ENISA. (2017). *ENISA Threat Landscape Report 2016.* Obtido de The European Union Agency for Cybersecurity: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016
[36] Zetter, K. (2017). *What Is Ransomware? A Guide to the Global Cyberattack's Scary Method*. Obtido de https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/

9. As ameaças internas - Podem ser causadas intencionalmente ou não intencionalmente. Os casos não intencionais podem envolver a manipulação incorreta de dados, o abuso de privilégios, a utilização de *hardware* não aprovado, entre outros aspetos. As ameaças internas relacionadas com informações confidenciais são propositadamente cometidas geralmente por dinheiro.[37]

10. A manipulação física - Pode não ser considerada como uma ameaça direta à segurança da informação, mas o roubo, a perda ou dano o de qualquer dispositivo pode ter resultados graves, tais como a fuga de informação, a violação de dados, entre outros aspetos. Uma das formas mais comuns de manipulação física é a fraude com cartões de crédito.[38]

11. Os *kits* de exploração – Procuram identificar vulnerabilidades do sistema ou falhas de segurança para espalhar o *malware*. Os *kits* de exploração oferecem canais de "crimeware-as-a-service" (CaaS), onde as pessoas podem pagar para espalhar o *malware* nos *sites* que querem que sejam comprometidos.[39]

12. As violações de dados - Ocorrem geralmente devido ao roubo de credenciais, o que pode desencadear um efeito de cascata e resultar em mais violações. As credenciais comprometidas são frequentemente vendidas no mercado negro a preços muito baixos, sendo posteriormente utilizadas para disseminar mensagens de *phishing* e/ou *spam*.[40]

13. O roubo de identidade - É considerado um caso especial ou um resultado bem-sucedido de uma violação de dados. Ocorre quando os cibercriminosos obtêm a propriedade das credenciais, tais como dados financeiros, bancários, de saúde, entre outros, que podem causar danos graves à vítima.[41]

14. A fuga de informação - Refere-se ao acesso não autorizado a dados e informações confidenciais, seja de forma acidental ou intencional. Embora ambos possam causar graves problemas, as fugas intencionais são geralmente muito mais prejudiciais em termos de impacto.[42]

---

[37] ENISA. (2017). *ENISA Threat Landscape Report 2016*. Obtido de The European Union Agency for Cybersecurity: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

[38] ENISA. (2017). *ENISA Threat Landscape Report 2016.* Obtido de The European Union Agency for Cybersecurity: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

[39] Future, R. (2016). *New Kit, Same Player: Top 10 Vulnerabilities Used by Exploit Kits in 2016.* Obtido de https://www.recordedfuture.com/top-vulnerabilities-2016

[40] ENISA. (2017). *ENISA Threat Landscape Report 2016.* Obtido de The European Union Agency for Cybersecurity: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

[41] ENISA. (2017). *ENISA Threat Landscape Report 2016*. Obtido de The European Union Agency for Cybersecurity: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

[42] Blasco, J. (2012). *Bypassing Information Leakage Protection with Trusted Applications*. Computers & Security, Elsevier.

15. A ciberespionagem – É predominantemente conduzida entre Estados, utiliza-se outros tipos de cibercrimes como meio. A ciberespionagem pode ser caracterizada pela criação estratégica de vantagens e desvantagens entre atores estatais.[43]

A cibersegurança enfrenta um panorama constantemente mutável e em constante evolução. As 15 principais ciberameaças mencionadas anteriormente são apenas uma amostra das diversas ameaças que surgem no cenário digital. É fundamental reconhecer que há novas ameaças que estão constantemente a surgir, impulsionadas pelo avanço da tecnologia, pelas mudanças nas táticas dos cibercriminosos e pelas complexidades das Relações Internacionais.

À medida que as organizações e os indivíduos se esforçam para protegerem os seus sistemas e as suas informações, é essencial manterem-se atualizados sobre as tendências e os desenvolvimentos no campo da cibersegurança. A natureza em constante evolução das ameaças exige uma abordagem proativa, adaptável e baseada na colaboração para se enfrentar os desafios atuais e futuros.

Além disso, é importante reconhecer a interconetividade cada vez maior dos sistemas e a dependência da tecnologia nas nossas vidas quotidianas. A segurança digital tornou-se uma preocupação central nas Relações Internacionais, com os Estados a procurarem fortalecer as suas capacidades defensivas e a colaborarem em esforços conjuntos para combater as ciberameaças transnacionais.

É importante ressaltar que as ciberameaças, quando resultam em vítimas, deixam de ser apenas ameaças e tornam-se em crimes. Portanto, iremos utilizar os termos ciberameaças e cibercrimes de forma intercambiável, considerando que um é um pré-requisito ou causa, e o outro é o resultado de uma execução "bem-sucedida" de uma ameaça.

Como afirmou Buchanan, todas as inovações digitais, assim como qualquer outra invenção na história, foram criadas graças a grandes visionários.[44] Infelizmente, nem todas as descobertas no âmbito digital são benevolentes, e os indivíduos com conhecimentos avançados em computação podem descobrir vulnerabilidades tecnológicas que podem ser exploradas para fins maliciosos.[45]

---

[43] Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press.
[44] Buchanan, B. (2016). *The Life Cycles of Cyber Threats (*Vol. 58). Routledge, part of the Taylor & Francis Group.
[45] Buchanan, B. (2016). *The Life Cycles of Cyber Threats* (Vol. 58). Routledge, part of the Taylor & Francis Group.

Os riscos e as ciberameaças estão em constante evolução, e aquilo que parece surpreendente hoje pode se tornar comum amanhã, e vice-versa. [46] Como não se espera que os utilizadores da *internet* descubram por si só os riscos e as ciberameaças, é fundamental aumentar-se a consciencialização pessoal sobre essas ameaças e adotar uma postura mais ciber-higiénica no ambiente *online*. A ciberhigiene deve ser garantida no mundo *online* da mesma forma que as práticas de higiene pública são asseguradas nos cuidados de saúde para prevenir a propagação de doenças.[47]

A ciberhigiene é um conceito que visa promover, sustentar e garantir a segurança e a saúde digital. Para alcançarmos esses objetivos, devem ser adotadas diversas ações: a promoção da ciberhigiene através da consciencialização e da educação sobre os riscos informáticos e a divulgação das boas práticas de cibersegurança.

Isso é realizado através de campanhas, formações, seminários e programas educacionais, com o intuito de disseminar o conhecimento e incentivar comportamentos seguros *online*. Já a sustentação da ciberhigiene é alcançada através da implementação de estratégias e diretrizes de segurança digital em organizações, empresas e instituições. Essas estratégias e diretrizes estabelecem padrões e práticas de segurança que devem ser seguidos por todos os utilizadores.

Além disso, a atualização regular dos sistemas, das aplicações e dos programas, assim como a utilização de senhas fortes e a proteção adequada de dispositivos móveis, desempenham um papel fundamental na sustentação da ciberhigiene.

A garantia da ciberhigiene é obtida através da adoção de soluções de segurança digital, tais como o antivírus, *firewalls* e ferramentas de deteção de *malware*. Essas soluções ajudam a proteger contra ciberameaças, assegurando a segurança dos sistemas e dos dados. Além disso, a realização regular de *backups* dos dados e a implementação de medidas de privacidade e proteção de dados contribuem para garantir a ciberhigiene.

A consciencialização crescente sobre a esfera digital levará a uma melhor ciberhigiene e, por sua vez, aumentará o nível de conhecimento em relação às ciberameaças e às medidas de prevenção e proteção necessárias.

---

[46] Kello, L. (2013). *The Meaning of the Cyber Revolution: Perils to Theory and Statecraft* (Vol. 38). The MIT Press.
[47] Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press.

A ciberhigiene é um princípio fundamental relacionado à segurança da informação, uma vez que, os indivíduos mais ciber-higiénicos são menos vulneráveis a ciberameaças.[48] A prática da ciberhigiene, de acordo com a análise da ENISA, envolve várias medidas, como manter um registo atualizado de todo o *hardware* e *software*, digitalizar *e-mail's* recebidos, fazer *backup* de dados regularmente, utilizar configurações seguras em dispositivos e contas, entre outros aspetos.[49]

Quantas mais pessoas estiverem preparadas para enfrentar consistentemente os riscos de cibersegurança no mundo *online*, melhor será para todos.[50] É por isso que queremos analisar formas de como é que as ciberameaças são perturbadoras para a segurança humana, avaliar se uma maior consciencialização mantém uma melhor segurança, e o que poderia ser feito para haver mais segurança.

No próximo sub-capítulo, vamos aprofundar a análise da segurança humana em relação à cibersegurança. Tendo em consideração a interconexão cada vez maior entre o mundo digital e as atividades humanas, é essencial compreender como é que as ciberameaças afetam a segurança e o bem-estar das pessoas.

2.3. A segurança humana em relação à cibersegurança

A segurança humana é um conceito que tem despertado discussões e controvérsias, uma vez que, ainda não alcançou um consenso verdadeiro. No entanto, pode ser entendida como uma abordagem que visa atender às necessidades fundamentais dos indivíduos, com ênfase na prevenção de conflitos e na compreensão das raízes estruturais das vulnerabilidades. O *Relatório das Nações Unidas sobre Desenvolvimento Humano*, de 1994, define a segurança humana como uma dimensão relacionada ao medo e às necessidades, com o objetivo de proteger as liberdades vitais, assim como as pessoas expostas a ameaças e situações críticas.

Permitindo que as pessoas ajam de acordo com os seus interesses pessoais, promovendo assim a autonomia e o empoderamento.

As Nações Unidas estabelecem sete componentes da segurança humana, que são interdependentes e complementares.

---

[48] Ware, B. (2013). *Why cyber hygiene isn't enough.* Obtido de http://www.networkworld.com/article/3086834/security/why-cyber-hygiene-isnt-enough.html

[49] ENISA. (2017). *ENISA Threat Landscape Report 2016.* Obtido de The European Union Agency for Cybersecurity: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

[50] Ware, B. (2013). *Why cyber hygiene isn't enough.* Obtido de http://www.networkworld.com/article/3086834/security/why-cyber-hygiene-isnt-enough.html

Essas componentes são:

- **Segurança Económica:** Refere-se à garantia de oportunidades económicas, de emprego adequado e de condições justas de trabalho, de forma a visar a proteção do bem-estar económico dos indivíduos.
- **Segurança Alimentar:** Envolve o acesso adequado e regular a alimentos nutritivos e suficientes para satisfazer as necessidades básicas das pessoas, de forma a garantir a sua saúde e o seu bem-estar.
- **Segurança Sanitária:** Diz respeito à disponibilidade de cuidados de saúde acessíveis e de qualidade, incluindo serviços médicos, prevenção de doenças e promoção do bem-estar físico e mental.
- **Segurança Ambiental:** Refere-se à proteção do meio ambiente e dos recursos naturais, assegurando a sustentabilidade e a preservação do planeta para as gerações presentes e futuras.
- **Segurança Pessoal:** Engloba a proteção contra ameaças à integridade física e psicológica dos indivíduos, incluindo a violência, a criminalidade, o terrorismo e os conflitos armados.
- **Segurança Comunitária:** Envolve a promoção de comunidades seguras e inclusivas, onde os indivíduos se sintam protegidos, participem ativamente e desfrutem da coesão social.
- **Segurança Política:** Refere-se à garantia do respeito pelos Direitos Humanos, do Estado de Direito, da participação política e da boa governação, de forma a visar a estabilidade política e a proteção dos direitos dos indivíduos.

As Nações Unidas apresentam características e dimensões importantes da Segurança Humana. Primeiramente, é centrada na pessoa humana, reconhecendo que os direitos humanos são universais e que a segurança deve ser garantida para todos os indivíduos. Além disso, defendem que a segurança humana é integradora, tendo em conta que as ameaças à segurança são transnacionais e diversas, exigindo uma abordagem holística e multidimensional.

As dimensões da segurança humana são interdependentes e indivisíveis, ou seja, as diferentes componentes estão relacionadas entre si e complementam-se. Por exemplo, é difícil alguém sentir-se seguro economicamente se não tiver acesso a alimentos adequados, cuidados de saúde, um ambiente saudável, proteção pessoal e uma comunidade segura.

Da mesma forma, que é difícil separar essas componentes, porque estão interligadas e influenciam-se umas às outras. Portanto, a melhoria numa componente pode contribuir para a segurança nas outras áreas.

A conquista da segurança humana requer uma ação cooperativa entre os Estados, as Organizações Internacionais, a Comunidade Internacional e as alianças. Embora a segurança seja uma responsabilidade dos Estados, é essencial uma cooperação efetiva entre eles, bem como com as organizações e iniciativas internacionais. Atualmente, muitas questões de segurança são abordadas de maneira mais eficaz através de ações cooperativas.

Em termos de operacionalizar o conceito de segurança humana, há três entidades que se destacam: o Japão, o Canadá e a União Europeia. Estes atores têm desenvolvido abordagens e políticas que procuram promover a segurança humana em diferentes âmbitos.

O Japão, por exemplo, tem se concentrado na ajuda humanitária, no desenvolvimento sustentável, assim como na promoção da paz e da segurança ao nível global.

O país tem adotado uma abordagem ampla da segurança humana, envolvendo questões como o desarmamento, a prevenção de conflitos, a erradicação da pobreza e a proteção dos Direitos Humanos.

O Canadá também desempenha um papel importante na promoção da Segurança Humana. O país tem adotado abordagens abrangentes e integradas, que envolvem a promoção dos Direitos Humanos, da igualdade de género, o desenvolvimento sustentável e a resiliência das comunidades. O Canadá tem sido um defensor ativo da inclusão da dimensão da segurança humana na agenda internacional.

A União Europeia (UE) tem adotado uma abordagem multidimensional da segurança humana, integrando-a nas suas Políticas de Segurança e de Desenvolvimento. A UE tem procurado promover a paz, a estabilidade e a prosperidade, através da cooperação regional, do fortalecimento do Estado de Direito, do combate ao crime organizado e do investimento no desenvolvimento sustentável.

A segurança humana no contexto *online* irá tornar-se cada vez mais relevante num futuro próximo. Nesta pesquisa, explicaremos porque é que a utilização do conceito de segurança humana como um quadro de análise é apropriado para entender as ciberameaças e os cibercrimes existentes sob a perspetiva individual. Será apresentada uma definição modernizada do conceito, a fim de aprimorar a análise neste estudo.

> O conceito de segurança humana é frequentemente citado no Relatório de Desenvolvimento Humano (RDH) do *Programa das Nações Unidas para o Desenvolvimento* (PNUD) de 1994, sendo essa a primeira menção ao conceito. Ele é composto por dois componentes principais: "liberdade do medo" e "liberdade da necessidade". Essa mudança de ênfase da segurança nacional para a segurança humana reflete uma preocupação maior com as ameaças à segurança enfrentadas pelos indivíduos, sejam elas relacionadas com crimes, conflitos armados, fome, pobreza, doenças ou desastres naturais. O RDH identifica sete categorias de ameaças à segurança humana: segurança económica, segurança alimentar, segurança sanitária, segurança ambiental, segurança pessoal, segurança comunitária e segurança política. Todas essas ameaças à segurança podem estar presentes no ambiente digital atualmente ou em cenários futuros de guerra.[51]

No entanto, esta dissertação irá concentrar-se principalmente na segurança pessoal. Através da análise da segurança humana no contexto digital, podemos compreender melhor como é que as pessoas são afetadas pelas ciberameaças e como é que as suas vidas e a sua dignidade são comprometidas.[52] Ao examinar as dimensões da segurança humana, podemos identificar como é que as ameaças virtuais impactam as interações sociais, a estabilidade dos Estados e até mesmo as Relações Internacionais.

De acordo com o quadro fornecido pelo *Programa das Nações Unidas para o Desenvolvimento* (PNUD), Jorge Nef (1999) define o conceito de segurança humana por meio de cinco subtópicos: "ecossistema, economia, sociedade, política e cultura."[53]

O autor argumenta que todos esses subtópicos estão interligados de diferentes formas e acredita que o conceito de segurança humana pode ser aplicado em qualquer parte do mundo.[54] É importante ressaltar que a publicação de Jorge Nef (1999) não incluí o ciberespaço, pois ele não teria como ter considerado esse aspeto na época. No entanto, é fundamental reconhecer a importância do ciberespaço como uma dimensão relevante para a segurança humana nos dias de hoje. [55]

---

[51] UNDP. (1994). *Human Development Report 1994.* Obtido de United Nations Development Programme: https://hdr.undp.org/system/files/documents/hdr1994encompletenostatspdf.pdf
[52]UNDP. (1994). *Human Development Report 1994.* Obtido de United Nations Development Programme: https://hdr.undp.org/system/files/documents/hdr1994encompletenostatspdf.pdf
[53] Nef, J. (1999). *Human Security and Mutual Vulnerability: The Global Political Economy of Development and Underdevelopment.* Ottawa: International Development Research Centre.
[54] Nef, J. (1999). *Human Security and Mutual Vulnerability: The Global Political Economy of Development and Underdevelopment.* Ottawa: International Development Research Centre.
[55] King, G., & Murray, C. J. (2002). *Rethinking Human Security* (Vol. 116). Political Science Quarterly.

Embora Shiratori King e Christopher Murray (2002) considerem a definição de segurança humana do PNUD controversa, concordam que ela teve um impacto revolucionário em diversos debates políticos. Estes autores acreditam que o conceito de segurança humana deve ser centrado na vida sem pobreza.[56]

Por outro lado, Neil MacFarlane e Yuen Khong (2006) adotam uma visão crítica em relação ao *Relatório de Desenvolvimento Humano* (RDH) do PNUD, argumentando que o enfoque nos seres humanos não resolve a questão do centrismo no Estado. Além disso, não é claro quem define a segurança humana quando se trata de alimentação, de saúde e de segurança económica.[57]

No entanto, a visão crítica destes autores não é especialmente relevante para esta dissertação, uma vez que as ciberameaças geralmente não têm um foco centralizado no Estado. É importante ressaltar que muitos estudiosos amplamente utilizam a definição do PNUD, e é necessário ter alguma perspetiva sobre a segurança humana para permitir debates e análises sobre o tema.

Outros estudiosos, como Mary Kaldor, Mary Martin e Sabine Selchow (2007), reconhecem a relevância do conceito de segurança humana em todas as formas de conflitos. Eles afirmam que o conceito de segurança humana não é necessariamente utilizado explicitamente nas Políticas de Segurança, mas indiretamente é algo que já é abordado, por exemplo, na *Política Comum de Segurança e Defesa da União Europeia*.[58]

Estes autores descrevem a "insegurança" não apenas como resultado da violência militar, mas também como consequência de perdas materiais, crimes ou violações dos Direitos Humanos. Para eles, a segurança humana é uma resposta tanto a ameaças físicas como a gestão de crises. Embora a perspetiva desses autores seja principalmente baseada em conflitos, eles também adotam uma abordagem centrada no ser humano em relação à segurança.

Taylor Owen (2004) aborda o conceito de segurança humana, ele acredita que as ameaças à segurança humana devem ser medidas pela sua gravidade, independentemente da ameaça ser o resultado de uma guerra, de uma doença, ou de outro aspeto.[59]

---

[56] King, G., & Murray, C. J. (2002). *Rethinking Human Security* (Vol. 116). Political Science Quarterly.
[57] MacFarlane, N., & Khong, Y. F. (2006). *Human Security and the UN: A Critical History*. Bloomington: Indiana University Press.
[58] Kaldor, M., Martin, M., & Selchow, S. (2007). *Human Security: A New Strategic Narrative for Europe*. Royal Institute of International Affairs.
[59] Kaldor, M., Martin, M., & Selchow, S. (2007). *Human Security: A New Strategic Narrative for Europe*. Royal Institute of International Affairs.

No contexto digital, essa abordagem poderia ser aplicada, embora atualmente as ciberameaças não ultrapassem o limiar de violência necessário para serem consideradas ameaças à segurança humana.

Por sua vez, Roland Paris (2001) destaca a existência de diversas interpretações do conceito de segurança humana e argumenta que "a segurança humana parece ser capaz de apoiar virtualmente qualquer hipótese".[60]

Paris não vê a segurança humana como um enquadramento abrangente para análise, mas como uma nova e ampla categoria de investigação nos estudos de segurança. Ele sugere que os estudos de segurança devem ir além do foco estatal, direcionando-se aos indivíduos, aos grupos e às comunidades.[61]

Tendo em consideração as diversas perspetivas sobre o conceito de segurança humana, esta dissertação procurará estabelecer uma definição original. As interpretações atuais do termo estão desatualizadas com o contexto atual, tendo conta o rápido desenvolvimento tecnológico. Antes da introdução do conceito de segurança humana, os estudos de segurança globais focavam-se principalmente na segurança militar, na perspetiva dos Estados e das suas relações.[62]

No entanto, é importante ressaltar que, embora as diversas definições do conceito de segurança humana não sejam adequadas para lidar com as questões de segurança global atuais, esta dissertação considera fundamental colocar a segurança do indivíduo em primeiro plano.

Inspirada no *Relatório de Desenvolvimento Humano* do *Programa das Nações Unidas para o Desenvolvimento* (PNUD), a nova interpretação do conceito de segurança humana irá concentrar-se não apenas na "liberdade de necessidade", como a pobreza ou os desastres naturais, mas também na "liberdade do medo", incluindo a cibersegurança como uma preocupação central.

Assim sendo, este sub-capítulo explora perspetivas e argumentos, de forma a procurar estabelecer uma definição atualizada da segurança humana no contexto da cibersegurança e a sua relação com os estudos de segurança internacionais. Isso fornecerá uma base teórica sólida para a análise e discussão subsequente.

---

[60] Owen, T. (2004). *Human Security – Conflict, Critique and Consensus: Colloquium Remarks and a Proposal for a Threshold-Based Definition* (Vol. 35). Sage Publications.
[61] Paris, R. (2001). *Human Security: Paradigm Shift or Hot Air?* (Vol. 26). International Security.
[62] Williams, P. D. (2013). *Security Studies an Introduction.* London Routledge.

O mundo contemporâneo tem vindo a presenciar uma mudança significativa nos medos e nas ameaças, muitos dos quais estão a emergir no ambiente digital. Neste contexto, o conceito de segurança humana tem expandindo-se para abranger as ameaças resultantes das ciberatividades.[63]

No entanto, apesar do potencial revolucionário desse conceito no século XXI, tem-se observado a sua subutilização e a falta de abordagem da perspetiva humana na esfera digital. Portanto, é fundamental considerar a esfera digital como parte integrante da segurança humana para que o conceito seja verdadeiramente transformador.

Neste sub-capítulo propomos uma nova definição de segurança humana que incluí a esfera digital e estabelece uma base conceitual para analisar a consciencialização em cibersegurança e as suas implicações para a segurança das pessoas.

Nos últimos anos, as ameaças enfrentadas pelas pessoas têm se diversificado e ampliado, e muitas delas têm origem no mundo digital. A cibersegurança desempenha um papel crucial na proteção das pessoas contra essas ameaças, garantindo que elas possam desfrutar dos seus direitos fundamentais no contexto do ciberespaço. No entanto, o conceito de segurança humana ainda não foi devidamente aplicado à esfera digital, o que limita a capacidade de abordar as preocupações e as necessidades das pessoas no século XXI."[64]

O *Manual Tallinn 2.0*, elaborado por um grupo de especialistas, destaca a importância de garantir os mesmos Direitos Humanos no ciberespaço que as pessoas desfrutam noutros contextos. Especialmente relevantes são os direitos à liberdade de expressão, à privacidade e a ter um processo adequado[65]. Portanto, é essencial considerar a esfera digital como parte integrante dos direitos fundamentais das pessoas no contexto das ciberameaças e cibercrimes existentes.

Com base nas discussões anteriores, propõe-se uma nova definição de segurança humana que incluí a esfera digital: "uma consideração individualizada dos direitos fundamentais das pessoas no contexto das ameaças e dos crimes existentes (incluindo a esfera digital) que possam ser perturbados por danos físicos e/ou psicológicos."

---

[63] UNDP. (1994). *Human Development Report 1994.* Obtido de United Nations Development Programme: https://hdr.undp.org/system/files/documents/hdr1994encompletenostatspdf.pdf

[64] Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge University Press.

[65] Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge University Press.

Esta definição ampliada reflete a importância de abordar as ameaças e os riscos enfrentados pelas pessoas no mundo digital e estabelece uma base sólida para a análise dos resultados do questionário sobre a consciencialização em cibersegurança.

A definição proposta de segurança humana abrange a consideração dos direitos fundamentais das pessoas em relação às ameaças e aos crimes existentes, tendo em conta a esfera digital. Ela enfatiza a necessidade de uma abordagem individualizada, e reconhece que cada pessoa tem direitos inalienáveis que devem ser protegidos.

Esta definição reconhece que as ameaças podem se manifestar tanto no mundo físico como no ambiente digital, e que podem causar danos físicos e/ou psicológicos. Ao incluir a esfera digital, a definição reconhece a crescente importância da tecnologia e da *internet* nas nossas vidas. Ela reconhece que as ameaças no mundo digital, como o cibercrime, também podem afetar a segurança e o bem-estar das pessoas. Portanto, a segurança humana deve abranger a dimensão digital, garantindo que os direitos fundamentais das pessoas sejam protegidos no contexto das ameaças e dos crimes que ocorrem nesse ambiente.

Esta definição está alinhada com as Relações Internacionais, uma vez que, reconhece a importância dos Direitos Humanos universalmente reconhecidos. Reforça a necessidade dos direitos das pessoas serem protegidos, independentemente do contexto em que se encontram, incluindo o ciberespaço. Dessa forma, a definição proposta procura abordar as preocupações relacionadas à segurança humana no mundo digital, considerando tanto as dimensões nacionais quanto as internacionais.

Esta dissertação representa um “teste” inovador ao aplicar o conceito de segurança humana à esfera digital, o que até ao momento não tinha sido explorado. O objetivo é investigar se as ciberameaças podem ser consideradas como perturbadoras da segurança humana e se uma maior consciencialização em cibersegurança pode reduzir os riscos e as ameaças à segurança das pessoas.

Esta pesquisa procura estabelecer uma nova investigação que complementará os estudos académicos existentes sobre a segurança humana e a cibersegurança.

Ao explorar o impacto das ciberameaças na segurança humana, bem como o papel da consciencialização em cibersegurança na redução dos riscos e das ameaças, esta pesquisa procura fornecer uma base sólida para o desenvolvimento de estratégias eficazes de proteção das pessoas no mundo digital.

2.4. Análise da relação entre as ciberatividades e as abordagens de segurança nacional e de segurança humana nas Relações Internacionais

A relação entre as ciberatividades e as abordagens de segurança nacional e de segurança humana nas Relações Internacionais é um tema de extrema relevância no cenário global atual. Com o avanço da tecnologia e o aumento das ciberameaças, é fundamental compreender como é que essas questões afetam tanto a segurança dos Estados quanto a segurança dos indivíduos e das comunidades.

Esta análise procura explorar essa relação, de forma a destacar a importância da cibersegurança como uma dimensão fundamental tanto da segurança nacional quanto da segurança humana.[66] A distinção entre a segurança nacional e a segurança humana é essencial para compreender as diferenças nas abordagens e nas preocupações destes conceitos.

Na segurança nacional, o Estado é o principal ator responsável pela garantia da estabilidade e da segurança do regime. Por outro lado, na segurança humana, os indivíduos são os principais atores, tanto a nível individual como parte integrante das comunidades. Enquanto a segurança nacional está focada principalmente na estabilidade do Estado e nas ameaças à sua soberania, a segurança humana preocupa-se com o bem-estar económico, com a saúde e a segurança individual dos indivíduos.[67]

Nesta perspetiva, as ameaças enfrentadas pela segurança nacional geralmente envolvem a coerção económica, militar ou diplomática por parte de outros Estados ou organizações internacionais. Por outro lado, as ameaças à segurança humana são mais abrangentes e podem incluir doenças, pobreza, criminalidade, ignorância e falta de acesso a recursos básicos, como o bem-estar económico, a saúde e a segurança individual. As origens dessas ameaças também variam entre a segurança nacional e a segurança humana. No caso da segurança nacional, as ameaças geralmente vêm de outros Estados, que podem ser considerados inimigos, rivais ou Estados Frágeis com estruturas de governança vulneráveis.

[66] Gil, I. (2021). *A Dimensão Humana da Segurança Contemporânea*. Lisboa: Universidade Autónoma de Lisboa.
[67] Gil, I. (2021). *A Dimensão Humana da Segurança Contemporânea.* Lisboa: Universidade Autónoma de Lisboa.

No entanto, as ameaças à segurança humana são mais diversas e podem ter origem nos Estados, em atores não estatais, como grupos terroristas como o autoproclamado Estado Islâmico, ou até mesmo em ameaças transnacionais, como as alterações climáticas, que afetam negativamente o bem-estar económico, a saúde e a segurança individual das populações. Além disso, os regimes repressivos dentro dos próprios Estados também podem representar uma ameaça à Segurança Humana. No que diz respeito às capacidades para manter a segurança, a segurança nacional tradicionalmente apoia-se no poder militar como a sua principal capacidade, mas também considera a produtividade económica e o controle de fronteiras, incluindo a gestão das fronteiras externas, como elementos importantes.

Já a segurança humana é fortemente influenciada pelo *Índice de Desenvolvimento Humano* (IDH), que mede o bem-estar geral dos indivíduos, tendo em consideração fatores como a saúde, a educação e a qualidade de vida.[68] No contexto da cibersegurança, tanto a segurança nacional quanto a segurança humana são afetadas pelas ciberameaças. A cibersegurança desempenha um papel crucial na proteção dos Estados contra os ciberataques que visam comprometer a sua segurança, a sua soberania e as suas infraestruturas críticas.

Para a segurança nacional, a cibersegurança é essencial para proteger as redes de comunicação, os sistemas de defesa e as infraestruturas críticas de um Estado contra os ciberataques de outras nações ou organizações. Isso incluí a proteção de informações estratégicas, de segredos militares, de dados governamentais sensíveis e de sistemas de controlo de fronteiras.

Por outro lado, para a segurança humana, a cibersegurança também desempenha um papel crucial na proteção dos indivíduos e das comunidades contra as ciberameaças que podem comprometer a sua segurança e o seu bem-estar. Isso incluí proteger as informações pessoais, os dados financeiros, os sistemas de saúde, as infraestruturas críticas como os sistemas de energia e de transporte, bem como garantir a segurança digital dos indivíduos nas suas interações *online*.[69]

Além disso, as ciberatividades também desempenham um papel importante nas Relações Internacionais, tanto na esfera da segurança nacional quanto na esfera da segurança humana. As ações informáticas de um Estado podem ter implicações significativas nas relações entre Estados, podendo levar a tensões, conflitos e até mesmo a uma ciberguerra.

[68] Gil, I. (2021). *A Dimensão Humana da Segurança Contemporânea*. Lisboa: Universidade Autónoma de Lisboa.
[69] Gil, I. (2021). *A Dimensão Humana da Segurança Contemporânea*. Lisboa: Universidade Autónoma de Lisboa.

A ciberespionagem, o roubo de propriedade intelectual, a desinformação e a manipulação de informações, os ciberataques a infraestruturas críticas (como hospitais ou sistemas de fornecimento de água) e a exploração de vulnerabilidades digitais são apenas alguns exemplos de como as ciberatividades podem afetar as Relações Internacionais e a segurança global. Portanto, a proteção contra as ciberameaças e o fortalecimento da cibersegurança são elementos essenciais para garantir a segurança global nas Relações Internacionais. O *Programa das Nações Unidas para o Desenvolvimento* (PNUD) definiu pela primeira vez o conceito de segurança humana em 1994.

Na segurança nacional, a unidade e a segurança do Estado estão relacionadas à prosperidade das suas fronteiras territoriais. Já na segurança humana, são duas as liberdades fundamentais.

A liberdade em relação à necessidade refere-se às ameaças de segurança relacionadas à fome, à doença, à repressão. A liberdade em relação ao medo diz respeito à proteção contra disrupções imponderáveis e imprevistas nos padrões do dia-a-dia, seja em relação às casas, aos empregos ou às comunidades.[70]

> Um importante indicador utilizado para medir o Desenvolvimento Humano dos Estados é o *Índice de Desenvolvimento Humano* (IDH), criado pelas Nações Unidas. O IDH classifica os países num *ranking*, e quanto mais elevada for a posição de um Estado nesse *ranking*, mais desenvolvido ele é do ponto de vista do Desenvolvimento Humano. No contexto das ciberatividades, tanto a segurança nacional quanto a segurança humana são afetadas. A cibersegurança tornou-se uma preocupação crucial, uma vez que as ciberameaças podem ter um impacto significativo na segurança de um país e na vida das pessoas. Questões como a proteção de infraestruturas críticas, a segurança de dados pessoais e a prevenção de ciberataques são fundamentais tanto para a segurança nacional como para a segurança humana. No contexto das ciberatividades, ambas as abordagens se entrelaçam, uma vez que a segurança dos Estados e a segurança das pessoas estão intimamente relacionadas no ciberespaço.[71]

As ciberatividades têm implicações nas Relações Internacionais, podem influenciar as dinâmicas de poder, a segurança global e a estabilidade das nações. Portanto, o estudo dessa relação é fundamental para entender e abordar os desafios emergentes na era digital e promover a segurança tanto a nível nacional quanto internacional.[72]

[70] Gil, I. (2021). *A Dimensão Humana da Segurança Contemporânea.* Lisboa: Universidade Autónoma de Lisboa.
[71] Gil, I. (2021). *A Dimensão Humana da Segurança Contemporânea*. Lisboa: Universidade Autónoma de Lisboa.
[72] Gil, I. (2021). *A Dimensão Humana da Segurança Contemporânea*. Lisboa: Universidade Autónoma de Lisboa.

2.5. Ciber-resiliência: Uma abordagem para a segurança humana nas relações internacionais

A cibersegurança tornou-se uma questão premente nas últimas décadas, com o crescente número de ciberincidentes e a dependência cada vez maior da sociedade global em relação às tecnologias digitais. No entanto, a abordagem tradicional centrada apenas na proteção dos sistemas e das redes já não é suficiente para enfrentar as complexidades e os desafios atuais.

É necessário um novo foco que incorpore uma perspetiva holística da segurança humana e que tenha em consideração as múltiplas dimensões envolvidas.[73]

A ciber-resiliência vai mais além da simples proteção contra as ciberameaças. Ela procura fortalecer a capacidade das sociedades para resistirem, adaptarem-se e recuperarem de ciberincidentes, minimizando os danos e mantendo a continuidade das atividades essenciais. Essa abordagem envolve a combinação de medidas preventivas, deteção e resposta eficazes, além do fortalecimento das capacidades técnicas, organizacionais e humanas.

A ciber-resiliência desempenha um papel crucial na promoção da segurança humana nas Relações Internacionais. Não é apenas uma preocupação doméstica, também tem implicações significativas para as Relações Internacionais. Os Estados enfrentam desafios transfronteiriços em relação à cibersegurança, portanto, é crucial promover a cooperação internacional e a coordenação entre os países para fortalecer a ciber resiliência global.[74]

Embora a ciber-resiliência seja uma abordagem promissora para fortalecer a segurança humana nas Relações Internacionais, existem desafios significativos a serem enfrentados. A rápida evolução das tecnologias, a sofisticação dos ciberataques e a falta de consenso em questões de governação global são apenas alguns exemplos desses desafios. Além disso, a ciber-resiliência deve ter em consideração a proteção dos Direitos Humanos e a garantia da privacidade, de forma a evitar ações excessivas de vigilância ou restrições indevidas às liberdades individuais. É necessário investir em capacitação e consciencialização, para que todos os atores envolvidos possam compreender os riscos e adotar medidas de segurança adequadas.

---

[73] Buchanan, B. (2017). *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations.* New York: Oxford University Press.

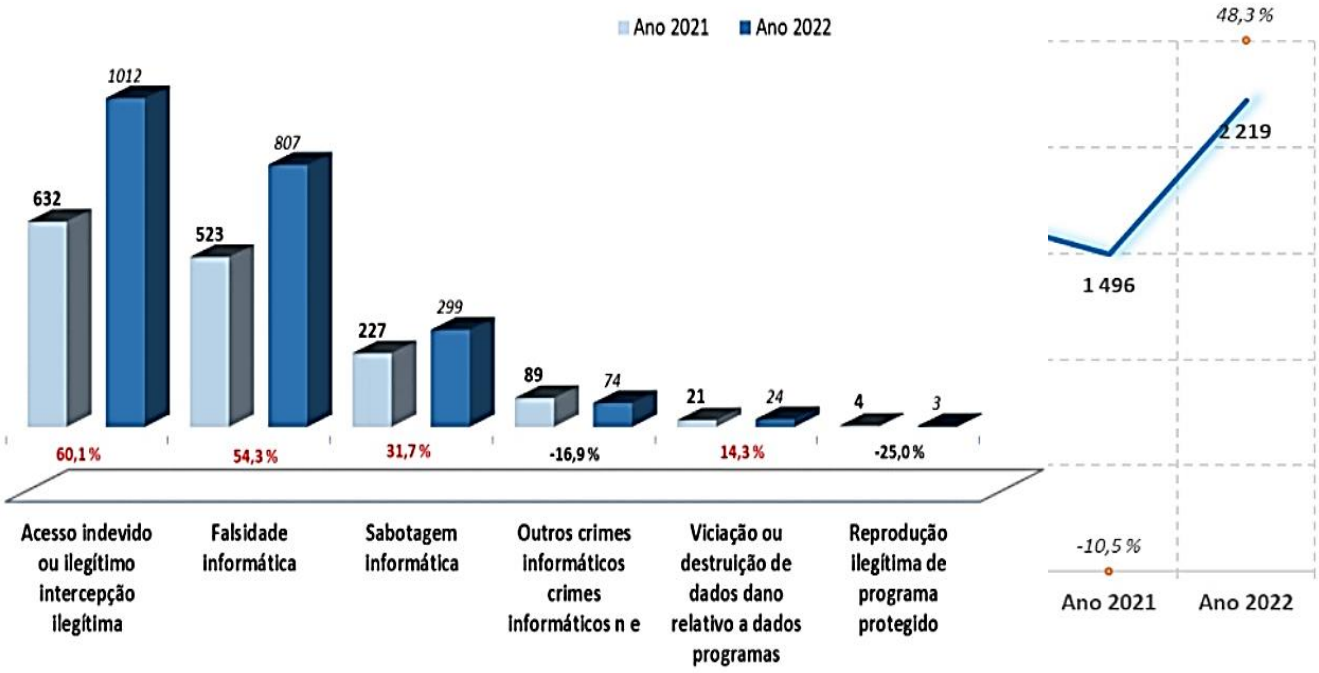
[74] Baylis, Smith, & Owens. (2011). *The Globalization of World Politics: An Introduction to International Relations.* Oxford University Press.

O fortalecimento da pesquisa e o desenvolvimento em cibersegurança também é fundamental para acompanhar a evolução das ameaças e desenvolverem-se soluções inovadoras.[75]

2.6. O aumento alarmante da cibercriminalidade em Portugal

O aumento dos crimes informáticos representa uma ameaça significativa para a segurança humana e para as Relações Internacionais. O *Relatório Anual de Segurança Interna* de 2022 revela um crescimento alarmante de cibercrimes em Portugal, com um aumento de 723 casos, o que equivale a um aumento de 48,3%.[76]

Ilustração 1 - O aumento exponencial da cibercriminalidade em Portugal



Fonte: Relatório Anual de Segurança Interna 2022

Estes dados indicam que houve um aumento preocupante nos crimes de acesso/interseção ilegítima, sabotagem informática e viciação ou destruição de dados. Essas atividades criminosas têm o potencial de causar danos substanciais, tanto para os indivíduos quanto para as organizações, e podem ter consequências diretas nas Relações Internacionais.

---

[75] Singer, P., & Friedman, A. (2021). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

[76] Interna, S. d. (2022). *Relatório Anual de Segurança Interna*. Obtido de https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDazMAQAhxRa3gUAAAA%3d

No contexto da segurança humana, o aumento do cibercrime coloca em risco a privacidade e a segurança pessoal das pessoas. Os indivíduos podem tornar-se vítimas de roubo de identidade, fraude financeira, assédio *online*, invasões de privacidade, entre outros aspetos, o que pode levar a sérios impactos psicológicos e/ou emocionais.[77] No âmbito das Relações Internacionais, o cibercrime representa um desafio significativo.

Os ciberataques podem ser conduzidos por atores estatais ou não estatais, e as suas motivações podem variar desde espionagem e roubo de propriedade intelectual ou até mesmo sabotagem de infraestruturas críticas e influência em processos eleitorais. Esses incidentes podem minar a confiança entre nações, criar tensões diplomáticas e ter repercussões económicas.[78]

Além disso, o aumento do cibercrime destaca a necessidade de uma maior cooperação internacional na luta contra essas ameaças. A partilha de informações e a coordenação de esforços entre os países tornam-se cada vez mais essenciais para mitigar os riscos associados ao cibercrime e para promover a segurança digital global.

[77] Interna, S. d. (2022). *Relatório Anual de Segurança Interna.* Obtido de https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDazMAQAhxRa3gUAAAA%3d

[78] Interna, S. d. (2022). *Relatório Anual de Segurança Interna.* Obtido de https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDazMAQAhxRa3gUAAAA%3d

3. Estrutura da investigação

A estrutura da investigação sobre "*Ameaças Cibernéticas e os seus impactos na Segurança Humana*" é apresentada de acordo com os diferentes tópicos relacionados com a segurança humana, as dimensões da segurança humana e as Relações Internacionais. A dissertação começa com uma introdução que fornece uma visão geral do tema, seguida pelo enquadramento teórico da problemática da cibersegurança, onde são abordados tópicos como a evolução das ciberameaças e o impacto da digitalização nas Relações Internacionais.

O debate sobre as ciberameaças compreende uma análise dos diferentes tipos de atividades maliciosas no mundo digital, bem como exemplos de ciberataques recentes e as suas consequências. A relação entre a segurança humana e a cibersegurança é explorada, onde é evidenciado as formas como as diferentes dimensões da segurança humana são afetadas pelas ciberameaças.

Além disso, é realizada uma análise da relação entre as ciberatividades e as abordagens da segurança nacional e da segurança humana nas Relações Internacionais, com foco nas contribuições da segurança humana para a cibersegurança. A importância da ciber-resiliência como uma abordagem para a segurança humana nas Relações Internacionais é debatida, enfatizando o conceito de ciber-resiliência e a sua relevância na proteção da segurança humana.

A estrutura da investigação incluí também uma secção dedicada à metodologia de investigação, onde é descrita a abordagem metodológica adotada, a recolha de dados e a análise dos mesmos.

Os resultados da investigação são apresentados através da análise de dados, do nível de consciencialização sobre a cibersegurança entre os inquiridos, da importância da educação em cibersegurança na prevenção do cibercrime, das experiências com a cibercriminalidade e da análise da segurança humana através do respetivo conceito.

As conclusões destacam o conceito de segurança humana relacionado com o espaço digital, a necessidade de educação/consciencialização em cibersegurança, a importância da literacia digital e do fator humano na promoção da segurança humana. A bibliografia utilizada na investigação é listada no final do texto, seguida pelos anexos, que incluí um questionário *online* utilizado na recolha dos dados.

No geral, esta estrutura de investigação aborda a problemática das ciberameaças e dos impactos na segurança humana, explorando as dimensões afetadas e relacionando-as com o campo das Relações Internacionais. Ela fornece uma análise abrangente e aprofundada sobre a relação entre cibersegurança, segurança humana e as dinâmicas internacionais, além de propor medidas educacionais e de consciencialização para mitigar os riscos e as ciberameaças.

3.2. Metodologia de investigação

Para avaliar o nível de consciencialização em cibersegurança, foi conduzido um questionário (Anexo 1) sobre as experiências das pessoas com as ciberameaças e a cibercriminalidade.

O *Relatório Anual* da ENISA sobre ciberameaças de 2016 serviu como base de pesquisa para apoiar a extensa lista de ciberameaças. O questionário foi criado através do Google Forms e foi direcionado a utilizadores da *internet* de todas as idades e origens.

A distribuição do questionário *online* ocorreu através de *e-mail's* e também através de canais de comunicação social, como o *Facebook*, o *LinkedIn* e o *Instagram*, com partilhas adicionais. Os dados dos inquiridos foram recolhidos anonimamente, a menos que o inquirido optasse por fornecer os seus dados pessoais. Um total de 106 pessoas responderam ao questionário.

Com base no questionário, os dados obtidos são principalmente sobre dois tópicos. A primeira parte do questionário centrou-se na consciencialização em cibersegurança das pessoas tendo em consideração a sua própria perceção e de algumas perguntas orientadoras, incluindo o seu conhecimento das ciberameaças existentes.

A segunda parte do questionário concentrou-se nas mesmas ameaças, mas sob a perspetiva das experiências e emoções pessoais dos inquiridos. Adicionalmente, o questionário foi concebido com a ideia de potencialmente aconselhar alguns dos inquiridos sobre as ameaças existentes e torná-los mais cuidadosos sobre o crime que ocorre *online*.

O questionário foi utilizado como recurso principal para dois objetivos. Em primeiro lugar, não existe investigação prévia sobre a ligação entre as ciberameaças e a segurança humana, pelo que, para se chegar a quaisquer conclusões, é necessário que haja alguns dados em que nos possamos basear. De uma perspetiva de segurança humana, as experiências individuais das pessoas são importantes para que possamos compreender tudo isto. O outro objetivo é o de apresentar uma ideia original com um resultado útil que poderia ser potencialmente mais desenvolvido.

As informações obtidas no questionário funcionaram como dados que serão analisados mais adiante, de forma a destacar as descobertas e as estatísticas mais interessantes, bem como a opinião de alguns dos inquiridos sobre as ciberameaças e o cibercrime. O questionário permitiu ter acesso ao público em geral dos utilizadores da *internet*.

É importante ressaltar que a linguagem utilizada no questionário e as redes específicas nas quais foi distribuído resultam numa amostra imperfeita da *internet* como um todo. No entanto, foi realizado dentro dos recursos e das capacidades disponíveis e 106 respostas proporcionaram uma amostra significativa, que geraram resultados valiosos. A composição da população que respondeu ao questionário será discutida no próximo capítulo.

Além disso, os resultados do questionário serão comparados com o conceito de segurança humana, conforme desenvolvido na revisão bibliográfica, para uma melhor compreensão de como é que a existência de ciberameaças e a vitimização pelo cibercrime afetam a segurança humana.

4. Resultados da investigação

O objetivo principal desta pesquisa é analisar profundamente as respostas ao questionário e estabelecer conclusões adicionais relacionando-as com o conceito de segurança humana, com a finalidade de compreender se as ciberameaças são perturbações ou danos para a segurança humana. A análise dos dados fornecerá uma visão geral dos antecedentes dos inquiridos e as suas opiniões sobre o panorama das ciberameaças.

Antes de analisar os resultados específicos, fornecemos uma descrição do perfil dos participantes da pesquisa. O questionário foi respondido por indivíduos de diferentes idades, de formações académicas e de origens geográficas diversas.

A participação abrangeu uma amostra diversificada para garantir uma representação abrangente das perceções e experiências em relação à cibersegurança.

Através da análise das respostas, foi possível identificar as principais preocupações e ameaças percecionadas pelos inquiridos. Além disso, explorou-se a perceção das pessoas em relação à gravidade dessas ameaças e a sua possível relação com a segurança humana. Essa análise contribuirá para a compreensão das preocupações emergentes e para a identificação de lacunas na consciencialização e na preparação para enfrentar essas ameaças.

A pesquisa também investigou o nível de consciencialização em cibersegurança entre os participantes. Isso incluiu perguntas sobre o conhecimento das boas práticas de cibersegurança, a adoção de medidas de proteção e a compreensão dos riscos associados às atividades *online*. A análise desses resultados ajudará a avaliar a eficácia das iniciativas educacionais existentes e a identificar as áreas onde a consciencialização precisa de ser fortalecida.

Outro aspeto importante da investigação foi a recolha de informações sobre as experiências passadas dos participantes com o cibercrime. Através de exemplos concretos fornecidos pelos inquiridos, foi possível compreender melhor os tipos de cibercrimes mais comuns e o impacto que eles têm nas vítimas. Além disso, explorou-se como é que essas experiências afetaram a sensação de segurança e de bem-estar dos indivíduos.

Essa análise contribuirá para ampliar a compreensão da relação entre o cibercrime e a segurança humana, bem como para identificar possíveis lacunas na proteção oferecida às vítimas.

A análise dos resultados será uma contribuição significativa para a literatura existente sobre a segurança humana na era digital. Ao relacionar as respostas dos participantes com o conceito de segurança humana, será possível identificar tendências e padrões que ajudarão a aprofundar o nosso entendimento sobre as interações entre a cibersegurança e a segurança humana.

Essa análise permitirá uma avaliação mais abrangente dos desafios enfrentados pela sociedade contemporânea no que diz respeito à proteção dos indivíduos e das comunidades contra as ciberameaças.

Em síntese, esta pesquisa procura explorar as perceções, as experiências e a consciencialização das pessoas em relação à cibersegurança, analisando a interseção entre a segurança humana, a cibersegurança e as Relações Internacionais.

4.1. Análise de dados sobre a cibersegurança e a segurança humana nas Relações Internacionais

Neste capítulo, realizaremos uma análise dos dados recolhidos através de um questionário *online* aplicado a 106 pessoas de 6 países diferentes: Portugal, Espanha, Brasil, Angola, Rússia e Moldávia.

O questionário decorreu ao longo de quatro semanas, do período de 6 de novembro de 2022 a 6 de dezembro de 2022. As perguntas incluíam tanto escolhas múltiplas como perguntas abertas. As perguntas abertas permitiram que os inquiridos expressassem os seus próprios pensamentos, opiniões e experiências relacionadas ao tema em questão.

Inicialmente, apresentaremos uma análise quantitativa dos dados recolhidos. Dos 106 participantes, 70 preencheram integralmente o questionário. Este número indica um bom nível de participação e confiabilidade dos resultados.

Em seguida, destacaremos algumas das principais descobertas obtidas através da análise das perguntas de escolha múltipla. As questões procuraram avaliar o nível de consciencialização dos participantes sobre questões de cibersegurança e as suas perceções sobre os desafios atuais nesse campo. Por exemplo, uma das perguntas foi: “Na sua opinião, o tema das ciberameaças tem exposição suficiente na atualidade?”

A análise completa dos dados, incluirá tabelas e gráficos detalhados. Além da análise quantitativa, também conduzimos uma análise qualitativa das respostas fornecidas nas perguntas abertas do questionário.

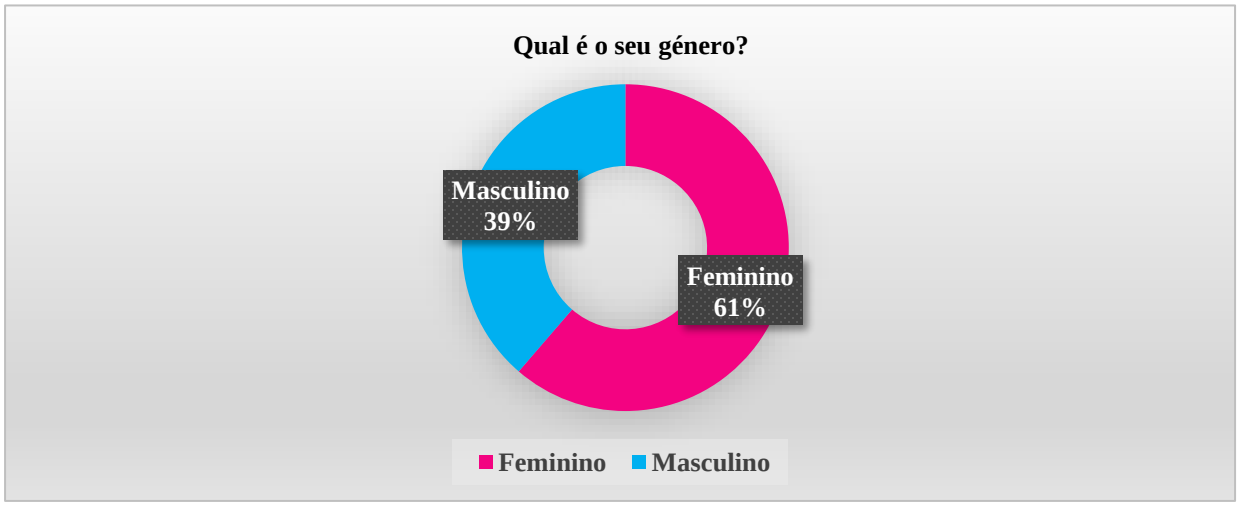
As perguntas abertas solicitavam aos inquiridos que partilhassem as suas opiniões sobre questões específicas de cibersegurança e de segurança humana, bem como as suas experiências pessoais relacionadas ao tema. Por exemplo, algumas das perguntas foram: “Sente-se pessoalmente ameaçado pelos cibercrimes?”, “A qual destes cibercrimes é que já esteve exposto?”

Ao analisar as respostas, identificaremos temas recorrentes, padrões e exemplos relevantes. Utilizaremos citações diretas e indiretas dos participantes para ilustrar e reforçar as nossas análises e conclusões. Por exemplo, uma citação de um participante que expressa as suas experiências pessoais será utilizada para ilustrar o impacto real de um ciberataque na vida de um indivíduo.

A análise qualitativa também nos permitirá identificar nuances e perspetivas adicionais que podem não ter sido capturadas pelas perguntas de escolha múltipla. Isso irá ajudar-nos a obter uma visão mais completa e aprofundada da relação entre a cibersegurança, a segurança humana e as Relações Internacionais.

A Figura 1, apresenta a distribuição de género dos participantes que preencheram o questionário.

Figura 1 - Género dos inquiridos



Fonte: Dados do questionário da pergunta n.º 1 (Anexo 1)

A análise desta figura permite compreender a representatividade de género entre os participantes da pesquisa e identificar possíveis discrepâncias ou tendências significativas que possam influenciar a perceção da cibersegurança e da segurança humana nas Relações Internacionais.

A distribuição de género observada nos resultados do questionário, com aproximadamente dois terços das respostas vindas de mulheres (61%) e um terço de homens (39%)[79], é interessante ao considerarmos a tendência de género na área da cibersegurança.

Historicamente, a área da cibersegurança tem sido predominantemente dominada por homens, com uma representação feminina relativamente baixa. No entanto, nos últimos anos, tem havido um esforço crescente para promover a diversidade de género nesse campo e atrair mais mulheres para as carreiras em cibersegurança.

Nesse sentido, a proporção de participantes do sexo feminino (61%) nos resultados do questionário sugere um aumento na representação das mulheres na área da cibersegurança.

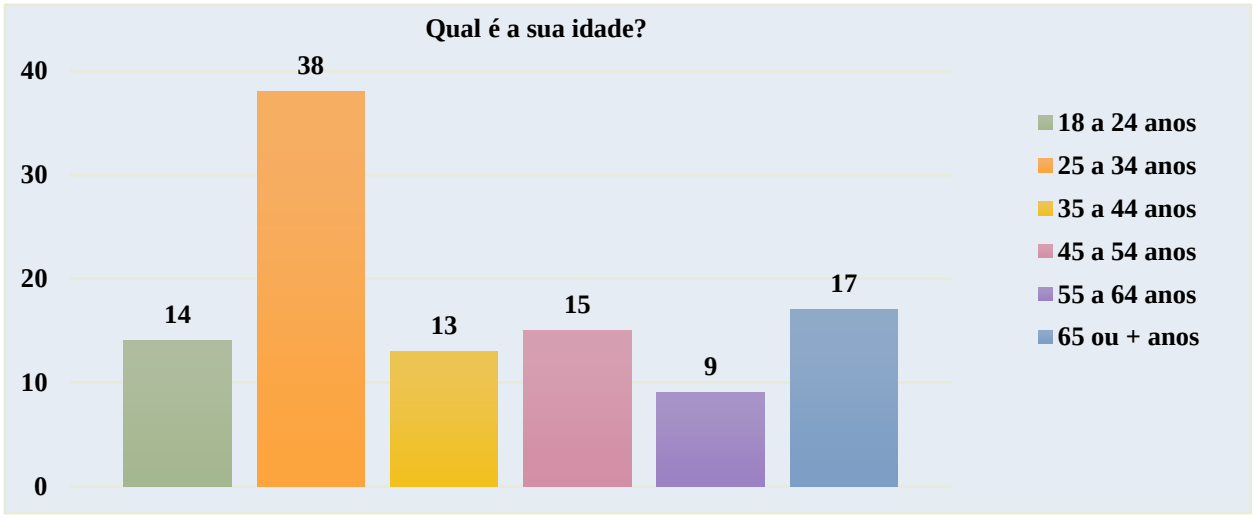
Isso pode ser considerado um reflexo positivo dos esforços para incentivar a participação feminina nesta área e evidencia uma maior diversidade de perspetivas e experiências relacionadas à cibersegurança.

No entanto, ainda há trabalho a ser feito para se alcançar uma maior equidade de género na área da cibersegurança. A distribuição de género nos resultados do questionário destaca a importância da inclusão e da diversidade na área da cibersegurança. A promoção da participação feminina e a redução das disparidades de género são cruciais para abordar os desafios da cibersegurança de forma mais abrangente e eficaz. A diversidade de perspetivas e experiências, incluindo as vozes femininas, fortalece a tomada de decisões, a inovação e a implementação de estratégias de cibersegurança mais inclusivas e holísticas.

[79] Respostas ao questionário à pergunta n.º 1 (Anexo 1)

A Figura 2, apresenta a distribuição da idade dos participantes do questionário.

Figura 2 - Idade dos inquiridos



Fonte: Dados do questionário da pergunta n.º 2 (Anexo 1)

A presença de inquiridos entre os 18 e os 24 anos pode indicar uma consciencialização crescente entre os jovens sobre a importância da cibersegurança. Essa faixa etária, que está altamente envolvida na utilização da tecnologia e das redes sociais, pode estar mais ciente dos riscos e desafios associados à segurança digital.

Com a maioria dos inquiridos na faixa etária dos 25 aos 34 anos, a representarem 36% do total, é possível que essa geração tenha um papel significativo na defesa contra as ciberameaças a nível internacional. Essa faixa etária geralmente está envolvida em setores relacionados à tecnologia, onde a cibersegurança é uma preocupação essencial.

A distribuição etária mostra que quase metade dos inquiridos (49%) tinha menos de 35 anos. Essa faixa etária pode ser caracterizada por um acesso mais amplo à informação e à tecnologia, o que pode afetar a forma como a segurança humana e as Relações Internacionais são compreendidas e abordadas. Isso pode levar a uma maior consciencialização e envolvimento em questões de segurança.

Ao considerar as diferentes faixas etárias, pode-se notar que cada uma delas pode enfrentar desafios específicos em relação à segurança humana, à cibersegurança e às Relações Internacionais.

Por exemplo, os inquiridos com idades entre os 45 e os 64 anos podem ter mais preocupações relacionadas à segurança financeira e ao envelhecimento da população, enquanto os inquiridos com 65 anos ou mais podem estar mais vulneráveis a ciberameaças direcionadas a idosos.

Estas análises fornecem algumas perspetivas de dados demográficos da idade dos inquiridos. No entanto, é importante considerarmos outros fatores e variáveis para uma compreensão mais abrangente do tema. .[80]

Na Figura 3, é apresentada a distribuição das nacionalidades dos participantes do questionário.

Figura 3 - Nacionalidade(s) dos inquiridos

Fonte: Dados do questionário da pergunta n.º 3 (Anexo 1)

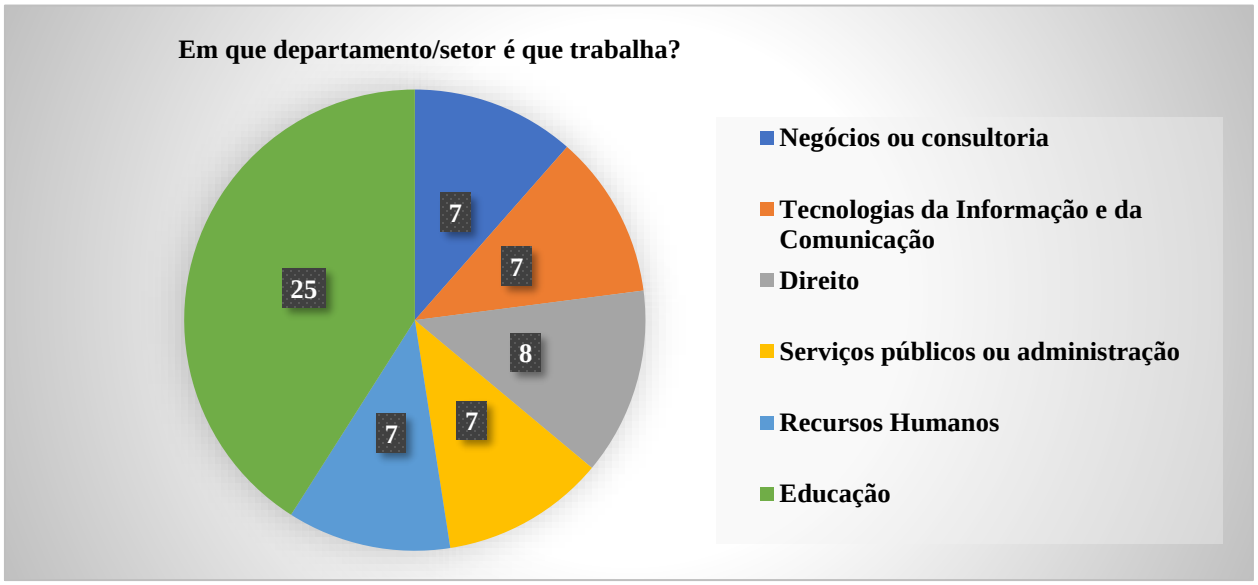
O facto de o questionário ter sido lançado na sociedade portuguesa indica que a amostra principal de inquiridos era composta por cidadãos portugueses. Isso pode ser relevante, pois cada país tem as suas próprias preocupações e desafios nesta área. A partir dos resultados do inquérito, investigaremos questões específicas relacionadas à cibersegurança em Portugal, como a consciencialização e a ocorrência de ciberincidentes.

[80] Respostas ao questionário à pergunta n.º 2 (Anexo 1)

A presença de inquiridos de diferentes nacionalidades na amostra indica que a segurança humana é uma questão importante que transcende fronteiras. Houve inquiridos que indicaram ter mais do que uma nacionalidade. Embora houvesse inquiridos de 7 países, apenas Portugal teve uma grande representação de pessoas - 97 inquiridos eram portugueses (92%), seguidos pelos brasileiros (5%) e Espanha (3%). Os outros inquiridos foram compostos pelas outras nacionalidades (angolana, russa, ucraniana e moldava) com uma percentagem de 0,9%.[81]

A Figura 4, apresenta a distribuição dos departamentos/setores dos participantes do questionário.

Figura 4 - Departamento/setor em que os inquiridos trabalham



Fonte: Dados do questionário da pergunta n.º 4 (Anexo 1)

Os antecedentes das pessoas são muito variados; trabalham mais frequentemente no setor da Educação (24%), o que parece estar relacionado com a Universidade Autónoma de Lisboa. O outro grupo com mais inquiridos é o de Direito (8%), o que sugere que os profissionais jurídicos estão envolvidos nas questões de cibersegurança e de segurança humana.

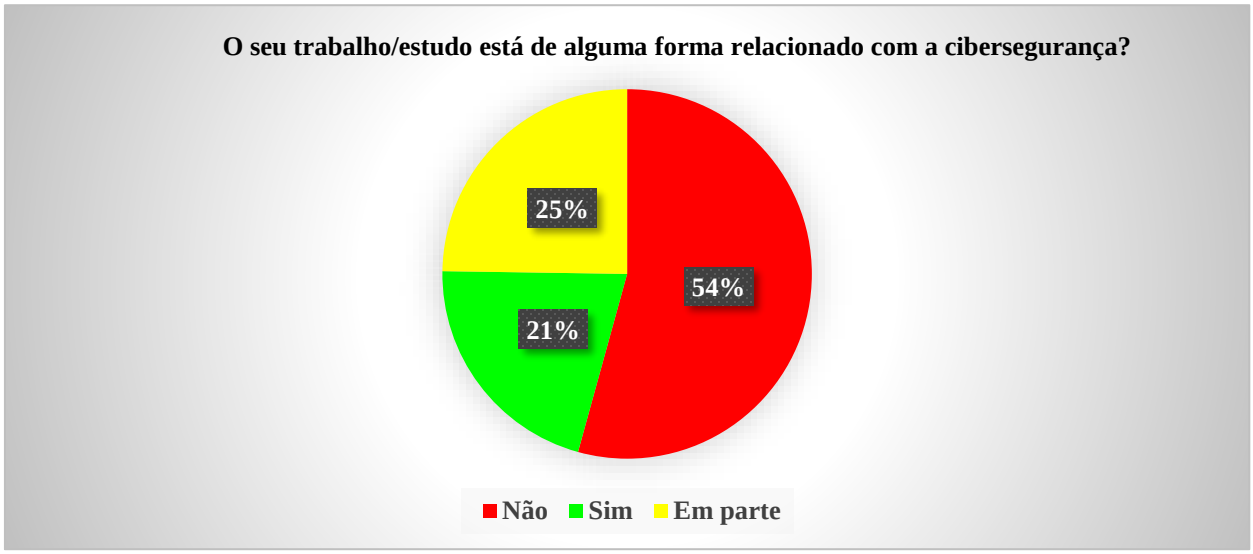
[81] Respostas ao questionário à pergunta n.º 3 (Anexo 1)

As outras áreas que se destacaram foram a das Tecnologias da Informação e da Comunicação, Negócios ou Consultoria, Serviços Públicos ou Administração, e Recursos Humanos, com 7% cada uma.[82] A área das Tecnologias da Informação e da Comunicação é boa para termos uma visão do tema desta dissertação.

Os outros três campos mais populares foram 1) Gestão; 2) Cuidados de Saúde; 3) Artes ou Design. Os antecedentes variados das pessoas que responderam ao questionário fornecem uma visão abrangente das áreas de atuação dos participantes.

Na Figura 5, é apresentada a relação entre o trabalho/estudos dos participantes com a cibersegurança.

Figura 5 - Relação do trabalho/estudos dos inquiridos com a cibersegurança



Fonte: Dados do questionário da pergunta n.º 5 (Anexo 1)

Com base nos dados apresentados, apenas 21% dos inquiridos consideraram que o seu trabalho ou estudos estão relacionados com a cibersegurança, enquanto 25% indicaram uma relação parcial. Estes números sugerem que a consciencialização e o envolvimento direto com a cibersegurança ainda não são tão prevalentes quanto o esperado.[83]

[82] Respostas ao questionário à pergunta n.º 4 (Anexo 1)
[83] Respostas ao questionário à pergunta n.º 5 (Anexo 1)

Esta tendência está alinhada com a crescente preocupação em relação às ciberameaças e à necessidade de proteção das informações pessoais e dos sistemas digitais. A falta de consciencialização em cibersegurança pode deixar os indivíduos e as organizações vulneráveis a ciberataques.[84]

No entanto, é importante ressaltar que os antecedentes dos inquiridos são variados, o que pode influenciar esses resultados. Os dados indicam que a pesquisa está mais relacionada com opiniões gerais sobre as ciberameaças e as experiências concretas do que com fatores demográficos específicos, como a idade ou a nacionalidade.

As ciberameaças podem afetar pessoas de diferentes origens e de diferentes áreas de atuação, portanto, é essencial adotar abordagens flexíveis e inclusivas para garantir a proteção digital de todos.[85]

4.2. Consciencialização sobre a cibersegurança entre os inquiridos

Neste sub-capítulo, analisaremos a perceção e o nível de conhecimento dos inquiridos em relação à cibersegurança. Através da análise detalhada dos resultados estatísticos do questionário, procuramos compreender o grau de familiaridade que os participantes têm em relação a conceitos-chave de cibersegurança, bem como a sua compreensão das boas práticas para protegerem-se contra as ameaças *online*.

Além disso, analisaremos a importância da consciencialização sobre a cibersegurança no contexto atual. Com a rápida evolução das ciberameaças e a sofisticação dos ataques, é crucial que os indivíduos estejam cientes dos perigos e saibam como se protegerem adequadamente. Iremos verificar como é que a falta de consciencialização pode resultar em vulnerabilidades e na exposição a ciberataques, e destacaremos a necessidade de educação sobre a cibersegurança em diversos setores da sociedade.

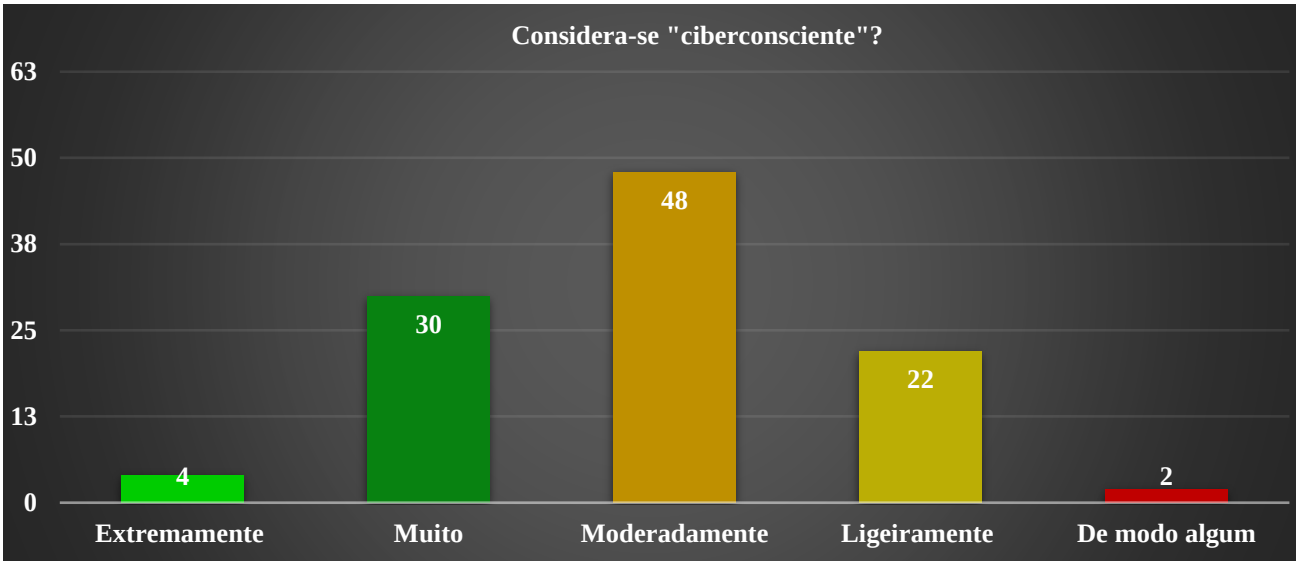
Ao compreendermos o nível de consciencialização sobre a cibersegurança entre os inquiridos, este estudo procura contribuir para o fortalecimento das estratégias de proteção e consciencialização nesta área vital.

[84] Respostas ao questionário à pergunta n.º 5 (Anexo 1)
[85] Respostas ao questionário à pergunta n.º 5 (Anexo 1)

Os resultados obtidos fornecerão informações valiosas sobre as lacunas de conhecimento, permitindo a criação de programas educacionais e de consciencialização mais eficazes, que visem mitigar os riscos e promovam uma postura proativa em relação à segurança digital.

Na Figura 6, é apresentada a perceção dos participantes em relação ao seu nível de conhecimento em cibersegurança.

Figura 6 - Perceção dos inquiridos sobre o seu conhecimento da cibersegurança



Fonte: Dados do questionário da pergunta n.º 6 (Anexo 1)

No que diz respeito ao conhecimento em cibersegurança, constatamos que apenas 48 inquiridos (45%) consideraram-se moderadamente ciberconscientes. Além disso, quase 30% dos participantes afirmaram ter conhecimentos muito bons no âmbito da segurança da informação. É importante ressaltar que, em relação às pessoas extremamente ciberconscientes, apenas 4 inquiridos (4%) é que se enquadram nessa categoria.

Por outro lado, 21% dos participantes (22 inquiridos) consideraram-se ligeiramente ciberconscientes. Surpreendentemente, dois inquiridos (2%) afirmaram não possuir conhecimentos em relação à cibersegurança. [86]

[86] Respostas ao questionário à pergunta n.º 6 (Anexo 1)

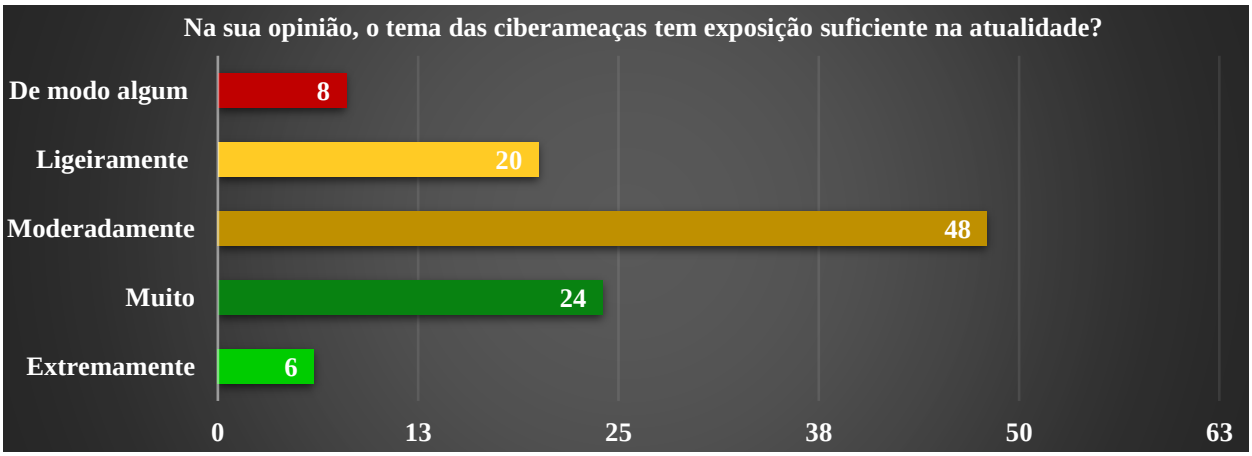
Estes dados revelam informações bastante interessantes e reforçam a importância da consciencialização sobre a segurança da informação. Destaca-se a necessidade de ampliar a consciencialização e o conhecimento em cibersegurança, uma vez que uma parcela significativa dos inquiridos possui apenas um nível moderado de consciencialização nesta área. [87]

Além disso, a presença de um número reduzido de pessoas extremamente ciberconscientes indica que há espaço para melhorias na promoção e na educação sobre a segurança digital. [88]

A falta de conhecimento em cibersegurança pode resultar em vulnerabilidades e exposição a ciberameaças, tornando a consciencialização numa peça fundamental na proteção contra ciberataques e na promoção de práticas seguras.[89]

Na Figura 7, é apresentada a perceção dos participantes em relação à exposição do tema das ciberameaças na atualidade.

Figura 7 - Perceção sobre se o tema das ciberameaças tem exposição suficiente na atualidade



Fonte: Dados do questionário da pergunta n.º 7 (Anexo 1)

A análise dos dados revela que quase metade dos inquiridos (44%) possui um sentimento moderado em relação à exposição às ameaças em cibersegurança. Isso sugere que eles têm uma perceção equilibrada em relação à importância e ao impacto das ciberameaças nas suas vidas. [90]

[87] Respostas ao questionário à pergunta n.º 6 (Anexo 1)
[88] Respostas ao questionário à pergunta n.º 6 (Anexo 1)
[89] Respostas ao questionário à pergunta n.º 6 (Anexo 1)
[90] Respostas ao questionário à pergunta n.º 7 (Anexo 1)

Por outro lado, 23% das pessoas acreditam que o tema das ciberameaças recebe muita atenção, indicando uma consciencialização elevada em relação aos perigos e aos riscos associados à segurança digital. Essa perceção pode ser resultado de uma maior exposição a notícias e a relatórios sobre os incidentes de segurança e sobre os ciberataques. [91] Porém, é interessante observar que 19% dos inquiridos consideram que as ciberameaças não recebem atenção suficiente.

Essa perspetiva sugere que esses indivíduos acreditam que as implicações e os riscos das ciberameaças não estão a ser adequadamente abordados pela sociedade em geral. Isso ressalta a importância de promover uma consciencialização mais ampla sobre a cibersegurança e sobre incentivar medidas proativas de proteção digital. [92]

É digno de nota que 8 pessoas (8%) expressaram a opinião de que as ciberameaças não recebem qualquer exposição. Essa visão destaca uma falta de consciencialização ou de compreensão em relação à gravidade e à frequência das ciberameaças na atualidade. Essa perceção equivocada pode representar um risco adicional, já que a falta de consciencialização pode levar à negligência em relação às práticas de segurança. [93]

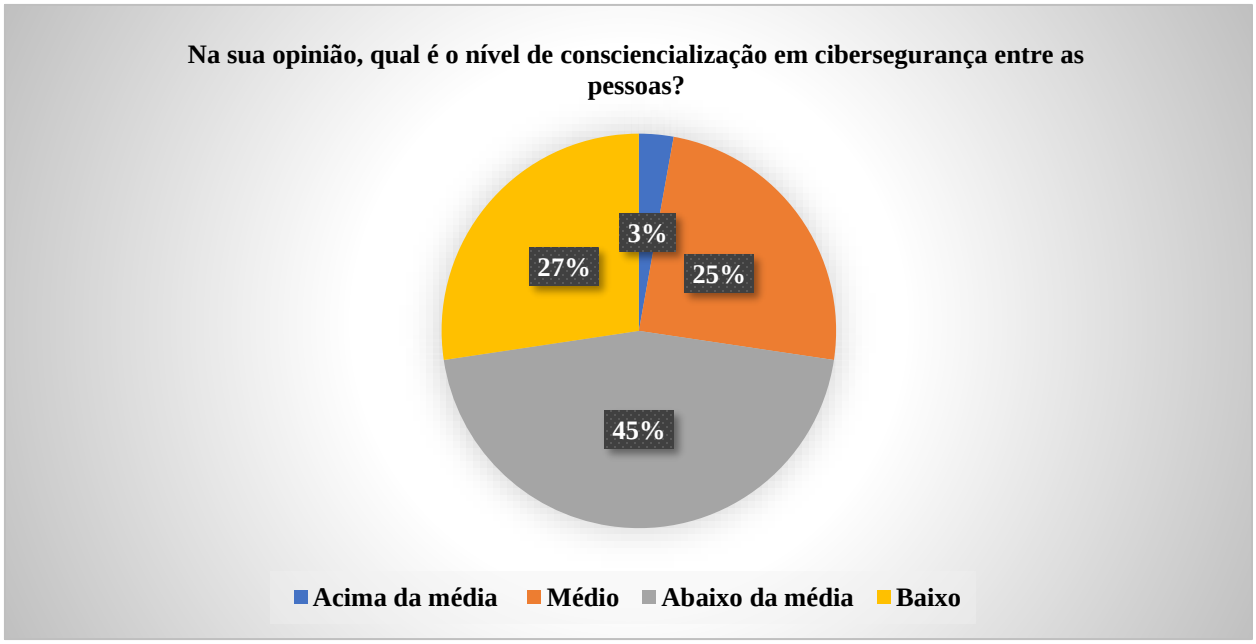
Além disso, 6 inquiridos (6%) consideraram que as ameaças à cibersegurança têm uma exposição extremamente alta na atualidade. Essa visão reflete uma compreensão aguçada sobre a amplitude e a gravidade das ciberameaças, provavelmente resultado de uma maior familiaridade com incidentes recentes ou notícias relacionadas à segurança digital. [94]

Esta variedade de perspetivas em relação à exposição às ameaças em cibersegurança destaca a necessidade de um equilíbrio adequado na consciencialização e na educação sobre o assunto. É essencial fornecer informações precisas e atualizadas para que as pessoas possam compreender adequadamente os riscos associados às ciberameaças e adotar medidas de segurança apropriadas.

[91] Respostas ao questionário à pergunta n.º 7 (Anexo 1)
[92] Respostas ao questionário à pergunta n.º 7 (Anexo 1)
[93] Respostas ao questionário à pergunta n.º 7 (Anexo 1)
[94] Respostas ao questionário à pergunta n.º 7 (Anexo 1)

Na Figura 8, é apresentada a perceção dos participantes em relação ao nível de consciencialização em cibersegurança.

Figura 8 - Perceção do nível de consciencialização em cibersegurança entre as pessoas



Fonte: Dados do questionário da pergunta n.º 8 (Anexo 1)

Ao analisarmos a Figura 8, que aborda a opinião dos participantes sobre o nível de consciencialização em cibersegurança de outras pessoas, podemos observar uma queda significativa nesse aspeto.

Cerca de 45% dos inquiridos acreditavam que o nível geral de consciencialização em cibersegurança estava abaixo da média, enquanto outros 27% consideravam que o nível era baixo. Isso significa que 73% dos participantes avaliaram o nível geral como abaixo da média, o que revela uma grande discrepância entre a perceção da própria consciencialização em cibersegurança dos inquiridos em comparação com a opinião sobre as outras pessoas. [95]

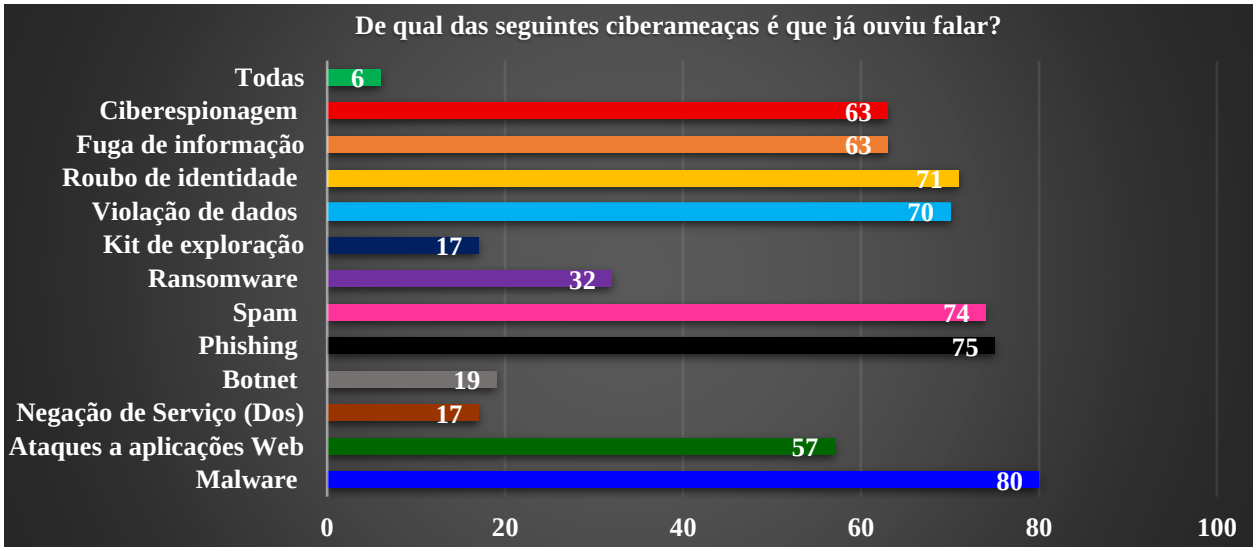
[95] Respostas ao questionário à pergunta n.º 8 (Anexo 1)

É importante ressaltar que os inquiridos possuem antecedentes e exposições muito diferentes no trabalho ou estudos em relação à cibersegurança. Essa diversidade de experiências pode levantar um debate sobre se as pessoas superestimam os seus próprios conhecimentos e a sua própria consciencialização ou se subestimam os conhecimentos e a consciencialização das outras pessoas.[96]

Estes resultados levantam questões sobre a autoavaliação da consciencialização em cibersegurança e destacam a importância de uma avaliação objetiva do nível de conhecimento e de consciencialização em cibersegurança. A discrepância entre a perceção pessoal e a opinião sobre os outros pode indicar a necessidade de programas educacionais e de consciencialização mais amplos, que tenham em consideração a diversidade de conhecimentos e de experiências dos indivíduos.

Na Figura 9, é apresentada a perceção dos participantes em relação ao nível de consciencialização em cibersegurança entre as pessoas.

Figura 9 - Perceção do nível de consciencialização em cibersegurança entre as pessoas



Fonte: Dados do questionário da pergunta n.º 9 (Anexo 1)

[96] Respostas ao questionário à pergunta n.º 8 (Anexo 1)

As ciberameaças foram avaliadas pelos participantes, permitindo a seleção de mais de uma opção. Através da observação dos resultados, constatamos que o *malware*, o *phishing* e o *spam* foram reconhecidos como ciberameaças por quase todos os inquiridos, enquanto outros cinco tipos de ameaças (o roubo de identidade, a violação de dados, a fuga de informação, a ciberespionagem e os ataques a aplicações *web*) foram conhecidos por 85% a 90% dos inquiridos. [97]

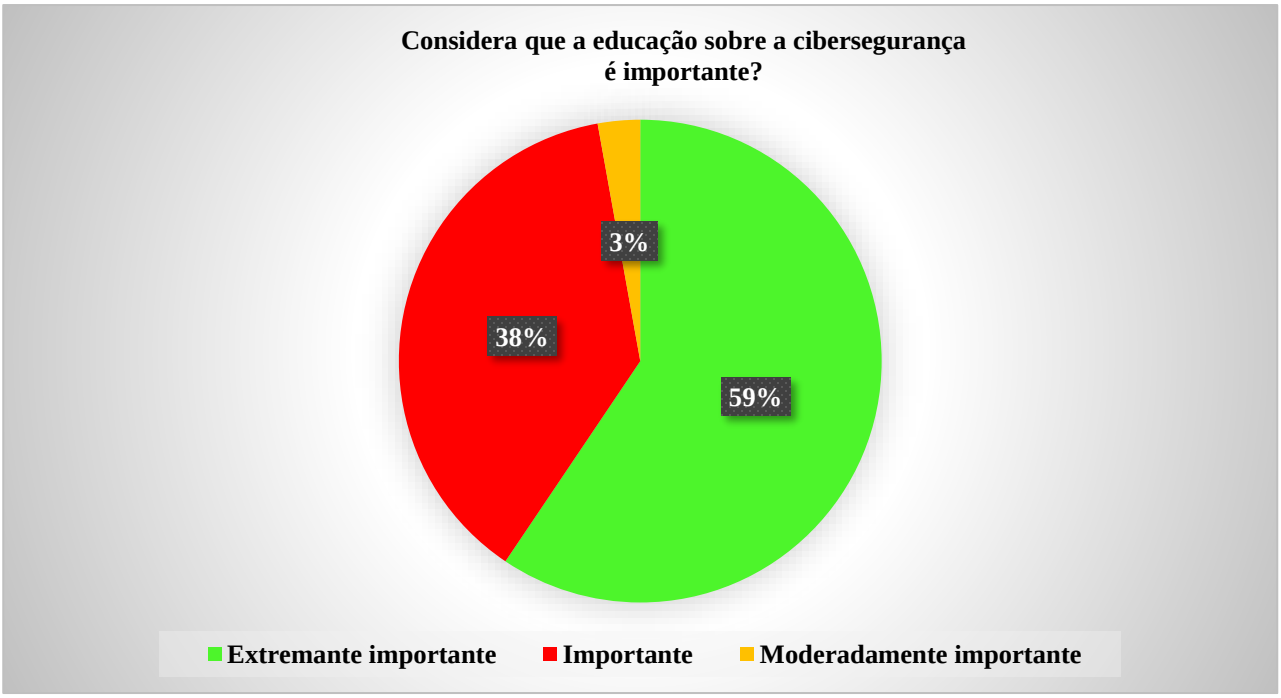
A maioria das outras ameaças foram reconhecidas por mais de 60% dos participantes, havendo apenas algumas ciberameaças menos conhecidas (o *botnet*, a negação de serviço (DoS) e o *kit* de exploração). [98]

Estes resultados indicam um nível relativamente alto de conhecimento das ciberameaças entre os participantes. Essa constatação é encorajadora, pois demonstra que a maioria dos inquiridos possui um entendimento sólido sobre as ciberameaças mais comuns. Mas, ainda assim, há a necessidade contínua de expandir a consciencialização e o conhecimento sobre as ameaças menos difundidas, com a finalidade de se garantir uma postura de segurança abrangente.

[97] Respostas ao questionário à pergunta n.º 9 (Anexo 1)
[98] Respostas ao questionário à pergunta n.º 9 (Anexo 1)

Na Figura 10, é apresentada a perceção dos participantes sobre a importância da educação sobre cibersegurança.

Figura 10 - Perceção dos inquiridos sobre a importância da educação sobre cibersegurança



Fonte: Dados do questionário da pergunta n.º 10 (Anexo 1)

Consequentemente, a educação sobre as ciberameaças existentes é considerada essencial por quase todos os participantes. Um total de 97% das pessoas afirmaram acreditar que é importante ou muito importante, enquanto nenhum participante respondeu de forma negativa. Apenas três inquiridos (3%) indicaram que consideram a educação sobre a cibersegurança como moderadamente importante. Isso demonstra um amplo consenso entre os participantes sobre a relevância e a necessidade de receberem educação adequada sobre a cibersegurança.

Estes resultados estão diretamente relacionados às tendências de cibersegurança observadas atualmente. A perceção quase unânime dos participantes de que a educação sobre as ciberameaças é essencial reflete a crescente consciencialização sobre os riscos e as ciberameaças que enfrentamos na sociedade contemporânea.

À medida em que a tecnologia avança e a interconetividade torna-se mais presente nas nossas vidas, as ciberameaças multiplicam-se e sofisticam-se. Nesse contexto, a educação sobre a cibersegurança desempenha um papel fundamental na proteção contra essas ameaças.

Ao estarem cientes das ciberameaças existentes e das boas práticas para se protegerem, os indivíduos podem adotar medidas proativas para reduzir a sua exposição aos ciberataques e manter a segurança das suas informações pessoais e profissionais.

A ampla aceitação da importância da educação sobre a cibersegurança demonstrada pelos participantes reflete uma crescente consciencialização e reconhecimento de que a segurança digital é uma responsabilidade partilhada. Não se trata apenas de nos protegermos a nós próprios, mas também de contribuir para um ambiente digital mais seguro para todos. Essa consciencialização coletiva é essencial para enfrentar os desafios cada vez mais complexos e em constante evolução da cibersegurança.[99]

Na pergunta número 11, referente à opinião dos inquiridos sobre se acredita que mais educação em cibersegurança contribuiria para evitar ou reduzir a ocorrência de cibercrimes, todos os participantes responderam afirmativamente. Além disso, alguns inquiridos apresentaram abordagens muito interessantes sobre o tema, contribuindo de forma positiva para esta dissertação. Entre as respostas, destacam-se as seguintes:

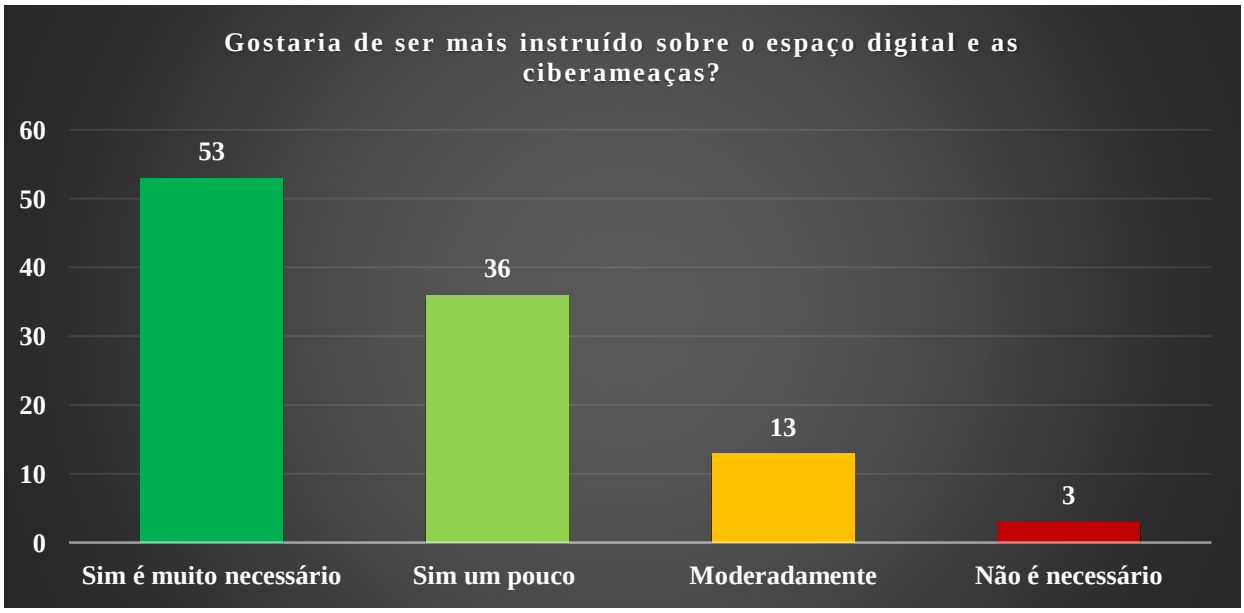
- "Estar consciente das ciberameaças é muito importante para evitar comportamentos de risco no ciberespaço";
- "Com a consciencialização, acredito que muitas situações do dia-a-dia poderiam ser evitadas, assim como alguns ciberataques teriam menos impacto";
- "Se as pessoas estiverem conscientes dos perigos da cibersegurança, estarão mais bem preparadas para utilizar o vasto mundo digital";
- "É necessário educar e consciencializar cada vez mais todos os cidadãos sobre estes assuntos";
- "Num mundo cada vez mais informatizado e em constante evolução, a consciencialização sobre os perigos da cibersegurança e os meios adequados de prevenção e combate são fundamentais para evitá-los, especialmente no que diz respeito ao cibercrime". [100]

[99] Respostas ao questionário à pergunta n.º 10 (Anexo 1)
[100] Respostas ao questionário à pergunta n.º 11 (Anexo 1)

Estas contribuições fornecidas pelos inquiridos ressaltam a importância da educação em cibersegurança como uma estratégia eficaz para prevenir e combater os cibercrimes. As respostas destacam a necessidade de consciencialização e preparação adequada das pessoas para enfrentarem os desafios do mundo digital. A educação em cibersegurança é vista como uma forma de capacitar os indivíduos a adotar comportamentos seguros, reduzir os riscos e lidar de forma adequada com as ciberameaças.

Na Figura 11, é apresentada a perceção dos participantes sobre se gostariam de receber mais formação/educação sobre a cibersegurança.

Figura 11 - Perceção dos inquiridos sobre se gostariam de ser mais instruídos sobre a cibersegurança



Fonte: Dados do questionário da pergunta n.º 12 (Anexo 1)

Sobre se gostariam de receber mais instruções sobre o espaço digital e as ciberameaças, constatamos que 96% dos inquiridos consideram que isso seria muito necessário ou necessário. Apenas três inquiridos afirmaram que não acham essa instrução necessária.[101]

Estes resultados destacam a importância da consciencialização digital e da cibereducação. Eles evidenciam que os participantes estão interessados em adquirir mais conhecimentos sobre esta temática.

[101] Respostas ao questionário à pergunta n.º 12 (Anexo 1)

Essa disposição em procurar mais informações e instrução reflete a compreensão de que a consciencialização em cibersegurança é um elemento essencial para protegerem-se efetivamente no espaço digital e reduzir os riscos das ciberameaças.[102]

A procura por mais instruções nesta área é um indicador significativo de que os indivíduos reconhecem a necessidade de estar bem informados e atualizados sobre as ameaças e os desafios enfrentados no mundo digital. Além disso, reforça a importância de fornecer educação e consciencialização sobre a cibersegurança de forma contínua para atender a essa necessidade crescente.

Em síntese, os resultados obtidos através do questionário destacam a relevância das Relações Internacionais no âmbito da cibersegurança. As respostas do questionário revelam a necessidade de cooperação entre os países para se enfrentar as ciberameaças de forma eficaz. As conclusões indicam que a troca de informações e a colaboração entre os atores internacionais são fundamentais para fortalecer a segurança digital a nível global. A promoção da cibereducação e da consciencialização em cibersegurança não se restringe apenas a um país ou a uma região, requer esforços conjuntos de diferentes nações.

Além disso, a falta de cibersegurança pode afetar as Relações Internacionais, uma vez que a confiança entre os países pode ser abalada por causa de ciberespionagem e/ou por causa de ciberataques, por exemplo. Portanto, promover a segurança digital contribui para a construção de um ambiente internacional onde a confiança mútua é fortalecida. Diante das conclusões, é evidente que a cibersegurança é uma questão que transcende as fronteiras nacionais e requer uma abordagem global. As conclusões deste estudo reforçam a necessidade de um diálogo contínuo e de uma ação conjunta entre os atores internacionais para fortalecer a segurança digital e construir um ambiente digital mais seguro e mais confiável para todos.

Os resultados do questionário reforçam a importância das Relações Internacionais no desenvolvimento de medidas e estratégias que incentivem a equidade de oportunidades para as mulheres. É fundamental destacar que a inclusão e a diversidade de género na cibersegurança também têm implicações nas Relações Internacionais.

[102] Respostas ao questionário à pergunta n.º 12 (Anexo 1)

A falta de representatividade feminina pode afetar a confiança e a cooperação entre os países. Portanto, promover a equidade de género na cibersegurança é essencial para fortalecer as Relações Internacionais e construir um ambiente de segurança digital mais inclusivo e equitativo. Para além disso, os resultados do questionário revelam um aumento na consciencialização entre os jovens, indicando uma mudança promissora de mentalidade nas gerações mais novas. Isso demonstra a importância de programas educativos e ações de consciencialização que abordem a cibersegurança de forma abrangente e contínua.

A falta de consciencialização em cibersegurança pode deixar tanto os indivíduos quanto as organizações vulneráveis a ciberameaças, e essa vulnerabilidade não conhece fronteiras. Portanto, é fundamental investir em esforços internacionais para aumentar a consciencialização e garantir que as pessoas estão preparadas com o conhecimento necessário para protegerem as suas informações e os seus sistemas digitais. A diversidade dos antecedentes dos participantes ressalta a necessidade de abordagens flexíveis e inclusivas que considerem as diferentes perspetivas e as diferentes necessidades dos indivíduos a nível global.

Outro aspeto importante é a rápida evolução das ciberameaças, o que evidencia a necessidade de consciencialização contínua em relação à cibersegurança. O avanço tecnológico e o surgimento constante de novas ameaças requerem uma abordagem proativa na educação e na consciencialização sobre os riscos digitais. Nesse contexto, as Relações Internacionais desempenham um papel crucial ao facilitar a partilha de informações permitindo que todos acompanhem os avanços tecnológicos e fortaleçam as suas capacidades de enfrentar as ciberameaças emergentes.

A escassa presença de pessoas que se consideram extremamente ciberconscientes destaca a importância de elevar o nível de consciencialização em toda a sociedade. Isso requer a colaboração entre os países para partilhar experiências e desenvolver estratégias eficazes de educação em segurança digital. Ao trabalhar em conjunto, os países podem promover uma cultura de ciberconsciência que seja abrangente e adaptada às necessidades das pessoas em diferentes contextos.

Além disso, a educação em cibersegurança é essencial para capacitar os indivíduos a protegerem-se contra as ciberameaças num mundo cada vez mais conectado. Ao fornecer uma educação abrangente, os países podem fortalecer a resiliência das pessoas e das organizações, reduzindo os riscos de ciberataques.

A pesquisa evidencia a ampla aceitação da relevância da educação como uma medida eficaz na proteção contra ciberameaças, refletindo o crescente reconhecimento de que a segurança digital é uma responsabilidade partilhada por todos os indivíduos.

Adicionalmente, as conclusões do questionário destacam a importância das Relações Internacionais na promoção da colaboração entre os governos, as empresas, as instituições educacionais e os indivíduos no combate aos cibercrimes e na construção de uma cultura de segurança digital efetiva.

Como bases nestas conclusões torna-se evidente que a cibereducação deve ser promovida em diferentes níveis, desde escolas até instituições de ensino superior, para garantir uma compreensão ampla e atualizada das ciberameaças e das medidas de proteção.

4.3. O papel da educação em cibersegurança na prevenção do cibercrime

Ao perguntar às pessoas sobre a sua opinião em relação à educação em cibersegurança e o seu impacto na prevenção e redução do cibercrime, todas expressaram a crença de que a educação em cibersegurança é fundamental para evitar que o cibercrime ocorra. No entanto, é importante ressaltar que o cibercrime, assim como qualquer outro tipo de crime, continuará a existir. É exatamente por isso que a educação em cibersegurança desempenha um papel crucial.

As respostas fornecidas na pergunta 11, evidenciam a necessidade premente da educação em cibersegurança. Um dos argumentos centrais para a importância dessa educação na prevenção e redução do cibercrime é que a chave para combater qualquer tipo de crime é a prevenção.

Em muitos casos, a confiança excessiva ou a falta de conhecimento tornam as pessoas mais vulneráveis ao cibercrime. Portanto, a consciencialização abrangente sobre o cibercrime é essencial para superar essa questão. Como mencionado por um dos inquiridos, "muitas pessoas não levam a sério as ciberameaças e ainda acreditam que o cibercrime é algo que afeta apenas os Estados e/ou empresas."[103]

Isto indica que muitas pessoas podem não estar cientes do que precisam de se proteger. Num artigo, Junger, Montoya e Overink destacaram como o conhecimento dos utilizadores da *internet* é geralmente limitado e como muitos deles desconhecem as consequências das suas ações.[104]

---

[103] Respostas ao questionário à pergunta n.º 11 (Anexo 1)

[104] Junger, M., Montoya, L., & Overink, F. (2017). *Priming and warnings are not effective to prevent social engineering attacks*. Computers in Human Behavior.

Um dos inquiridos explicou a mesma ideia, afirmando que "as pessoas simplesmente não consideram a possibilidade de terem os seus dados roubados, utilizados contra elas ou algo semelhante."[105]

Como mencionado anteriormente, um maior nível de consciencialização gera cautela e precaução, leva as pessoas a adotarem boas práticas de cibersegurança e a aprenderem a protegerem-se contra possíveis ciberameaças. É importante reconhecer que haverá sempre ciberataques em grande escala que são difíceis de prever. No entanto, é essencial que todas as pessoas sejam capazes de se protegerem contra as ciberameaças em menor escala, como o *phishing* e o *spam*, por exemplo.

As ideias apresentadas pelos inquiridos, como a implementação de uma melhor educação em cibersegurança nas escolas, nas universidades e a realização de campanhas de consciencialização abrangentes, são propostas pertinentes.[106] O ambiente digital é altamente dinâmico, e como mencionado por um dos inquiridos, "os ciberatacantes estão constantemente à procura de novas opções e frequentemente um passo à frente."[107] Os ciberataques são conduzidos por especialistas inovadores no mundo digital, com objetivos maliciosos. [108]

É importante reconhecer que nem todos os utilizadores da *internet* terão o mesmo nível de conhecimento em cibersegurança. Conforme argumentado por um dos inquiridos, "educar as pessoas de forma eficiente e adequada provavelmente só funciona em organizações onde as pessoas são constantemente confrontadas com questões de cibersegurança."[109] No entanto, um passo fundamental seria que as pessoas se educassem e se tornassem mais ciberconscientes.

Além disso, como corretamente mencionado por um dos inquiridos, "a maioria dos dados das pessoas encontram-se em sistemas de terceiros, sobre os quais não têm controlo."[110] Isto destaca a importância da consciencialização em cibersegurança como uma forma de combater o cibercrime e de preparar todas as pessoas para lidar com essas questões. Ao aumentar a consciencialização, os indivíduos estarão mais bem preparados para proteger os seus dados e enfrentarem os desafios da cibersegurança.

---

[105] Respostas ao questionário à pergunta n.º 11 (Anexo 1)
[106] Respostas ao questionário à pergunta n.º 11 (Anexo 1)
[107] Respostas ao questionário à pergunta n.º 11 (Anexo 1)
[108] Thomas Rid, B. B. (2015). *Attributing Cyber Attacks* (Vol. 38). The Journal of Strategic Studies.
[109] Respostas ao questionário à pergunta n.º 11 (Anexo 1)
[110] Respostas ao questionário à pergunta n.º 11 (Anexo 1)

Outra grande ciberameaça é o fato de que, à medida que mais pessoas se interessam pelo campo da cibersegurança, as vulnerabilidades e os novos tipos de ciberameaças estão a aumentar significativamente. Diante disso, os resultados da análise indicam a necessidade de uma maior educação e consciencialização em cibersegurança. Na medida em que, a educação e a consciencialização são elementos essenciais para reduzir e prevenir a cibercriminalidade, além de promoverem uma melhor higiene digital entre os utilizadores da *internet* e ajudar as pessoas a adotarem uma postura mais cautelosa, contribuindo assim para um ambiente digital mais seguro.

Mesmo que a consciencialização não possa impedir a ocorrência de certos cibercrimes, é melhor do que a falta de conhecimento. Além disso, a educação em cibersegurança precisa de acompanhar a natureza em constante desenvolvimento da tecnologia. Portanto, é fundamental começar o mais cedo possível, para garantir que as pessoas adquirem habilidades e conhecimentos atualizados para se protegerem no ambiente digital.

4.4. Impactos da cibercriminalidade: Experiências e consequências

Neste sub-capítulo, abordaremos as experiências vivenciadas pelos indivíduos no contexto da cibercriminalidade e as suas consequências. Com o avanço da tecnologia e a crescente dependência do ambiente digital nas nossas vidas quotidianas, o aumento dos incidentes de cibercrime tornou-se uma realidade preocupante. Através de relatos, exploraremos as diversas formas de cibercriminalidade enfrentadas pelos indivíduos, bem como os impactos emocionais, financeiros e/ou psicológicos resultantes dessas experiências.

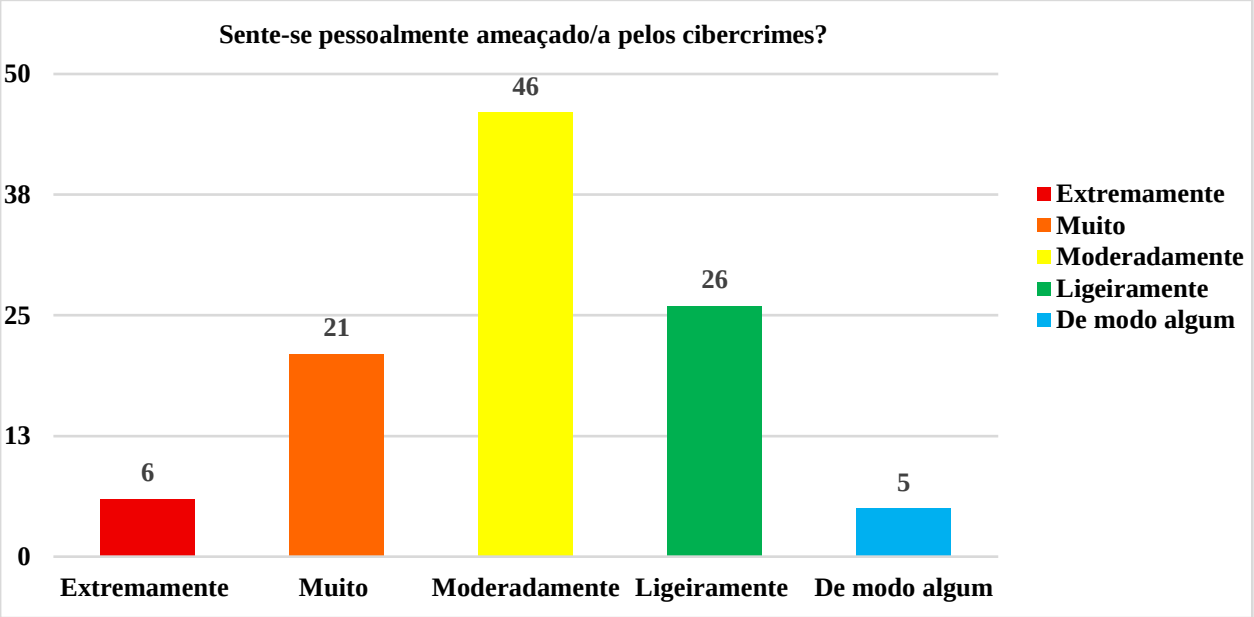
Ao analisarmos as experiências com a cibercriminalidade, podemos compreender melhor a natureza das ciberameaças que os indivíduos enfrentam e como é que elas afetam as suas vidas pessoais e/ou profissionais.

Também analisaremos as estratégias utilizadas pelos indivíduos para lidar com as consequências da cibercriminalidade, incluindo a procura por apoio, ações legais e a adoção de medidas preventivas para evitar futuros incidentes. Além disso, iremos analisar a importância da consciencialização em cibersegurança e da educação sobre os riscos associados à cibercriminalidade. Ao compreender as experiências dos indivíduos, poderemos identificar lacunas na consciencialização e na preparação em cibersegurança, bem como propor medidas e estratégias que possam ajudar a proteger e a capacitar os indivíduos contra as ciberameaças.

Através desta análise das experiências com a cibercriminalidade, procuramos contribuir para a construção de um ambiente digital mais seguro e resiliente, onde os indivíduos possam sentir-se protegidos e confiantes nas suas interações *online*.

Na Figura 12, é apresentada a perceção dos inquiridos em relação à sensação de ameaça em relação aos cibercrimes.

Figura 12 - Exposição dos inquiridos à cibercriminalidade



Fonte: Dados do questionário da pergunta n.º 13 (Anexo 1)

Os resultados indicam que os inquiridos se consideram acima da média em termos de consciencialização sobre a cibersegurança, e que não se sentem significativamente ameaçados pelo cibercrime. Cerca de 50% das pessoas relataram sentir-se moderadamente intimidadas, enquanto aproximadamente 30% sentiram uma ligeira sensação de intimidação. É interessante notar que apenas cerca de 25% dos inquiridos afirmaram sentir-se efetivamente ameaçados pelo cibercrime, o que representa uma proporção relativamente pequena.

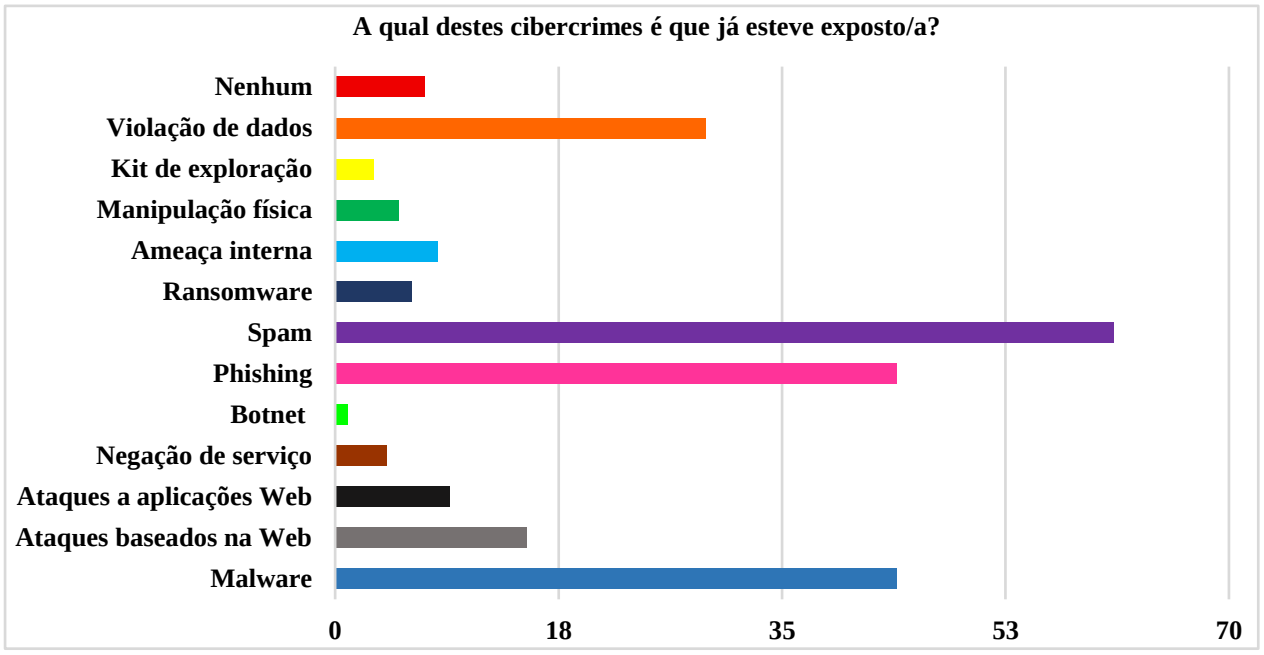
Existem duas possíveis explicações para esses resultados. Por um lado, é possível que as pessoas se considerem suficientemente ciberconscientes para reconhecer as ciberameaças e adotar medidas de proteção adequadas, o que pode contribuir para uma sensação de segurança.

Por outro lado, é possível que essas pessoas não tenham sido expostas a incidentes graves de cibercrime que as fizessem sentir-se significativamente ameaçadas. Estas descobertas ressaltam a importância da consciencialização em cibersegurança e da necessidade contínua de educar as pessoas sobre os riscos e as medidas de proteção no ambiente digital.

Embora seja positivo que uma proporção significativa dos inquiridos se considere ciberconsciente, é essencial garantir que essa consciência seja acompanhada de uma compreensão realista dos riscos e das ameaças enfrentadas no mundo digital.[111]

Na Figura 13, são apresentadas as perceções dos inquiridos em relação aos cibercrimes aos quais já estiveram expostos.

Figura 13 - Perceção sobre os cibercrimes a que os inquiridos já estiveram expostos



Fonte: Dados do questionário da pergunta n.º 14 (Anexo 1)

Esta opção permitia selecionar mais do que uma opção. Na Figura 13, é possível observar as perceções dos inquiridos em relação aos cibercrimes aos quais já estiveram expostos.

[111] Respostas ao questionário à pergunta n.º 13 (Anexo 1)

Os três cibercrimes mais comuns mencionados pelos participantes foram o *spam* (58%), o *phishing* (42%) e o *malware* (42%). Embora a maioria das pessoas tenha relatado ter sido exposta ao *spam*, essa ameaça foi considerada menos preocupante com base nas respostas do questionário.

Para muitos, o *spam* foi mais uma inconveniência do que uma ameaça real. Algumas pessoas ficaram surpresas ao descobrir que o *spam* é considerado uma ciberameaça.

Por outro lado, o *malware* foi identificado como um dos cibercrimes mais comuns e perturbadores, conforme indicado pelas respostas às perguntas 9 e 14. Houve relatos de indivíduos que tiveram de reparar os seus computadores após ataques de *malware*, reiniciar o sistema ou formatar o disco rígido, o que por sua vez, resultou na perda de dados. Alguns até mencionaram que precisaram de comprar computadores novos.

Além disso, o *malware* foi considerado por alguns inquiridos como um meio para facilitar outros cibercrimes, como violações de dados ou fugas de informações.[112] O *phishing* foi percebido como algo que a maioria dos inquiridos seria capaz de detetar, embora houvesse preocupações expressas de que os *e-mail's* de *phishing* estão a tornar-se mais sofisticados, o que dificulta a distinção entre um *e-mail* legítimo de um cliente, de um amigo ou de um ator malicioso.[113]

Algumas pessoas partilharam experiências negativas relacionadas ao *phishing*, incluindo danos nos seus computadores e até mesmo perda de dinheiro. Um inquirido relatou uma história em que recebeu um *e-mail* de *phishing* que parecia genuíno, enviado por um amigo próximo, e a mensagem era muito convincente.[114]

Uma observação relevante é que uma grande quantidade de violações de dados ocorre devido ao baixo nível de segurança dos utilizadores da *internet*, como a utilização de senhas fracas ou reutilizadas. Nesse sentido, é fundamental adotar medidas preventivas, como alterar as senhas imediatamente após uma violação de segurança. Em relação às demais ciberameaças, foi constatado que menos de 10% dos inquiridos as experimentaram.

Muitas pessoas expressaram receio em relação ao roubo de identidade, nas respostas às perguntas 15 e 16, destacaram a preocupação com os danos pessoais e com os impactos na reputação.

---

[112] Respostas ao questionário à pergunta n.º 14 (Anexo 1)
[113] Resposta ao questionário à pergunta n.º 15 (Anexo 1)
[114] Resposta ao questionário à pergunta n.º 15 (Anexo 1)

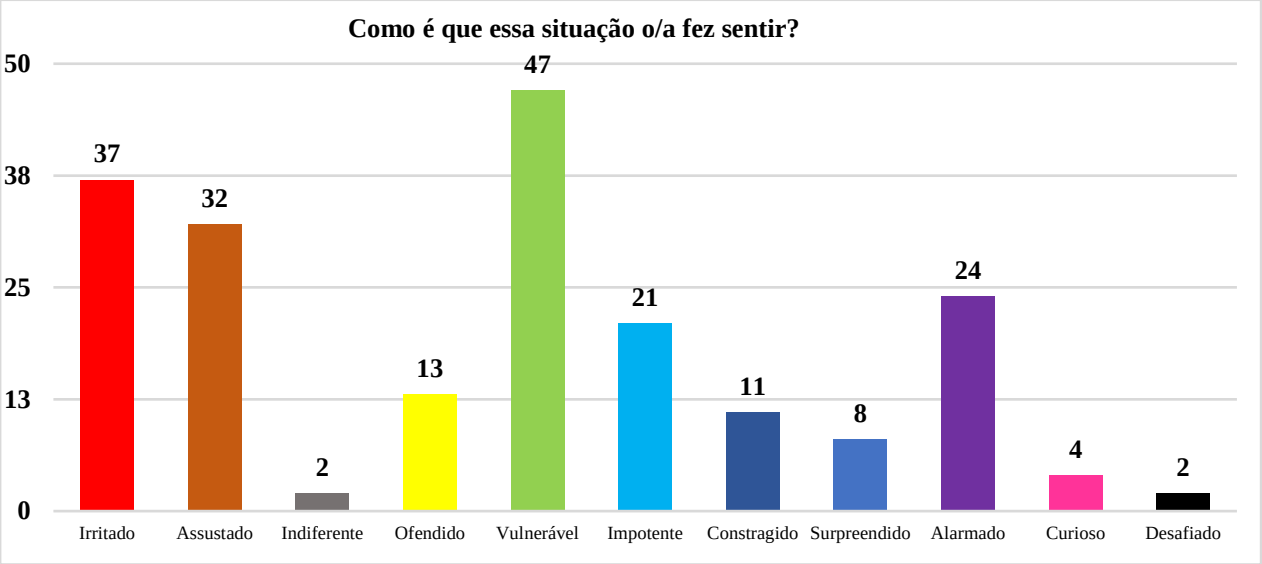
Um dos tipos de ataque mencionados foi o *ransomware*, um dos inquiridos partilhou uma história complexa, na qual todos os arquivos do seu computador foram encriptados, com mensagens a solicitar o pagamento de uma determinada quantia em criptomoedas para desbloqueá-los. Outro inquirido mencionou que na organização onde trabalha, a equipa de apoio técnico teve várias semanas a trabalhar intensamente até conseguirem desencriptar e recuperar os arquivos. [115] Os piores casos que alguns dos inquiridos tinham experimentado foi a perda de dinheiro, tendo mesmo chegado a efetuar uma queixa-crime.

Estes relatos destacam a gravidade e a complexidade das ciberameaças enfrentadas pelos inquiridos. É importante que se definam estratégias de segurança digital, com foco na prevenção e na resposta eficiente a essas ameaças, de forma a proteger os indivíduos contra danos e perdas decorrentes da cibercriminalidade.

[115] Resposta ao questionário à pergunta n.º 16 (Anexo 1)

Na Figura 14, são apresentados os sentimentos relatados pelos inquiridos em relação às suas experiências com a cibercriminalidade.

Figura 14 - Sentimentos dos inquiridos em relação à experiência de cibercriminalidade



Fonte: Dados do questionário da pergunta n.º 17 (Anexo 1)

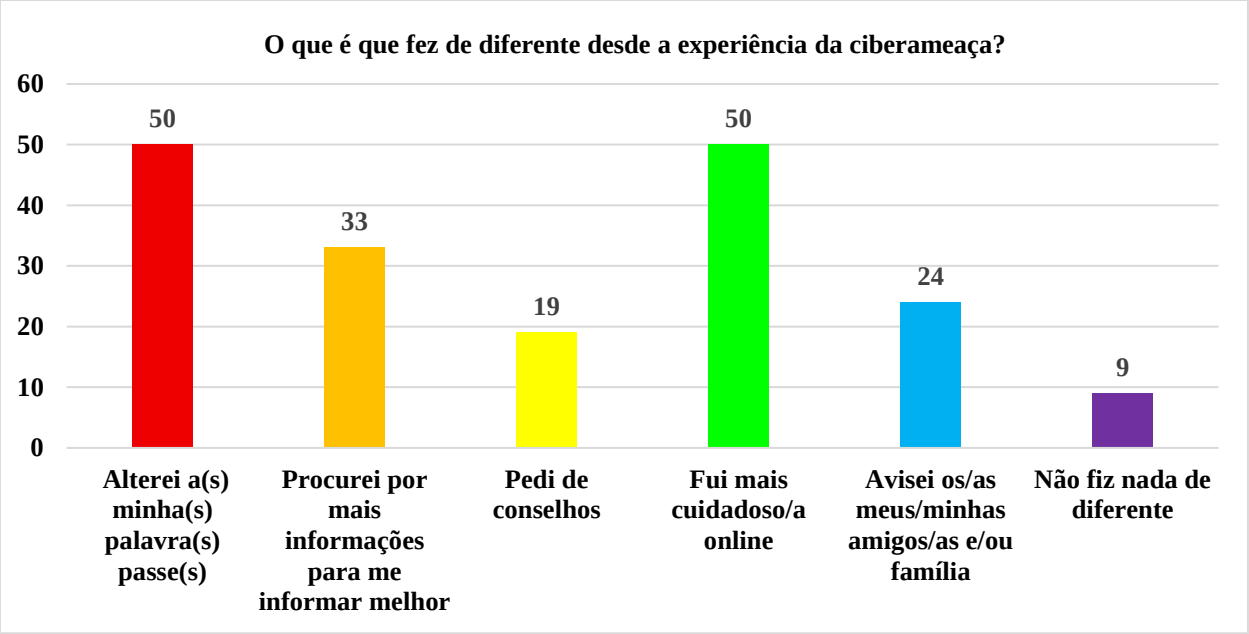
Os inquiridos tiveram a oportunidade de expressar as suas emoções em relação às ciberameaças que experimentaram, conforme apresentado na Figura 14. Classificaram as suas emoções com base nas suas experiências, e as principais emoções relatadas foram vulnerável, irritado e assustado. Estes resultados são esperados, dado o contexto em que vivemos atualmente, onde a segurança digital é uma preocupação constante. A emoção mais comum, a vulnerabilidade, faz todo o sentido, uma vez que as pessoas reconhecem a exposição e os riscos associados às ciberameaças.

Além disso, o sentimento de encorajamento pode indicar que os inquiridos estão interessados e motivados a aprender mais sobre a cibersegurança. O sentimento de constrangimento é compreensível, especialmente em relação a violações de dados e roubos de identidade, uma vez que, essas situações envolvem a possibilidade de divulgação de informações pessoais sensíveis. O constrangimento está diretamente relacionado à perturbação da segurança pessoal. As emoções de irritação, de medo e de alarme foram bastante prevalentes, o que indica que as ciberameaças geram uma grande preocupação e ansiedade entre as pessoas.

O sentimento de ofensa e de impotência também foi representado de forma significativa. Estas emoções refletem a natureza intrusiva e ameaçadora das ciberameaças e ressaltam a importância da consciencialização e de educar as pessoas sobre os riscos informáticos e as medidas de proteção adequadas.[116]

Na Figura 15, são apresentadas as medidas adotadas pelos inquiridos após terem vivenciado experiências com ciberameaças.

Figura 15 - Perceção dos inquiridos das medidas que adotaram após terem tido experiências com ciberameaças



Fonte: Dados do questionário da pergunta n.º 18 (Anexo 1)

A análise dos resultados revelou que a maioria dos inquiridos adotou medidas proativas após terem sido vítimas de ciberameaças. Um dos principais comportamentos adotados foi o aumento da cautela, com as pessoas a serem mais cuidadosas, ao não abrirem arquivos suspeitos e ao aumentarem os filtros de *spam*.

[116] Respostas ao questionário à pergunta n.º 17 (Anexo 1)

Essa mudança de comportamento reflete o reconhecimento de que as próprias ações podem ser fonte de vulnerabilidades e destaca a importância da educação em cibersegurança. Além disso, a maioria dos inquiridos relatou ter alterado as suas senhas como medida de proteção adicional. Essa ação demonstra a importância da consciencialização sobre senhas fortes e únicas na prevenção de acessos não autorizados.

Cerca de 30% dos inquiridos procuraram mais informações sobre a segurança digital ou partilharam conhecimentos com amigos e familiares. Essa iniciativa reflete a vontade de se envolverem ativamente na disseminação da consciencialização sobre a cibersegurança, contribuindo para uma cultura coletiva de proteção.

É importante destacar que apenas 8% dos participantes afirmaram não ter adotado nenhuma medida após serem vítimas de cibercrime. Embora seja uma percentagem pequena, é fundamental reconhecer que a falta de ação individual pode ter impacto na segurança coletiva.

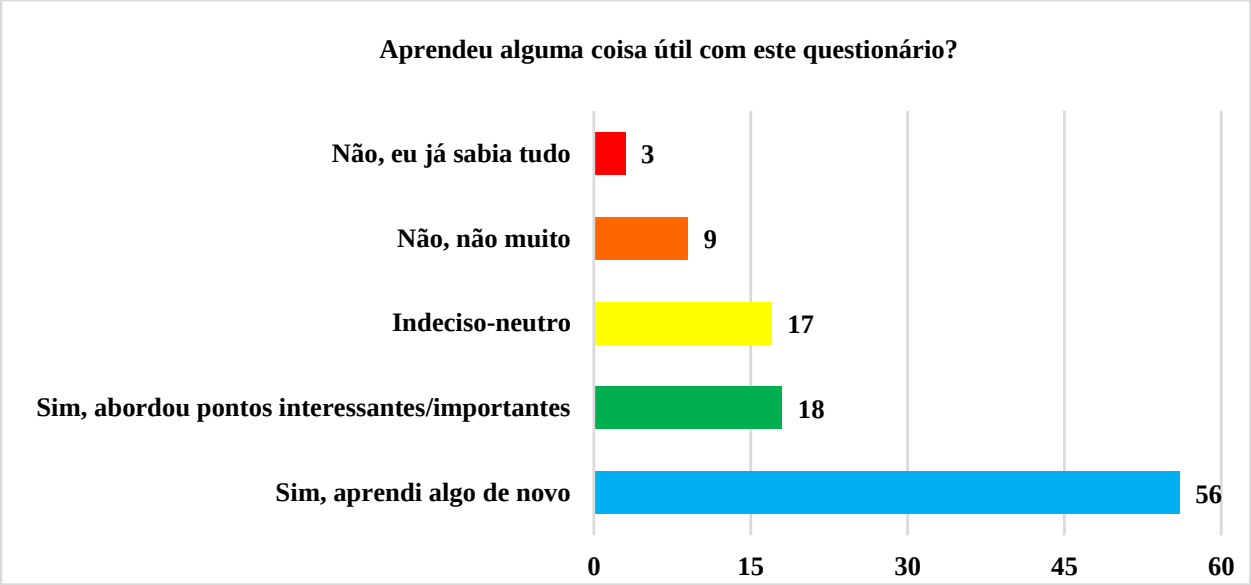
Outras ideias mencionadas pelos inquiridos incluíram a utilização de melhores *softwares*, antivírus, serviços de armazenamento em nuvem, discos rígidos externos e a adoção da autenticação de multifator. Essas medidas refletem a procura por soluções tecnológicas mais avançadas e adicionais para fortalecer a proteção contra as ciberameaças.

As respostas à pergunta 16 demonstram a vontade dos inquiridos em aprender, adaptar-se e utilizar recursos tecnológicos mais seguros. Essas ações individuais contribuem para a construção de uma postura mais resiliente diante das ciberameaças.[117]

[117] Respostas ao questionário à pergunta n.º 16 (Anexo 1)

Na Figura 16, são apresentadas as perceções dos inquiridos sobre a utilidade do questionário em termos de aprendizagem.

Figura 16 - Perceção sobre se os inquiridos consideram que aprenderam algo de útil com este questionário



Fonte: Dados do questionário da pergunta n.º 19 (Anexo 1)

Os resultados revelam que aproximadamente 70% dos inquiridos reconheceram que o questionário foi útil, uma vez que, proporcionou novos conhecimentos ou abordou tópicos relevantes e interessantes. Essa alta percentagem reflete a relevância e a contribuição do questionário para o enriquecimento do conhecimento dos participantes nesta investigação.

Por outro lado, cerca de 16% dos inquiridos manifestaram uma posição neutra ou indecisa em relação à utilidade do questionário, expressaram incerteza sobre o valor da aprendizagem. É importante destacar que a neutralidade pode ser resultado de diferentes fatores, como a familiaridade prévia com o tema abordado ou a falta de clareza sobre a aplicação prática dos conhecimentos adquiridos.

Uma pequena percentagem de apenas 8% dos inquiridos afirmou que o questionário não foi útil para a sua aprendizagem. É relevante considerar as razões subjacentes a essa perceção, como possíveis limitações do questionário em atender às expectativas dos participantes ou à necessidade de abordar de forma mais abrangente certos tópicos relacionados com a cibersegurança.

Apenas 2% dos inquiridos afirmaram que já possuíam um conhecimento abrangente sobre os temas abordados no questionário, indicaram que não consideraram a experiência de aprendizagem como significativa. Essa pequena percentagem pode ser atribuída a um grupo de participantes com um conhecimento prévio mais aprofundado na área de cibersegurança.

Em síntese, os resultados da Figura 16 demonstram que a grande maioria dos inquiridos reconheceu a utilidade do questionário como uma ferramenta de aprendizagem, seja através da aquisição de novos conhecimentos ou da exploração de pontos relevantes e interessantes. Estes resultados apoiam a eficácia do questionário na promoção da consciencialização em cibersegurança, assim como reforçam a importância da educação e do desenvolvimento contínuo nesta área.[118]

Os dados obtidos através do questionário revelaram várias informações importantes. É essencial reduzir as disparidades de género e promover mais equidade na área da cibersegurança. A diversidade de antecedentes dos inquiridos destaca a necessidade de abordagens flexíveis e inclusivas para garantir a proteção digital de todos.

A crescente consciencialização entre os jovens sobre a importância da cibersegurança é um desenvolvimento encorajador. Para além disso, à medida que a tecnologia avança e as ameaças multiplicam-se e sofisticam-se, a educação em cibersegurança desempenha um papel fundamental na proteção contra as ciberameaças. É imperativo que os indivíduos estejam cientes das ciberameaças existentes e adotem medidas proativas para reduzir a sua exposição a ciberataques e para protegerem as suas informações pessoais e profissionais. A segurança digital é uma responsabilidade partilhada por todos. Outro dado muito interessante, é que todos os participantes do questionário concordaram que mais educação em cibersegurança contribuiria para evitar ou reduzir a ocorrência de cibercrimes.

No entanto, é importante observar que o aumento do interesse pela cibersegurança também resulta no aumento de vulnerabilidades e no aumento de novos tipos de ciberameaças. Embora o nível de conhecimento das ciberameaças seja relativamente alto entre os inquiridos, há a necessidade de expandir a consciencialização sobre as ciberameaças menos difundidas.

[118] Resposta ao questionário à pergunta n.º 18 (Anexo 1)

A colaboração entre os governos, as empresas, as instituições educacionais e os indivíduos é fundamental para promover uma cultura de segurança digital e enfrentar os desafios do cibercrime. É um esforço coletivo que requer a participação ativa de todos os membros da sociedade.

Em síntese, as ciberameaças representam uma ameaça real à segurança humana. A educação em cibersegurança e a consciencialização sobre as ciberameaças são fundamentais para proteger a sociedade como um todo.

É necessário continuar a investir em educação, consciencialização e medidas de proteção para garantir um ambiente digital mais seguro e mais protegido para todos.

4.5. As perturbações da cibercriminalidade na segurança humana

A cibercriminalidade representa uma ameaça significativa à segurança humana na nossa era digital. Ao analisar esse fenómeno, as suas implicações nas Relações Internacionais são importantes. Há que ter em conta duas dimensões cruciais da cibercriminalidade relacionadas à segurança humana: o caráter pessoal ou não pessoal dos ciberataques e a possibilidade de evitar tornar-se vítima.

Além disso, foram exploradas as informações fornecidas pelo *Relatório das Ciberameaças* da ENISA, comparando-as com os dados obtidos através dos questionários que foram aplicados aos inquiridos.

No âmbito da segurança humana, os ciberataques menos graves são aqueles que não possuem um caráter pessoal e podem ser potencialmente evitados pelas pessoas. Entre esses ataques, destacam-se o *spam*, o *phishing* e as violações de dados.

Conforme evidenciado pelos resultados do questionário *online* (Figura 13), esses três tipos de cibercrime estão entre os mais comuns relatados pelos participantes. O *spam* e o *phishing* são ameaças frequentes à segurança humana que as pessoas enfrentam através do correio eletrónico. No entanto, nenhum dano real é causado até que anexos maliciosos sejam abertos, *websites* suspeitos sejam acedidos ou instruções maliciosas sejam seguidas.

Embora muitos participantes do questionário relatem não terem caído em golpes de *phishing*, existe uma preocupação crescente com a constante melhoria na qualidade dos *e-mail's* de *phishing*. Alguns participantes mencionaram experiências prejudiciais anteriores, o que por sua vez, destaca a necessidade de uma maior vigilância.

Por outro lado, as violações de dados representam uma ameaça mais grave à segurança humana, pois são menos evitáveis. Embora as pessoas possam adotar melhores práticas de cibersegurança para preveni-las, as grandes plataformas *web* também enfrentam falhas de segurança que resultam em violações de dados em larga escala. Nesses casos, nem sempre é possível proteger totalmente. De acordo com os relatos de alguns participantes, as violações de dados têm consequências graves, como perdas de informações ou de dinheiro.

Um participante expressou a dificuldade em identificar essas violações antes que causem danos significativos, tendo evidenciado a gravidade desse tipo de cibercrime.[119] Há diversos tipos de ciberataques, como *botnets*, ataques a aplicações *web* e ataques de negação de serviço (DoS), como evidenciado *pelo Relatório sobre Ciberameaças* da ENISA. Embora esses ataques atuem de maneira ampla e impessoal, eles figuram no topo das classificações, apresentam um baixo nível de personalização e previsibilidade. De facto, aproximadamente metade das ciberameaças identificadas enquadram-se nesse grupo, de acordo com os resultados obtidos no questionário.

Ao analisar a relação entre a cibercriminalidade e as dimensões da segurança humana, é possível identificar os impactos negativos causados por esses ataques. Um aspeto perturbador é o facto de os dispositivos pessoais infetados poderem-se tornar, inadvertidamente, ciberatacantes, propagando *malware* e causar danos nas redes sociais dos proprietários.

Essa realidade tem consequências tanto para os atacantes quanto para as vítimas, abalando a segurança humana de ambos os lados do ciberataque.[120] Os resgates, a ciberespionagem e as ameaças internas são exemplos de ciberameaças que frequentemente afetam o ambiente de trabalho das pessoas.

Essas perturbações não podem ser facilmente previstas por indivíduos, por esse motivo tornam-se uma ameaça significativa à segurança humana. Com base nos comentários dos inquiridos às perguntas 15 e 16, os resgates são percebidos como altamente perturbadores, podem causar danos tanto psicológicos quanto físicos. As ameaças internas são particularmente difíceis de combater, uma vez que a sua prevenção depende da consciencialização de todos os utilizadores da rede.[121]

---

[119] Resposta ao questionário à pergunta n.º 20 (Anexo 1)
[120] ENISA. (2017). *ENISA Threat Landscape Report 2016*. Obtido de The European Union Agency for Cybersecurity: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016
[121] ENISA. (2017). *ENISA Threat Landscape Report 2016*. Obtido de The European Union Agency for Cybersecurity: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

Um inquirido relatou ser vítima de ciberespionagem no trabalho e mencionou que "os colaboradores foram aconselhados a ter muito cuidado."[122] Nesse contexto, a cooperação internacional desempenha um papel fundamental na troca de informações e boas práticas para a prevenção e resposta a ameaças internas.

Os *kits* de exploração e ataques baseados na *web* são serviços que entregam *malware* a dispositivos através de *sites* comprometidos. Esses ataques frequentemente ocorrem em *sites* suspeitos e podem ser evitados através de boas práticas de segurança da informação. A transmissão ilegal de filmes em *sites* não confiáveis ou a instalação de *software* de fontes maliciosas desconhecidas torna os indivíduos alvos fáceis para os ciberatacantes.[123]

Quanto mais personalizado é um ataque, maiores são os danos causados à segurança humana. Os ataques personalizados representam potenciais violações graves da segurança humana, uma vez que são direcionados a indivíduos, que muitas vezes têm dificuldades em se protegerem contra eles. Embora ataques personalizados não sejam tão comuns, há dois exemplos de cibercrimes que se destacam: o *malware* e a fuga de informação.

Embora esses ataques sejam geralmente considerados não personalizados, esta dissertação aborda-os como personalizados pelas seguintes razões: há várias formas de disseminar *malware*, como *botnets*, *phishing* e *kits* de exploração.

Além disso, para que o *malware* seja instalado com sucesso no dispositivo do alvo, os ciberatacantes procuram variações de *malware* que sejam adequadas aos dispositivos em questão.[124]

O *malware* é uma ameaça comum e nociva que afeta pessoas e organizações em todo o mundo. Através da troca de informações, da colaboração internacional e da coordenação entre os países, é possível fortalecer as defesas contra o *malware* e proteger a segurança humana no ambiente digital. A formação e a consciencialização dos utilizadores são fundamentais para reduzir as infeções por *malware*.

---

[122] Resposta ao questionário à pergunta n.º 16 (Anexo 1)
[123] ENISA. (2017). *ENISA Threat Landscape Report 2016*. Obtido de The European Union Agency for Cybersecurity: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016
[124] ENISA. (2017). *ENISA Threat Landscape Report 2016*. Obtido de The European Union Agency for Cybersecurity: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

Nesse sentido, a cooperação internacional desempenha um papel crucial ao permitir a partilha de boas práticas de cibersegurança e de recursos educacionais. Isso possibilita a disseminação de conhecimentos e capacidades para uma utilização segura da tecnologia em todos os países, contribuindo assim para fortalecer a segurança digital global. Além disso, a cooperação internacional é essencial para combater os responsáveis pelo desenvolvimento e disseminação de *malware*. Os países devem trabalhar em conjunto para identificar, investigar e responsabilizar os perpetradores desses cibercrimes. Isso contribui para dissuadir futuros ataques e fortalecer a cibersegurança.[125]

Adicionalmente, as fugas de informação têm um impacto negativo considerável nas empresas, nas comunidades e nas plataformas, expondo dados sensíveis das pessoas e gerando preocupações sobre os danos à reputação. A falta de conhecimento sobre os *hackers* responsáveis e o uso indevido das informações roubadas foram destacados pelos inquiridos como aspetos graves e com impacto negativo.[126] O roubo de identidade, que é uma consequência das fugas de informação, é particularmente preocupante, podendo resultar em perdas financeiras significativas e danos à reputação dos indivíduos. A cooperação internacional é fundamental para o desenvolvimento de medidas e estratégias que visem proteger os dados pessoais e fortalecer a segurança digital. Os países devem trabalhar em conjunto para estabelecer padrões comuns de proteção de dados e promover a responsabilização dos responsáveis por violações de segurança.[127]

4.6. A importância da consciencialização em cibersegurança para a segurança humana

Independentemente de as ameaças serem pessoais ou não pessoais, muitas vezes há um certo nível de prevenção possível para as perturbações na segurança humana no espaço digital. No entanto, a principal questão reside na falta de compreensão da gravidade dos ciberataques por parte das pessoas. Muitos indivíduos só adotam práticas de cibersegurança adequadas depois de terem sido expostos a um cibercrime, por exemplo a mudança regular de senhas, senhas seguras, a utilização da autenticação por multifator, atualizações de *software* e outras medidas de proteção.[128]

---

[125] ENISA. (2017). *ENISA Threat Landscape Report 2016*. Obtido de The European Union Agency for Cybersecurity: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016
[126] Resposta ao questionário à pergunta n.º 15 (Anexo 1)
[127] ENISA. (2017). *ENISA Threat Landscape Report 2016*. Obtido de The European Union Agency for Cybersecurity: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016
[128] Resposta ao questionário à pergunta n.º 20 (Anexo 1)

Ao perguntar aos inquiridos se sentiam-se ameaçados pelo cibercrime, constatou-se que a maioria (80%) sentiam-se apenas moderadamente ou ligeiramente ameaçados. Esse resultado é surpreendente, tendo em consideração que uma quantidade semelhante de pessoas indicou ter uma consciencialização acima da média. Isso sugere que, embora as pessoas acreditem compreender as questões de segurança humana no ambiente digital, não estão tão comprometidas quando se trata das suas próprias práticas.

Um dos inquiridos destacou que estar consciente das ameaças não significa compreender plenamente os possíveis resultados do cibercrime. [129] Isso ressalta a importância de educar as pessoas sobre os riscos e as consequências reais da cibercriminalidade. Os resultados da análise do questionário revelaram dois pontos importantes: a utilidade do questionário para aprender sobre novas ciberameaças e despertar o interesse, e a compreensão da importância da educação em cibersegurança, com 70% dos inquiridos considerando-a importante ou mesmo muito importante.[130]

Ao tornarmo-nos mais instruídos sobre a cibersegurança contribuímos para a consciencialização das pessoas, isto resulta numa segurança humana mais robusta. A educação em cibersegurança pode prevenir o cibercrime através da adoção de práticas adequadas de ciberhigiene. Embora a prevenção do cibercrime não seja capaz de eliminar todas as ciberameaças, a educação em cibersegurança é fundamental para criar um ambiente digital mais seguro.

Os resultados do questionário apoiam a ideia de implementar a educação em cibersegurança desde cedo e em diversos setores, como uma estratégia efetiva para fortalecer a segurança humana.

[129] Resposta ao questionário à pergunta n.º 19 (Anexo 1)
[130] Resposta ao questionário à pergunta n.º 15 (Anexo 1)

5. Conclusões

O capítulo final desta dissertação traz as conclusões alcançadas sobre as "*Ameaças Cibernéticas e os seus impactos na Segurança Humana*", com foco na cibersegurança, nas dimensões abrangentes da segurança humana e nas Relações Internacionais.

Nesta era em que a tecnologia avança rapidamente e torna-se cada vez mais presente nas nossas vidas, os riscos digitais também têm vindo a intensificar-se. Ficou evidente que confiar exclusivamente em soluções tecnológicas não é suficiente para proteger a segurança humana.

A falta de conhecimento e de preparação adequada aumenta a vulnerabilidade das pessoas e das organizações diante das ciberameaças, o que por sua vez, pode resultar em danos financeiros, em perda de privacidade e até mesmo impactos físicos e psicológicos.

Para enfrentar esses desafios de forma eficaz, é essencial promover uma cultura de consciencialização em cibersegurança. A capacitação das pessoas e a disseminação de boas práticas nesta área desempenham um papel fundamental na construção da resiliência digital das organizações e na proteção da segurança humana no mundo digital. Isto incluí a adoção de medidas preventivas, como a utilização de senhas fortes, a atualização de *software,* a autenticação de dois fatores e a constante vigilância contra possíveis ciberataques.

No contexto específico de Portugal, identificámos a necessidade de um investimento contínuo em medidas preventivas e na promoção da consciencialização em cibersegurança. Essas iniciativas devem envolver tanto o setor público quanto o privado, e requerem estratégias de segurança da informação que incorporem a participação ativa das pessoas.

Além disso, reconhecemos a importância das Relações Internacionais na procura por soluções eficazes para os desafios globais da cibercriminalidade. A cooperação entre os países, a partilha de informações e a adoção de estratégias conjuntas são elementos-chave para enfrentar as ciberameaças em constante evolução.

As conclusões desta dissertação destacam a importância de uma abordagem holística, que considere tanto os aspetos técnicos quanto o fator humano na proteção contra as ciberameaças. A tecnologia evoluí de forma contínua, e a nossa compreensão das vulnerabilidades e ameaças deve acompanhar esse processo.

Concluindo, esta dissertação alcançou todos os objetivos propostos, oferecendo uma visão panorâmica e profunda das ciberameaças e dos seus impactos na segurança humana.

Devemos reconhecer o poder que temos nas mãos para proteger os nossos dados, a nossa privacidade, assim como a nossa segurança física e emocional no mundo digital. Cada um de nós pode tornar-se num defensor da cibersegurança, capacitando-se e partilhando esse conhecimento com aqueles que estão ao nosso redor.

O futuro da cibersegurança está nas mãos de todos nós. Podemos moldá-lo, fortalecendo as nossas defesas, adaptando-nos às mudanças tecnológicas e aprendendo com os desafios que encontramos. Cada obstáculo é uma oportunidade para crescer, inovar e avançar. Com resiliência e determinação, podemos construir uma sociedade mais segura, mais confiante e mais preparada para enfrentar as ciberameaças do século XXI.

5.1. O conceito de segurança humana relacionado com o espaço digital

Este sub-capítulo aborda o conceito de segurança humana no espaço digital. É essencial adotar-se medidas de proteção no ambiente digital, equiparando-as às adotadas no mundo físico, a fim de garantir a segurança das pessoas. No entanto, a falta de tangibilidade e a perceção das ameaças não físicas muitas vezes levam ao subestimar da importância da segurança digital.

O espaço digital é caracterizado pela ausência de fronteiras e pela acessibilidade universal, o que gera preocupações, como o anonimato excessivo, as dificuldades de atribuição e a falta de consciencialização sobre a cibersegurança entre o público em geral. Neste contexto, o questionário foi desenvolvido para explorar as perceções das pessoas em relação à sua segurança pessoal no espaço digital, identificar possíveis lacunas na consciencialização sobre a cibersegurança e avaliar a importância atribuída à proteção dos indivíduos nesse ambiente. A análise das respostas obtidas permitiu identificar as preocupações e os desafios enfrentados pelas pessoas em relação à cibersegurança, destacando a necessidade de consciencialização e ações efetivas para enfrentar essas ameaças.

Esta pesquisa desempenhou um papel fundamental ao investigar a dimensão da segurança humana no espaço digital, ampliando o escopo da discussão sobre a cibersegurança além das preocupações estatais. A abordagem do conceito de segurança humana em relação ao ambiente digital e as suas ameaças foi benéfica, proporcionando uma perspetiva inovadora. Embora a aplicação desse conceito tenha apresentado desafios, devido à falta de uma definição clara e estruturada para o contexto digital, permitiu uma compreensão mais ampla das implicações da cibersegurança para os indivíduos e para a sociedade.

Isso destaca a importância de proteger não apenas os sistemas e as infraestruturas digitais, mas também as pessoas que os utilizam. A ciberhigiene desempenha um papel crucial na prevenção do cibercrime, envolvendo a adoção de práticas seguras e conscientes para evitar ameaças digitais, como o *spam*, o *phishing* e as violações de dados. No entanto, é fundamental reconhecer que algumas ameaças são mais evitáveis do que outras, exigindo consciencialização e educação adequadas. Os resultados desta pesquisa são úteis para pesquisadores no campo da cibersegurança e da segurança humana, explorando as conexões entre essas áreas que ainda não foram completamente estudadas. Além disso, podem ser aplicados em debates estratégicos, especialmente no planeamento de programas de educação em cibersegurança.

Com base nas descobertas, é possível direcionar esforços para aprimorar a consciencialização das pessoas, promover a adoção de práticas seguras e desenvolver estratégias eficazes de proteção no espaço digital. É importante ressaltar que os resultados do questionário são aplicáveis apenas à amostra da população que respondeu, composta por 106 pessoas. Para uma compreensão mais abrangente, é recomendado realizar pesquisas futuras que envolvam diferentes grupos etários, áreas geográficas e identidades nacionais específicas. Embora o objetivo desta pesquisa não tenha sido generalizar os resultados para a população mundial, o estudo procurou obter uma visão horizontal das perturbações da segurança humana no espaço digital e uma compreensão da opinião pública de pessoas de diversas origens. Essa abordagem inovadora amplia o escopo da pesquisa académica e oferece perspetivas valiosas sobre a consciencialização das pessoas, sobre as suas experiências e lacunas em relação à segurança humana e ao ambiente digital.

Os resultados desta pesquisa têm relevância tanto para pesquisadores no campo da cibersegurança e da segurança humana quanto para os formuladores de estratégias. As descobertas podem ser utilizadas para criar ações estratégicas e políticas relacionadas com a educação em cibersegurança. É fundamental fortalecer a consciencialização das pessoas e promover a implementação de medidas de proteção no espaço digital, garantindo assim a segurança e o bem-estar das pessoas no mundo digital em constante evolução.

5.2. A necessidade de educação em cibersegurança

Este sub-capítulo da dissertação aborda a necessidade da educação em cibersegurança. O objetivo é promover um ambiente ciberseguro, tanto no âmbito individual quanto coletivo, através de uma ciberhigiene melhor entre todos os cidadãos.

Ao longo desta dissertação, foi ressaltada a necessidade de se aprimorar o conhecimento em cibersegurança. Apenas 2% dos inquiridos acreditam saber tudo sobre as ciberameaças, enquanto 96% expressaram que gostariam de obter mais conhecimentos sobre o espaço digital.[131] Mesmo aqueles que se consideram muito bem informados reconhecem a natureza em constante evolução do espaço digital e entendem que nunca se pode ter conhecimento demais, há sempre algo novo a aprender.[132]

Muitos inquiridos manifestaram o desconhecimento em relação às ciberameaças mencionadas, ressaltando a importância de priorizar a educação em cibersegurança, de forma a estarem conscientes dos perigos e a manterem-se constantemente atualizados. [133] Uma forma de prevenção contra novas vulnerabilidades é praticar uma ciberhigiene mais adequada. Medidas como a utilização de *software*, antivírus, a utilização de senhas mais fortes e a autenticação de multifator são algumas das recomendações da ENISA.[134] Um dos inquiridos destacou, na pergunta 15 do questionário, que "a consciencialização sobre as ciberameaças e a adoção de medidas de proteção devem receber atenção sistemática."[135]

Com base nisso, partilharemos três dos resultados mais relevantes entre os inquiridos, com o objetivo de promover uma ampla implementação da educação em cibersegurança no mundo atual, com o intuito de prevenir a ocorrência de cibercrimes.

---

[131] Respostas ao questionário à pergunta n.º 15 (Anexo 1)
[132] Respostas ao questionário à pergunta n.º 15 (Anexo 1)
[133] Respostas ao questionário à pergunta n.º 20 (Anexo 1)
[134] ENISA. (2017). *Cyber Hygiene.* Obtido de The European Union Agency for Cybersecurity: https://www.enisa.europa.eu/publications/cyber-hygiene
[135] Respostas ao questionário à pergunta n.º 20 (Anexo 1)

1. É fundamental iniciar a educação em cibersegurança desde cedo, conforme foi reforçado pelos inquiridos. Eles acreditam que a literacia digital deve começar na infância. Além disso, é importante que as pessoas tenham conhecimentos básicos para compreender a importância da cibereducação e para se protegerem.[136]

2. É necessário fornecer formação e realizar exercícios práticos, tendo em conta a atualidade e o aumento das ciberameaças. Os inquiridos destacaram a importância de sessões de formação e de exercícios práticos, que permitiriam às pessoas reconhecerem diversas ciberameaças e entenderem melhor os seus impactos.[137]

3. A implementação de campanhas de consciencialização em cibersegurança é uma sugestão pertinente na atualidade, uma vez que tais campanhas frequentemente visam sensibilizar os cidadãos para questões específicas. A educação resultante dessas campanhas contribuiria para um maior cuidado e, consequentemente, para a redução da cibercriminalidade.[138]

Para alcançarmos um planeamento eficaz da cibereducação e estabelecermos boas práticas de segurança da informação, é fundamental realizarmos uma pesquisa aprofundada, com a finalidade de obter uma compreensão equilibrada deste tema crucial. Estamos convictos da necessidade imperativa de uma educação avançada em cibersegurança para todas as idades. Essa abordagem capacitaria indivíduos a aprimorarem a sua ciberhigiene e a assegurarem a proteção das suas vidas digitais. O mundo digital está em constante evolução, e é o nosso dever abraçar o desafio de nos mantermos atualizados e de adotarmos medidas preventivas. Através da educação em cibersegurança, podemos fortalecer a nossa resiliência, empoderar-nos e proteger as nossas identidades, as nossas informações e as nossas conexões *online*.

Não podemos subestimar o poder transformador da educação e da consciencialização. Ao adotarmos uma postura proativa em relação à segurança digital, podemos construir um ambiente digital mais seguro, onde todos os indivíduos possam desfrutar dos benefícios da tecnologia sem medo ou ameaças.

---

[136] Resposta ao questionário à pergunta n.º 15 (Anexo 1)
[137] Resposta ao questionário à pergunta n.º 15 (Anexo 1)
[138] Resposta ao questionário à pergunta n.º 15 (Anexo 1)

A cibersegurança é uma jornada contínua e coletiva. Através da partilha de conhecimentos, da colaboração entre diferentes setores e da implementação de estratégias eficazes, podemos trilhar um caminho de confiança, proteção e progresso. Vamos agir agora, inspirados pela visão de um mundo digital mais seguro, e trabalhar incansavelmente para tornar esta visão uma realidade. Todos juntos, podemos construir um futuro onde a segurança digital seja um pilar fundamental, capacitando-nos a prosperar num mundo cada vez mais conectado.

5.3. A importância da literacia digital e do fator humano

Ao reconhecermos a importância da literacia digital e compreendermos o poder do fator humano, estamos a capacitar-nos para construir um futuro digital mais seguro e próspero. Cada passo que damos em direção à compreensão e aplicação dessas habilidades aproxima-nos de um mundo digital resiliente, onde podemos explorar todo o potencial da tecnologia com confiança. As nossas competências como o pensamento crítico, a comunicação eficaz e a resolução de problemas desempenham um papel crucial na defesa contra as ciberameaças. À medida que desenvolvemos uma maior auto-consciencialização e nos tornamos peritos na análise e processamento de informações, fortalecemos as nossas defesas pessoais e coletivas no ciberespaço.

O fator humano, constantemente presente e influente, é uma força imutável que deve ser entendida e valorizada. Ao reconhecermos a importância desse fator nas nossas estratégias de segurança digital, estamos a construir bases sólidas para a proteção dos Estados, das organizações e dos indivíduos em todo o mundo. Unamos forças e embarquemos juntos na jornada em direção a um ambiente digital seguro, onde a literacia digital e o fator humano complementam-se harmoniosamente. À medida que nos educamos, partilhamos conhecimentos e colaboramos à escala global, estaremos a construir um caminho sólido rumo a uma era digital de prosperidade, confiança e resiliência.

Que a dedicação à aprendizagem contínua seja o combustível para impulsionar a transformação positiva no mundo digital. Ao fortalecermos as nossas habilidades, aumentarmos a nossa consciencialização e fomentarmos a cooperação, estaremos a construir as bases para uma comunidade digital segura e confiável. Portanto, todos unidos por esta visão, avancemos com coragem, determinação e otimismo. Ao trabalharmos juntos, podemos criar um ambiente digital que promova oportunidades, conectividade e confiança para todos. O futuro digital mais seguro que procuramos está ao nosso alcance. Cabe a todos nós, seguirmos em frente e construirmos essa realidade em conjunto.

A síntese que se acha possível dos resultados mais salientes desta investigação é que as ciberameaças representam uma ameaça significativa para a segurança humana no mundo digital em constante evolução. A confiança exclusiva em soluções tecnológicas não é suficiente para proteger efetivamente as pessoas contra essas ameaças. É crucial considerar o fator humano, promovendo uma cultura de consciencialização em cibersegurança e capacitando as pessoas com conhecimentos e boas práticas de cibersegurança. Medidas preventivas, como senhas fortes e atualização de *software*, são fundamentais para enfrentar os desafios das ciberameaças. Em Portugal, é necessário um investimento contínuo em medidas preventivas e na promoção da consciencialização em cibersegurança, com a participação tanto do setor público como do setor privado. A cooperação internacional, a partilha de informações e a adoção de estratégias conjuntas são essenciais para enfrentar as ciberameaças em evolução. Destaca-se a importância de uma abordagem holística que tenha em conta os aspetos técnicos e humanos da segurança digital. Cada pessoa pode desempenhar um papel na defesa da cibersegurança, capacitando-se e partilhando conhecimento. O futuro da cibersegurança depende do fortalecimento das defesas, da adaptação às mudanças tecnológicas e da aprendizagem com os desafios encontrados.

Diante das ciberameaças e dos seus impactos na segurança humana, é imperativo adotar medidas de proteção no ambiente digital, equiparando-as às adotadas no mundo físico. A consciencialização sobre a cibersegurança é essencial, tendo em consideração as preocupações geradas pelo anonimato excessivo e pela falta de conhecimento geral sobre o assunto. A abordagem da segurança humana no espaço digital amplia a discussão sobre a cibersegurança, exigindo a proteção não apenas dos sistemas, mas também das pessoas que os utilizam.

A pesquisa realizada fornece perspetivas relevantes para pesquisadores e formuladores de estratégias, destacando a importância da ciberhigiene e da adoção de práticas seguras para prevenir o cibercrime. A educação em cibersegurança desde a infância e a promoção da literacia digital são fundamentais para garantir a segurança no mundo digital. O aprimoramento da consciencialização, a formação adequada e a atualização constante são essenciais para enfrentar o aumento das ciberameaças. Assim, é possível construir uma sociedade mais segura e protegida no mundo digital, com estratégias eficazes que garantam o bem-estar das pessoas.

À medida que o mundo avança rapidamente no século XXI, as ameaças à segurança humana assumem uma nova forma e dimensão. Neste contexto, as ciberameaças emergem como uma preocupação crítica para as Relações Internacionais, afetando profundamente os Estados, as Organizações Internacionais e as pessoas em geral.

A presente dissertação procurou explorar os impactos dessas ciberameaças na segurança humana, através de um olhar aprofundado sobre este tema crucial para a nossa era digital. Ao longo desta pesquisa, ficou evidente que as ciberameaças transcendem fronteiras nacionais, não respeitando as barreiras geográficas e políticas tradicionais. O advento da tecnologia digital trouxe consigo um potencial transformador e disruptivo, que tanto pode promover a cooperação global como criar vulnerabilidades sem precedentes. A interconexão entre os sistemas informáticos e a dependência crescente das tecnologias da informação e da comunicação geram um ambiente propício para ciberataques que podem afetar a segurança dos Estados e o bem-estar das pessoas.

Através desta dissertação, procuramos destacar a importância de uma abordagem holística e cooperativa no combate às ciberameaças. Os Estados devem reconhecer que a segurança digital é uma responsabilidade partilhada, que exige esforços coordenados e cooperação entre os governos, as Organizações Internacionais e o setor privado. Além disso, é essencial que as medidas e as estratégias de segurança humana sejam atualizadas de forma a incluírem os desafios e as consequências das ciberameaças.

A segurança humana, no contexto das ciberameaças, implica a proteção dos indivíduos e das comunidades, bem como a salvaguarda das infraestruturas críticas e dos sistemas de informação. A crescente interdependência global exige uma atenção redobrada para garantir a integridade dos processos sociais, económicos e políticos que sustentam a nossa sociedade.

É imperativo que sejamos proativos na adoção de medidas preventivas, investindo em capacidades defensivas robustas, na educação e na consciencialização sobre a cibersegurança.

Em síntese, esta dissertação destacou a necessidade urgente de uma cooperação mais estreita e uma ação decisiva para enfrentar as ciberameaças que afetam a segurança humana. As Relações Internacionais desempenham um papel fundamental na criação de um ambiente favorável à colaboração entre os Estados e as Organizações Internacionais, promovendo a partilha de informações e a implementação de estratégias abrangentes de segurança digital. Só através de um esforço conjunto é que poderemos enfrentar com sucesso os desafios emergentes no ciberespaço e garantir um futuro mais seguro e mais próspero para todos.

Espera-se que esta dissertação possa ser um contributo para debates mais aprofundados e ações efetivas, fortalecendo as bases do conhecimento em Relações Internacionais e impulsionando esforços globais para lidar com as ciberameaças de forma holística. Que possamos trilhar um caminho de segurança digital, que promova uma ordem internacional mais resiliente focada em proteger os interesses e a dignidade de todas as pessoas.

6. Bibliografia

Amoroso, E. G. (2011). *Cyber Attacks: Protecting National Infrastructure*. Burlington: Butterworth-Heinemann.

Baylis, J., Wirtz, J. J., & Johnson, J. L. (2015). *Strategy in the Contemporary World.* Oxford University Press.

Baylis, Smith, & Owens. (2011). *The Globalization of World Politics: An Introduction to International Relations.* Oxford University Press.

Beautiful, I. I. (2021). *World's Biggest Data Breaches & Hacks*. Obtido de https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Blasco, J. (2012). *Bypassing Information Leakage Protection With Trusted Applications.* Computers & Security, Elsevier.

Buchanan, B. (2016). *The Life Cycles of Cyber Threats* (Vol. 58). Routledge, part of the Taylor & Francis Group.

Buchanan, B. (2017). *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations.* New York: Oxford University Press.

Bustelo, R. V. (2019). *O Processo do Manual de Tallin e a Evolução da Estratégia de Dissuasão no Ciberespaço*. Obtido de https://comum.rcaap.pt/bitstream/10400.26/29895/3/O%20processo%20do%20Manual%20de%20Tallinn%20e%20a%20evolu%c3%a7%c3%a3o%20da%20estrat%c3%a9gia%20de%20dissuas%c3%a3o%20no%20ciberespa%c3%a7o_BUSTELO.pdf

Clarke, R. A., & Knake, R. (2011). *Cyber War: The Next Threat to National Security and What to Do About It* . Paperback.

ENISA. (2017). *Cyber Hygiene*. Obtido de The European Union Agency for Cybersecurity: https://www.enisa.europa.eu/publications/cyber-hygiene

ENISA. (2017). *ENISA Threat Landscape Report 2016*. Obtido de The European Union Agency for Cybersecurity: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

Future, R. (2016). *New Kit, Same Player: Top 10 Vulnerabilities Used by Exploit Kits in 2016.* Obtido de https://www.recordedfuture.com/top-vulnerabilities-2016

Gil, I. (2021). *A Dimensão Humana da Segurança Contemporânea.* Lisboa: Universidade Autónoma de Lisboa.

Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers.* Doubleday.

Interna, S. d. (2022). *Relatório Anual de Segurança Interna*. Obtido de https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDazMAQAhxRa3gUAAAA%3d

Junger, M., Montoya, L., & Overink, F. (2017). *Priming and warnings are not effective to prevent social engineering attacks.* Computers in Human Behavior.

Kaldor, M., Martin, M., & Selchow, S. (2007). *Human Security: A New Strategic Narrative for Europe.* Royal Institute of International Affairs.

Kello, L. (2013). *The Meaning of the Cyber Revolution: Perils to Theory and Statecraft* (Vol. 38). The MIT Press.

King, G., & Murray, C. J. (2002). *Rethinking Human Security* (Vol. 116). Political Science Quarterly.

Lewis, J. A. (2014). *National Perceptions of Cyber Threats. Strategic Analysis,* (Vol. 38). Strategic Analysis.

MacFarlane, N., & Khong, Y. F. (2006). *Human Security and the UN: A Critical History.* Bloomington: Indiana University Press.

Mouton, F., Leenen, L., & Venter, H. (2016). *Social Engineering Attack Examples, Templates and Scenarios* (Vol. 59). Computers & Security, Elsevier.

Nef, J. (1999). *Human Security and Mutual Vulnerability: The Global Political Economy of Development and Underdevelopment.* Ottawa: International Development Research Centre.

Owen, T. (2004). *Human Security – Conflict, Critique and Consensus: Colloquium Remarks and a Proposal for a Threshold-Based Definition* (Vol. 35). Sage Publications.

Paris, R. (2001). *Human Security: Paradigm Shift or Hot Air?* (Vol. 26). International Security.

Pereira, F., & Pablo, J. (2005). *Seguridad Humana.* Universidad Autónoma de Barcelona.

Rid, T. (2012). *Cyber War Will Not Take Place* (Vol. 35). Journal of Strategic Studies.

Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge University Press.

Security, U. N. (2016). *Humana Security Handbook.* New York : Human Security Unit .

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know.* New York: Oxford University Press.

Stone, J. (2013). *Cyber War Will Take Place* (Vol. 36). Journal of Strategic Studies.

Sunga, L. S. (2009). *The Concept of Human Security: Does it Add Anything of Value to International Legal Theory or Practice?* Routledge.

Thomas Rid, B. B. (2015). *Attributing Cyber Attacks* (Vol. 38). The Journal of Strategic Studies.

Tikk, E. (2011). *Ten Rules for Cyber Security* (Vol. 53). Survival.

Tikk, E., Kaska, K., & Vihul, L. (2011). *International Cyber Incidents: Legal Considerations.* Cooperative Cyber Defense Centre of Excellence.

UNDP. (1994). *Human Development Report 1994*. Obtido de United Nations Development Programme: https://hdr.undp.org/system/files/documents/hdr1994encompletenostatspdf.pdf

W, A. (2011). *Military Culture and Cyber Security* (Vol. 53). Survival.

Ware, B. (2013). *Why cyber hygiene isn't enough*. Obtido de http://www.networkworld.com/article/3086834/security/why-cyber-hygiene-isnt-enough.html

Williams, P. D. (2013). *Security Studies An Introduction.* London Routledge.

Zetter, K. (2015). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* Crown.

Zetter, K. (2017). *What Is Ransomware? A Guide to the Global Cyberattack's Scary Method*. Obtido de https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/

7. Anexos

Anexo 1. Questionário *online*

O questionário foi criado com o conceito de segurança humana em mente. O conceito foi deliberadamente omitido do questionário, com a finalidade de não confundir os participantes. As perguntas foram formuladas de forma a poderem ser utilizadas para a análise do conceito de segurança humana. A análise dos resultados procurou explorar a forma como a consciencialização em cibersegurança das pessoas e as suas experiências com o cibercrime estão relacionadas com a segurança humana. Para além disso, também foi analisado as formas como a consciencialização em cibersegurança pode influenciar a segurança e o bem-estar dos indivíduos no ambiente digital.

Questionário

O meu nome é Inês Gil e sou estudante do Mestrado de Relações Internacionais na Universidade Autónoma de Lisboa. Estou atualmente a realizar uma investigação para a dissertação de mestrado sobre as ciberameaças. Este estudo significa analisar a nocividade das ciberameaças e o nível de consciencialização em cibersegurança. As respostas ajudar-me-ão a compreender melhor qual é o nível geral de conhecimento sobre ciberameaças e exposição ao cibercrime.

Muito obrigada desde já,
Inês Gil
Estudante do Mestrado em Relações Internacionais da Universidade Autónoma de Lisboa

1. Qual é o seu género?*

- Feminino
- Masculino

2. Qual é a sua idade?*

- Menos de 18 anos
- 18 a 24 anos
- 25 a 34 anos

- 35 a 44 anos
- 45 a 54 anos
- 55 a 64 anos
- 65 ou + anos

3. Qual é a sua nacionalidade?* (Pergunta aberta)

R.:_____

4. Em que departamento/setor é que trabalha?*

- Contabilidade, banca ou finanças
- Negócios ou consultoria
- Caridade/trabalho voluntário
- Artes ou design
- Energia ou serviços públicos
- Engenharia ou fabrico
- Ambiente ou agricultura
- Cuidados de saúde
- Eventos
- Gestão
- Tecnologias da Informação e da Comunicação
- Direito
- Aplicação da lei e segurança
- Marketing, publicidade ou Relações-Públicas
- Serviços públicos ou administração
- Recursos Humanos
- Retalho
- Vendas
- Ciência ou farmácia
- Assistência Social
- Educação
- Transporte ou logística
- Outros (por favor, especificar)_____

5. O seu trabalho/estudos está de alguma forma relacionado com a cibersegurança?*

- Sim
- Não
- Em parte
- Outro (por favor, especificar)_____

6. Considera-se "ciberconsciente"? *

- Extremamente
- Muito
- Moderadamente
- Ligeiramente
- De modo algum

Conhecimento sobre as ciberameaças

As perguntas seguintes irão centrar-se no seu conhecimento sobre as ciberameaças existentes atualmente. Por favor, utilize a sua própria experiência e antecedentes, de forma a obter-se uma exatidão dos resultados.

7. Na sua opinião, o tema das ciberameaças tem exposição suficiente na atualidade?*

- Extremamente
- Muito
- Moderadamente
- Ligeiramente
- De modo algum

8. Na sua opinião, qual é o nível geral de consciencialização em cibersegurança entre as pessoas?*

- Excelente
- Acima da média
- Médio
- Abaixo da média
- Baixo
- Outros (por favor, especifica)_____

9. De qual das seguintes ciberameaças é que já ouviu falar?*

- ***Malware*** (instalação de *software* malicioso, os chamados "vírus")
- **Ataques baseados na *web*** (utilização de *websites* como superfície de ataque, por exemplo, *streaming*)
- **Ataques a aplicações *web*** (ataques contra aplicações *web* e/ou serviços *web*, aplicações móveis incluídas)
- **Ataques de negação de serviço** (*DoS*, recursos da rede intencionalmente indisponíveis para os utilizadores, por exemplo, sem acesso ao *homebanking*)
- ***Botnet*** (também são conhecidos como "computadores *zombies*", apoderam-se dos dispositivos dos utilizadores da *internet*, de maneira que os utilizadores nunca se apercebam que os seus computadores são ou fizeram parte de um *Botnet*)
- ***Phishing*** (tentativa de obter informações através de uma entidade de confiança, por exemplo, alguém a fazer passar-se por um colega)
- ***Spam*** (publicidade em massa para intenções maliciosas, por exemplo, enganar nos pagamentos)
- ***Ransomware*** ("data hostage" para que não possa mais ter acesso à informação, seria preciso pagar um resgate para obter a informação de volta)
- **Ameaça interna** (ataque intencional ou não intencional dentro de uma entidade)
- **Manipulação física** (roubo, perda e/ou dano de um dispositivo)
- ***Kit* de exploração** (identificação de vulnerabilidades de *software* de um dispositivo)

- **Violação de dados** (divulgação de informação segura ou privada/confidencial, por exemplo, palavra-passe *hackeada*)
- **Roubo de identidade** (ocorre quando os cibercriminosos obtêm a propriedade sobre as credenciais, tais como financeiras, bancárias, dados sobre a saúde, entre outros aspetos, que podem causar grandes danos à vítima)
- **Fuga de informação** (abuso de fraquezas/ erros do sistema para fuga de informação importante)
- **Ciberespionagem** (prática de obtenção de informação sem a permissão, geralmente praticada por atores estatais)
- **Outro** (por favor, especifica)_____

10. Considera que a educação em cibersegurança é importante?*

- Extremamente importante
- Importante
- Moderadamente importante
- Um pouco importante
- Não muito importante
- Não é necessária

11. Acha que se houvesse mais educação em cibersegurança isso iria contribuir para evitar/reduzir a ocorrência de ciberameaças?*

Por favor, explica (Pergunta aberta)_____

12. Gostaria de ser mais instruído/a sobre o espaço digital e as ciberameaças?*

- Sim, é muito necessário
- Sim, um pouco
- Moderadamente
- Não é necessário
- Não, eu já sei tudo
- Outros (por favor, especifica)_____

Exposição ao cibercrime

Partilhou as suas opiniões e conhecimentos sobre as ciberameaças, mas agora imagine um cenário onde uma ciberameaça transforma-se num verdadeiro cibercrime. Por favor, reflita tendo em conta as suas próprias experiências e tendo em consideração situações que pareciam suspeitas e em que um crime esteve perto de acontecer.

13. Sente-se pessoalmente ameaçado/a pelos cibercrimes?*

- Extremamente
- Muito
- Moderadamente
- Ligeiramente
- De modo algum

14. A qual destes cibercrimes é que já esteve exposto/a?*

- *Malware*
- Ataques baseados na *web*
- Ataques a aplicações *web*
- Negação de serviço
- *Botnet*
- *Phishing*
- *Spam*
- *Ransomware*
- Ameaça interna
- Manipulação física
- *Kit* de Exploração
- Violação de dados
- Roubo de identidade
- Fuga de informação
- Ciberespionagem

15. Dos cibercrimes acima mencionados a que foi exposto/a, qual é que considera que seja o pior? Por favor, dê uma explicação. (Pergunta aberta)

R.: _____

16. Quais é que foram as consequências? (Pergunta aberta)

R.: _____

17. Como é que essa situação o/a fez sentir?

- Irritado
- Assustado
- Indiferente
- Ofendido
- Vulnerável
- Impotente
- Constrangido
- Surpreendido
- Alarmado
- Curioso
- Desafiado
- Encorajado
- Interessado

18. O que é que fez de diferente desde a experiência da ciberameaça?

- Alterei a(s) minha(s) palavra(s) passe(s)
- Procurei por mais informações para me informar melhor
- Pedi de conselhos
- Fui mais cuidadoso *online*
- Avisei os meus amigos e/ou família
- Não fiz nada de diferente
- Outro (por favor, especifica)_____

Questões finais

Muito obrigada pela sua colaboração e vontade de ajudar! Aqui estão algumas perguntas finais para apoiar o desenvolvimento da investigação desta dissertação. Se conhecer outras pessoas, que possam estar interessadas em responder a este questionário, por favor, pode partilhá-lo com elas.

Muito obrigada!

Inês Gil

19. Aprendeu alguma coisa útil com este questionário?*

- Sim, aprendi algo de novo
- Sim, abordou pontos interessantes /importantes
- Indeciso/a-neutro/a
- Não, não muito
- Não, eu já sabia tudo
- Outros (por favor, especifique)_____

20. Se aprendeu, por favor, explique o que foi. (Pergunta aberta)

R.: _____

21. Tem alguma sugestão/recomendação para a investigação? (Pergunta aberta)

R.: _____

22. Se estiver interessado/a e disposto a falar comigo sobre este tema, por favor deixe o seu endereço de e-mail e/ou número de telefone, para que possa entrar em contacto. Muito obrigada, uma vez mais! (Pergunta aberta)

R.: _____

NOTA: As questões com asterisco (*) são de caráter obrigatório.