ATLÂNTICA INSTITUTO UNIVERSITÁRIO

Mestrado em Gestão de Sistemas e Tecnologias de Informação

Dissertação para obtenção do grau de Mestre em Gestão de Sistemas e Tecnologias de Informação

ANÁLISE DO CONHECIMENTO DOS UTILIZADORES SOBRE CIBERATAQUES BASEADOS EM INTELIGÊNCIA ARTIFICIAL

Elaborado por: Valdemar António Pacheco, Aluno n.º 20131810

Orientadora Académica: Dra. Carla Sofia Rocha da Silva

Barcarena, novembro 2025

Atlântica – Instituto Universitário

Mestrado em Gestão de Sistemas e Tecnologias de Informação

Dissertação para obtenção do grau de Mestre em Gestão de Sistemas e Tecnologias de Informação

ANÁLISE DO CONHECIMENTO DOS UTILIZADORES SOBRE CIBERATAQUES BASEADOS EM INTELIGÊNCIA ARTIFICIAL

Elaborado por: Valdemar António Pacheco, Aluno n.º 20131810

Orientadora Académica: Dra. Carla Sofia Rocha da Silva

Barcarena, novembro 2025

“o autor é o único responsável pelas ideias expressas neste relatório”

Análise do Conhecimento dos Utilizadores sobre Ciberataques Baseados em Inteligência Artificial
- Gestão de Sistemas e Tecnologias da Informação -

Valdemar António Pacheco – novembro 2025 - Atlântica

PENSAMENTO

"A utilização da Inteligência Artificial em ciberataques e a evolução das ameaças são preocupações constantes e críticas. A análise técnica dos riscos da Inteligência Artificial nos ciberataques é um campo crucial, visando entender as implicações dessa interseção."

- Gabriel Laroche Borba e Luís Felipe Araújo Mota, 2024.

DEDICATÓRIA

Dedico este trabalho a todos os que me acompanharam nesta dissertação, cuja orientação, apoio e inspiração foram fundamentais para a realização deste projeto. A sua sabedoria e encorajamento constante motivaram-me a superar desafios e a procurar a excelência. Estou eternamente grato pela sua presença e influência na minha jornada académica e profissional.

Valdemar António Pacheco – novembro 2025 - Atlântica

LISTA DE SIGLAS E ABREVIATURAS

ANNs: *Artificial Neural Networks*

APTs: *Advanced Persistent Threat*

CERTs: *Computer Emergency Response Team*

DDoS: *Distributed Denial of Service*

IA: Inteligência Artificial

I&D: Investigação e Desenvolvimento

IDS: *Intrusion Detection Systems*

IPS: *Intrusion Prevention Systems*

IoT: *Internet of Things*

MFA: *Multi-Factor Authentication*

ML: *Machine Learning*

NLP: *Natural Language Processing*

GLOSSÁRIO

No âmbito desta investigação, utilizam-se diversas siglas e conceitos técnicos que facilitam a leitura e compreensão do tema. Entre eles, destacam-se:

- ***ANNs (Artificial Neural Networks)****:* Redes neurais artificiais inspiradas no cérebro humano, compostas por camadas de nós que processam informação e aprendem ajustando os pesos das ligações.
- ***APTs (Advanced Persistent Threat)****:* Ataques sofisticados e persistentes, conduzidos por grupos organizados, que visam infiltrar-se em sistemas durante longos períodos sem serem detetados.
- ***CERTs (Computer Emergency Response Team)****:* Equipas especializadas na resposta a incidentes de segurança informática.
- ***DDoS (Distributed Denial of Service)****:* Ataques que sobrecarregam servidores ou redes através de múltiplas fontes, tornando serviços indisponíveis.
- **IA (Inteligência Artificial)**: Área da ciência computacional dedicada ao desenvolvimento de sistemas capazes de simular capacidades humanas.
- **I&D (Investigação e Desenvolvimento)**: Processo de criação e inovação tecnológica aplicada à Cibersegurança.
- ***IDS (Intrusion Detection Systems)****:* Sistemas que monitorizam tráfego de rede para identificar atividades suspeitas.
- ***IPS (Intrusion Prevention Systems)****:* Sistemas que bloqueiam ou mitigam ataques em tempo real.
- ***IoT (Internet of Things)****:* Rede de dispositivos inteligentes interconectados que comunicam entre si através da internet.
- ***MFA (Multi-Factor Authentication)****:* Método de autenticação que utiliza múltiplos fatores para reforçar a segurança.

- ***ML (Machine Learning)****:* Subárea da IA que permite aos sistemas aprenderem a partir de dados.
- ***NLP (Natural Language Processing)****:* Campo da IA que possibilita a interação entre computadores e linguagem humana.
- ***Phishing*** **personalizado**: Técnica de engenharia social que utiliza informações específicas sobre a vítima para criar mensagens falsas altamente convincentes.
- ***Deepfakes****:* Conteúdos multimédia manipulados com IA para parecerem autênticos, usados em desinformação ou fraude.
- ***Malware*** **adaptativo**: Software malicioso capaz de alterar o seu comportamento ou código para evitar deteção e aumentar a eficácia dos ataques.

RESUMO

A Inteligência Artificial (IA) tem vindo a transformar de forma significativa o panorama da Cibersegurança, trazendo benefícios na deteção e mitigação de ameaças, mas também potenciando novos riscos através da sua utilização em ciberataques sofisticados. Este trabalho tem como objetivo analisar o nível de conhecimento dos utilizadores sobre ciberataques baseados em IA, identificando lacunas de informação, perceções sobre a gravidade e frequência dessas ameaças e avaliando a eficácia das estratégias de consciencialização existentes. A investigação foi conduzida através de questionários online e revisão sistemática da literatura, abrangendo diferentes perfis de utilizadores, desde académicos e profissionais de tecnologia até ao público em geral. Os resultados revelaram que, embora exista alguma familiaridade com conceitos básicos de IA e Cibersegurança, persistem fragilidades significativas na compreensão dos riscos específicos associados a ataques como *phishing* avançado, *deepfakes* e *malware* adaptativo. Constatou-se ainda que a falta de educação e formação direcionada contribui para comportamentos inseguros e maior vulnerabilidade digital. Com base nestas conclusões, são propostas recomendações para programas de consciencialização e educação mais eficazes, capazes de promover uma cultura de segurança cibernética robusta e preparar os utilizadores para enfrentar as ameaças emergentes potenciadas pela Inteligência Artificial.

Palavras-chave: Inteligência Artificial, Ciberataques, Segurança Cibernética, Consciencialização, Educação.

ABSTRACT

Artificial Intelligence (AI) has been significantly transforming the cybersecurity landscape, bringing benefits in the detection and mitigation of threats, but also creating new risks through its use in sophisticated cyberattacks. This study aims to analyze the level of users' knowledge about AI-based cyberattacks, identifying information gaps, perceptions of the severity and frequency of these threats, and assessing the effectiveness of existing awareness strategies. The research was conducted through online questionnaires and a systematic literature review, covering different user profiles, from academics and technology professionals to the general public. The results revealed that, although there is some familiarity with basic concepts of AI and Cybersecurity, significant weaknesses remain in understanding the specific risks associated with attacks such as advanced phishing, deepfakes, and adaptive malware. It was also found that the lack of targeted education and training contributes to unsafe behaviors and greater digital vulnerability. Based on these conclusions, recommendations are proposed for more effective awareness and education programs, capable of promoting a robust cybersecurity culture and preparing users to face emerging threats amplified by Artificial Intelligence.

Keywords: *Artificial Intelligence, Cyberattacks, Cybersecurity, Awareness, Education.*

Índice

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

INTRODUÇÃO

1. CONTEXTUALIZAÇÃO

A estrutura da investigação sobre "Análise do Conhecimento dos Utilizadores sobre Ciberataques Baseados em Inteligência Artificial" é apresentada de acordo com os diferentes tópicos relacionados, Cibersegurança, Ciberataques e Inteligência Artificial. 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, ciberataques baseados em IA e respetivas medidas de defesa.

A rápida evolução da tecnologia tem proporcionado avanços significativos em diversas áreas, incluindo a Cibersegurança. No entanto, essa mesma evolução também trouxe novos desafios, especialmente com a integração da Inteligência Artificial (IA) em ciberataques. Ciberataques baseados em IA utilizam técnicas avançadas para automatizar e aprimorar as suas operações, tornando-se cada vez mais sofisticados e difíceis de detetar (Laroche Borba & Araújo Mota, 2024).

Este trabalho tem como objetivo analisar o nível de conhecimento dos utilizadores sobre ciberataques que utilizam IA. A escolha deste tema é justificada pela crescente sofisticação dos ciberataques e pela utilização de IA por cibercriminosos para aumentar a eficácia e a complexidade dos ataques (Cruz, Casemiro, Gallizzi & Kalili, 2024).

Compreender o conhecimento dos utilizadores é crucial para identificar lacunas na consciencialização e desenvolver estratégias eficazes de mitigação.

A análise técnica dos riscos da IA nos ciberataques é um campo crucial, visando entender as implicações dessa interseção. Estudos indicam que, embora a IA contribua para o fortalecimento de sistemas de segurança, ela também intensifica a complexidade dos ataques cibernéticos (Souza & Morais, 2021).

Portanto, é essencial promover uma cultura de segurança cibernética robusta e preparar melhor a sociedade para enfrentar os desafios futuros.

1.1.Identificação do Problema

A crescente utilização da Inteligência Artificial (IA) em diversas áreas trouxe avanços significativos, mas também novos desafios, especialmente no campo da Cibersegurança. Ciberataques baseados em IA representam uma ameaça emergente, caracterizada pela sua sofisticação e capacidade de adaptação. Esses ataques utilizam técnicas avançadas de IA para automatizar e aprimorar as suas operações, tornando-se cada vez mais difíceis de detetar e mitigar (Borba & Mota, 2024).

O problema central deste estudo é a falta de conhecimento dos utilizadores sobre ciberataques que utilizam IA. Muitos utilizadores não estão cientes das técnicas avançadas empregadas por cibercriminosos e subestimam os riscos associados a esses ataques. Essa falta de conhecimento pode levar a comportamentos inseguros, aumentando a vulnerabilidade a ciberataques e comprometendo a segurança de informações sensíveis.

O problema foi identificado ao verificar que os utilizadores possuem conhecimento limitado sobre ciberataques baseados em IA, não percebem plenamente os riscos associados e carecem de programas de formação e consciencialização adequados. Essa constatação emergiu da revisão da literatura e da análise preliminar dos comportamentos e perceções dos utilizadores, evidenciando a necessidade urgente de reforçar a educação em cibersegurança.

Além disso, a rápida evolução das técnicas de ataque baseadas em IA dificulta a manutenção de um nível adequado de consciencialização entre os utilizadores. A ausência de programas de educação e consciencialização específicos sobre ciberataques baseados em IA agrava ainda mais o problema, deixando os utilizadores desprotegidos contra ameaças emergentes.

Portanto, a identificação do problema neste contexto envolve:

1.1.1 Desconhecimento das Técnicas de Ataque Baseadas em IA:

Muitos utilizadores não compreendem como a IA é utilizada para realizar ciberataques, como ataques de força bruta, *phishing* avançado e *deepfakes*.

1.1.2 Subestimação dos Riscos Associados:

A falta de perceção sobre a gravidade e a sofisticação dos ciberataques baseados em IA leva os utilizadores a subestimar os riscos e a não adotar medidas de proteção adequadas (Ferreira, 2025).

1.1.3 Falta de Educação e Consciencialização:

A ausência de programas de formação e campanhas de consciencialização específicas sobre ciberataques baseados em IA contribui para a manutenção das lacunas no conhecimento dos utilizadores (ENISA, 2021).

1.1.4 Impacto na Segurança Cibernética:

A combinação desses fatores resulta num ambiente digital mais vulnerável, onde os utilizadores estão mais suscetíveis a serem vítimas de ciberataques sofisticados.

A identificação do problema destaca a necessidade urgente de aumentar o conhecimento dos utilizadores sobre ciberataques baseados em IA. Abordar essas lacunas através de programas de educação e consciencialização é essencial para fortalecer a segurança cibernética e proteger os utilizadores contra ameaças emergentes.

1.2.Objetivo do Estudo

O objetivo principal deste estudo é analisar o conhecimento dos utilizadores sobre ciberataques baseados em Inteligência Artificial (IA), com o intuito de identificar lacunas no entendimento e propor soluções educacionais que possam aumentar a resiliência cibernética. Este objetivo é desdobrado em várias metas específicas, que incluem:

1.2.1 Avaliar o Conhecimento Atual:

- Medir o nível de conhecimento dos utilizadores sobre ciberataques baseados em IA, identificando o grau de familiaridade com as técnicas e métodos utilizados por cibercriminosos.

1.2.2 Identificar Lacunas de Conhecimento:

- Descobrir áreas onde os utilizadores têm menos compreensão ou estão mais vulneráveis, permitindo a identificação de pontos fracos que podem ser explorados por cibercriminosos.

1.2.3 Analisar Perceções:

- Compreender como os utilizadores percebem a gravidade e a frequência dos ciberataques, investigando a sua capacidade de reconhecer e avaliar essas ameaças.

1.2.4 Propor Soluções Educacionais:

- Desenvolver métodos para melhorar o conhecimento e a preparação dos utilizadores contra essas ameaças, incluindo programas de formação e campanhas de consciencialização.

1.2.5 Impacto das Ameaças:

- Examinar como o nível de conhecimento afeta a vulnerabilidade dos utilizadores a ciberataques, destacando a importância da educação em Cibersegurança para a proteção contra ameaças emergentes.

1.2.6 Consciencialização e Comportamento:

- Investigar como a consciencialização sobre Cibersegurança influencia as práticas e o comportamento online dos utilizadores, promovendo comportamentos mais seguros e responsáveis.

Ao atingir esses objetivos, o estudo pretende não apenas avaliar o conhecimento atual dos utilizadores sobre ciberataques baseados em IA, mas também identificar áreas de melhoria e propor soluções práticas para aumentar a segurança cibernética. Através da educação e consciencialização, espera-se reduzir a vulnerabilidade dos utilizadores e fortalecer a defesa contra ameaças emergentes.

1.3.Fundamentos do Objetivo do Estudo

Os objetivos delineados neste trabalho foram embasados em três dimensões complementares que asseguram a sua relevância e rigor académico. Em primeiro lugar, a revisão da literatura permitiu identificar que a utilização da Inteligência Artificial em ciberataques tem aumentado a sofisticação e a complexidade das ameaças digitais, enquanto revelou lacunas significativas no conhecimento dos utilizadores sobre estas novas formas de ataque (Borba & Mota, 2024). Estudos recentes, relatórios técnicos e publicações científicas destacam a necessidade de maior consciencialização e educação para enfrentar riscos como phishing avançado, deepfakes e malware adaptativo (Cruz, Casemiro, Gallizzi & Kalili, 2024; ENISA, 2021; Jakkal, 2021; CloudTarget, 2024).

Em segundo lugar, a observação da realidade atual evidenciou que muitos utilizadores subestimam os riscos associados à aplicação da IA em ciberataques, adotando comportamentos inseguros que aumentam a vulnerabilidade digital. Esta constatação reforçou a pertinência de objetivos voltados para a avaliação do conhecimento, a identificação de lacunas e a análise das perceções dos utilizadores (ENISA, 2021; CloudTarget, 2024).

Por fim, a metodologia de investigação escolhida, baseada em questionários online e análise quantitativa e qualitativa, foi concebida para transformar estas preocupações em metas mensuráveis e verificáveis. Assim, cada objetivo específico — desde a avaliação do conhecimento atual até à proposta de soluções educacionais — encontra-se sustentado por uma base teórica sólida, por evidências contextuais e por instrumentos metodológicos adequados (Borba & Mota, 2024; Cruz et al., 2024).

Deste modo, os objetivos do estudo refletem uma abordagem integrada que combina teoria, prática e método, garantindo que a investigação contribua de forma efetiva para o fortalecimento da cultura de segurança cibernética e para a preparação dos utilizadores face às ameaças emergentes potenciadas pela Inteligência Artificial.

1.4.Relevância e Importância do Estudo

A análise do conhecimento dos utilizadores sobre ciberataques baseados em Inteligência Artificial (IA) é um tema de extrema relevância e importância na atualidade. Abaixo estão os principais pontos que justificam a pertinência deste estudo:

1.4.1 Sofisticação Crescente dos Ciberataques:

Com o avanço da tecnologia, os ciberataques tornaram-se mais sofisticados e frequentes. A utilização de IA por cibercriminosos permite a automação e a personalização dos ataques, aumentando a sua eficácia e complexidade (Laroche Borba & Araújo Mota, 2024).

Este cenário exige uma compreensão aprofundada das novas ameaças para desenvolver defesas eficazes.

1.4.2 Impacto na Segurança das Informações:

A segurança das informações é uma preocupação crítica para indivíduos, empresas e governos. Ciberataques baseados em IA podem comprometer dados sensíveis, resultando em perdas financeiras, danos à reputação e riscos à privacidade (Jakkal,2021).

Portanto, é essencial que os utilizadores estejam cientes dessas ameaças e saibam como se proteger.

1.4.3 Lacunas no Conhecimento dos Utilizadores:

Estudos indicam que muitos utilizadores têm um conhecimento limitado sobre ciberataques baseados em IA e subestimam os riscos associados (Cloud Target, 2024).

Identificar essas lacunas é crucial para desenvolver programas de educação e consciencialização que possam aumentar a resiliência cibernética.

1.4.4 Necessidade de Educação e Consciencialização:

A educação e a consciencialização são fundamentais para mitigar os riscos de ciberataques. Ao entender melhor o nível de conhecimento dos utilizadores, é possível criar estratégias de treinamento mais eficazes e campanhas de consciencialização direcionadas. Isso ajuda a construir uma cultura de segurança cibernética mais robusta (Jakkal,2021).

1.4.5 Contribuição para a Literatura Académica:

Este estudo contribui para a literatura acadêmica ao fornecer dados e insights sobre o conhecimento dos utilizadores em relação a ciberataques baseados em IA. As descobertas podem ser utilizadas por investigadores e profissionais de Cibersegurança para desenvolver melhores práticas e políticas de defesa. (Laroche Borba & Araújo Mota, 2024)

1.4.6 Preparação para Futuras Ameaças:

A rápida evolução das técnicas de ataque baseadas em IA exige uma preparação contínua. Compreender as perceções e o conhecimento dos utilizadores permite antecipar futuras ameaças e adaptar as estratégias de defesa de forma proativa (Cloud Target, 2024).

A análise do conhecimento dos utilizadores sobre ciberataques baseados em IA é um tema de grande relevância na atualidade. Este estudo não só identifica lacunas no conhecimento, mas também propõe soluções para melhorar a segurança cibernética. Ao aumentar a consciencialização e a educação, podemos criar um ambiente digital mais seguro e resiliente contra ameaças emergentes.

1.5.Metodologia

1.5.1 Definição do Objeto de Investigação

O objeto de investigação deste estudo é o conhecimento dos utilizadores sobre ciberataques baseados em Inteligência Artificial (IA). O estudo centra-se em identificar o nível de compreensão dos utilizadores, as lacunas de conhecimento e as perceções sobre a gravidade e a frequência desses ataques.

1.5.2 Revisão da Literatura

A revisão da literatura será realizada para fundamentar teoricamente o estudo. Serão analisados artigos científicos, livros e relatórios técnicos que abordam ciberataques baseados em IA, a eficácia das técnicas de IA em Cibersegurança e estudos anteriores sobre o conhecimento dos utilizadores em Cibersegurança. Esta revisão ajudará a identificar lacunas no conhecimento existente e a justificar a relevância do estudo.

1.5.3 Escolha do Tipo de Investigação

Este estudo será de natureza descritiva e exploratória. A investigação descritiva permitirá medir o nível de conhecimento dos utilizadores, enquanto a investigação exploratória ajudará a identificar novas perceções e áreas de vulnerabilidade que ainda não foram amplamente estudadas.

1.5.4 Instrumentos de Recolha de Dados

Para a recolha de dados, serão utilizados questionários:

Serão aplicados questionários online para uma amostra representativa de utilizadores. Os questionários incluirão perguntas fechadas para avaliar o conhecimento sobre ciberataques baseados em IA.

1.5.5 Estabelecimento de Cronograma

O cronograma da investigação será dividido em várias etapas:

Tabela 1 - Cronograma de Trabalho

Cronograma de Trabalho

Etapa	Duração	Período Estimado
Revisão da Literatura	1 mês	Semana 1 – Semana 4
Desenvolvimento dos Instrumentos de Recolha de Dados	2 semanas	Semana 5 – Semana 6
Recolha de Dados	1 mês	Semana 7 – Semana 10
Análise dos Dados	1 mês	Semana 11 – Semana 14
Redação do Relatório Final	1 mês	Semana 15 – Semana 18

Fonte: Autor

1.5.6 Recolha de Dados

A recolha de dados será realizada conforme os métodos definidos. Os questionários serão distribuídos.

1.5.7 Análise dos Dados

Os dados recolhidos serão analisados utilizando técnicas estatísticas e de análise de conteúdo:

Análise Estatística: Os dados quantitativos dos questionários serão analisados utilizando software estatístico para identificar padrões e tendências no conhecimento dos utilizadores.

1.5.8 Elaboração do Relatório

O relatório final da investigação será elaborado apresentando os resultados, e conclusões. O relatório incluirá gráficos e tabelas para ilustrar os dados recolhidos e fornecerá recomendações para melhorar a educação e a consciencialização sobre ciberataques baseados em IA.

1.5.9 Conclusão da Metodologia

As linhas metodológicas delineadas garantem que o estudo seja conduzido de forma sistemática e rigorosa, permitindo uma análise abrangente do conhecimento dos utilizadores sobre ciberataques baseados em IA. Através desta abordagem, espera-se contribuir para a literatura académica e fornecer insights valiosos para o desenvolvimento de estratégias de Cibersegurança mais eficazes.

1.6.Estrutura do Trabalho

Este documento estará dividido em 5 capítulos, representando os diferentes passos seguidos para se obter o resultado. A estrutura seguida será a seguinte:

1.6.1 Introdução

Contextualização do tema abordado ao longo do documento, apresentação dos diferentes conceitos a estudar, objetivo do estudo e qual o caminho a seguir para obter o resultado pretendido.

1.6.2 Revisão de Literatura

Descrição detalhada dos conceitos fundamentais para a realização deste estudo. A Inteligência Artificial e a Cibersegurança serão os conceitos abordados neste capítulo. Existirá ainda uma secção referente à Revisão Sistemática de Literatura onde serão selecionadas diferentes palavras-chave que irão devolver diferentes artigos. Estes serão analisados e os artigos relevantes selecionados, isto é, que abordem a utilização da Inteligência Artificial em situações onde possam ocorrer ciberataques.

1.6.3 Metodologia

Apresentação e detalhe do método abordado na realização do presente estudo, isto é, qual a estratégia que será seguida de forma a implementar o estudo.

1.6.4 Resultados da Investigação

Análise realizada após a conclusão da Revisão Sistemática da Literatura, onde será construído um estudo, no qual se irão cruzar as técnicas de Inteligência Artificial com as técnicas de Cibersegurança.

1.6.5 Conclusão

Análise do resultado obtido nos pontos anteriores e resumo do que foi possível obter com o presente estudo, bem como, quais foram as limitações encontradas no processo de desenvolvimento do estudo e o que se pretende realizar de forma a resolver no futuro as limitações encontradas.

1.7.Declaração Metodológica

Parte da elaboração deste trabalho contou com o apoio da ferramenta de inteligência artificial Microsoft Copilot, utilizada para gerar explicações preliminares e exemplos de conceitos. O conteúdo produzido pela IA foi tratado como apoio complementar, sendo posteriormente analisado, validado e confrontado com fontes acadêmicas e científicas tradicionais. A utilização da IA visou otimizar o processo de redação e ampliar a clareza das ideias, sem substituir a investigação bibliográfica e a reflexão crítica do autor.

2. REVISÃO DA LITERATURA

Neste capítulo, irão ser apresentadas as bases teóricas que serão utilizadas para o desenvolvimento deste projeto.

A revisão da literatura é uma etapa fundamental em qualquer investigação académica. Ela envolve a análise crítica de estudos e publicações existentes sobre um determinado tema, com o objetivo de identificar lacunas, tendências e estabelecer um contexto teórico para a investigação. No caso da "Análise do Conhecimento dos Utilizadores sobre Ciberataques Baseados em Inteligência Artificial", a revisão da literatura permite compreender o estado atual do conhecimento e as perceções dos utilizadores sobre as ameaças cibernéticas impulsionadas por IA.

Na primeira parte, foram investigados os principais conceitos, bem como as áreas associadas à

Cibersegurança e à Inteligência Artificial.

Na segunda parte, tendo como base de investigação os conceitos investigados na secção anterior, foi realizada uma Revisão Sistemática de Literatura onde foram definidas as seguintes questões de investigação, para o qual pretendemos obter resposta:

- Quais são os níveis de conhecimento e perceção dos utilizadores sobre os riscos e métodos de prevenção de ciberataques baseados em inteligência artificial?
- Como o nível de conhecimento dos utilizadores afeta a sua vulnerabilidade a ciberataques?

2.1 Conceitos

2.1.1 Cibersegurança

A Cibersegurança, também conhecida como segurança cibernética, refere-se ao conjunto de práticas, tecnologias e processos destinados a proteger sistemas, redes, dispositivos e dados contra-ataques cibernéticos e acessos não autorizados. O objetivo principal da Cibersegurança é garantir a confidencialidade, integridade e disponibilidade das informações digitais, além de assegurar a autenticidade e o não repúdio das ações realizadas no ambiente digital (Sousa, 2023).

A Cibersegurança é essencial para proteger dados sensíveis e sistemas críticos de empresas, governos e indivíduos. Com o aumento da conectividade e da dependência de tecnologias digitais, a proteção contra ameaças cibernéticas tornou-se uma prioridade. As principais áreas de atuação da Cibersegurança incluem a prevenção de invasões, a deteção de atividades maliciosas, a resposta a incidentes e a recuperação de sistemas comprometidos (Shimabukuro, 2025).

2.1.2 Definição e História da Cibersegurança

- Definição de Cibersegurança

"Cibersegurança é uma propriedade do Ciberespaço que trata a capacidade para resistir, responder e recuperar de ameaças intencionais e não intencionais". (Rauscher & Yaschenko, 2011)

- História e evolução das ameaças cibernéticas

As ameaças cibernéticas têm evoluído significativamente desde os primeiros dias da computação. Nos anos 1980, os vírus de computador começaram a surgir, com programas como o "*Brain*" e o "*Morris Worm*" causando os primeiros grandes incidentes de segurança. Esses vírus eram relativamente simples e espalhavam-se principalmente através de disquetes.

Na década de **1990**, com a popularização da Internet, as ameaças cibernéticas tornaram-se mais sofisticadas e disseminadas. Surgiram os primeiros ataques de negação de serviço (*DDoS*) e os cavalos de Troia, que permitiam aos atacantes obter acesso não autorizado a sistemas. O aumento do comércio eletrónico também trouxe à tona novas formas de fraude online e roubo de identidade.

Os anos **2000** marcaram uma nova era de ameaças cibernéticas com o surgimento de *worms* como o "*ILOVEYOU*" e o "*Code Red*", que se espalhavam rapidamente pela Internet, causando danos generalizados. Além disso, o advento das redes sociais e dos dispositivos móveis ampliou a superfície de ataque, introduzindo novas vulnerabilidades.

Na **última década**, as ameaças cibernéticas tornaram-se ainda mais complexas e direcionadas. Ataques de *ransomware*, como o "*WannaCry*" e o "*NotPetya*", demonstraram a capacidade de paralisar infraestruturas críticas e causar prejuízos financeiros significativos. Além disso, o

aumento das ameaças persistentes avançadas (APTs) e dos ataques patrocinados por estados-nação sublinhou a necessidade de estratégias de Cibersegurança mais robustas e proativas.

Hoje, as ameaças cibernéticas continuam a evoluir, impulsionadas por tecnologias emergentes como a Internet das Coisas (IoT) e a inteligência artificial. A Cibersegurança deve acompanhar essa evolução, adotando abordagens inovadoras para proteger dados e sistemas contra um cenário de ameaças em constante mudança. (Silva & Glória Júnior, 2023), (Almeida, 2020), (Costa da Conceição, 2023), (Shaikh & Siponen, 2024)

- Métodos tradicionais de cibersegurança e suas limitações

Os métodos tradicionais de Cibersegurança incluem uma variedade de técnicas e ferramentas projetadas para proteger sistemas e dados contra ameaças cibernéticas. Entre os métodos mais comuns estão:

Figura 1 - Métodos tradicionais de Cibersegurança

Fonte: Autor

1. ***Firewalls***: Dispositivos ou softwares que monitoram e controlam o tráfego de rede com base em regras de segurança predefinidas. Embora eficazes para bloquear tráfego não autorizado, as *firewalls* podem ser contornadas por ataques sofisticados.

2. **Antivírus e *Antimalware***: Programas que detetam e removem software malicioso. No entanto, esses programas dependem de assinaturas conhecidas de *malware*, o que os torna menos eficazes contra ameaças novas ou desconhecidas.

3. **Sistemas de Deteção e Prevenção de Intrusões (IDS/IPS)**: Ferramentas que monitorizam redes e sistemas á procura de atividades suspeitas e tomam medidas para prevenir ataques. Apesar da sua utilidade, eles podem gerar muitos falsos positivos e requerem configuração e manutenção contínuas.

4. **Criptografia**: Técnica de codificação de dados para torná-los inacessíveis a utilizadores não autorizados. Embora essencial para proteger dados sensíveis, a criptografia pode ser complexa de implementar e gerir.

5. **Autenticação Multifator (MFA)**: Método de verificação de identidade que exige múltiplas formas de autenticação. Embora aumente a segurança, pode ser inconveniente para os utilizadores e não é infalível contra-ataques sofisticados.

Apesar da sua importância, os métodos tradicionais de Cibersegurança têm limitações significativas. Eles frequentemente dependem de assinaturas e regras predefinidas, o que os torna menos eficazes contra novas ameaças e desconhecidas. Além disso, a crescente complexidade e volume de ataques cibernéticos exigem soluções mais avançadas e adaptativas, capazes de responder rapidamente a um cenário de ameaças em constante mudança (Morais, 2022).

2.1.3 Inteligência Artificial

A Inteligência Artificial (IA) refere-se ao campo da ciência da computação dedicado ao desenvolvimento de sistemas e algoritmos que podem realizar tarefas que normalmente requerem inteligência humana. Essas tarefas incluem aprendizagem, raciocínio, resolução de problemas, perceção e compreensão da linguagem natural. A IA pode ser dividida em duas categorias principais: IA estreita (ou fraca), que é projetada para realizar uma tarefa específica, e IA geral (ou forte), que possui capacidades cognitivas amplas e pode realizar qualquer tarefa intelectual que um ser humano possa. (Morais, 2022)

2.1.4 Definição e conceitos básicos de IA

A IA tem se tornado uma tecnologia fundamental em diversas áreas, incluindo saúde, finanças, transporte e segurança. Ela permite a automação de processos complexos, melhora a eficiência operacional e oferece novas oportunidades para inovação. A capacidade da IA de analisar grandes volumes de dados e identificar padrões ocultos é uma das suas características mais valiosas (Goodfellow, Bengio & Courville, 2016).

- Definição de Inteligência Artificial (IA)

A Inteligência Artificial (IA) é um campo da ciência da computação que se concentra na criação de sistemas capazes de realizar tarefas que normalmente requerem inteligência humana. Essas tarefas incluem, mas não se limitam ao reconhecimento de fala, tomada de decisão, tradução de idiomas, e reconhecimento de padrões. A IA procura desenvolver algoritmos e modelos que permitam aos computadores aprenderem com dados, adaptarem-se a novas informações e realizarem tarefas de forma autónoma (SciELO Brasil, 2021), (Russell & Norvig, 2020).

- Conceitos Básicos de IA

A Inteligência Artificial (IA) constitui um campo multidisciplinar que abrange diversas subáreas fundamentais. Entre elas, destaca-se a **aprendizagem de máquina (Machine Learning – ML)**, que permite aos computadores aprenderem a partir de dados, seja por meio de aprendizagem supervisionada, não supervisionada ou por reforço (Mitchell, 1997).

Um dos pilares da IA são as **redes neurais artificiais (ANNs)**, modelos inspirados no funcionamento do cérebro humano, compostos por camadas de nós que processam informações e ajustam os pesos das ligações para melhorar o desempenho (Goodfellow, Bengio, & Courville, 2016). A evolução destas redes deu origem ao **deep learning**, que utiliza arquiteturas profundas para modelar padrões complexos em grandes volumes de dados, sendo particularmente eficaz em tarefas como reconhecimento de imagem e processamento de linguagem natural (Goodfellow et al., 2016).

No campo do **processamento de linguagem natural (NLP)**, a IA possibilita a interação entre computadores e linguagem humana, permitindo que sistemas compreendam, interpretem e respondam de forma adequada (Jurafsky & Martin, 2023). Paralelamente, a **visão**

computacional capacita máquinas a interpretar informações visuais, com aplicações que vão desde o reconhecimento facial até à análise de imagens médicas (Szeliski, 2022).

Por fim, os **agentes inteligentes** representam sistemas capazes de perceber o ambiente e tomar decisões que maximizem as hipóteses de alcançar objetivos, sendo aplicados em assistentes virtuais e robôs autónomos (Russell & Norvig, 2021).

Em síntese, estes conceitos formam a base da IA e sustentam as suas aplicações em diversos setores, oferecendo novas oportunidades para inovação e eficiência.

2.2 Ciberataques Baseados em Inteligência Artificial

A inteligência artificial (IA) tem revolucionado diversas áreas, incluindo a Cibersegurança. No entanto, essa mesma tecnologia também está sendo explorada por cibercriminosos para realizar ataques mais sofisticados e difíceis de detetar. Este capítulo examina como a IA está a ser utilizada em ciberataques, os tipos de ataques mais comuns e as estratégias de defesa, com base em artigos científicos recentes.

2.2.1 A Evolução dos Ciberataques com IA

A integração da IA em ciberataques tem permitido que cibercriminosos automatizem e aprimorem suas técnicas. A capacidade da IA de processar grandes volumes de dados e aprender com padrões torna-a uma ferramenta poderosa para identificar vulnerabilidades em sistemas e criar ataques personalizados (Laroche Borba & Araújo Mota, 2024).

2.2.2 Tipos de Ciberataques Baseados em IA

- Quebra de Senhas

A quebra de senhas é uma técnica comum onde a IA é utilizada para tentar inúmeras combinações de senhas até encontrar a correta. Ferramentas de IA, como o *PassGAN*, podem quebrar senhas comumente utilizadas em questão de minutos, representando uma ameaça significativa para a segurança de contas online (Cruz, Casemiro, Gallizzi & Kalili, 2024).

- *Phishing* e Engenharia Social

A IA pode gerar e-mails de *phishing* altamente convincentes, imitando o estilo e o tom de comunicações legítimas. Isso torna mais difícil para as vítimas distinguirem entre e-mails reais e fraudulentos. Além disso, a IA pode ser usada para personalizar ataques de engenharia social com base em informações recolhidas online (Cruz, Casemiro, Gallizzi & Kalili, 2024).

- *Deepfakes*

Deepfakes são vídeos ou áudios falsificados criados com IA que podem ser utilizados para personificar indivíduos de forma convincente. Cibercriminosos podem usar *deepfakes* para se passar por executivos em chamadas de vídeo, induzindo funcionários a realizar transferências financeiras ou divulgar informações sensíveis (Laroche Borba & Araújo Mota, 2024).

2.3 Medidas de Defesa Contra Ciberataques com IA

2.3.1 Autenticação Forte

Implementar autenticação multifator (MFA) pode dificultar a quebra de senhas, adicionando camadas extras de segurança. Além disso, o uso de senhas fortes e únicas para cada conta é essencial (De Almeida Souza & De Moraes, 2021).

2.3.2 Formação e Consciencialização

Educar funcionários e utilizadores sobre os riscos de *phishing* e engenharia social é crucial. Formações regulares podem ajudar a identificar e-mails suspeitos e evitar que informações sensíveis sejam divulgadas (De Almeida Souza & De Moraes, 2021).

2.3.3 Monitorização e Deteção

Ferramentas de segurança baseadas em IA podem ser utilizadas para monitorizar atividades suspeitas e detetar anomalias em tempo real. Isso permite uma resposta rápida a possíveis ameaças antes que causem danos significativos (De Almeida Souza & De Moraes, 2021).

2.3.4 Síntese da Revisão da Literatura

A inteligência artificial está a transformar o cenário dos ciberataques, tornando-os mais sofisticados e difíceis de detetar. No entanto, com as medidas de defesa adequadas, é possível

mitigar os riscos e proteger sistemas e dados contra essas ameaças emergentes. A consciencialização e a preparação são fundamentais para enfrentar os desafios impostos pelos ciberataques baseados em IA.

3. CIBERSEGURANÇA EM PORTUGAL NA ERA DA INTELIGÊNCIA ARTIFICIAL: DESAFIOS E AMEAÇAS EMERGENTES

A Cibersegurança em Portugal enfrenta um cenário em constante evolução, impulsionado pela crescente digitalização da sociedade e pela sofisticação das ameaças cibernéticas (CNCS, 2024). Num contexto global marcado pela proliferação de tecnologias baseadas em Inteligência Artificial (IA), o panorama da segurança cibernética nacional é particularmente desafiador, exigindo uma análise aprofundada dos ciberataques potenciados pela IA e a implementação de estratégias de defesa proativas e inovadoras (ENISA, 2023; Borba & Mota, 2024; Jakkal, 2021; Observatório de Cibersegurança, 2024; CloudTarget, 2024).

3.1 O Duplo Gume da Inteligência Artificial na Cibersegurança

A Inteligência Artificial, com a sua capacidade de análise de grandes volumes de dados, reconhecimento de padrões complexos e tomada de decisões autónomas, apresenta um duplo gume no domínio da Cibersegurança. Por um lado, constitui uma ferramenta defensiva que permite análise comportamental, deteção de anomalias e automatização de processos de segurança (Goodfellow, Bengio, & Courville, 2016). Por outro lado, a mesma tecnologia pode ser utilizada como ferramenta ofensiva, capacitando atacantes com novas metodologias e vetores de ataque, tornando as defesas tradicionais menos eficazes (Brundage et al., 2018; ENISA, 2023; Jakkal, 2021). Este duplo papel da IA evidencia a necessidade de estratégias de defesa proativas e inovadoras, capazes de equilibrar os benefícios da sua aplicação com os riscos emergentes.

3.2 Vulnerabilidades em Portugal

Em Portugal, a crescente dependência de infraestruturas críticas digitais em setores como a energia, as finanças, a saúde e a administração pública torna o país particularmente vulnerável a ciberataques sofisticados (CNCS, 2025). Num contexto global marcado pela proliferação de tecnologias baseadas em Inteligência Artificial (IA), estes ataques representam uma ameaça emergente com potencial para causar disrupções significativas e prejuízos económicos

consideráveis (ENISA, 2023; Prosegur Cipher, 2025; PwC Portugal, 2025; Universidade de Coimbra & Indra Group, 2025).

3.3 Tipos de Ciberataques Baseados em IA

3.3.1 *Phishing* e Engenharia Social Avançados

A IA permite a criação de mensagens e perfis falsos altamente convincentes, personalizados para indivíduos específicos, aumentando a eficácia das campanhas de *phishing* e da manipulação psicológica (Hadnagy, 2010).

Impacto: Maior vulnerabilidade em setores como banca e saúde.

Defesa: Programas de literacia digital e sistemas de deteção baseados em IA.

3.3.2 Geração Automática de *Malware* Polimórfico

A IA pode ser utilizada para gerar automaticamente novas variantes de *malware*, capazes de evadir as assinaturas e os mecanismos de deteção tradicionais. (Raff, Sylvester & Nicholas, 2017)

Impacto: Aumento da dificuldade de resposta rápida em infraestruturas críticas.
Defesa: Soluções de sandboxing e análise comportamental dinâmica.

3.3.3 Ataques de Negação de Serviço Distribuídos (DDoS) Inteligentes

IA pode otimizar a coordenação e a intensidade dos ataques DDoS, tornando-os mais difíceis de mitigar (Mirkovic & Reiher, 2004).

Impacto: Paralisação de serviços públicos e privados.

Defesa: Sistemas de mitigação adaptativos e redes de distribuição de tráfego.

3.3.4 Ataques Direcionados e Persistentes (APT) Sofisticados

A IA pode auxiliar na identificação de vulnerabilidades específicas em sistemas e redes, bem como na automatização de processos de infiltração e exfiltração de dados, tornando os APTs mais furtivos e eficazes (Callegari et al., 2016).

Impacto: Roubo de propriedade intelectual e espionagem estatal.

Defesa: Monitorização contínua e inteligência de ameaças.

3.3.5 Manipulação de Informação e Desinformação em Larga Escala

A IA pode ser utilizada para criar e disseminar notícias falsas e propaganda de forma automatizada e personalizada, com o objetivo de influenciar a opinião pública e desestabilizar instituições (Vosoughi et al., 2018).

Impacto: Risco para a democracia e confiança social.

Defesa: Fact-checking automatizado e políticas de regulação de conteúdos digitais.

3.4 Estratégias de Resposta em Portugal

3.4.1 **Investimento em investigação e desenvolvimento (I&D:** A resposta a estas ameaças exige uma abordagem multifacetada em Portugal. É crucial o investimento em investigação e desenvolvimento de soluções de Cibersegurança baseadas em Inteligência Artificial, como sistemas de deteção de intrusão inteligentes, análise preditiva de ameaças e resposta automatizada a incidentes (PwC Portugal, 2025; Compete 2030, 2025; Indra Group, 2025; CNCS, 2025; ENISA, 2023).

3.4.2 **Colaboração entre setores:** Adicionalmente, o reforço da colaboração entre o setor público, o setor privado e a academia são fundamental para partilhar informações sobre ameaças, desenvolver boas práticas e promover a formação de profissionais especializados em Cibersegurança (European Union Agency for Cybersecurity - ENISA, 2021).

3.4.3 **Políticas e regulamentações robustas:** A nível nacional, a implementação de políticas e regulamentações robustas que abordem os desafios específicos da Cibersegurança na era da IA é igualmente essencial. Isto inclui a promoção de uma cultura de Cibersegurança em toda a sociedade, através de programas de sensibilização e educação para os riscos cibernéticos, bem como o apoio ao desenvolvimento de competências digitais avançadas (CNCS, 2025; ENISA, 2023).

3.5 Síntese

Em suma, a Cibersegurança em Portugal enfrenta um ponto de inflexão com a crescente sofisticação dos ciberataques baseados em IA. A capacidade de antecipar, detetar e responder eficazmente a estas ameaças emergentes dependerá da implementação de estratégias proativas, do investimento em inovação tecnológica e da colaboração entre diversos atores. A negligência destes desafios poderá ter consequências significativas para a segurança e a prosperidade digital do país.

4. ESTRUTURA DA INVESTIGAÇÃO

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 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. Ela fornece uma análise abrangente e aprofundada sobre a relação entre Cibersegurança, segurança humana além de propor medidas educacionais e de consciencialização para mitigar os riscos e as ciberameaças.

4.1 Metodologia da Investigação

4.1.1 Questionário

Para avaliar o nível de consciencialização em Cibersegurança, foi conduzido um questionário (Anexo 1) sobre as experiências das pessoas com as ciberameaças baseados em IA.

4.1.2 Público-Alvo

O questionário foi criado através do Google Forms e foi direcionado a três grupos distintos:

- **Académicos** – docentes, investigadores e estudantes ligados ao ensino superior.
- **Profissionais de tecnologia** – especialistas em TI, cibersegurança e áreas técnicas relacionadas.

- **Outros setores** – público em geral, com diferentes formações e profissões, incluídos para avaliar a perceção fora do meio técnico.

4.1.3 Distribuição e Amostra

A distribuição do questionário online ocorreu por e-mail. Os dados dos inquiridos foram recolhidos anonimamente. Um total de **74 pessoas** responderam ao questionário.

4.1.4 Estrutura do Questionário

Com base no questionário, os dados obtidos são principalmente sobre dois tópicos.

- **Primeira parte:** conhecimento dos utilizadores sobre ciberataques baseados em IA e avaliação do nível de familiaridade.
- **Segunda parte:** perceção e consciencialização dos utilizadores sobre essas ameaças.
- 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.

4.1.5 Objetivos do Questionário

O questionário foi utilizado como recurso principal para três objetivos:

1. Em primeiro lugar, avaliar quais são os níveis de conhecimento e perceção dos utilizadores sobre os riscos e métodos de prevenção de ciberataques baseados em inteligência artificial, 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.
2. Em segundo lugar é o de compreender como o nível de conhecimento dos utilizadores afeta a sua vulnerabilidade a ciberataques.
3. Em terceiro lugar é apresentar uma ideia original com um resultado útil que poderia ser potencialmente mais desenvolvido.

4.2 Implementação da Investigação

4.2.1 Condução do Questionário

Após a definição da metodologia, procedeu-se à aplicação prática do questionário elaborado (Anexo 1). O instrumento foi disponibilizado através da plataforma Google Forms e distribuído por via eletrónica, garantindo acessibilidade e rapidez na recolha de dados.

4.2.2 Participação e Respostas Obtidas

A amostra final foi composta por **74 participantes**, que responderam de forma **anónima**, assegurando a confidencialidade das informações recolhidas. O questionário foi direcionado a três grupos distintos: utilizadores académicos, profissionais de tecnologia e público em geral. Esta diversidade permitiu obter uma visão abrangente sobre diferentes níveis de conhecimento e perceção relativamente às ciberameaças baseadas em Inteligência Artificial.

4.2.3 Observações Durante a Aplicação

Durante a aplicação do questionário, verificou-se que alguns inquiridos demonstraram interesse em aprofundar os temas abordados, o que reforça o carácter **educativo e de sensibilização** do instrumento. Além de recolher dados quantitativos e qualitativos, o questionário contribuiu para aumentar a consciencialização dos participantes sobre os riscos associados às ciberameaças potenciadas pela IA.

4.2.4 Síntese

Este capítulo descreve a **execução prática da investigação**, desde a aplicação do questionário até à recolha da amostra e observações relevantes. A implementação permitiu obter dados concretos que servirão de base para a análise e discussão dos resultados no capítulo seguinte.

5. RESULTADOS DA INVESTIGAÇÃO

A rápida integração da Inteligência Artificial em diversas esferas da sociedade tem revolucionado a forma como interagimos com a tecnologia (Goodfellow, Bengio, & Courville, 2016). Contudo, esta evolução também abriu novas vias para atores maliciosos, que exploram as capacidades da IA para desenvolver ciberataques mais sofisticados, adaptáveis e eficazes (Brundage et al., 2018; ENISA, 2023; Jakkal, 2021). Compreender o nível de conhecimento dos utilizadores finais sobre estas ameaças emergentes é fundamental para fortalecer a postura de segurança cibernética, uma vez que estes representam frequentemente a primeira linha de defesa contra ataques (CNCS, 2025).

A presente investigação debruça-se sobre a análise do conhecimento dos utilizadores relativamente aos ciberataques baseados em Inteligência Artificial. Através da aplicação de um questionário estruturado, procurou-se obter dados empíricos que permitam:

- **Avaliar o Conhecimento sobre Ciberataques Baseados em IA**, identificando o nível de familiaridade dos participantes com as características e tipologias destes ataques;
- **Identificar Lacunas de Conhecimento sobre Ciberataques Baseados em IA**, mapeando as áreas onde a compreensão dos utilizadores é mais limitada;
- **Analisar as Perceções sobre Ciberataques Baseados em IA**, investigando as crenças e atitudes dos participantes em relação à probabilidade e ao potencial impacto destas ameaças;
- Recolher **Propostas Educacionais para Melhorar o Conhecimento sobre Ciberataques Baseados em IA**, auscultando as sugestões dos utilizadores sobre as melhores abordagens para aumentar a sua literacia nesta área;
- Compreender a perceção do **Impacto das Ameaças de Ciberataques Baseados em IA** na sua vida digital e nas organizações; e
- Avaliar a relação entre o conhecimento sobre estas ameaças e a sua **Consciencialização e Comportamento em Cibersegurança** no quotidiano.

Os resultados obtidos através da análise das respostas ao questionário oferecem um panorama detalhado do conhecimento e das perceções dos utilizadores sobre os ciberataques potenciados

pela Inteligência Artificial. Esta análise permitirá identificar as áreas críticas onde o conhecimento é deficitário, as perceções que podem levar a comportamentos de risco e as preferências dos utilizadores relativamente a futuras iniciativas de educação e sensibilização. Em última análise, esta investigação visa fornecer informações valiosas para o desenvolvimento de estratégias mais eficazes no combate à crescente ameaça dos ciberataques baseados em IA, capacitando os utilizadores com o conhecimento necessário para se protegerem num cenário digital em constante mutação.

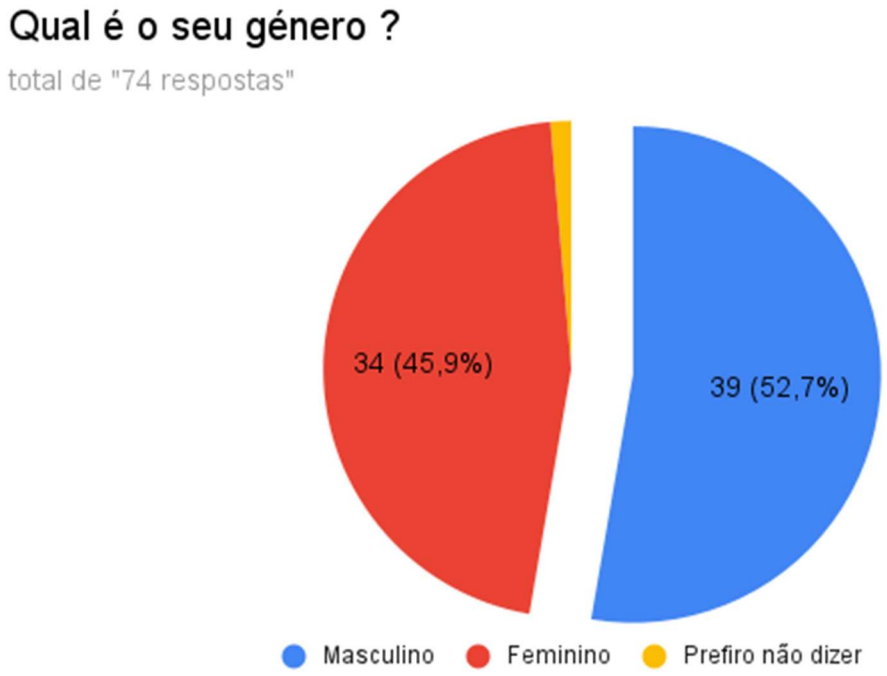
5.1 Analise dos dados sobre o conhecimento dos utilizadores sobre ciberataques baseados em IA

Neste capítulo, realizaremos uma análise dos dados recolhidos através de um questionário online aplicado a 74 pessoas em Portugal. O questionário decorreu ao longo de quatro semanas, do período de 01 de maio de 2025 a 31 de maio de 2025. As perguntas incluem escolhas múltiplas. Apresentarei uma análise quantitativa dos dados recolhidos.

- **Participação**: Dos 74 participantes, todos preencheram integralmente o questionário. Este número indica um bom nível de participação e confiabilidade dos resultados.
- **Estrutura**: Em seguida, destacarei 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.
- **Resultados**: A análise completa dos dados, incluirá gráficos detalhados. Isso irá ajudar-nos a obter uma visão mais completa e aprofundada do conhecimento dos utilizadores sobre ciberataques baseados em IA.

A Figura 2, apresenta a distribuição de género dos participantes que preencheram o questionário.

Figura 2 - Género dos Inquiridos



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

Análise do Gráfico de Distribuição de Género

O gráfico apresentado é um gráfico de pizza (ou setor) que ilustra a distribuição das respostas para a pergunta "Qual é o seu género?". O título indica que a investigação obteve um total de "74 respostas".

As categorias de género apresentadas na legenda são:

Tabela 2 - Categorias de Género

Categoria de Género	Cor Representada
Masculino	Azul
Feminino	Laranja/Vermelho
Outro	Amarelo
Prefiro não dizer	Verde

Fonte: Autor

A análise das proporções percentuais revela o seguinte:

- **Masculino:** Constitui a maior parcela dos inquiridos, com **52,7%** das 74 respostas. Este é o setor azul, que ocupa um pouco mais da metade do gráfico.
- **Feminino:** Representa a segunda maior fatia, com **45,9%** das respostas. Este é o setor laranja/vermelho, ligeiramente menor que a categoria masculina.
- **Outro:** A fatia amarela, que representa "Outro", é visivelmente muito pequena, indicando uma percentagem muito baixa de inquiridos.
- **Prefiro não dizer:** A fatia verde, correspondente a "Prefiro não dizer", é igualmente muito pequena, quase impercetível, sugerindo uma percentagem muito baixa.

Observações e Implicações:

1. **Predominância:** Há uma ligeira predominância de inquiridos que se identificam como masculinos (52,7%) em comparação com os que se identificam como femininos

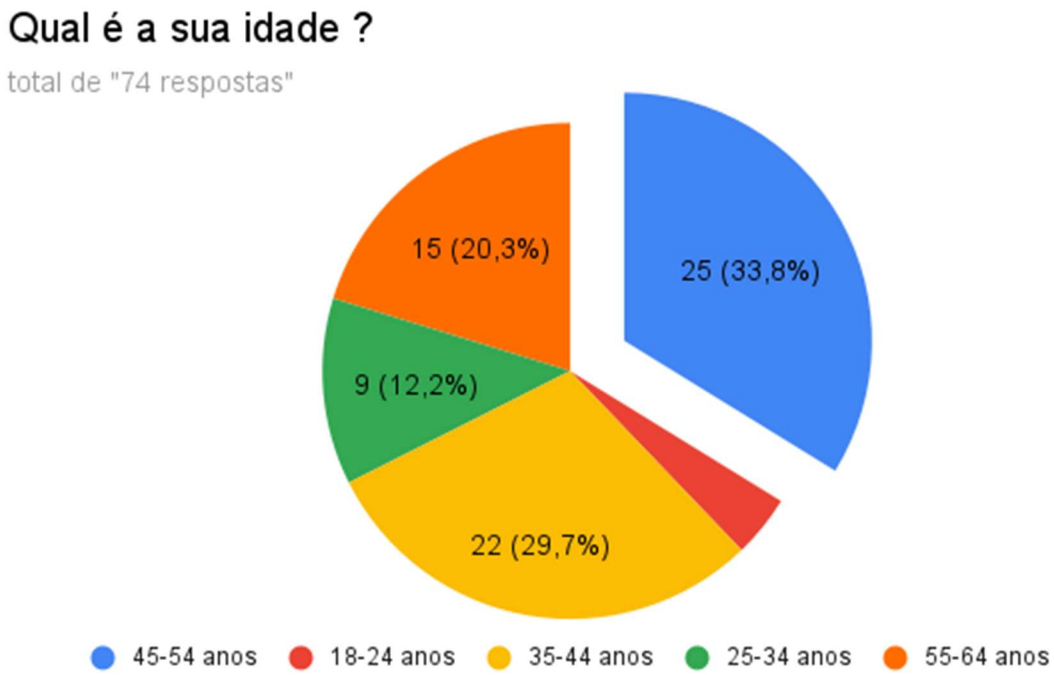
(45,9%). A diferença entre as duas categorias principais é de apenas 6,8 pontos percentuais.

2. **Soma das Percentagens:** A soma das percentagens visíveis (52,7% + 45,9%) totaliza 98,6%. A diferença para 100% (1,4%) corresponde à soma das percentagens das categorias "Outro" e "Prefiro não dizer", o que confirma visualmente a sua pequena representatividade. Sem os valores exatos para estas últimas categorias, não é possível quantificar individualmente a sua proporção.
3. **Representatividade:** Para um estudo que visa uma amostra equitativa entre géneros binários, a distribuição está razoavelmente equilibrada, embora com uma pequena inclinação para o género masculino. A baixa representatividade das categorias "Outro" e "Prefiro não dizer" sugere que a amostra é predominantemente composta por indivíduos que se identificam com os géneros binários tradicionais ou que a opção "Outro" não foi largamente utilizada/aplicada para esta amostra específica.

Em resumo, o gráfico fornece uma representação clara da distribuição de género entre os 74 inquiridos, destacando uma divisão quase igualitária entre masculino e feminino, com uma ligeira vantagem para o primeiro, e uma proporção muito pequena de outras identificações ou de respostas omitidas.

A Figura 3, apresenta a distribuição da idade dos participantes do questionário.

Figura 3 - Idade dos inquiridos



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

Análise do Gráfico de Distribuição Etária

O gráfico de setores em questão ilustra a distribuição por faixa etária dos 74 inquiridos, conforme indicado pelo título "Qual é a sua idade?" e o subtítulo "74 respostas". As faixas etárias estão divididas em seis categorias, representadas por diferentes cores:

Tabela 3 - Faixas Etárias

Faixa Etária	Cor Representada
18–24 anos	Azul

Faixa Etária	Cor Representada
25–34 anos	Vermelho/Laranja-escuro
35–44 anos	Laranja
45–54 anos	Verde
55–64 anos	Roxo
65 anos ou mais	Azul-claro/Ciano

Fonte: Autor

Principais Observações:

1. **Grupo Maioritário:** A faixa etária de **45-54 anos** (verde) é a mais representativa, englobando **33,8%** dos inquiridos. Isso sugere que aproximadamente um terço da amostra está nesse grupo etário.
2. **Segundo Maior Grupo:** A faixa de **35-44 anos** (laranja) vem em segundo lugar, com **29,7%** das respostas. Juntamente com o grupo de 45-54 anos, essas duas faixas etárias compreendem a maioria esmagadora da amostra, totalizando 63,5% (33,8% + 29,7%).
3. **Terceiro Grupo Significativo:** A faixa de **55-64 anos** (roxo) representa uma parcela considerável, com **20,3%** dos inquiridos.
4. **Menos representados:**
    - O grupo de **25-34 anos** (vermelho/laranja-escuro) corresponde a **12,2%**.
    - A faixa etária **18-24 anos** (azul) é a menos representada entre as faixas com percentual visível, com uma fatia muito pequena. Embora o percentual não esteja explícito na imagem para este setor, ele é claramente o menor.

- A categoria **65 anos ou mais** (azul-claro/ciano) é visualmente quase impercetível, indicando uma representatividade extremamente baixa ou nula na amostra.

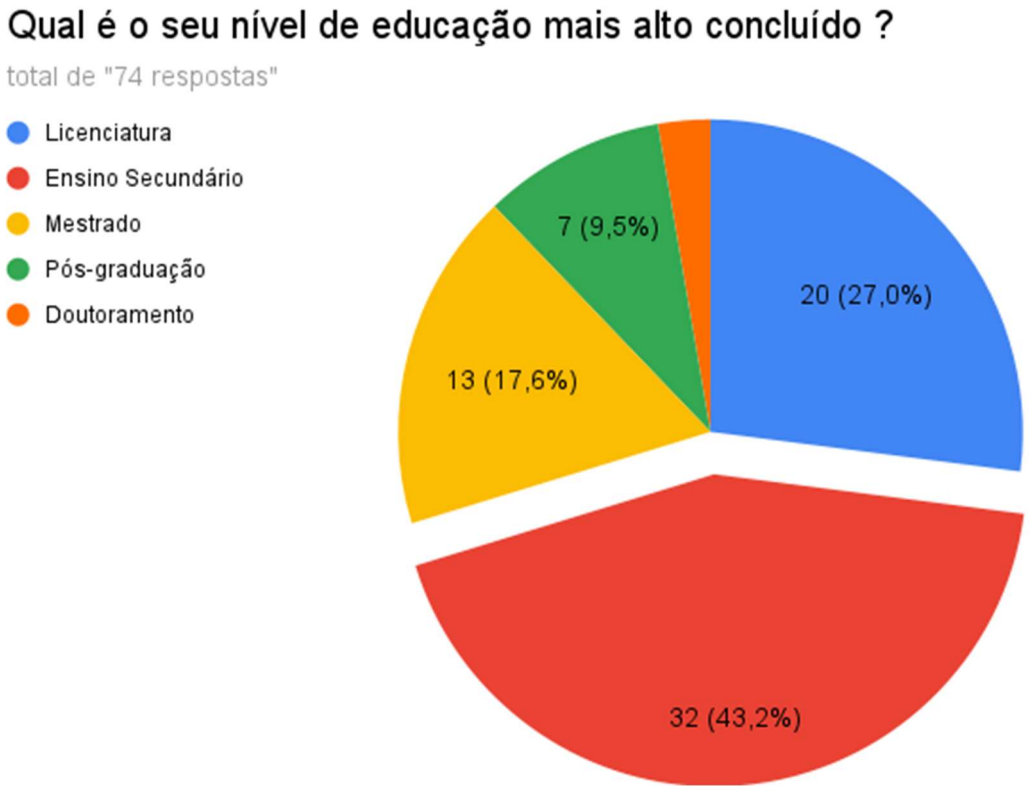
Implicações:

- **Perfil da Amostra:** A amostra é predominantemente composta por indivíduos de meia-idade, com um forte agrupamento nas faixas dos 35 aos 64 anos. Os jovens adultos (18-34 anos) e os idosos (65 anos ou mais) estão sub-representados.
- **Viés da Amostra:** Dependendo do objetivo do estudo, esta distribuição etária pode introduzir um viés. Se a investigação pretende ser representativa da população geral ou de faixas etárias específicas (como jovens ou idosos), a metodologia de amostragem pode precisar ser ajustada em estudos futuros para garantir uma representação mais equilibrada ou direcionada.
- **Contexto da Investigação:** A concentração em faixas etárias mais maduras pode ser apropriada se a investigação estiver focada em temas relevantes para esse grupo demográfico (e.g., carreira, família, questões de saúde em idade adulta).

Em resumo, o gráfico demonstra que a maioria dos participantes na investigação situa-se nas faixas etárias intermediárias (35-64 anos), com uma notável concentração entre os 35 e 54 anos, enquanto os grupos mais jovens e mais velhos são significativamente menos representados.

A Figura 4, apresenta a distribuição do nível de educação dos participantes do questionário.

Figura 4 - Nível de educação dos inquiridos



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

Análise do Gráfico de Nível de Educação Mais Alto Concluído

O gráfico de setores em análise apresenta a distribuição do nível de educação mais alto concluído por 74 inquiridos, conforme indicado pelo título "Qual é o seu nível de educação mais alto concluído?" e o subtítulo "74 respostas". As categorias de nível de educação são as seguintes, com suas respetivas representações visuais:

Tabela 4 - Nível de Escolaridade

Nível de Escolaridade	Cor Representada
Ensino Básico	Azul
Ensino Secundário	Vermelho/Laranja-escuro
Licenciatura	Laranja
Pós-graduação	Verde
Mestrado	Roxo
Doutoramento	Azul-claro/Ciano
Outro	Rosa/Magenta

Fonte: Autor

Principais Observações:

1. **Ensino Secundário como Nível Mais Comum:** A categoria de **Ensino Secundário** é, de longe, a mais prevalente entre os inquiridos, representando **43,2%** do total. Isso indica que quase metade dos participantes concluiu o ensino secundário como seu nível mais alto de escolaridade.
2. **Licenciatura em Segundo Lugar:** A **Licenciatura** é o segundo nível de educação mais comum, correspondendo a **27%** dos inquiridos. Juntas, as categorias de Ensino Secundário e Licenciatura somam 70,2% (43,2% + 27%), o que significa que mais de dois terços da amostra possui um desses dois níveis de escolaridade como o mais alto.
3. **Mestrado com Proporção Significativa:** O nível de **Mestrado** representa uma parcela notável de **17,6%** dos inquiridos.

4. **Pós-graduação:** A **Pós-graduação** (sem especificação de mestrado ou doutoramento) foi concluída por **9,5%** dos participantes. É importante notar que esta categoria pode, por vezes, sobrepor-se ou ser interpretada de forma diferente em relação ao Mestrado/Doutoramento, dependendo da definição utilizada na investigação.
5. **Níveis Menos Representados:**
    - O **Ensino Básico** (azul) é visualmente uma fatia muito pequena, o que sugere um percentual muito baixo de inquiridos com este como seu nível mais alto de educação.
    - O **Doutoramento** (azul-claro/ciano) também é uma fatia extremamente pequena, quase impercetível, indicando uma representação muito baixa.
    - A categoria **"Outro"** (rosa/magenta) não é visível no gráfico, o que implica que nenhum inquirido selecionou essa opção ou que o percentual é tão insignificante que não aparece.

Implicações:

- **Perfil Educacional da Amostra:** A amostra apresenta um perfil educacional maioritariamente de nível secundário e superior (licenciatura e mestrado), com menor representatividade de níveis básicos ou de doutoramento. Isso pode ser relevante para a interpretação dos resultados do estudo, especialmente se a escolaridade for um fator influente nas variáveis em análise.
- **Acessibilidade da Investigação:** A predominância de níveis de escolaridade mais altos pode indicar que a investigação foi mais acessível ou de maior interesse para indivíduos com Ensino Secundário ou superior, ou que a população-alvo do estudo se enquadra predominantemente nesses níveis educacionais.
- **Limitações:** A falta de percentagens explícitas para as categorias "Ensino Básico", "Doutoramento" e "Outro" impede uma análise quantitativa precisa dessas parcelas, embora visualmente se saiba que são muito pequenas.

Em síntese, o gráfico demonstra que a maioria dos 74 inquiridos possui Ensino Secundário ou Licenciatura como seu nível de educação mais alto concluído, seguido por Mestrado e Pós-

graduação, com níveis de escolaridade básicos e de doutoramento sendo muito menos comuns na amostra.

A Figura 5, apresenta a distribuição da área profissional dos participantes do questionário.

Figura 5 - Área profissional dos inquiridos

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

Análise do Gráfico de Área de Atuação Profissional

O gráfico de setores em questão ilustra a distribuição das áreas de atuação profissional dos 74 inquiridos, conforme indicado pelo título "Em qual área você atua profissionalmente?" e o subtítulo "74 respostas". As categorias de área profissional, com suas respetivas representações visuais, são:

Tabela 5 - Categorias de Área Profissional

Setor Profissional	**Cor Representada**
Tecnologias da Informação e da Comunicação (TIC)	Azul
Serviços Públicos ou Administração	Vermelho/Laranja-escuro
Recursos Humanos	Laranja
Negócios ou Consultadoria	Verde
Outro	Roxo

Fonte: Autor

Principais Observações:

1. **Serviços Públicos ou Administração Dominante:** A área de **Serviços públicos ou Administração** é a mais prevalente, compreendendo **44,6%** dos inquiridos. Isso significa que quase metade da amostra atua nesse setor.
2. **"Outro" como Segundo Maior Grupo:** A categoria **"Outro"** surpreendentemente representa a segunda maior fatia, com **37,8%** dos respondentes. A alta percentagem nesta categoria genérica sugere que uma parcela significativa da amostra atua em áreas não especificadas pelas opções listadas. Isso pode indicar que as categorias predefinidas não cobriram adequadamente todas as áreas de atuação dos participantes.
3. **Tecnologias da Informação e da Comunicação:** A área de **Tecnologias da Informação e da Comunicação (TIC)** responde por **10,8%** da amostra.
4. **Menos representados:** As categorias **Recursos Humanos** (laranja) e **Negócios ou consultadoria** (verde) são visualmente muito pequenas, indicando percentagens muito baixas de inquiridos. Sem os valores exatos para estas categorias, não é possível quantificar sua proporção precisa, mas são claramente minoritárias.

Implicações:

- **Concentração Setorial:** A amostra é fortemente concentrada nos setores de Serviços Públicos/Administração e numa variedade de outras áreas não especificadas. Isso pode influenciar os resultados de qualquer investigação que dependa da experiência ou perspetiva profissional dos participantes.
- **Abrangência das Categorias:** A grande proporção na categoria "Outro" levanta uma questão sobre a exaustividade das opções de resposta fornecidas. Para futuras investigações, seria benéfico rever e expandir as categorias de área de atuação profissional para capturar uma gama mais precisa das ocupações dos inquiridos, ou, pelo menos, permitir que os inquiridos especifiquem a sua área quando escolhem "Outro".
- **Contexto do Estudo:** Se o estudo visa a uma visão geral de diversos setores, a alta concentração pode limitar a generalização dos resultados. Se, no entanto, o foco é precisamente em Serviços Públicos/Administração, então a amostra é bastante adequada para esse propósito.

Em suma, o gráfico revela que a maioria dos 74 inquiridos atua em **Serviços públicos ou Administração**, seguido por uma grande variedade de outras áreas que não foram especificamente categorizadas. O setor de Tecnologias da Informação e da Comunicação tem uma representação menor, e outras áreas como Recursos Humanos e Negócios/Consultadoria são pouco representadas na amostra.

5.2 Avaliar o conhecimento atual: medir o nível de conhecimento dos utilizadores sobre ciberataques baseados em IA.

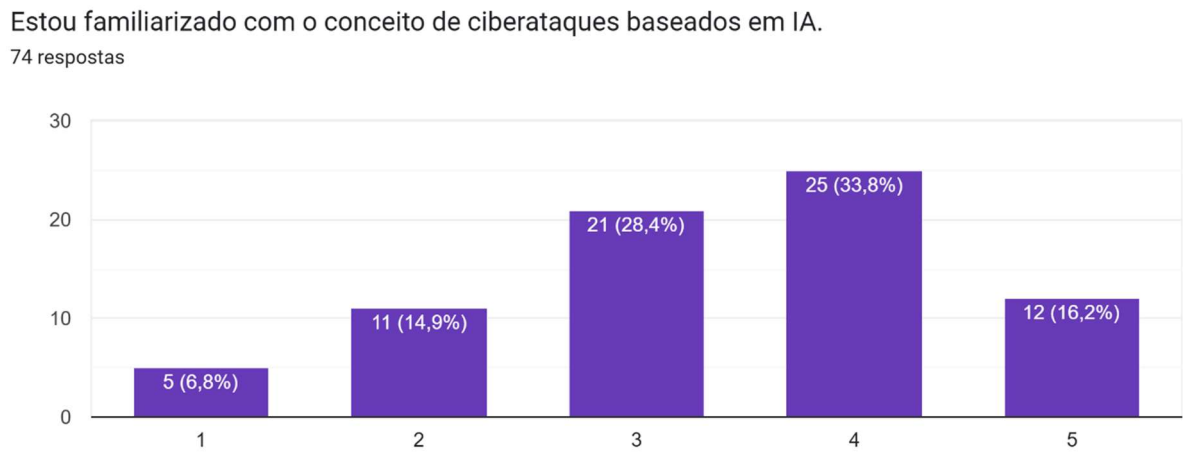
A rápida evolução da Inteligência Artificial (IA) tem proporcionado avanços significativos em diversas áreas, desde a automação de processos até a personalização de serviços digitais. No entanto, esse progresso também tem sido acompanhado por um aumento nas ameaças cibernéticas que exploram as capacidades da IA para fins maliciosos. Ciberataques baseados em IA representam uma nova geração de riscos digitais, caracterizados por sua sofisticação, adaptabilidade e potencial de causar danos em larga escala.

Diante desse cenário, torna-se essencial compreender o nível de conhecimento que os utilizadores possuem sobre esse tipo específico de ameaça. A familiaridade com os mecanismos, impactos e formas de prevenção desses ataques é um fator determinante para a eficácia das estratégias de cibersegurança, tanto no âmbito individual quanto organizacional.

Este subcapítulo tem como objetivo principal avaliar o conhecimento atual dos utilizadores sobre ciberataques baseados em IA. Através da análise de dados recolhidos por meio de questionário, pretende-se identificar o grau de familiaridade dos participantes com o tema, bem como possíveis lacunas de conhecimento que possam comprometer a sua segurança digital. Os resultados obtidos servirão de base para recomendações futuras em termos de formação, sensibilização e desenvolvimento de políticas de proteção cibernética.

A Figura 6, apresenta a familiarização com o conceito de ciberataques baseados em IA por parte dos participantes do questionário.

Figura 6 - Familiarização com o conceito de ciberataques baseados em IA por parte dos inquiridos



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

Este gráfico de barras apresenta os resultados de uma investigação sobre a familiaridade dos participantes com o conceito de ciberataques baseados em IA. A pergunta específica que os

participantes avaliaram é "Estou familiarizado com o conceito de ciberataques baseados em IA.", com um total de 74 respostas.

Com a escala fornecida:

- **1 (Discordo totalmente):** Implica que a pessoa discorda totalmente da afirmação "Estou familiarizado...", ou seja, não está nada familiarizada.
- **2 (Discordo):** Implica que a pessoa discorda da afirmação, indicando pouca familiaridade.
- **3 (Neutro):** Implica uma posição neutra, possivelmente uma familiaridade moderada ou incerta.
- **4 (Concordo):** Implica que a pessoa concorda com a afirmação, indicando boa familiaridade.
- **5 (Concordo totalmente):** Implica que a pessoa concorda totalmente com a afirmação, indicando muita familiaridade.

Análise dos Resultados com a Escala Fornecida:

- **1 (Discordo totalmente - Nada familiarizado):** 5 respostas (6,8%). Uma pequena percentagem dos respondentes indica que não está familiarizada com o conceito.
- **2 (Discordo - Pouca familiaridade):** 11 respostas (14,9%). Este grupo, embora maior que o anterior, ainda demonstra pouca familiaridade.
- **3 (Neutro - Familiaridade moderada/incerta):** 21 respostas (28,4%). Quase um terço dos participantes tem uma familiaridade moderada ou está numa posição neutra em relação à sua familiaridade.
- **4 (Concordo - Boa familiaridade):** 25 respostas (33,8%). Esta é a categoria com maior número de respostas, indicando que a maioria dos respondentes concorda que está familiarizada com o conceito.
- **5 (Concordo totalmente - Muita familiaridade):** 12 respostas (16,2%). Um número significativo de participantes concorda totalmente que está muito familiarizada.

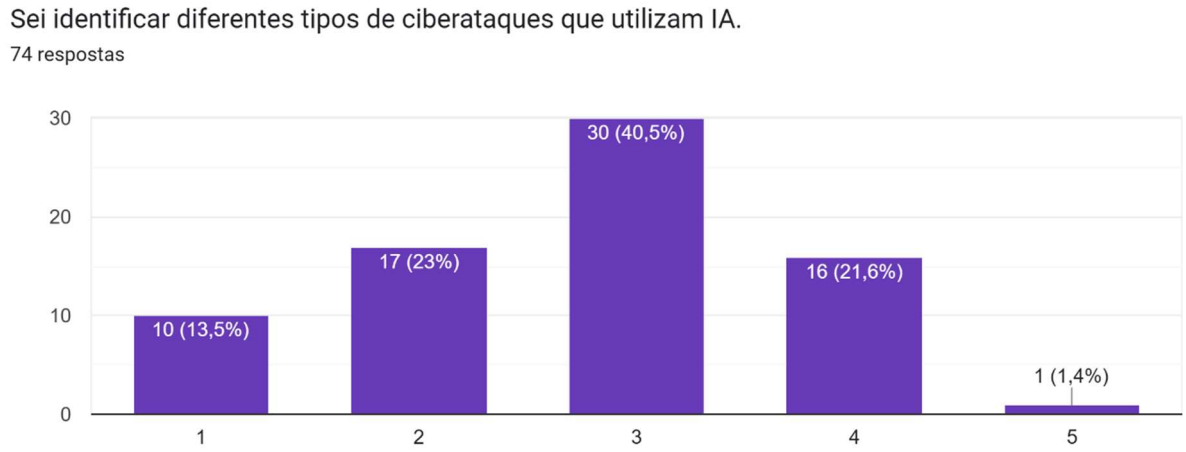
Conclusões Principais:

- **Familiaridade Predominante:** A maioria dos respondentes concorda (nível 4) ou concorda totalmente (nível 5) com a afirmação de que estão familiarizados com o conceito de ciberataques baseados em IA. Juntos, estes dois grupos representam 33,8% + 16,2% = **50%** dos participantes.
- **Conhecimento Considerável:** Se incluirmos os que estão numa posição neutra (nível 3), que podem ter uma familiaridade moderada, a percentagem de pessoas com algum grau de familiaridade (níveis 3, 4 e 5) ascende a 28,4% + 33,8% + 16,2% = **78,4%**.
- **Baixo Nível de Desconhecimento:** Apenas uma minoria dos participantes discorda (nível 2) ou discorda totalmente (nível 1) da sua familiaridade, somando 14,9% + 6,8% = **21,7%**.

Em resumo, a análise do gráfico com a escala de concordância revela que uma parte significativa da audiência investigada já possui um bom nível de familiaridade com o conceito de ciberataques baseados em IA. Há uma clara inclinação para a concordância com a afirmação, sugerindo que o tópico não é totalmente desconhecido para a maioria.

A Figura 7, apresenta a capacidade de identificação de ciberataques Baseados em IA por parte dos participantes do questionário.

Figura 7 - Capacidade de Identificação de Ciberataques Baseados em IA



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

Este gráfico de barras ilustra os resultados de uma investigação que avaliou a capacidade dos participantes em identificar diferentes tipos de ciberataques que utilizam IA. A questão específica avaliada foi "Sei identificar diferentes tipos de ciberataques que utilizam IA.", com um total de 74 respostas.

Utilizando a escala de concordância fornecida:

- **1 (Discordo totalmente):** A pessoa discorda completamente da afirmação, indicando que não consegue identificar os diferentes tipos de ciberataques que utilizam IA.
- **2 (Discordo):** A pessoa discorda da afirmação, sugerindo que tem pouca capacidade de identificação.
- **3 (Neutro):** A pessoa está numa posição neutra, possivelmente com uma capacidade moderada ou incerta de identificação.

- **4 (Concordo):** A pessoa concorda com a afirmação, indicando que é capaz de identificar bem diferentes tipos de ciberataques que utilizam IA.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação, sugerindo que é plenamente capaz de identificar esses ataques.

Análise dos Resultados com a Escala Fornecida:

- **1 (Discordo totalmente - Incapacidade de identificar):** 10 respostas (13,5%). Uma parcela dos respondentes sente-se incapaz de identificar os tipos de ataques.
- **2 (Discordo - Pouca capacidade de identificar):** 17 respostas (23,0%). Um grupo maior que o anterior, mas que ainda indica pouca capacidade.
- **3 (Neutro - Capacidade moderada/incerta):** 30 respostas (40,5%). Esta é a categoria mais expressiva, mostrando que a maioria dos participantes tem uma capacidade moderada ou incerta para identificar esses ataques.
- **4 (Concordo - Boa capacidade de identificar):** 16 respostas (21,6%). Um número considerável de respondentes concorda que tem uma boa capacidade.
- **5 (Concordo totalmente - Plenamente capaz de identificar):** 1 resposta (1,4%). Apenas um participante se sente plenamente capaz de identificar os diferentes tipos de ciberataques que utilizam IA.

Conclusões Principais:

- **Maioria com Capacidade Limitada/Moderada:** A maior concentração de respostas está na categoria "Neutro" (40,5%), o que sugere que a maioria dos participantes tem apenas uma capacidade moderada ou incerta de identificar os diferentes tipos de ciberataques baseados em IA.
- **Lacuna de Conhecimento Específico:** Embora a familiaridade geral com o conceito de ciberataques baseados em IA (em gráficos anteriores) fosse alta, este gráfico revela uma lacuna no conhecimento mais aprofundado e na capacidade de identificação

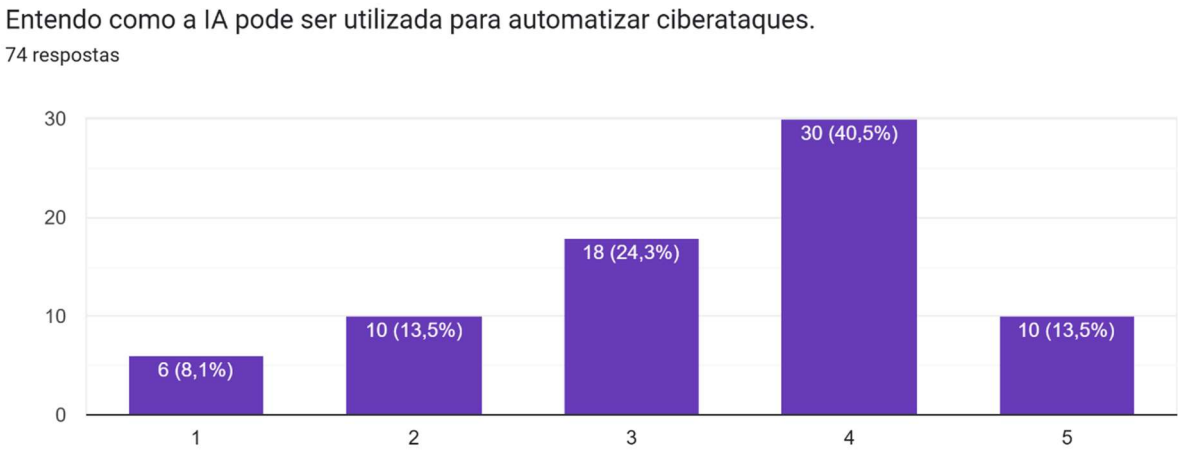
detalhada. Apenas 21,6% (Concordo) e 1,4% (Concordo totalmente) se sentem seguros na identificação, totalizando **23%**.

- **Necessidade de Formação/Informação:** Um número significativo de participantes discorda ou discorda totalmente da sua capacidade de identificação (13,5% + 23% = **36,5%**). Isso aponta para uma necessidade de mais formação ou informação específica sobre as tipologias de ciberataques que utilizam IA.
- **Poucos Especialistas:** O facto de apenas uma pessoa (1,4%) se sentir plenamente capaz de identificar esses ataques destaca a escassez de conhecimento especializado detalhado na amostra.

Em síntese, o gráfico indica que, apesar de uma possível familiaridade geral com a temática, a capacidade específica de identificar e diferenciar os vários tipos de ciberataques que utilizam IA é uma área onde a maioria dos participantes ainda tem uma capacidade moderada a limitada, e há poucos indivíduos que se consideram especialistas.

A Figura 8, apresenta a Perceção dos Utilizadores sobre o Uso da IA em Ciberataques Automatizados

Figura 8 - Perceção sobre o Uso da IA em Ciberataques Automatizados por parte dos inquiridos



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

Este gráfico de barras apresenta os resultados de uma investigação que avaliou o entendimento dos participantes sobre como a Inteligência Artificial (IA) pode ser utilizada para automatizar ciberataques. A pergunta avaliada foi "Entendo como a IA pode ser utilizada para automatizar ciberataques.", com um total de 74 respostas.

Utilizando a escala de concordância fornecida:

- **1 (Discordo totalmente):** A pessoa discorda completamente da afirmação, indicando que não entende como a IA pode automatizar ciberataques.
- **2 (Discordo):** A pessoa discorda da afirmação, sugerindo que tem pouco entendimento.
- **3 (Neutro):** A pessoa está numa posição neutra, possivelmente com um entendimento moderado ou incerto.
- **4 (Concordo):** A pessoa concorda com a afirmação, indicando que entende bem como a IA pode automatizar ciberataques.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação, sugerindo que tem um entendimento muito aprofundado.

Análise dos Resultados com a Escala Fornecida:

- **1 (Discordo totalmente - Não entende):** 6 respostas (8,1%). Uma pequena parcela dos respondentes não entende como a IA pode ser usada para automatizar ciberataques.
- **2 (Discordo - Pouco entendimento):** 10 respostas (13,5%). Este grupo, um pouco maior, indica ter pouco entendimento.
- **3 (Neutro - Entendimento moderado/incerto):** 18 respostas (24,3%). Quase um quarto dos participantes está numa posição neutra, possivelmente com um entendimento razoável, mas não profundo.
- **4 (Concordo - Bom entendimento):** 30 respostas (40,5%). Esta é a categoria mais populosa, indicando que a maioria dos respondentes concorda que entende bem como a IA pode automatizar ciberataques.

- **5 (Concordo totalmente - Entendimento muito aprofundado):** 10 respostas (13,5%). Um número considerável de participantes concorda totalmente, indicando um entendimento aprofundado.

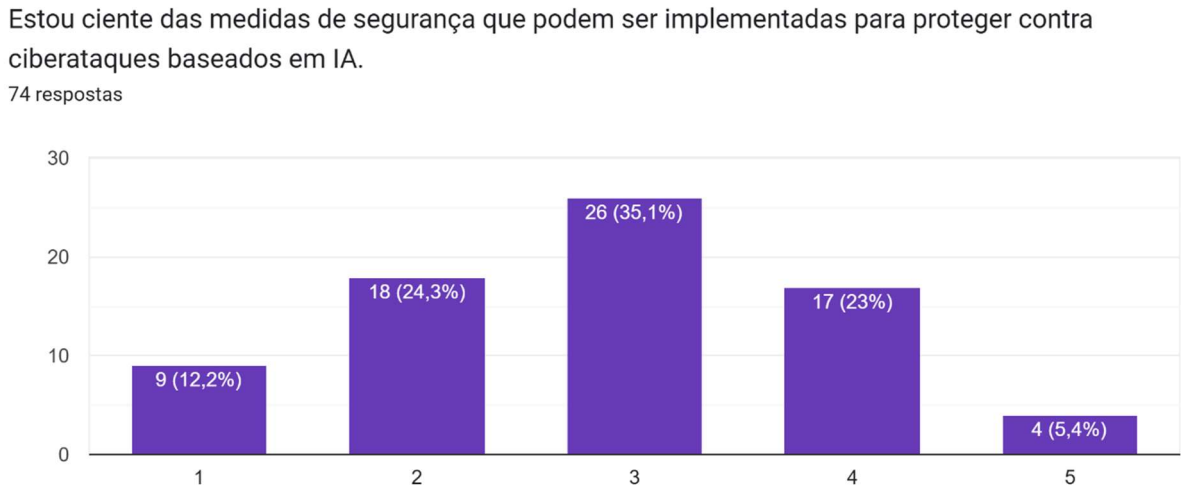
Conclusões Principais:

- **Entendimento Predominante:** A maioria dos participantes (somando as categorias 4 e 5) concorda ou concorda totalmente com a afirmação de que entendem como a IA pode automatizar ciberataques. Juntos, estes grupos representam 40,5% + 13,5% = **54%** dos respondentes.
- **Entendimento Geralmente Bom:** Incluindo aqueles que estão na categoria "Neutro" (que podem ter um entendimento moderado), 24,3% + 40,5% + 13,5% = **78,3%** dos participantes demonstram algum nível de entendimento sobre o tema.
- **Menos Desconhecimento:** A percentagem de pessoas que discorda ou discorda totalmente (níveis 1 e 2) é de 8,1% + 13,5% = **21,6%**, o que é uma minoria significativa, mas indica que a maioria tem pelo menos alguma compreensão.

Em síntese, o gráfico sugere que uma parte considerável da audiência investigadada tem um bom a excelente entendimento sobre como a Inteligência Artificial pode ser utilizada para automatizar ciberataques. A maior concentração de respostas nas categorias de concordância indica que este conceito é relativamente bem compreendido entre os participantes.

A Figura 9, apresenta a Perceção dos inquiridos sobre Medidas de Proteção contra Ciberataques com IA

Figura 9 - Perceção dos Inquiridos sobre Medidas de Proteção contra Ciberataques com IA



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

Este gráfico de barras exibe os resultados de uma investigação que avaliou o conhecimento dos participantes sobre as medidas de segurança contra ciberataques baseados em IA. A pergunta específica era "Estou ciente das medidas de segurança que podem ser implementadas para proteger contra ciberataques baseados em IA.", com um total de 74 respostas.

Utilizando a escala de concordância fornecida:

- **1 (Discordo totalmente):** A pessoa discorda completamente da afirmação, indicando que não está ciente de nenhuma medida de segurança.
- **2 (Discordo):** A pessoa discorda da afirmação, sugerindo que tem pouca ou nenhuma ciência das medidas de segurança.
- **3 (Neutro):** A pessoa está numa posição neutra, possivelmente com uma consciência moderada das medidas de segurança ou incerta.

- **4 (Concordo):** A pessoa concorda com a afirmação, indicando que está bem ciente das medidas de segurança.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação, sugerindo que está muito ciente e informada sobre as medidas de segurança.

Análise dos Resultados com a Escala Fornecida:

- **1 (Discordo totalmente - Sem ciência):** 9 respostas (12,2%). Uma parcela significativa dos respondentes não está ciente das medidas de segurança.
- **2 (Discordo - Pouca ciência):** 18 respostas (24,3%). Este grupo é o segundo maior e indica que tem pouca consciência das medidas de segurança.
- **3 (Neutro - Consciência moderada/incerta):** 26 respostas (35,1%). Esta é a categoria mais numerosa, sugerindo que a maioria dos participantes tem uma consciência moderada ou está em uma posição neutra em relação ao seu conhecimento sobre as medidas de segurança.
- **4 (Concordo - Boa ciência):** 17 respostas (23,0%). Um número considerável de respondentes concorda que está ciente das medidas de segurança.
- **5 (Concordo totalmente - Muito ciente):** 4 respostas (5,4%). Poucos participantes se consideram muito cientes das medidas de segurança.

Conclusões Principais:

- **Preocupação com a Consciencialização:** A maior parte dos respondentes se encontra nas categorias de "Neutro" (35,1%) ou "Discordo" (24,3% + 12,2% = 36,5%). Isso significa que **mais de 70%** dos participantes (35,1% + 36,5% = 71,6%) têm uma consciência moderada, pouca ou nenhuma consciência das medidas de segurança contra ciberataques baseados em IA.
- **Lacuna no Conhecimento de Proteção:** Embora em gráficos anteriores houvesse alguma familiaridade e entendimento sobre os ciberataques de IA, este gráfico revela uma lacuna notável no conhecimento sobre como se proteger deles. Apenas **28,4%**

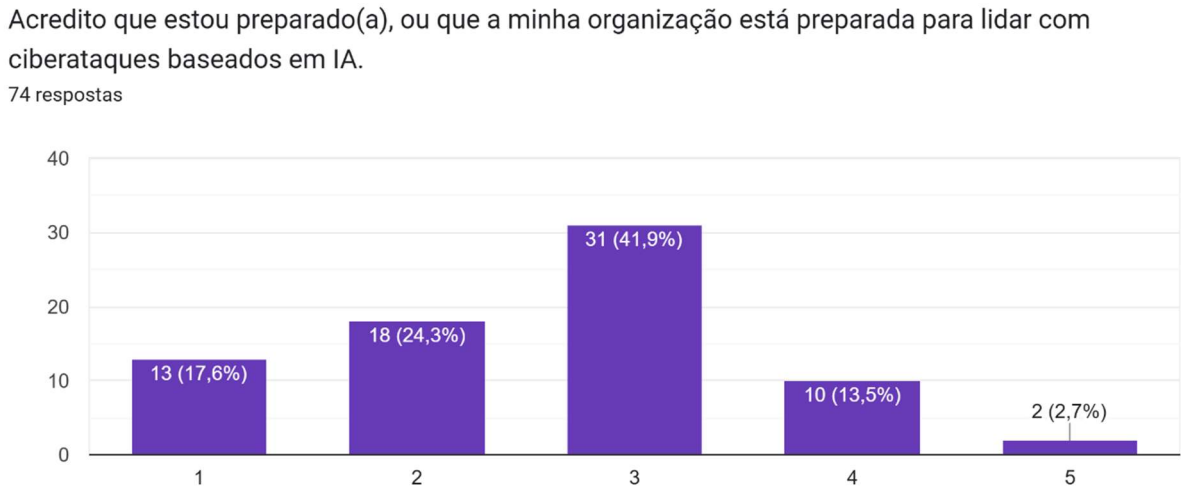
(23,0% + 5,4%) dos respondentes concordam ou concordam totalmente que estão cientes das medidas de segurança.

- **Necessidade Urgente de Educação/Treinamento:** Os resultados indicam uma forte necessidade de programas de educação e consciencialização sobre medidas de segurança específicas para combater ciberataques baseados em IA. Há uma clara deficiência no conhecimento prático de proteção.
- **Poucos Especialistas em Defesa:** O número muito baixo de respondentes na categoria 5 (5,4%) reforça que poucas pessoas se consideram especialistas ou muito bem informadas sobre as estratégias de defesa.

Em síntese, o gráfico sublinha uma deficiência significativa no conhecimento sobre as medidas de segurança para proteger contra ciberataques baseados em IA. A maioria dos participantes não se sente plenamente informada sobre como se defender, o que destaca uma área crítica para intervenção e educação.

A Figura 10, apresenta a Preparação Individual e Organizacional frente a Ciberataques com IA

Figura 10 - Preparação Individual e Organizacional frente a Ciberataques com IA



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

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a perceção dos participantes sobre a sua preparação (ou da sua organização) para lidar com ciberataques baseados em IA. A pergunta específica foi "Acredito que estou preparado(a), ou que a minha organização está preparada para lidar com ciberataques baseados em IA.", com um total de 74 respostas.

Utilizando a escala de concordância fornecida:

- **1 (Discordo totalmente):** A pessoa discorda completamente da afirmação, indicando que não se sente preparada, nem a sua organização.
- **2 (Discordo):** A pessoa discorda da afirmação, sugerindo pouca preparação.
- **3 (Neutro):** A pessoa está numa posição neutra, possivelmente com uma preparação moderada, ou incerta sobre a sua preparação/da organização.
- **4 (Concordo):** A pessoa concorda com a afirmação, indicando que se sente bem preparada, ou que a sua organização está.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação, sugerindo que se sente muito bem preparada, ou que a sua organização está.

Análise dos Resultados com a Escala Fornecida:

- **1 (Discordo totalmente - Não preparado):** 13 respostas (17,6%). Uma parte significativa dos respondentes sente que não está preparada.
- **2 (Discordo - Pouco preparado):** 18 respostas (24,3%). Este grupo, o segundo maior, também indica pouca preparação.
- **3 (Neutro - Moderadamente preparado/Incerteza):** 31 respostas (41,9%). Esta é a categoria mais numerosa, representando a maioria dos respondentes. Sugere que muitos estão numa posição de incerteza ou percebem uma preparação apenas moderada.
- **4 (Concordo - Bem preparado):** 10 respostas (13,5%). Um número relativamente pequeno de respondentes sente-se ou vê a sua organização como bem preparada.

- **5 (Concordo totalmente - Muito bem preparado):** 2 respostas (2,7%). Apenas uma minoria se sente ou vê a sua organização como muito bem preparada.

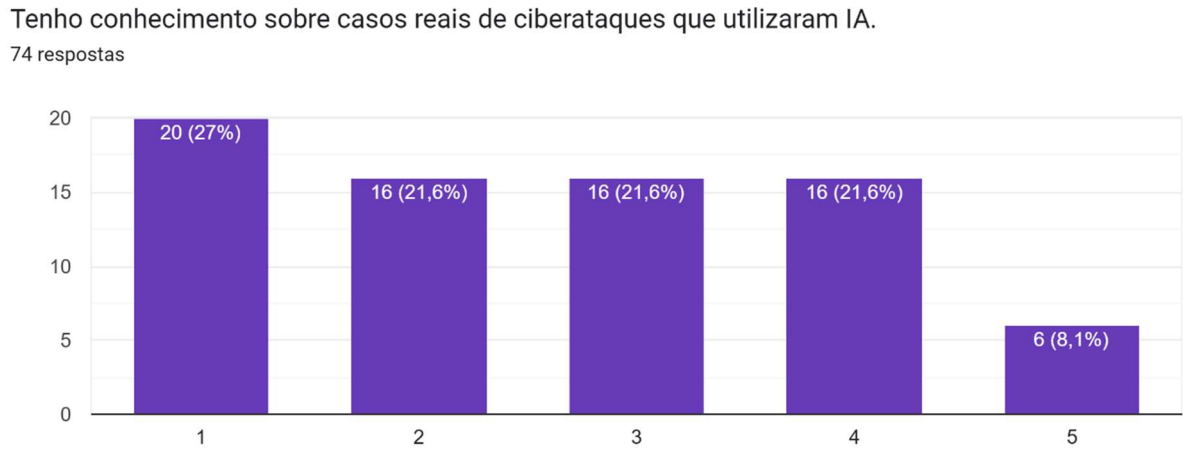
Conclusões Principais:

- **Preocupação com a Preparação:** A soma das categorias que indicam pouca ou nenhuma preparação (Discordo totalmente e Discordo) é de 17,6% + 24,3% = **41,9%**. Este é um valor substancial, igual à categoria mais alta (Neutro), e indica que uma grande parte dos respondentes não se sente preparada.
- **Incerteza ou Preparação Moderada Prevalente:** A maior parte dos respondentes (41,9%) encontra-se na categoria "Neutro", o que sugere que muitos não têm uma convicção forte sobre a sua preparação ou a da sua organização, ou consideram que esta é apenas moderada.
- **Pouca Confiança na Preparação:** Apenas uma minoria dos respondentes (13,5% + 2,7% = **16,2%**) concorda ou concorda totalmente que estão preparados para lidar com ciberataques baseados em IA.
- **Lacuna entre Conhecimento e Prontidão:** Comparando com gráficos anteriores, onde havia alguma familiaridade e entendimento sobre os ciberataques de IA, este gráfico mostra uma grande desconexão entre o conhecimento teórico e a perceção de prontidão prática para lidar com eles. Parece que o conhecimento existente não se traduz em confiança na capacidade de resposta.
- **Necessidade Urgente de Melhorar a Preparação:** Os resultados indicam uma necessidade crítica de fortalecer as defesas e a preparação, tanto a nível individual quanto organizacional, para enfrentar as ameaças de ciberataques baseados em IA.

Em suma, o gráfico revela que a grande maioria dos participantes não se sente totalmente preparada, ou tem dúvidas sobre a sua preparação/da sua organização, para lidar com ciberataques baseados em IA. Há uma clara necessidade de investimentos em medidas de segurança, formação e estratégias de resposta para aumentar a confiança e a resiliência contra estas ameaças.

A Figura 11, apresenta o Nível de Conhecimento sobre Incidentes Reais de Ciberataques Baseados em IA por parte dos inquiridos

Figura 11 - Nível de Conhecimento sobre Incidentes Reais de Ciberataques Baseados em IA



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

Este gráfico de barras apresenta os resultados de uma investigação que avaliou o conhecimento dos participantes sobre casos reais de ciberataques que utilizaram IA. A pergunta específica foi "Tenho conhecimento sobre casos reais de ciberataques que utilizaram IA.", com um total de 74 respostas.

Utilizando a escala de concordância fornecida:

- **1 (Discordo totalmente):** A pessoa discorda completamente da afirmação, indicando que não tem conhecimento sobre casos reais.
- **2 (Discordo):** A pessoa discorda da afirmação, sugerindo que tem pouco ou nenhum conhecimento sobre casos reais.
- **3 (Neutro):** A pessoa está numa posição neutra, possivelmente com um conhecimento moderado ou incerto sobre casos reais.

- **4 (Concordo):** A pessoa concorda com a afirmação, indicando que tem um bom conhecimento sobre casos reais.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação, sugerindo que tem um conhecimento muito aprofundado e abrangente sobre casos reais.

Análise dos Resultados com a Escala Fornecida:

- **1 (Discordo totalmente - Sem conhecimento):** 20 respostas (27%). Este é o maior grupo, indicando que uma parte significativa dos respondentes não tem conhecimento sobre casos reais de ciberataques que utilizaram IA.
- **2 (Discordo - Pouco conhecimento):** 16 respostas (21,6%). Este grupo, também considerável, indica pouco conhecimento.
- **3 (Neutro - Conhecimento moderado/incerto):** 16 respostas (21,6%). Este grupo tem a mesma dimensão que o anterior, indicando uma posição neutra ou conhecimento moderado.
- **4 (Concordo - Bom conhecimento):** 16 respostas (21,6%). Curiosamente, este grupo também tem o mesmo número de respostas, mostrando que um número igual de pessoas concorda que tem um bom conhecimento.
- **5 (Concordo totalmente - Muito conhecimento):** 6 respostas (8,1%). Uma pequena minoria se considera muito conhecedora de casos reais.

Conclusões Principais:

- **Divisão no Conhecimento:** Há uma divisão quase equitativa entre os que têm pouco ou nenhum conhecimento (1 e 2 somam 27% + 21,6% = **48,6%**) e os que têm algum conhecimento (3 e 4 somam 21,6% + 21,6% = **43,2%**).
- **Desconhecimento de Casos Reais Prevalente:** O maior grupo (27%) discorda totalmente, sugerindo que a falta de conhecimento sobre casos reais é um problema significativo. Somando os que discordam totalmente e os que discordam, quase metade

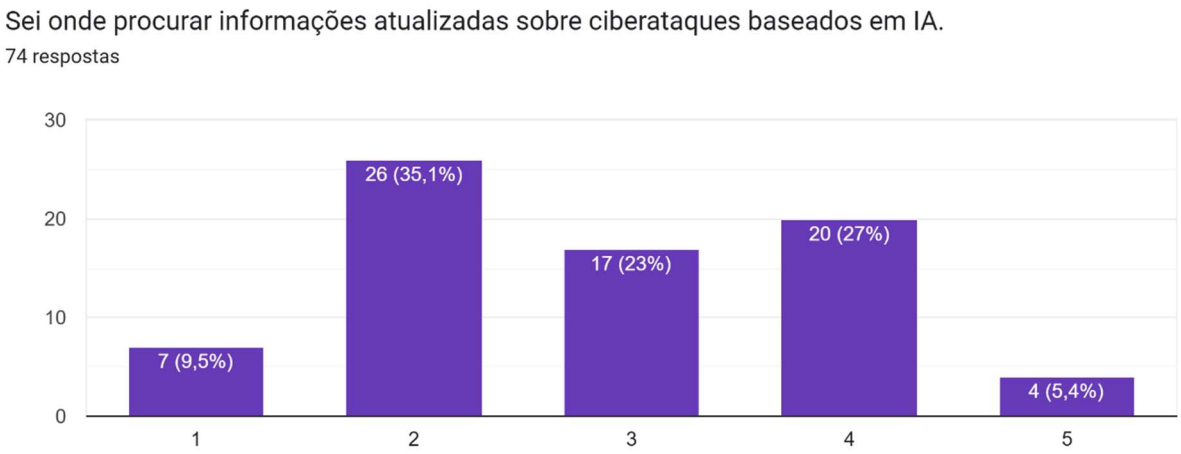
dos respondentes (48,6%) não possui conhecimento de casos reais ou possui muito pouco.

- **Baixo Número de Especialistas:** Apenas 8,1% dos respondentes concordam totalmente que têm conhecimento sobre casos reais, indicando que o número de especialistas ou de pessoas bem informadas sobre incidentes reais envolvendo IA em ciberataques é muito baixo.
- **Contraste com a Familiaridade Geral:** Embora gráficos anteriores pudessem indicar uma familiaridade com o conceito de ciberataques baseados em IA, este gráfico sugere que essa familiaridade não se traduz necessariamente em conhecimento de exemplos concretos e casos reais.

Em suma, o gráfico revela que a maioria dos participantes tem pouco ou nenhum conhecimento prático sobre casos reais de ciberataques que utilizaram IA. Isso pode indicar uma carência na divulgação de informações sobre incidentes concretos ou uma dificuldade em reconhecer a aplicação de IA em ataques já conhecidos. Esta lacuna no conhecimento empírico pode impactar a perceção da ameaça e a urgência na implementação de medidas de proteção.

A Figura 12, apresenta a Capacidade de Localizar Informações Atualizadas sobre Ciberataques com IA por parte dos inquiridos

Figura 12 - Capacidade de Localizar Informações Atualizadas sobre Ciberataques com IA



Fonte: Dados do questionário da pergunta n.º 11 (Anexo I)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a capacidade dos participantes de saber onde procurar informações atualizadas sobre ciberataques baseados em IA. A pergunta específica foi "Sei onde procurar informações atualizadas sobre ciberataques baseados em IA.", com um total de 74 respostas.

Utilizando a escala de concordância fornecida:

- **1 (Discordo totalmente):** A pessoa discorda completamente da afirmação, indicando que não sabe de todo onde procurar informações atualizadas.
- **2 (Discordo):** A pessoa discorda da afirmação, sugerindo que tem pouca ideia de onde procurar informações.
- **3 (Neutro):** A pessoa está numa posição neutra, possivelmente com alguma ideia, mas não uma clareza total, ou um conhecimento moderado das fontes.
- **4 (Concordo):** A pessoa concorda com a afirmação, indicando que sabe bem onde procurar informações atualizadas.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação, sugerindo que sabe muito bem e confia nas suas fontes de informação.

Análise dos Resultados com a Escala Fornecida:

- **1 (Discordo totalmente - Não sei procurar):** 7 respostas (9,5%). Uma minoria dos respondentes não sabe onde procurar informações.
- **2 (Discordo - Pouca ideia de onde procurar):** 26 respostas (35,1%). Este é o maior grupo, indicando que uma parte significativa dos respondentes tem pouca ou nenhuma ideia de onde procurar informações atualizadas.
- **3 (Neutro - Alguma ideia/incerteza):** 17 respostas (23%). Um quarto dos participantes está numa posição neutra, com uma perceção moderada sobre o conhecimento de fontes.
- **4 (Concordo - Sei procurar bem):** 20 respostas (27%). Um número considerável de respondentes concorda que sabe onde procurar informações.

- **5 (Concordo totalmente - Sei muito bem procurar):** 4 respostas (5,4%). Uma pequena minoria se considera muito informada sobre as fontes de informação.

Conclusões Principais:

- **Dificuldade em Encontrar Fontes Atualizadas:** A maior parte dos respondentes (somando as categorias 1 e 2) Discorda totalmente ou Discorda da afirmação, o que significa que **44,6%** (9,5% + 35,1%) dos participantes não sabem ou têm dificuldade em saber onde procurar informações atualizadas sobre ciberataques baseados em IA.
- **Conhecimento Moderado de Fontes:** A categoria "Neutro" (23%) indica que quase um quarto dos respondentes tem apenas uma ideia moderada ou incerta sobre as fontes de informação.
- **Minoria Confia nas Suas Fontes:** Apenas **32,4%** (27% + 5,4%) dos participantes concordam ou concordam totalmente que sabem onde procurar informações atualizadas.
- **Lacuna na Gestão da Informação:** Apesar de, em outros gráficos, ter havido alguma familiaridade com o conceito e até entendimento sobre a automação de ataques por IA, este gráfico revela uma deficiência na capacidade de se manter atualizado. Isso é crítico num campo tão dinâmico como a cibersegurança.
- **Necessidade de Orientação:** Os resultados sugerem que há uma necessidade de orientar os profissionais e o público em geral sobre as fontes confiáveis e atualizadas de informação sobre ciberataques baseados em IA.

Em resumo, o gráfico indica que existe uma dificuldade generalizada em saber onde encontrar informações atualizadas sobre ciberataques baseados em IA. A maioria dos participantes tem pouca clareza sobre as fontes de conhecimento, o que pode comprometer a sua capacidade de se manterem informados e preparados perante as evoluções das ameaças cibernéticas impulsionadas pela IA.

5.3 Identificar lacunas de conhecimento: descobrir áreas onde os utilizadores têm menos compreensão ou estão mais vulneráveis.

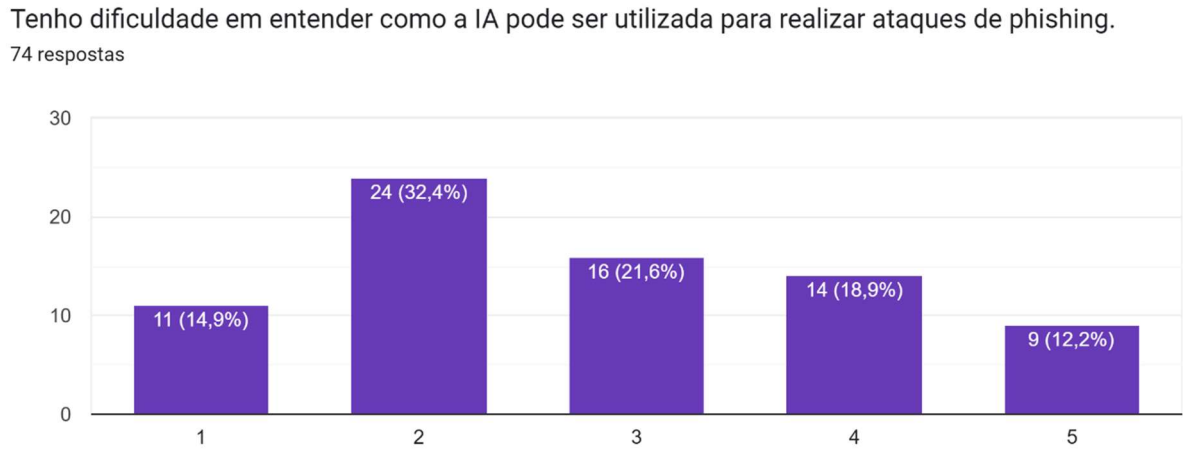
A eficácia das estratégias de cibersegurança depende não apenas da existência de tecnologias de proteção, mas também do nível de conhecimento dos utilizadores sobre as ameaças emergentes. No contexto dos ciberataques baseados em Inteligência Artificial (IA), essa premissa torna-se ainda mais relevante, dado o carácter sofisticado e em constante evolução dessas ameaças.

Este subcapítulo tem como objetivo identificar as principais lacunas de conhecimento entre os utilizadores, com base na análise de dados recolhidos em questionário. Ao mapear as áreas em que os participantes demonstram menor compreensão ou maior vulnerabilidade — como o reconhecimento de ataques, a compreensão de medidas de proteção ou o acesso a fontes de informação atualizadas — será possível delinear prioridades para ações de formação, sensibilização e desenvolvimento de competências.

A identificação dessas lacunas é fundamental para orientar intervenções educativas mais eficazes e para fortalecer a resiliência digital individual e organizacional frente aos desafios impostos pela IA no domínio da cibersegurança.

A Figura 13, apresenta a Dificuldade em Entender a Aplicação da IA em Estratégias de *Phishing* por parte dos inquiridos

Figura 13 - Dificuldade em Entender a Aplicação da IA em Estratégias de Phishing



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

Este gráfico de barras exibe os resultados de uma investigação que avaliou a dificuldade dos participantes em entender como a IA pode ser utilizada para realizar ataques de *phishing*. A pergunta específica foi "Tenho dificuldade em entender como a IA pode ser utilizada para realizar ataques de *phishing*.", com um total de 74 respostas.

Utilizando a escala de concordância fornecida:

- **1 (Discordo totalmente):** A pessoa discorda totalmente da afirmação, ou seja, **não tem dificuldade** em entender como a IA pode ser usada para *phishing*. Implica que entende bem.
- **2 (Discordo):** A pessoa discorda da afirmação, indicando que **tem pouca ou nenhuma dificuldade**, ou seja, entende razoavelmente bem.
- **3 (Neutro):** A pessoa está numa posição neutra, podendo ter uma dificuldade moderada ou estar incerta.

- **4 (Concordo):** A pessoa concorda com a afirmação, indicando que **tem dificuldade** em entender como a IA pode ser usada para *phishing*.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação, indicando que **tem muita dificuldade** em entender como a IA pode ser usada para *phishing*.

Análise dos Resultados com a Escala Fornecida:

- **1 (Discordo totalmente - Entende bem):** 11 respostas (14,9%). Uma parte dos respondentes entende bem o uso de IA em ataques de *phishing*.
- **2 (Discordo - Entende razoavelmente bem):** 24 respostas (32,4%). Este é o maior grupo, indicando que a maioria dos participantes tem uma compreensão razoável sobre o uso de IA em *phishing*.
- **3 (Neutro - Dificuldade moderada/incerteza):** 16 respostas (21,6%). Quase um quarto dos respondentes tem uma dificuldade moderada ou está incerto sobre o seu entendimento.
- **4 (Concordo - Tem dificuldade):** 14 respostas (18,9%). Um número considerável de respondentes concorda que tem dificuldade em entender este conceito.
- **5 (Concordo totalmente - Tem muita dificuldade):** 9 respostas (12,2%). Uma minoria significativa tem muita dificuldade.

Conclusões Principais:

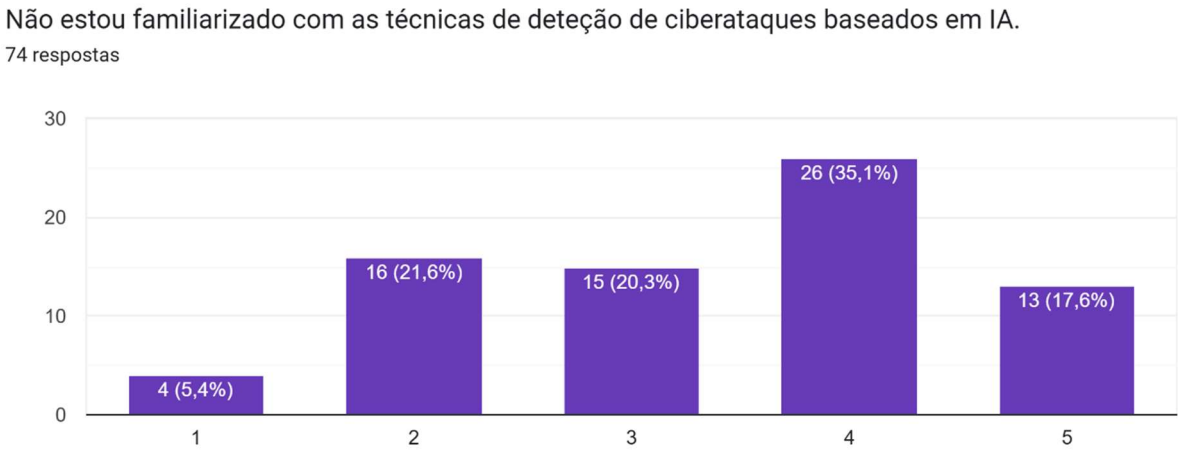
- **Entendimento Geralmente Bom sobre *Phishing* e IA:** A maioria dos participantes **não tem dificuldade** em entender como a IA pode ser usada para phishing. Somando as categorias 1 e 2 (que indicam pouca ou nenhuma dificuldade), temos 14,9% + 32,4% = **47,3%** dos respondentes. Isto sugere que quase metade dos participantes já compreende este vetor de ataque.
- **Dificuldade Presente para uma Minoria Considerável:** No entanto, uma parte significativa dos respondentes **tem dificuldade** em entender este conceito. As categorias 4 e 5 (que indicam alguma dificuldade) somam 18,9% + 12,2% = **31,1%**. Isto significa que quase um terço dos participantes ainda luta para compreender esta nuance.

- **Grupo Neutro Relevante:** A categoria "Neutro" (21,6%) representa aqueles que não discordam nem concordam, sugerindo uma compreensão intermediária ou incerta.
- **Área para Esclarecimento:** Apesar do bom entendimento geral, a percentagem considerável de pessoas que têm dificuldade (31,1%) aponta para a necessidade de mais esclarecimento sobre como as capacidades da IA (como geração de texto natural, análise de dados para personalização) podem ser exploradas em ataques de *phishing*.

Em síntese, o gráfico revela que, embora uma parcela considerável dos participantes já entenda como a IA pode ser usada para ataques de *phishing*, ainda há uma fatia significativa que enfrenta dificuldades em compreender este mecanismo. Isso indica que, apesar de o *phishing* ser um ataque conhecido, a camada de sofisticação adicionada pela IA ainda não é plenamente compreendida por todos.

A Figura 14, apresenta Perceção dos inquiridos sobre Técnicas de Deteção de Ciberataques com IA

Figura 14 - Perceção dos Inquiridos sobre Técnicas de Deteção de Ciberataques com IA



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

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a familiaridade dos participantes com as técnicas de deteção de ciberataques baseados em IA. A pergunta específica foi "Não estou familiarizado com as técnicas de deteção de ciberataques baseados em IA.", com um total de 74 respostas.

Para a análise, é crucial notar que a pergunta está formulada na negativa ("Não estou familiarizado..."). Isso inverte o significado usual da escala de concordância:

- **1 (Discordo totalmente):** A pessoa discorda totalmente da afirmação "Não estou familiarizado...", o que significa que ela **está muito familiarizada** com as técnicas de deteção.
- **2 (Discordo):** A pessoa discorda da afirmação, indicando que **está familiarizada** ou tem alguma familiaridade.
- **3 (Neutro):** A pessoa está numa posição neutra, podendo ter uma familiaridade moderada ou incerta.
- **4 (Concordo):** A pessoa concorda com a afirmação "Não estou familiarizado...", o que significa que **tem pouca familiaridade** com as técnicas de deteção.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação "Não estou familiarizado...", o que significa que **não está nada familiarizada** com as técnicas de deteção.

Análise dos Resultados com a Escala Fornecida e a Formulação da Pergunta:

- **1 (Discordo totalmente - MUITO FAMILIARIZADO):** 4 respostas (5,4%). Uma pequena percentagem dos respondentes está muito familiarizada com as técnicas de deteção.
- **2 (Discordo - FAMILIARIZADO):** 16 respostas (21,6%). Um grupo que indica estar familiarizado com as técnicas.

- **3 (Neutro - Familiaridade moderada/incerta):** 15 respostas (20,3%). Quase um quarto dos respondentes está numa posição neutra em relação à sua familiaridade.
- **4 (Concordo - POUCA FAMILIARIDADE):** 26 respostas (35,1%). Esta é a categoria mais numerosa. Indica que a maioria dos respondentes não está familiarizada ou tem pouca familiaridade com as técnicas de deteção.
- **5 (Concordo totalmente - NADA FAMILIARIZADO):** 13 respostas (17,6%). Um número significativo de participantes concorda totalmente que não está familiarizado com as técnicas de deteção.

Conclusões Principais:

- **Baixa Familiaridade com Técnicas de Deteção:** A maioria dos participantes tem pouca ou nenhuma familiaridade com as técnicas de deteção de ciberataques baseados em IA. Somando as categorias 4 e 5 (que indicam pouca ou nenhuma familiaridade), obtemos 35,1% + 17,6% = **52,7%** dos inquiridos. Mais da metade dos participantes não se sente familiarizada com as defesas.
- **Lacuna no Conhecimento de Defesa:** Comparando com os gráficos anteriores que mostraram alguma familiaridade com o conceito de ataques de IA e o entendimento de como a IA pode automatizá-los, este gráfico revela uma lacuna crítica no conhecimento das contramedidas. As pessoas podem estar cientes da ameaça, mas não das ferramentas para combatê-la.
- **Poucos Especialistas em Deteção:** Apenas **27%** (5,4% + 21,6%) dos inquiridos indicam estar familiarizados ou muito familiarizados com as técnicas de deteção (categorias 1 e 2). Este é um grupo minoritário.
- **Necessidade Urgente de Formação em Defesa:** Os resultados apontam para uma necessidade premente de educação e treino focados nas técnicas de deteção de

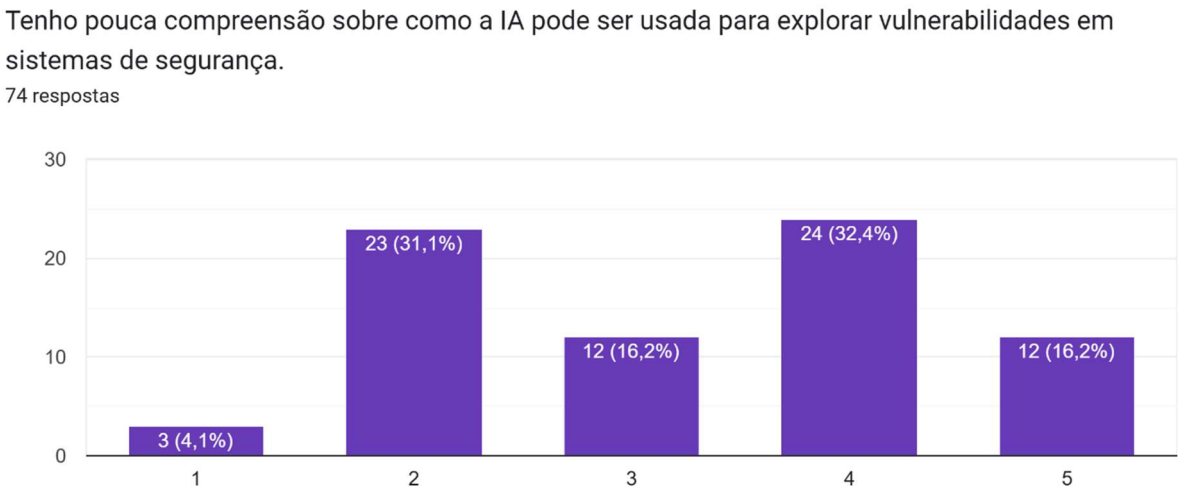
ciberataques que utilizam IA. É fundamental capacitar os profissionais para reconhecer e mitigar estas ameaças crescentes.

Em resumo, o gráfico indica que, embora haja uma consciência da existência de ciberataques baseados em IA, a maioria dos inquiridos não está familiarizada com as técnicas necessárias para detetá-los.

Esta falta de familiaridade com as defesas é um ponto vulnerável significativo que precisa ser abordado.

A Figura 15, apresenta o Nível de Compreensão sobre o Uso da IA para Explorar Vulnerabilidades em Sistemas de Segurança.

Figura 15 - Perceção dos Inquiridos sobre a Capacidade da IA de Explorar Vulnerabilidades



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

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a compreensão dos participantes sobre como a IA pode ser utilizada para explorar vulnerabilidades em sistemas de segurança. A pergunta específica foi "Tenho pouca compreensão sobre como a IA pode ser usada para explorar vulnerabilidades em sistemas de segurança.", com um total de 74 respostas.

Para uma análise correta, é crucial notar que a pergunta está formulada na negativa ("Tenho pouca compreensão..."). Isso inverte o significado usual da escala de concordância:

- **1 (Discordo totalmente):** A pessoa discorda totalmente da afirmação "Tenho pouca compreensão...", o que significa que ela **tem muita compreensão** sobre como a IA explora vulnerabilidades.
- **2 (Discordo):** A pessoa discorda da afirmação, indicando que **tem boa compreensão** ou alguma compreensão.
- **3 (Neutro):** A pessoa está numa posição neutra, podendo ter uma compreensão moderada ou incerta.
- **4 (Concordo):** A pessoa concorda com a afirmação "Tenho pouca compreensão...", o que significa que **tem pouca compreensão** sobre como a IA explora vulnerabilidades.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação "Tenho pouca compreensão...", o que significa que **não tem praticamente nenhuma compreensão** sobre como a IA explora vulnerabilidades.

Análise dos Resultados com a Escala Fornecida e a Formulação da Pergunta:

- **1 (Discordo totalmente - MUITA COMPREENSÃO):** 3 respostas (4,1%). Uma minoria dos inquiridos tem muita compreensão sobre o uso de IA na exploração de vulnerabilidades.
- **2 (Discordo - BOA COMPREENSÃO):** 23 respostas (31,1%). Este é o segundo maior grupo, indicando que uma parte considerável dos inquiridos tem boa compreensão.
- **3 (Neutro - Compreensão moderada/incerta):** 12 respostas (16,2%). Este grupo representa aqueles com uma compreensão intermediária ou incerta.
- **4 (Concordo - POUCA COMPREENSÃO):** 24 respostas (32,4%). Esta é a categoria mais numerosa. Indica que a maioria dos inquiridos tem pouca compreensão sobre como a IA pode ser usada para explorar vulnerabilidades.

- **5 (Concordo totalmente - QUASE NENHUMA COMPREENSÃO):** 12 respostas (16,2%). Um número significativo de participantes concorda totalmente que tem pouca compreensão.

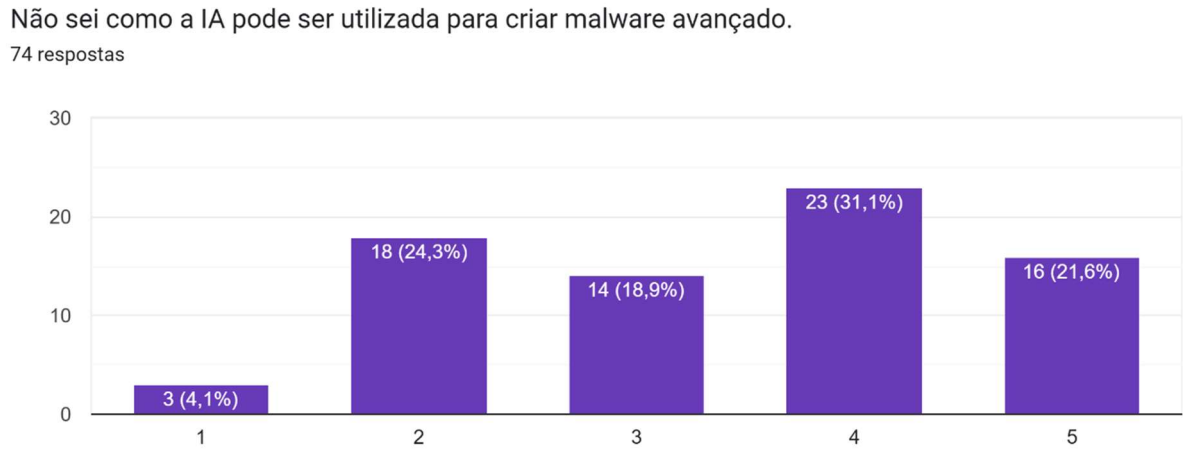
Conclusões Principais:

- **Pouca Compreensão Prevalente:** A maioria dos participantes tem pouca ou quase nenhuma compreensão sobre como a IA pode ser usada para explorar vulnerabilidades. Somando as categorias 4 e 5 (que indicam pouca ou nenhuma compreensão), obtemos 32,4% + 16,2% = **48,6%** dos inquiridos. Quase metade dos participantes encaixa-se nesta descrição.
- **Compreensão Adequada para uma Minoria:** Apenas **35,2%** (4,1% + 31,1%) dos inquiridos discordam da afirmação, ou seja, têm uma boa ou muita compreensão (categorias 1 e 2).
- **Lacuna no Conhecimento de Táticas Ofensivas de IA:** Embora possa haver uma familiaridade geral com os ciberataques de IA, o conhecimento específico sobre como a IA pode ser utilizada para identificar e explorar falhas em sistemas de segurança parece ser limitado para a maioria.
- **Necessidade de Aprofundamento Técnico:** Os resultados sugerem que há uma necessidade clara de aprofundar o conhecimento técnico sobre as capacidades ofensivas da IA no contexto da cibersegurança. Compreender como os atacantes podem usar a IA é fundamental para desenvolver defesas eficazes.

Em suma, o gráfico revela que a maioria dos participantes da investigação tem pouca ou muito pouca compreensão sobre como a Inteligência Artificial pode ser empregue para explorar vulnerabilidades em sistemas de segurança. Esta é uma área crítica que necessita de maior esclarecimento e educação para que os profissionais possam antecipar e mitigar ameaças sofisticadas.

A Figura 16, apresenta a Perceção dos Inquiridos sobre o Conhecimento da IA na Criação de *Malware* Avançado

Figura 16 - Perceção dos Inquiridos sobre o Conhecimento da IA na Criação de Malware Avançado



Fonte: Dados do questionário da pergunta n.º 15 (Anexo I)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a perceção dos participantes sobre o seu conhecimento acerca de como a Inteligência Artificial pode ser utilizada para criar *malware* avançado. A pergunta específica da investigação foi "Não sei como a IA pode ser utilizada para criar malware avançado.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa discorda completamente da afirmação "Não sei...", o que significa que ela **sabe muito bem** como a IA pode ser utilizada para criar *malware* avançado.
- **2 (Discordo):** A pessoa discorda da afirmação "Não sei...", indicando que **sabe razoavelmente bem** como a IA pode ser utilizada para criar *malware* avançado.
- **3 (Neutro):** A pessoa está numa posição neutra, o que pode indicar um conhecimento moderado ou incerteza sobre o tema.

- **4 (Concordo):** A pessoa concorda com a afirmação "Não sei...", o que significa que **tem pouca compreensão** sobre como a IA pode ser utilizada para criar *malware* avançado.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação "Não sei...", o que significa que **não tem qualquer compreensão** sobre como a IA pode ser utilizada para criar *malware* avançado.

Análise dos Resultados:

- **Nível 1 (Sabe muito bem):** 3 respostas (4,1%) – Uma minoria muito pequena dos inquiridos demonstra um conhecimento muito aprofundado sobre o tema.
- **Nível 2 (Sabe razoavelmente bem):** 18 respostas (24,3%) – Uma parte considerável dos inquiridos indica que possui um conhecimento razoável.
- **Nível 3 (Conhecimento moderado/Incerteza):** 14 respostas (18,9%) – Quase um quinto dos participantes tem um conhecimento intermédio ou não tem uma posição definida.
- **Nível 4 (Pouca compreensão):** 23 respostas (31,1%) – Esta é a categoria com o maior número de respostas. Revela que a maior parte dos participantes tem pouca compreensão sobre como a IA pode ser usada para criar *malware* avançado.
- **Nível 5 (Nenhuma compreensão):** 16 respostas (21,6%) – Um grupo significativo de inquiridos admite que não tem qualquer compreensão sobre o assunto.

Conclusões Principais:

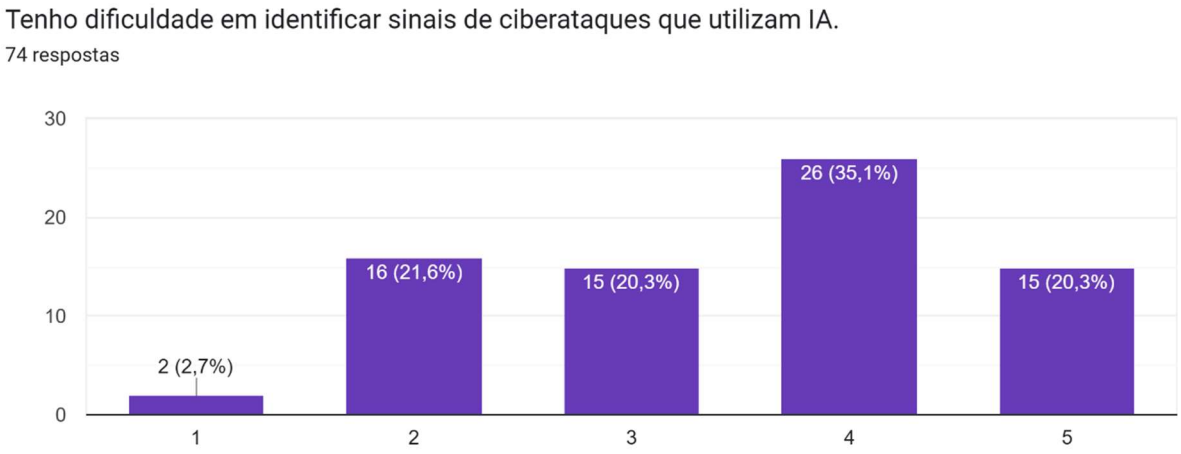
- **Lacuna de Conhecimento Específico:** Os resultados indicam uma **lacuna notável no conhecimento** sobre como a Inteligência Artificial pode ser empregue na criação de *malware* avançado. A maioria dos participantes (somando as categorias 4 e 5, que representam 31,1% + 21,6% = **52,7%**) expressa que tem pouca ou nenhuma compreensão sobre este aspeto.

- **Minoria Informada:** Apenas uma minoria dos inquiridos (somando as categorias 1 e 2, que representam 4,1% + 24,3% = **28,4%**) demonstra ter um bom ou muito bom conhecimento sobre o assunto.
- **Necessidade de Educação:** O facto de mais de metade dos inquiridos admitir ter pouco ou nenhum conhecimento nesta área técnica sugere uma necessidade clara de iniciativas de educação e formação para aumentar a compreensão sobre as capacidades ofensivas da IA no campo da cibersegurança. Compreender estas táticas é essencial para desenvolver defesas eficazes.

Em suma, este gráfico sublinha que, apesar do reconhecimento geral da IA, o conhecimento sobre as suas aplicações avançadas em ciberataques, nomeadamente na criação de *malware*, é limitado para a maioria da população inquirida.

A Figura 17, apresenta o Nível de Dificuldade em Identificar Sinais de Ciberataques com Uso de Inteligência Artificial

Figura 17 - Nível de Dificuldade em Identificar Sinais de Ciberataques com Uso de Inteligência Artificial



Fonte: Dados do questionário da pergunta n.º 16 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a perceção dos participantes sobre a sua dificuldade em identificar sinais de ciberataques que utilizam Inteligência Artificial (IA). A pergunta específica da investigação foi "Tenho dificuldade em identificar sinais de ciberataques que utilizam IA.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte (com interpretação invertida devido à negativa na pergunta):

- **1 (Discordo totalmente):** A pessoa discorda totalmente de "Tenho dificuldade...", o que significa que ela **não tem nenhuma dificuldade** em identificar sinais de ciberataques que utilizam IA (ou seja, consegue identificar muito bem).
- **2 (Discordo):** A pessoa discorda de "Tenho dificuldade...", indicando que **tem pouca dificuldade** em identificar sinais de ciberataques que utilizam IA (ou seja, consegue identificar razoavelmente bem).
- **3 (Neutro):** A pessoa está numa posição neutra, o que pode indicar uma dificuldade moderada ou incerteza.
- **4 (Concordo):** A pessoa concorda com "Tenho dificuldade...", o que significa que **tem dificuldade** em identificar sinais de ciberataques que utilizam IA.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com "Tenho dificuldade...", o que significa que **tem muita dificuldade** em identificar sinais de ciberataques que utilizam IA.

Análise dos Resultados:

- **Nível 1 (Não tem nenhuma dificuldade / Identifica muito bem):** 2 respostas (2,7%) – Uma minoria muito pequena não tem dificuldade.
- **Nível 2 (Tem pouca dificuldade / Identifica razoavelmente bem):** 16 respostas (21,6%) – Este grupo indica que consegue identificar razoavelmente bem os sinais.
- **Nível 3 (Dificuldade moderada/Incerteza):** 15 respostas (20,3%) – Quase um quinto dos participantes tem uma dificuldade moderada ou está incerto.

- **Nível 4 (Tem dificuldade):** 26 respostas (35,1%) – Esta é a categoria mais frequente. Indica que a maioria dos participantes concorda que tem dificuldade em identificar os sinais de ciberataques que utilizam IA.
- **Nível 5 (Tem muita dificuldade):** 15 respostas (20,3%) – Um grupo significativo de inquiridos admite que tem muita dificuldade.

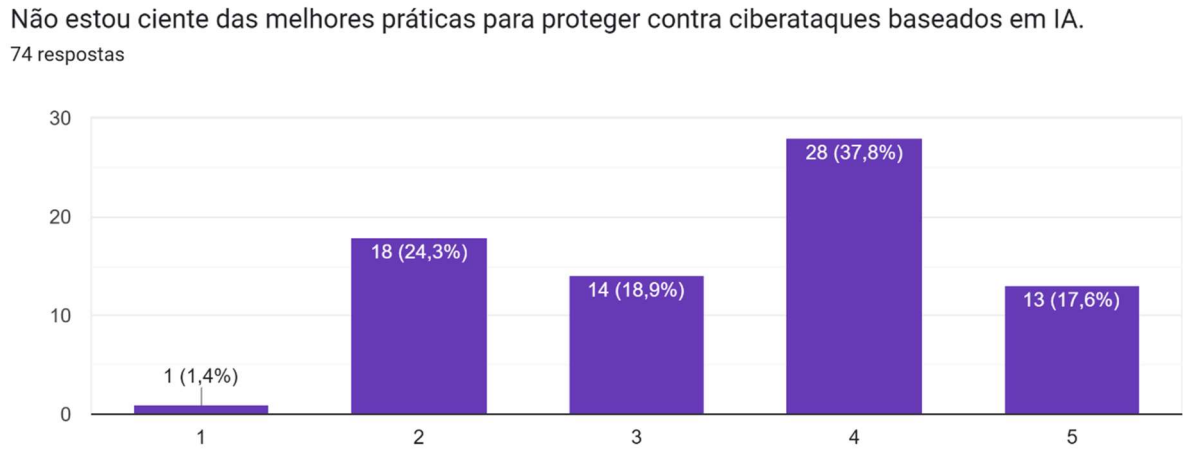
Conclusões Principais:

- **Dificuldade Generalizada na Identificação de Sinais:** A maioria dos participantes (somando as categorias 4 e 5, que representam 35,1% + 20,3% = **55,4%**) concorda que tem **dificuldade ou muita dificuldade** em identificar os sinais de ciberataques que utilizam IA.
- **Pouca Capacidade de Deteção Antecipada:** Apenas uma minoria (somando as categorias 1 e 2, que representam 2,7% + 21,6% = **24,3%**) sente que tem pouca ou nenhuma dificuldade (ou seja, consegue identificar bem os sinais).
- **Lacuna Crítica em Cibersegurança:** Este resultado é alarmante, pois a capacidade de identificar sinais precoces de ataques é crucial para a defesa cibernética. A falta de compreensão aqui pode levar a atrasos na resposta e a maiores danos.
- **Necessidade de Treinamento em Deteção:** Os dados apontam para uma necessidade urgente de programas de treino focados na deteção de anomalias e comportamentos incomuns que possam indicar ciberataques impulsionados por IA.

Em suma, este gráfico revela que a maioria dos inquiridos tem dificuldade em identificar os sinais de ciberataques que utilizam IA, sublinhando uma vulnerabilidade significativa na capacidade de deteção proativa e de resposta a ameaças.

A Figura 18, apresenta o Nível de Consciencialização sobre Boas Práticas de Proteção contra Ciberataques com IA

Figura 18 - Nível de Consciencialização sobre Boas Práticas de Proteção contra Ciberataques com IA



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

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a consciência dos participantes sobre as melhores práticas para proteger contra ciberataques baseados em Inteligência Artificial (IA). A pergunta específica da investigação foi "Não estou ciente das melhores práticas para proteger contra ciberataques baseados em IA.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte (com interpretação invertida devido à negativa na pergunta):

- **1 (Discordo totalmente):** A pessoa discorda totalmente de "Não estou ciente...", o que significa que ela **está muito ciente** das melhores práticas para proteção contra ciberataques baseados em IA.
- **2 (Discordo):** A pessoa discorda de "Não estou ciente...", indicando que **está razoavelmente ciente** das melhores práticas.

- **3 (Neutro):** A pessoa está numa posição neutra, o que pode significar uma consciência moderada ou incerteza.
- **4 (Concordo):** A pessoa concorda com "Não estou ciente...", o que significa que **tem pouca consciência** das melhores práticas para proteção contra ciberataques baseados em IA.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com "Não estou ciente...", o que significa que **não tem qualquer consciência** das melhores práticas para proteção contra ciberataques baseados em IA.

Análise dos Resultados:

- **Nível 1 (Muito ciente):** 1 resposta (1,4%) – Uma minoria muito pequena está muito ciente das melhores práticas.
- **Nível 2 (Razoavelmente ciente):** 18 respostas (24,3%) – Um grupo que demonstra estar razoavelmente ciente das melhores práticas.
- **Nível 3 (Consciência moderada/Incerteza):** 14 respostas (18,9%) – Quase um quinto dos participantes tem uma consciência moderada ou incerteza.
- **Nível 4 (Pouca consciência):** 28 respostas (37,8%) – Esta é a categoria com o maior número de respostas. Indica que a maioria dos participantes concorda que tem pouca consciência das melhores práticas.
- **Nível 5 (Nenhuma consciência):** 13 respostas (17,6%) – Um grupo significativo de inquiridos admite não ter qualquer consciência das melhores práticas.

Conclusões Principais:

- **Baixa Consciência das Melhores Práticas:** A maioria dos participantes (somando as categorias 4 e 5, que representam 37,8% + 17,6% = **55,4%**) admite ter **pouca ou nenhuma consciência** sobre as melhores práticas para proteger contra ciberataques baseados em IA.

- **Lacuna Crítica na Proteção:** Apenas uma minoria (somando as categorias 1 e 2, que representam 1,4% + 24,3% = **25,7%**) indica estar ciente ou muito ciente das melhores práticas.
- **Necessidade de Educação em Defesa:** Os resultados apontam para uma necessidade premente de programas de educação e disseminação de conhecimento sobre as melhores práticas e estratégias de defesa contra ciberataques impulsionados por IA, para capacitar indivíduos e organizações a protegerem-se eficazmente.

Em suma, este gráfico revela uma grande lacuna na consciência sobre as melhores práticas de proteção contra ciberataques baseados em IA, indicando que a maioria dos inquiridos não se sente informada sobre como se defender eficazmente.

A Figura 19, apresenta o Nível de Compreensão sobre o Uso da Inteligência Artificial em Ataques DDoS

Figura 19 - Nível de Compreensão sobre o Uso da Inteligência Artificial em Ataques DDoS

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

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a perceção dos participantes sobre a sua compreensão acerca de como a Inteligência Artificial (IA) pode ser utilizada para realizar ataques de negação de serviço distribuído (DDoS). A pergunta específica da investigação foi "Tenho pouca compreensão sobre como a IA pode ser usada para realizar ataques de negação de serviço (DDoS).", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte (com interpretação invertida devido à negativa na pergunta "Tenho pouca compreensão..."):

- **1 (Discordo totalmente):** A pessoa discorda totalmente de "Tenho pouca compreensão...", o que significa que ela **não tem pouca compreensão** (ou seja, entende muito bem) sobre como a IA pode ser usada para realizar ataques DDoS.
- **2 (Discordo):** A pessoa discorda de "Tenho pouca compreensão...", indicando que **não tem muita pouca compreensão** (ou seja, entende razoavelmente bem) sobre como a IA pode ser usada para realizar ataques DDoS.
- **3 (Neutro):** A pessoa está numa posição neutra, o que pode indicar uma compreensão moderada ou incerteza.
- **4 (Concordo):** A pessoa concorda com "Tenho pouca compreensão...", o que significa que **tem pouca compreensão** sobre como a IA pode ser usada para realizar ataques DDoS.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com "Tenho pouca compreensão...", o que significa que **não tem qualquer compreensão** sobre como a IA pode ser usada para realizar ataques DDoS.

Análise dos Resultados:

- **Nível 1 (Entende muito bem):** Apenas 2 respostas (2,7%) indicam que estes participantes compreendem muito bem o uso de IA em ataques DDoS.
- **Nível 2 (Entende razoavelmente bem):** 16 respostas (21,6%) mostram que este grupo tem uma compreensão razoável sobre o tema.

- **Nível 3 (Compreensão moderada/Incerteza):** 10 respostas (13,5%) revelam que uma percentagem menor dos inquiridos tem uma compreensão moderada ou está incerta.
- **Nível 4 (Tem pouca compreensão):** Com 28 respostas (37,8%), esta é a categoria mais frequente. Sugere que a maioria dos participantes concorda que tem pouca compreensão sobre como a IA pode ser usada para ataques DDoS.
- **Nível 5 (Não tem qualquer compreensão):** 18 respostas (24,3%) indicam que um número significativo de inquiridos admite não ter qualquer compreensão sobre o tema.

Conclusões Principais:

- **Lacuna na Compreensão de DDoS e IA:** A maioria dos participantes (somando as categorias 4 e 5) expressa que tem **pouca ou nenhuma compreensão** sobre como a IA pode ser usada para realizar ataques de negação de serviço (DDoS). Juntas, estas categorias representam 37,8% + 24,3% = **62,1%** dos inquiridos.
- **Minoria com Bom Entendimento:** Apenas uma minoria (somando as categorias 1 e 2) demonstra ter um bom ou razoável entendimento sobre o tema. Juntas, estas categorias somam 2,7% + 21,6% = **24,3%**.
- **Necessidade de Consciencialização Específica:** O elevado número de pessoas com pouca ou nenhuma compreensão sobre este tipo específico de ataque realça a necessidade de programas de educação mais focados e detalhados sobre as técnicas específicas de ciberataques impulsionados por IA, como os ataques DDoS.

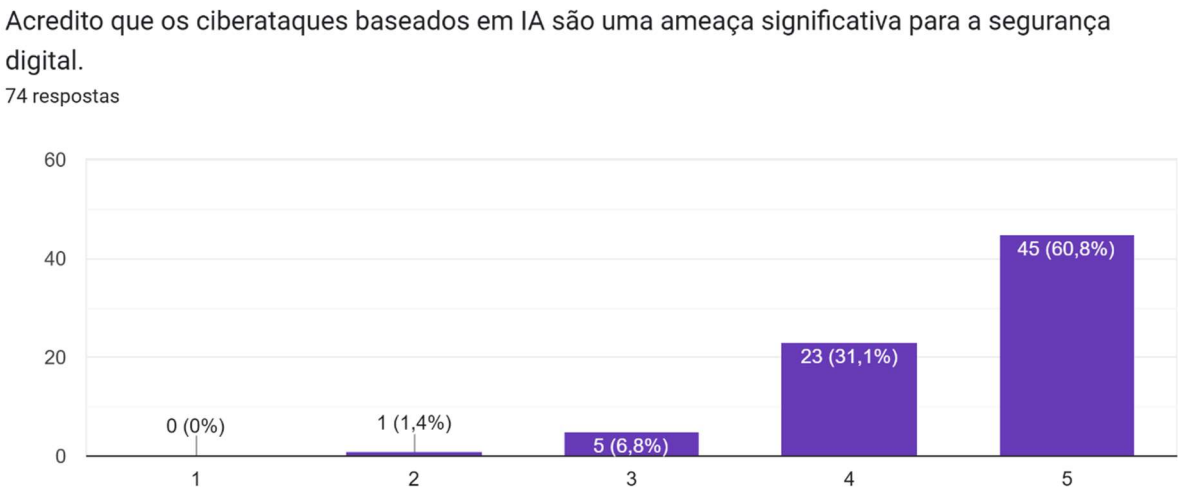
Em suma, este gráfico revela que a maior parte dos inquiridos tem uma compreensão limitada sobre como a Inteligência Artificial pode ser utilizada para orquestrar ataques de negação de serviço, indicando uma área crítica para o aprofundamento do conhecimento em cibersegurança.

5.4 Analisar perceções: compreender como os utilizadores percebem a gravidade e a frequência dos ciberataques.

Num cenário digital cada vez mais marcado por ameaças cibernéticas, torna-se essencial compreender não apenas os aspetos técnicos dos ciberataques, mas também a forma como estes são percecionados pelos utilizadores. A perceção individual da gravidade e da frequência dos ataques influencia diretamente o comportamento online, o nível de precaução adotado e a adesão a práticas de cibersegurança. Este subcapítulo tem como objetivo analisar essas perceções, explorando como diferentes perfis de utilizadores interpretam os riscos associados aos ciberataques, que fatores moldam essas interpretações e de que forma essas perceções podem impactar a eficácia das estratégias de prevenção e resposta. Ao compreender melhor o ponto de vista dos utilizadores, é possível desenvolver abordagens mais eficazes e personalizadas para a educação e sensibilização em cibersegurança.

A Figura 20, apresenta a Perceção sobre a Ameaça dos Ciberataques Baseados em IA para a Segurança Digital

Figura 20 - Perceção sobre a Ameaça dos Ciberataques Baseados em IA para a Segurança Digital



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

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a perceção dos participantes sobre a significância dos ciberataques baseados em Inteligência Artificial (IA) como uma ameaça à segurança digital. A pergunta específica da investigação foi "Acredito que os ciberataques baseados em IA são uma ameaça significativa para a segurança digital.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa discorda completamente da afirmação, ou seja, não acredita que ciberataques baseados em IA são uma ameaça significativa.
- **2 (Discordo):** A pessoa discorda da afirmação, indicando que não considera esses ciberataques uma ameaça muito significativa.
- **3 (Neutro):** A pessoa está numa posição neutra, o que pode indicar incerteza ou uma perceção de ameaça moderada.
- **4 (Concordo):** A pessoa concorda com a afirmação, indicando que acredita que ciberataques baseados em IA são uma ameaça significativa.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação, indicando uma forte crença de que ciberataques baseados em IA representam uma ameaça muito significativa.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 0 respostas (0%) – Nenhum dos participantes discorda totalmente, o que sugere um consenso sobre a existência, pelo menos, de alguma ameaça.
- **Nível 2 (Discordo):** 1 resposta (1,4%) – Apenas uma minoria insignificante não vê os ciberataques baseados em IA como uma ameaça significativa.
- **Nível 3 (Neutro):** 5 respostas (6,8%) – Uma pequena percentagem dos inquiridos está neutra, talvez indicando incerteza ou uma visão mais moderada da ameaça.

- **Nível 4 (Concordo):** 23 respostas (31,1%) – Um número considerável de participantes concorda que os ciberataques baseados em IA são uma ameaça significativa.
- **Nível 5 (Concordo totalmente):** 45 respostas (60,8%) – Esta é a categoria dominante, com a maioria esmagadora dos inquiridos a concordar totalmente que os ciberataques baseados em IA são uma ameaça muito significativa para a segurança digital.

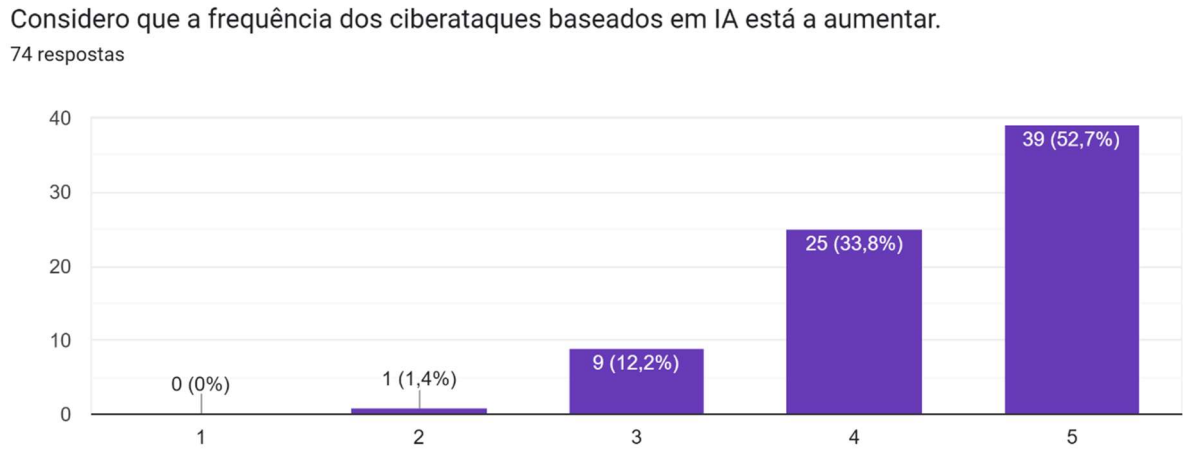
Conclusões Principais:

- **Perceção Generalizada de Ameaça Elevada:** A grande maioria dos participantes (somando as categorias 4 e 5, que representam 31,1% + 60,8% = **91,9%**) acredita que os ciberataques baseados em IA são uma ameaça significativa ou muito significativa para a segurança digital.
- **Consciência da Gravidade:** Os resultados demonstram uma forte consciência e preocupação na audiência inquirida sobre a gravidade da ameaça que a IA representa no cenário da cibersegurança.
- **Pequeno Grupo de Descrentes/Neutros:** Praticamente não há participantes que discordem da afirmação (0%) e apenas uma percentagem muito pequena (1,4%) discorda, com um grupo ligeiramente maior (6,8%) a permanecer neutro.

Em suma, este gráfico indica que a perceção geral entre os inquiridos é que os ciberataques baseados em IA constituem uma ameaça muito real e significativa para a segurança digital. Esta forte concordância sugere um reconhecimento generalizado do potencial disruptivo e perigoso da IA nas mãos de ciberatacantes.

A Figura 21, apresenta a Perceção sobre o Aumento da Frequência de Ciberataques com Inteligência Artificial

Figura 21 - Perceção sobre o Aumento da Frequência de Ciberataques com Inteligência Artificial



Fonte: Dados do questionário da pergunta n.º 20 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a perceção dos participantes sobre a tendência de frequência dos ciberataques baseados em Inteligência Artificial (IA). A pergunta específica da investigação foi "Considero que a frequência dos ciberataques baseados em IA está a aumentar.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa discorda completamente da afirmação, ou seja, não acredita que a frequência dos ciberataques baseados em IA esteja a aumentar.
- **2 (Discordo):** A pessoa discorda da afirmação, indicando que não percebe um aumento na frequência.
- **3 (Neutro):** A pessoa está numa posição neutra, o que pode indicar incerteza ou uma perceção de frequência estável.
- **4 (Concordo):** A pessoa concorda com a afirmação, indicando que acredita que a frequência dos ciberataques baseados em IA está a aumentar.

- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação, indicando uma forte crença de que a frequência dos ciberataques baseados em IA está a aumentar significativamente.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 0 respostas (0%) – Nenhum dos participantes discorda totalmente, o que sugere um consenso de que a frequência não está a diminuir.
- **Nível 2 (Discordo):** 1 resposta (1,4%) – Apenas uma minoria insignificante discorda da afirmação.
- **Nível 3 (Neutro):** 9 respostas (12,2%) – Uma pequena percentagem dos inquiridos está neutra, talvez indicando incerteza sobre a tendência.
- **Nível 4 (Concordo):** 25 respostas (33,8%) – Um número considerável de participantes concorda que a frequência dos ciberataques baseados em IA está a aumentar.
- **Nível 5 (Concordo totalmente):** 39 respostas (52,7%) – Esta é a categoria dominante, com a maioria esmagadora dos inquiridos a concordar totalmente que a frequência dos ciberataques baseados em IA está a aumentar.

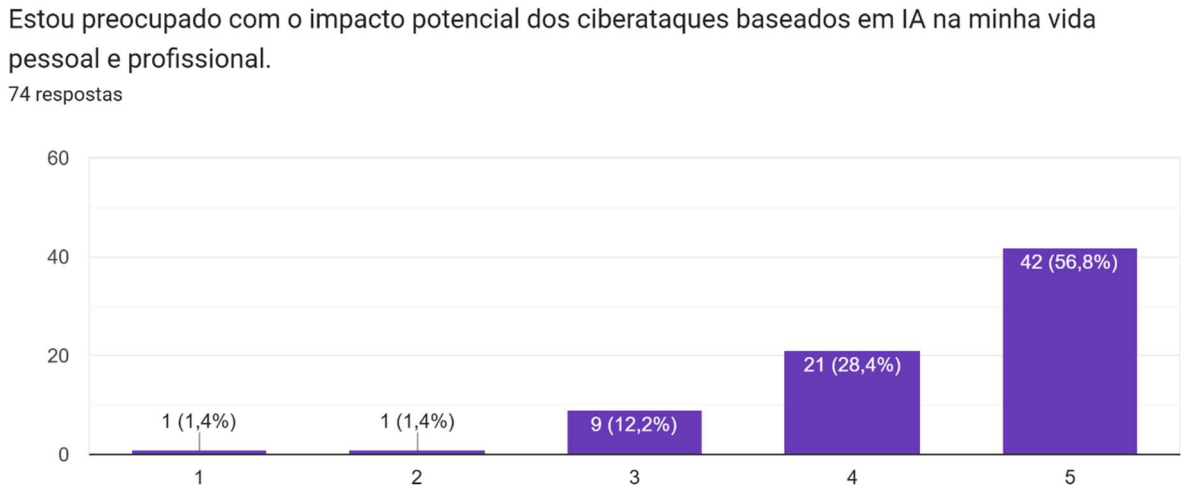
Conclusões Principais:

- **Perceção Quase Unânime de Aumento:** A vasta maioria dos participantes (somando as categorias 4 e 5, que representam 33,8% + 52,7% = **86,5%**) acredita fortemente que a frequência dos ciberataques baseados em IA está a aumentar.
- **Consciência da Escalada da Ameaça:** Os resultados demonstram uma clara perceção na audiência inquirida de que a ameaça de ciberataques impulsionados por IA não é apenas significativa (como visto num gráfico anterior), mas também está em ascensão.
- **Baixo Desconhecimento da Tendência:** Praticamente não há participantes que discordem da afirmação, com uma percentagem muito pequena a permanecer neutra.

Em suma, este gráfico indica uma forte e generalizada perceção de que a frequência dos ciberataques que utilizam IA está em crescimento, sublinhando uma preocupação crescente e uma consciência da evolução do panorama das ameaças cibernéticas.

A Figura 22, apresenta o Nível de Preocupação com o Impacto dos Ciberataques com IA na Vida Pessoal e Profissional

Figura 22 - Nível de Preocupação com o Impacto dos Ciberataques com IA na Vida Pessoal e Profissional



Fonte: Dados do questionário da pergunta n.º 21 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou o nível de preocupação dos participantes em relação ao impacto potencial dos ciberataques baseados em Inteligência Artificial (IA) nas suas vidas pessoal e profissional. A pergunta específica da investigação foi "Estou preocupado com o impacto potencial dos ciberataques baseados em IA na minha vida pessoal e profissional.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não está nada preocupada com o impacto dos ciberataques baseados em IA na sua vida pessoal e profissional.
- **2 (Discordo):** A pessoa tem pouca preocupação com o impacto dos ciberataques baseados em IA.
- **3 (Neutro):** A pessoa está numa posição neutra, o que pode indicar alguma preocupação, mas não de forma significativa, ou incerteza.

- **4 (Concordo):** A pessoa concorda com a afirmação, indicando que está preocupada com o impacto potencial dos ciberataques baseados em IA.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação, indicando uma preocupação muito forte e significativa com o impacto potencial dos ciberataques baseados em IA.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente - Sem preocupação):** 1 resposta (1,4%) – Uma minoria muito pequena não demonstra preocupação.
- **Nível 2 (Discordo - Pouca preocupação):** 1 resposta (1,4%) – Outra minoria muito pequena tem pouca preocupação.
- **Nível 3 (Neutro - Preocupação moderada/incerteza):** 9 respostas (12,2%) – Uma pequena percentagem dos inquiridos está numa posição neutra.
- **Nível 4 (Concordo - Preocupado):** 21 respostas (28,4%) – Um número considerável de participantes concorda que está preocupado.
- **Nível 5 (Concordo totalmente - Muito preocupado):** 42 respostas (56,8%) – Esta é a categoria dominante, com a maioria esmagadora dos inquiridos a concordar totalmente que está muito preocupada.

Conclusões Principais:

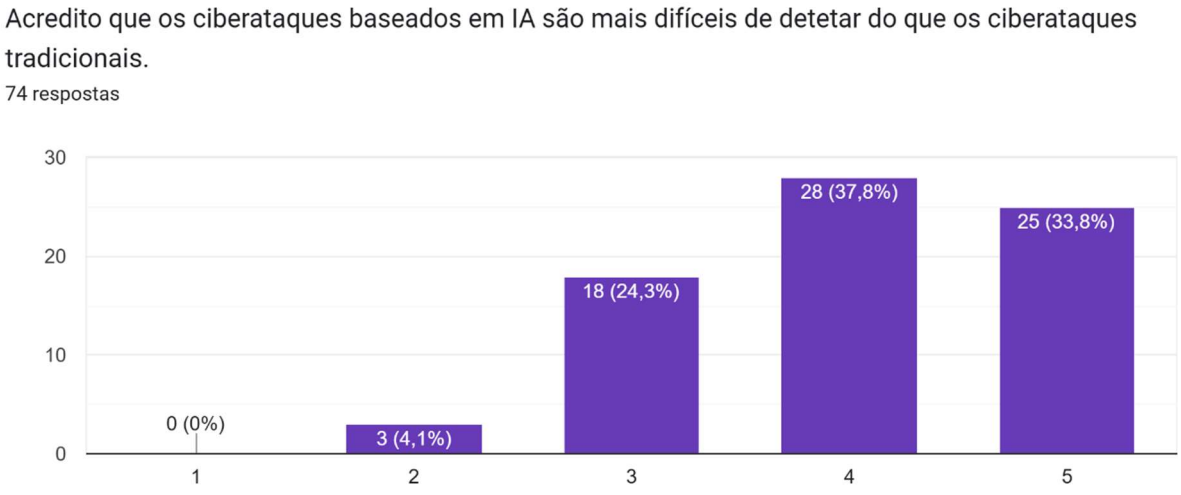
- **Elevado Nível de Preocupação:** A grande maioria dos participantes (somando as categorias 4 e 5, que representam 28,4% + 56,8% = **85,2%**) expressa que está preocupada ou muito preocupada com o impacto potencial dos ciberataques baseados em IA nas suas vidas pessoal e profissional.
- **Reconhecimento da Ameaça Pessoal/Profissional:** Os resultados demonstram uma forte consciência e perceção da ameaça direta que os ciberataques baseados em IA podem representar para o bem-estar e segurança individuais, tanto no âmbito pessoal quanto no profissional.

- **Baixa Indiferença:** Apenas uma percentagem mínima de inquiridos (1,4% + 1,4% = 2,8%) não demonstra preocupação, sublinhando que a questão dos ciberataques baseados em IA é amplamente reconhecida como um problema sério pela audiência inquirida.

Em suma, este gráfico revela uma preocupação generalizada e significativa por parte dos participantes em relação ao impacto dos ciberataques impulsionados por IA nas suas vidas diárias, tanto a nível pessoal como profissional.

A Figura 23, apresenta a Perceção sobre a Dificuldade de Detetar Ciberataques com IA em Comparação com Ataques Tradicionais

Figura 23 - Perceção sobre a Dificuldade de Detetar Ciberataques com IA em Comparação com Ataques Tradicionais



Fonte: Dados do questionário da pergunta n.º 22 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a perceção dos participantes sobre a dificuldade de deteção de ciberataques baseados em Inteligência Artificial (IA) em comparação com os ciberataques tradicionais. A pergunta específica da investigação

foi "Acredito que os ciberataques baseados em IA são mais difíceis de detetar do que os ciberataques tradicionais.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa discorda completamente da afirmação, ou seja, acredita que os ciberataques baseados em IA **não são mais difíceis** de detetar do que os tradicionais.
- **2 (Discordo):** A pessoa discorda da afirmação, indicando que considera que os ciberataques baseados em IA são apenas ligeiramente mais difíceis, ou não mais difíceis, de detetar.
- **3 (Neutro):** A pessoa está numa posição neutra, o que pode indicar incerteza, ou que considera a dificuldade de deteção semelhante entre ambos os tipos de ataques.
- **4 (Concordo):** A pessoa concorda com a afirmação, indicando que acredita que os ciberataques baseados em IA são mais difíceis de detetar.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação, indicando uma forte crença de que os ciberataques baseados em IA são significativamente mais difíceis de detetar do que os ciberataques tradicionais.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 0 respostas (0%) – Ninguém discorda totalmente, o que sugere um consenso de que os ataques baseados em IA são, no mínimo, tão difíceis de detetar.
- **Nível 2 (Discordo):** 3 respostas (4,1%) – Uma minoria muito pequena discorda da afirmação, talvez por acreditar que a dificuldade é comparável ou por estar mais familiarizada com técnicas de defesa contra IA.
- **Nível 3 (Neutro):** 18 respostas (24,3%) – Quase um quarto dos inquiridos está numa posição neutra, o que pode indicar incerteza ou uma perceção de dificuldade similar.

- **Nível 4 (Concordo):** 28 respostas (37,8%) – Esta é a categoria mais frequente, indicando que a maioria dos participantes concorda que os ciberataques baseados em IA são mais difíceis de detetar.
- **Nível 5 (Concordo totalmente):** 25 respostas (33,8%) – Um número significativo de inquiridos concorda totalmente, reforçando a perceção de que a IA adiciona uma camada de complexidade à deteção.

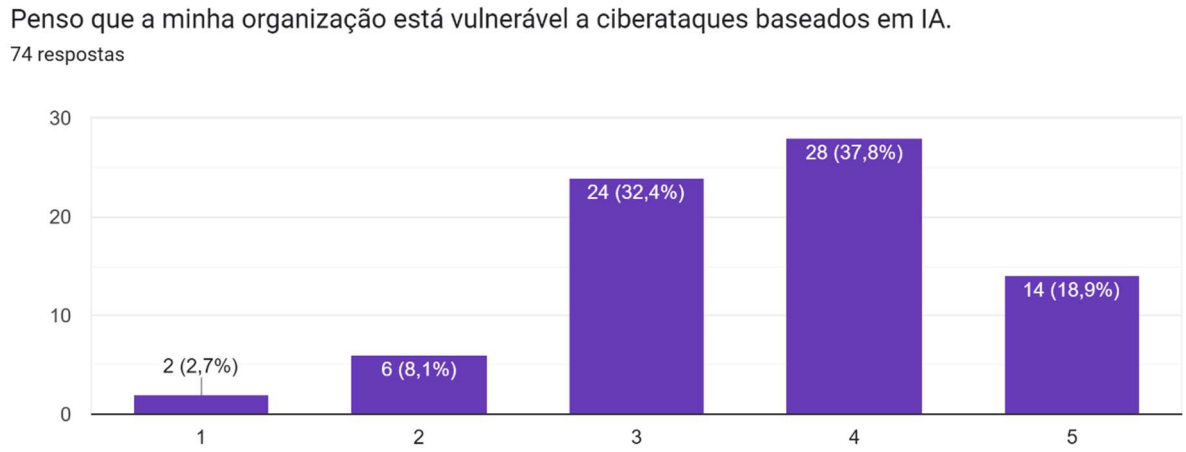
Conclusões Principais:

- **Perceção Generalizada de Maior Dificuldade de Deteção:** Uma grande maioria dos participantes (somando as categorias 4 e 5, que representam 37,8% + 33,8% = **71,6%**) acredita que os ciberataques baseados em IA são mais difíceis de detetar do que os ciberataques tradicionais.
- **Reconhecimento do Desafio da IA na Cibersegurança:** Os resultados demonstram que existe uma forte consciência da complexidade adicional que a IA introduz na deteção de ameaças cibernéticas.
- **Necessidade de Avanços em Deteção:** A perceção de maior dificuldade pode indicar uma lacuna nas capacidades atuais de deteção ou na familiaridade com ferramentas e técnicas de defesa específicas contra ataques de IA.

Em suma, este gráfico sugere que há um reconhecimento generalizado de que a IA aumenta a sofisticação dos ciberataques, tornando-os mais desafiadores de identificar em comparação com os métodos tradicionais.

A Figura 24, apresenta a Perceção de Vulnerabilidade Organizacional a Ciberataques com Inteligência Artificial

Figura 24 - Perceção de Vulnerabilidade Organizacional a Ciberataques com Inteligência Artificial



Fonte: Dados do questionário da pergunta n.º 23 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a perceção dos participantes sobre a vulnerabilidade da sua organização a ciberataques baseados em Inteligência Artificial (IA). A pergunta específica da investigação foi "Penso que a minha organização está vulnerável a ciberataques baseados em IA.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa discorda completamente da afirmação, ou seja, acredita que a sua organização **não é vulnerável** a ciberataques baseados em IA.
- **2 (Discordo):** A pessoa discorda da afirmação, indicando que a sua organização é **pouco vulnerável** a esses ataques.
- **3 (Neutro):** A pessoa está numa posição neutra, o que pode indicar incerteza sobre a vulnerabilidade da organização, ou uma perceção de vulnerabilidade moderada.

- **4 (Concordo):** A pessoa concorda com a afirmação, indicando que acredita que a sua organização está **vulnerável** a ciberataques baseados em IA.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação, indicando uma forte crença de que a sua organização está **muito vulnerável** a ciberataques baseados em IA.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente - Não vulnerável):** 2 respostas (2,7%) – Uma minoria muito pequena acredita que a sua organização não é vulnerável.
- **Nível 2 (Discordo - Pouco vulnerável):** 6 respostas (8,1%) – Outra pequena minoria considera a sua organização pouco vulnerável.
- **Nível 3 (Neutro - Vulnerabilidade moderada/incerteza):** 24 respostas (32,4%) – Este grupo representa uma porção significativa dos inquiridos, indicando incerteza ou uma perceção de vulnerabilidade moderada.
- **Nível 4 (Concordo - Vulnerável):** 28 respostas (37,8%) – Esta é a categoria mais frequente, sugerindo que a maioria dos participantes concorda que a sua organização está vulnerável.
- **Nível 5 (Concordo totalmente - Muito vulnerável):** 14 respostas (18,9%) – Um número considerável de inquiridos concorda totalmente, indicando uma forte perceção de vulnerabilidade.

Conclusões Principais:

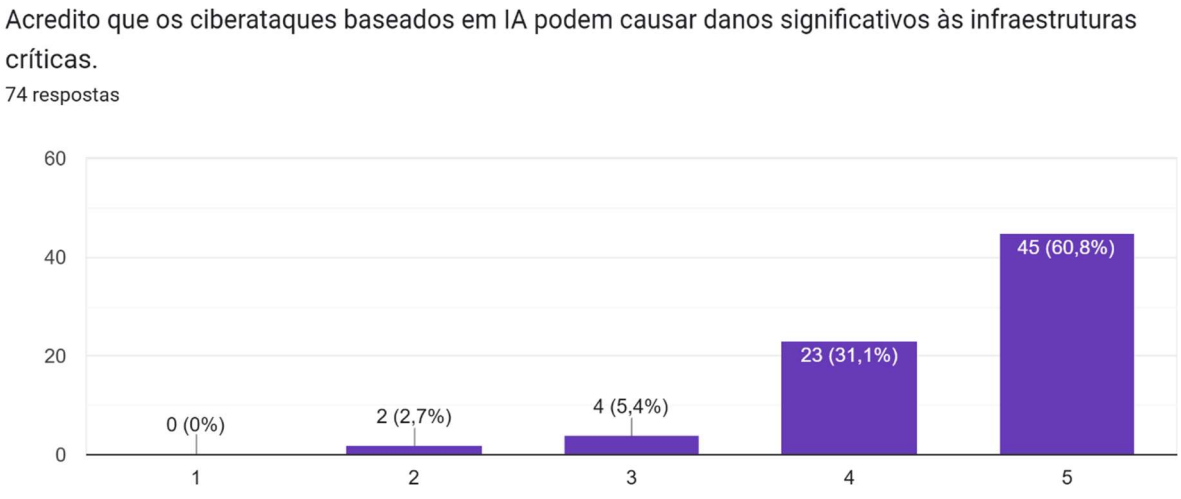
- **Perceção de Vulnerabilidade Elevada:** A maioria dos participantes (somando as categorias 4 e 5, que representam 37,8% + 18,9% = **56,7%**) acredita que a sua organização está vulnerável ou muito vulnerável a ciberataques baseados em IA.
- **Incerteza Significativa:** Quase um terço dos inquiridos (32,4%) está na categoria "Neutro", o que pode indicar falta de clareza sobre o nível de segurança da sua organização face a estas ameaças.

- **Baixa Confiança na Resiliência:** Apenas uma pequena minoria (2,7% + 8,1% = 10,8%) discorda ou discorda totalmente da vulnerabilidade da sua organização, sugerindo que a confiança na resiliência é baixa.
- **Implicação para Estratégias de Segurança:** Esta perceção generalizada de vulnerabilidade, combinada com uma parcela significativa de incerteza, aponta para a necessidade urgente de as organizações avaliarem e reforçarem as suas defesas contra ciberataques baseados em IA.

Em suma, o gráfico revela que a maioria dos participantes percebe as suas organizações como vulneráveis a ciberataques baseados em IA, com uma porção considerável a demonstrar incerteza, sublinhando a importância de fortalecer as estratégias de cibersegurança neste domínio.

A Figura 25, apresenta a Perceção sobre o Impacto dos Ciberataques com IA nas Infraestruturas Críticas

Figura 25 - Perceção sobre o Impacto dos Ciberataques com IA nas Infraestruturas Críticas



Fonte: Dados do questionário da pergunta n.º 24 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a crença dos participantes sobre o potencial dos ciberataques baseados em Inteligência Artificial (IA) em causar danos significativos às infraestruturas críticas. A pergunta específica da investigação foi "Acredito que os ciberataques baseados em IA podem causar danos significativos às infraestruturas críticas.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não acredita que ciberataques baseados em IA possam causar danos significativos às infraestruturas críticas.
- **2 (Discordo):** A pessoa tem pouca crença no potencial de danos significativos.
- **3 (Neutro):** A pessoa está numa posição neutra, indicando incerteza ou uma crença moderada no potencial de dano.
- **4 (Concordo):** A pessoa concorda com a afirmação, acreditando que ciberataques baseados em IA podem causar danos significativos às infraestruturas críticas.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação, tendo uma forte crença de que esses ciberataques representam um perigo muito significativo para as infraestruturas críticas.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 0 respostas (0%) – Ninguém discorda totalmente, o que indica um consenso de que há, no mínimo, algum potencial de dano.
- **Nível 2 (Discordo):** 2 respostas (2,7%) – Uma minoria muito pequena dos inquiridos tem pouca crença no potencial de dano significativo.
- **Nível 3 (Neutro):** 4 respostas (5,4%) – Uma pequena percentagem está neutra, o que pode indicar incerteza sobre a extensão do potencial de dano.
- **Nível 4 (Concordo):** 23 respostas (31,1%) – Um número considerável de participantes concorda que os ciberataques baseados em IA podem causar danos significativos.

- **Nível 5 (Concordo totalmente):** 45 respostas (60,8%) – Esta é a categoria dominante, com a maioria esmagadora dos inquiridos a concordar totalmente com a afirmação, indicando uma forte crença no alto potencial destrutivo.

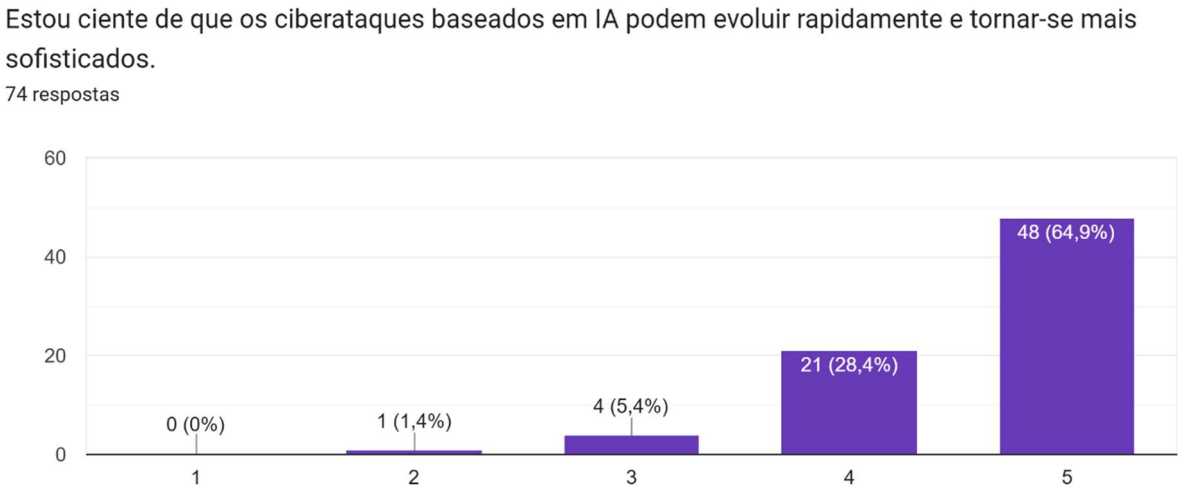
Conclusões Principais:

- **Elevada Preocupação com Infraestruturas Críticas:** A grande maioria dos participantes (somando as categorias 4 e 5, que representam 31,1% + 60,8% = **91,9%**) acredita que os ciberataques baseados em IA podem causar danos significativos às infraestruturas críticas.
- **Reconhecimento da Vulnerabilidade Estratégica:** Os resultados demonstram uma forte consciência da ameaça séria que a IA representa para sistemas essenciais e serviços públicos.
- **Consenso Quase Total:** A ausência de respostas nas categorias de desacordo total e o baixo número nas categorias de desacordo e neutro sublinham um consenso quase unânime sobre a gravidade da ameaça.

Em suma, este gráfico revela que a audiência inquirida tem uma perceção muito elevada e generalizada de que os ciberataques baseados em IA representam um perigo significativo e potencialmente devastador para as infraestruturas críticas.

A Figura 26, apresenta a Perceção da Rapidez e Complexidade Crescente dos Ciberataques Baseados em IA

Figura 26 - Perceção da Rapidez e Complexidade Crescente dos Ciberataques Baseados em IA



Fonte: Dados do questionário da pergunta n.º 25 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a consciência dos participantes sobre a capacidade de evolução e sofisticação dos ciberataques baseados em Inteligência Artificial (IA). A pergunta específica da investigação foi "Estou ciente de que os ciberataques baseados em IA podem evoluir rapidamente e tornar-se mais sofisticados.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não está ciente ou não acredita que os ciberataques baseados em IA evoluam rapidamente ou se tornem mais sofisticados.
- **2 (Discordo):** A pessoa tem pouca consciência ou não acredita fortemente na evolução rápida e sofisticação desses ataques.
- **3 (Neutro):** A pessoa está numa posição neutra, o que pode indicar incerteza ou uma consciência moderada.

- **4 (Concordo):** A pessoa concorda com a afirmação, indicando que está ciente da evolução rápida e sofisticação dos ciberataques baseados em IA.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação, indicando uma forte consciência da capacidade de rápida evolução e sofisticação desses ciberataques.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 0 respostas (0%) – Nenhum dos participantes discorda totalmente, o que sugere um consenso de que os ciberataques baseados em IA, pelo menos, têm alguma capacidade de evolução.
- **Nível 2 (Discordo):** 1 resposta (1,4%) – Apenas uma minoria insignificante discorda da afirmação.
- **Nível 3 (Neutro):** 4 respostas (5,4%) – Uma pequena percentagem dos inquiridos está neutra, talvez indicando alguma incerteza ou menor perceção da velocidade dessa evolução.
- **Nível 4 (Concordo):** 21 respostas (28,4%) – Um número considerável de participantes concorda que os ciberataques baseados em IA podem evoluir rapidamente e tornar-se mais sofisticados.
- **Nível 5 (Concordo totalmente):** 48 respostas (64,9%) – Esta é a categoria dominante, com a maioria esmagadora dos inquiridos a concordar totalmente com a afirmação, indicando uma forte consciência da dinâmica evolutiva desses ciberataques.

Conclusões Principais:

- **Elevada Consciência da Dinâmica Evolutiva:** A grande maioria dos participantes (somando as categorias 4 e 5, que representam 28,4% + 64,9% = **93,3%**) está ciente de que os ciberataques baseados em IA podem evoluir rapidamente e tornar-se mais sofisticados.
- **Reconhecimento da Natureza Mutável da Ameaça:** Os resultados demonstram um entendimento sólido por parte da audiência inquirida de que a IA não só representa uma

ameaça significativa (como visto em gráficos anteriores), mas também é uma ameaça em constante mudança e aperfeiçoamento.

- **Implicações para a Defesa:** Esta alta consciência implica que há um reconhecimento generalizado da necessidade de abordagens de cibersegurança proativas e adaptativas, capazes de acompanhar a evolução das ameaças.

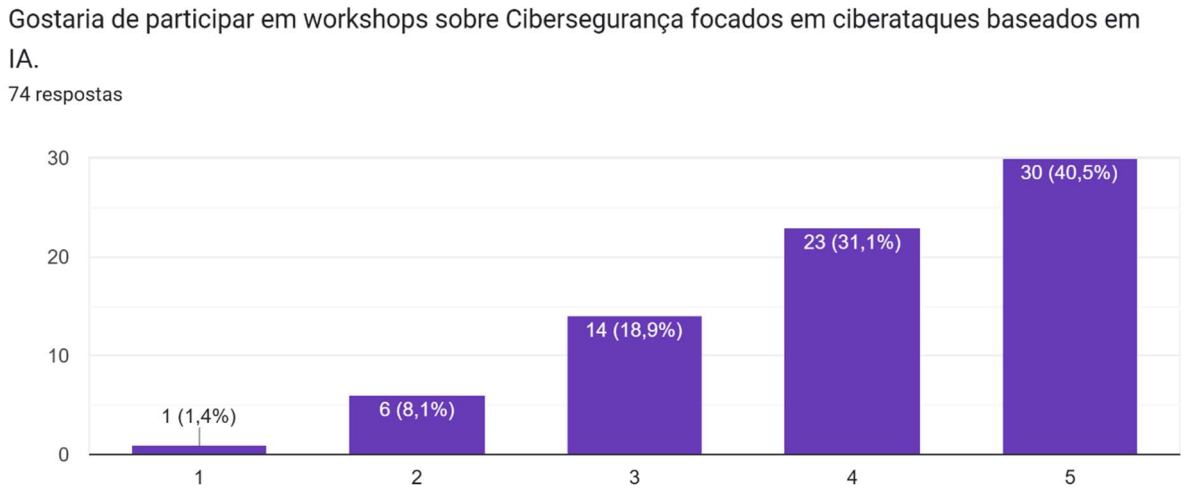
Em suma, este gráfico indica um forte e quase unânime reconhecimento de que os ciberataques impulsionados por IA são uma ameaça dinâmica e em constante evolução, o que é crucial para o desenvolvimento de estratégias de defesa eficazes.

5.5 Propor soluções educacionais: desenvolver métodos para melhorar o conhecimento e a preparação dos utilizadores contra essas ameaças.

A crescente sofisticação e frequência dos ciberataques exige não apenas soluções tecnológicas robustas, mas também uma resposta educativa eficaz. A preparação dos utilizadores para enfrentar ameaças digitais depende, em grande medida, do seu nível de literacia em cibersegurança. Este subcapítulo propõe-se a desenvolver e apresentar métodos educativos que visam melhorar o conhecimento, a perceção de risco e a capacidade de resposta dos utilizadores face a incidentes cibernéticos. Através da análise de boas práticas, programas de formação e abordagens pedagógicas inovadoras, pretende-se delinear estratégias que promovam comportamentos mais seguros e conscientes no ambiente digital. O objetivo é contribuir para uma cultura de cibersegurança mais sólida e participativa, onde cada utilizador desempenha um papel ativo na proteção do ecossistema digital.

A Figura 27, apresenta o Nível de Interesse em Participar em Workshops sobre Ciberataques com IA

Figura 27 - Nível de Interesse em Participar em Workshops sobre Ciberataques com IA



Fonte: Dados do questionário da pergunta n.º 26 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou o interesse dos participantes em frequentar *workshops* sobre Cibersegurança com foco em ciberataques baseados em Inteligência Artificial (IA). A pergunta específica da investigação foi "Gostaria de participar em workshops sobre Cibersegurança focados em ciberataques baseados em IA.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não tem nenhum interesse em participar de tais *workshops*.
- **2 (Discordo):** A pessoa tem pouco interesse em participar.
- **3 (Neutro):** A pessoa tem um interesse moderado ou está indecisa sobre a participação.
- **4 (Concordo):** A pessoa tem interesse em participar dos *workshops*.

- **5 (Concordo totalmente):** A pessoa tem um interesse muito forte em participar dos *workshops*.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 1 resposta (1,4%) – Uma minoria muito pequena não tem interesse.
- **Nível 2 (Discordo):** 6 respostas (8,1%) – Um pequeno grupo tem pouco interesse.
- **Nível 3 (Neutro):** 14 respostas (18,9%) – Quase um quinto dos inquiridos está neutro, indicando que o interesse não é nem forte nem ausente.
- **Nível 4 (Concordo):** 23 respostas (31,1%) – Um número considerável de participantes expressa interesse em participar.
- **Nível 5 (Concordo totalmente):** 30 respostas (40,5%) – Esta é a categoria dominante, com a maior parte dos inquiridos a manifestar um interesse muito forte em participar.

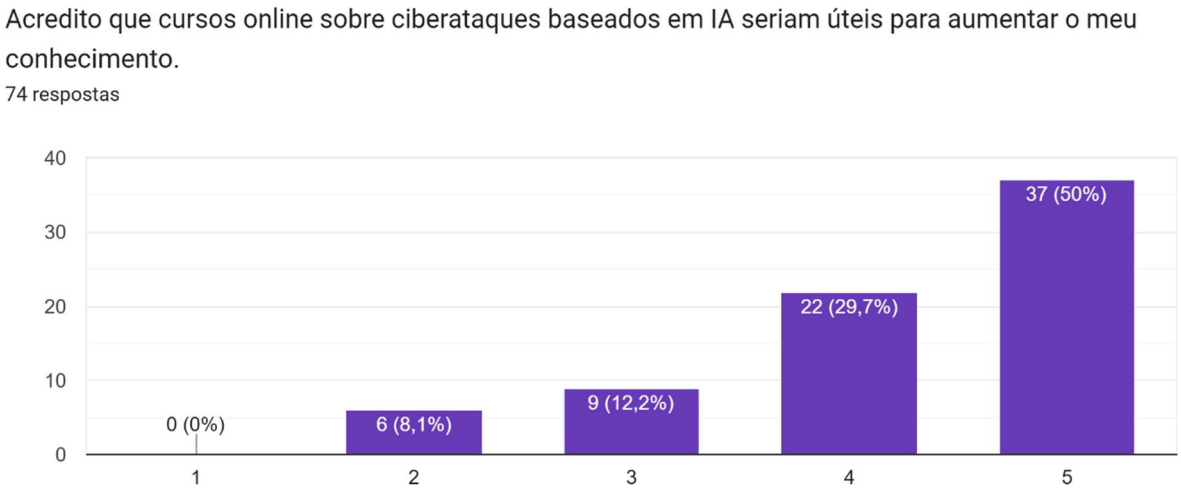
Conclusões Principais:

- **Elevado Interesse em Formação Específica:** A grande maioria dos participantes (somando as categorias 4 e 5, que representam 31,1% + 40,5% = **71,6%**) tem interesse ou muito interesse em participar de *workshops* sobre cibersegurança focados em ciberataques baseados em IA.
- **Procura por Conhecimento Especializado:** Este resultado indica uma forte procura por conhecimento e formação aprofundada sobre as nuances dos ciberataques impulsionados pela IA, refletindo a perceção de ameaça e a necessidade de se manter atualizado.
- **Oportunidade para Educação:** A elevada vontade de participar sugere uma excelente oportunidade para o desenvolvimento e oferta de programas de capacitação e *workshops* nesta área.

Em suma, o gráfico demonstra um claro e expressivo desejo por parte da audiência inquirida em aprofundar os seus conhecimentos sobre cibersegurança e ataques baseados em IA através de formação especializada.

A Figura 28, apresenta a Perceção sobre a Utilidade de Cursos Online sobre Ciberataques com IA

Figura 28 - Perceção sobre a Utilidade de Cursos Online sobre Ciberataques com IA



Fonte: Dados do questionário da pergunta n.º 27 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a perceção dos participantes sobre a utilidade de cursos online focados em ciberataques baseados em Inteligência Artificial (IA) para aumentar o seu conhecimento. A pergunta específica da investigação foi "Acredito que cursos online sobre ciberataques baseados em IA seriam úteis para aumentar o meu conhecimento.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não acredita que cursos online seriam úteis para aumentar o seu conhecimento sobre o tema.
- **2 (Discordo):** A pessoa acredita que seriam pouco úteis.
- **3 (Neutro):** A pessoa está numa posição neutra, o que pode indicar incerteza sobre a utilidade, ou uma utilidade moderada.

- **4 (Concordo):** A pessoa concorda com a afirmação, acreditando que cursos online seriam úteis para aumentar o seu conhecimento.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação, tendo uma forte crença na utilidade desses cursos para o aumento do conhecimento.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 0 respostas (0%) – Ninguém discorda totalmente, o que sugere um consenso de que os cursos online teriam, pelo menos, alguma utilidade.
- **Nível 2 (Discordo):** 6 respostas (8,1%) – Uma pequena minoria acredita que os cursos online seriam pouco úteis.
- **Nível 3 (Neutro):** 9 respostas (12,2%) – Uma percentagem menor dos inquiridos está neutra.
- **Nível 4 (Concordo):** 22 respostas (29,7%) – Um número considerável de participantes concorda que cursos online seriam úteis.
- **Nível 5 (Concordo totalmente):** 37 respostas (50%) – Esta é a categoria dominante, com metade dos inquiridos a concordar totalmente que cursos online seriam muito úteis para aumentar o seu conhecimento.

Conclusões Principais:

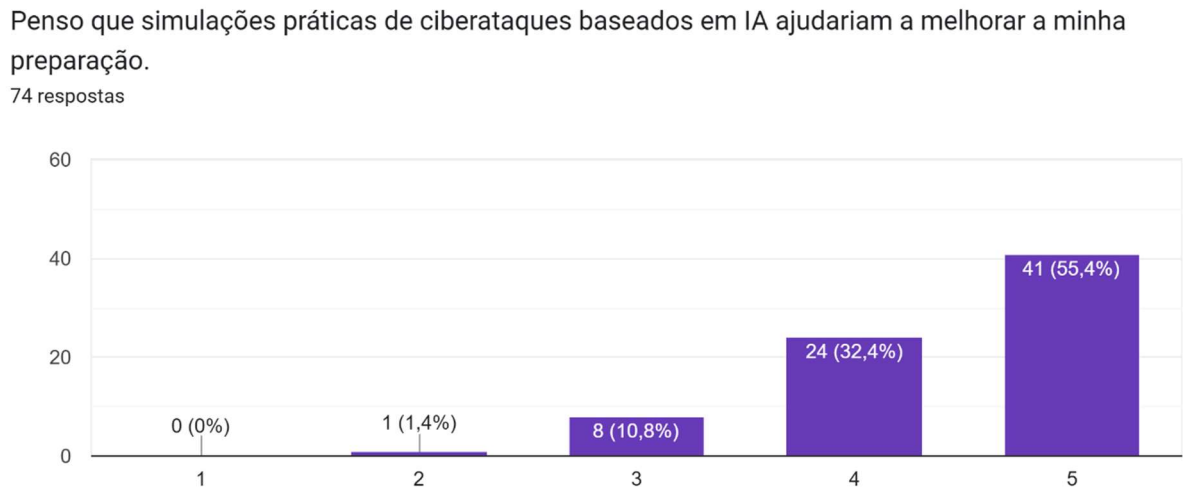
- **Elevada Perceção de Utilidade de Cursos Online:** A grande maioria dos participantes (somando as categorias 4 e 5, que representam 29,7% + 50% = **79,7%**) acredita que cursos online sobre ciberataques baseados em IA seriam úteis ou muito úteis para aumentar o seu conhecimento.
- **Preferência por Formatos Flexíveis:** Este resultado, em conjunto com o interesse em *workshops* (observado em gráficos anteriores), indica uma forte procura por oportunidades de aprendizagem sobre ciberataques baseados em IA, com uma clara aceitação e preferência por formatos flexíveis como os cursos online.

- **Oportunidade para Desenvolvimento de Conteúdo:** A alta percentagem de concordância nas categorias mais elevadas sugere uma demanda significativa por recursos educacionais online nesta área.

Em suma, este gráfico revela um desejo claro e generalizado por parte da audiência inquirida em expandir o seu conhecimento sobre ciberataques baseados em IA através de cursos *online*, indicando um mercado recetivo para tais ofertas educacionais.

A Figura 29, apresenta a Perceção da Utilidade de Simulações de Ciberataques Baseados em IA para Preparação Pessoal

Figura 29 - Perceção da Utilidade de Simulações de Ciberataques Baseados em IA para Preparação Pessoal



Fonte: Dados do questionário da pergunta n.º 28 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a perceção dos participantes sobre a utilidade de simulações práticas de ciberataques baseados em Inteligência Artificial (IA) para melhorar a sua preparação. A pergunta específica da investigação foi "Penso que simulações práticas de ciberataques baseados em IA ajudariam a melhorar a minha preparação.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não acredita que simulações práticas seriam úteis para a sua preparação.
- **2 (Discordo):** A pessoa acredita que seriam pouco úteis.
- **3 (Neutro):** A pessoa tem uma opinião neutra ou incerta sobre a utilidade das simulações.
- **4 (Concordo):** A pessoa concorda que simulações práticas seriam úteis para melhorar a sua preparação.
- **5 (Concordo totalmente):** A pessoa concorda totalmente que simulações práticas seriam muito úteis para a sua preparação.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 0 respostas (0%) – Nenhum dos participantes discorda totalmente, indicando um consenso de que as simulações práticas teriam, no mínimo, alguma utilidade.
- **Nível 2 (Discordo):** 1 resposta (1,4%) – Uma minoria muito pequena não vê grande utilidade em simulações.
- **Nível 3 (Neutro):** 8 respostas (10,8%) – Uma pequena percentagem dos inquiridos está neutra.
- **Nível 4 (Concordo):** 24 respostas (32,4%) – Um número significativo de participantes concorda que simulações práticas seriam úteis.
- **Nível 5 (Concordo totalmente):** 41 respostas (55,4%) – Esta é a categoria dominante, com a maioria dos inquiridos a concordar totalmente que simulações práticas seriam muito úteis para melhorar a sua preparação.

Conclusões Principais:

- **Grande Desejo por Experiência Prática:** Uma esmagadora maioria dos participantes (somando as categorias 4 e 5, que representam 32,4% + 55,4% = **87,8%**) acredita que

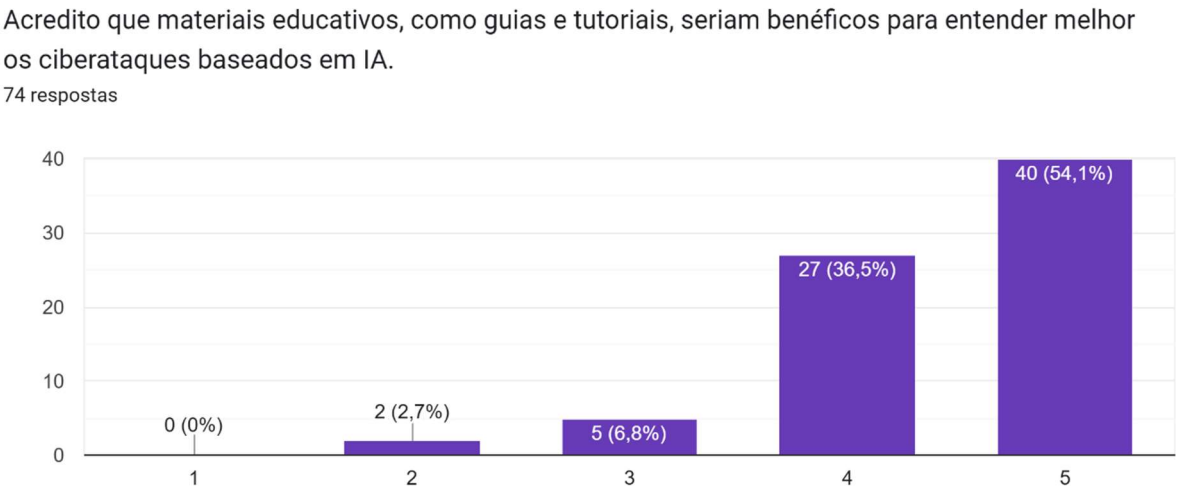
simulações práticas de ciberataques baseados em IA seriam úteis ou muito úteis para melhorar a sua preparação.

- **Reconhecimento da Eficácia da Aprendizagem Ativa:** Este resultado sugere que os inquiridos valorizam a aprendizagem prática e experiencial como um método eficaz para se prepararem para ameaças complexas como os ciberataques impulsionados por IA.
- **Procura por Ferramentas de Treino Avançadas:** A alta percentagem de concordância indica uma forte procura por ambientes de simulação e ferramentas de treino que permitam aos indivíduos praticar a defesa contra este tipo de ataques.

Em suma, o gráfico demonstra um desejo muito forte e generalizado por parte da audiência inquirida em participar de simulações práticas de ciberataques baseados em IA, reconhecendo o valor dessas experiências para melhorar a sua preparação e capacidade de resposta.

A Figura 30, apresenta a Perceção da Eficácia de Guias e Tutoriais sobre Ciberataques Baseados em IA

Figura 30 - Perceção da Eficácia de Guias e Tutoriais sobre Ciberataques Baseados em IA



Fonte: Dados do questionário da pergunta n.º 29 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a perceção dos participantes sobre a utilidade de materiais educativos (guias e tutoriais) para melhorar a sua compreensão sobre ciberataques baseados em Inteligência Artificial (IA). A pergunta específica da investigação foi "Acredito que materiais educativos, como guias e tutoriais, seriam benéficos para entender melhor os ciberataques baseados em IA.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não acredita que materiais educativos seriam benéficos.
- **2 (Discordo):** A pessoa acredita que seriam pouco benéficos.
- **3 (Neutro):** A pessoa tem uma opinião neutra ou incerta sobre o benefício desses materiais.
- **4 (Concordo):** A pessoa concorda que materiais educativos seriam benéficos para entender melhor os ciberataques baseados em IA.
- **5 (Concordo totalmente):** A pessoa concorda totalmente que materiais educativos seriam muito benéficos.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 0 respostas (0%) – Ninguém discorda totalmente, o que sugere um consenso de que esses materiais teriam, no mínimo, algum benefício.
- **Nível 2 (Discordo):** 2 respostas (2,7%) – Uma minoria muito pequena não vê grande benefício em materiais educativos.
- **Nível 3 (Neutro):** 5 respostas (6,8%) – Uma pequena percentagem dos respondentes está neutra.
- **Nível 4 (Concordo):** 27 respostas (36,5%) – Um número expressivo de participantes concorda que materiais educativos seriam benéficos.

- **Nível 5 (Concordo totalmente):** 40 respostas (54,1%) – Esta é a categoria dominante, com a maioria dos inquiridos a concordar totalmente que esses materiais seriam muito benéficos para a sua compreensão.

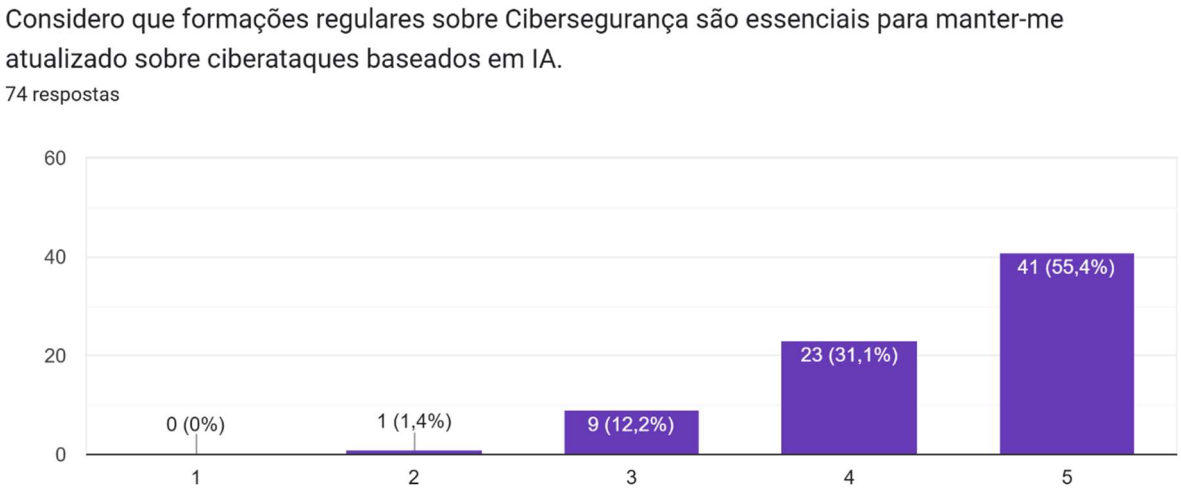
Conclusões Principais:

- **Alta Valorização de Materiais Educativos:** Uma vasta maioria dos participantes (somando as categorias 4 e 5, que representam 36,5% + 54,1% = **90,6%**) acredita que guias e tutoriais seriam benéficos ou muito benéficos para entender ciberataques baseados em IA.
- **Preferência por Recursos Acessíveis:** O resultado indica uma forte preferência por formatos de aprendizagem mais passivos e acessíveis, como guias e tutoriais, complementando o interesse por *workshops* e cursos *online* visto em gráficos anteriores.
- **Procura por Conteúdo Claro e Direto:** A alta adesão a esta categoria sugere uma clara necessidade de desenvolvimento e disponibilização de materiais informativos bem estruturados e fáceis de consumir, que expliquem a complexidade dos ciberataques baseados em IA.

Em suma, este gráfico demonstra um desejo muito forte e generalizado por parte da audiência em ter acesso a materiais educativos de fácil consumo, como guias e tutoriais, para aprofundar a sua compreensão sobre ciberataques baseados em IA.

A Figura 31, apresenta a Perceção sobre a Relevância de Formação Contínua em Cibersegurança com Foco em IA

Figura 31 - Perceção sobre a Relevância de Formação Contínua em Cibersegurança com Foco em IA



Fonte: Dados do questionário da pergunta n.º 30 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a perceção dos participantes sobre a essencialidade de formações regulares em Cibersegurança para se manterem atualizados sobre ciberataques baseados em Inteligência Artificial (IA). A pergunta específica da investigação foi "Considero que formações regulares sobre Cibersegurança são essenciais para manter-me atualizado sobre ciberataques baseados em IA.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não considera formações regulares essenciais.
- **2 (Discordo):** A pessoa considera-as pouco essenciais.
- **3 (Neutro):** A pessoa tem uma opinião neutra ou incerta sobre a essencialidade dessas formações.

- **4 (Concordo):** A pessoa concorda que formações regulares são essenciais para se manter atualizado.
- **5 (Concordo totalmente):** A pessoa concorda totalmente que formações regulares são muito essenciais para se manter atualizado.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 0 respostas (0%) – Nenhum dos participantes discorda totalmente, indicando um consenso de que a formação regular é, no mínimo, algo importante.
- **Nível 2 (Discordo):** 1 resposta (1,4%) – Uma minoria muito pequena não considera as formações regulares essenciais.
- **Nível 3 (Neutro):** 9 respostas (12,2%) – Uma pequena percentagem dos inquiridos está neutra.
- **Nível 4 (Concordo):** 23 respostas (31,1%) – Um número considerável de participantes concorda que as formações regulares são essenciais.
- **Nível 5 (Concordo totalmente):** 41 respostas (55,4%) – Esta é a categoria dominante, com a maioria dos inquiridos a concordar totalmente que as formações regulares são muito essenciais para se manterem atualizados.

Conclusões Principais:

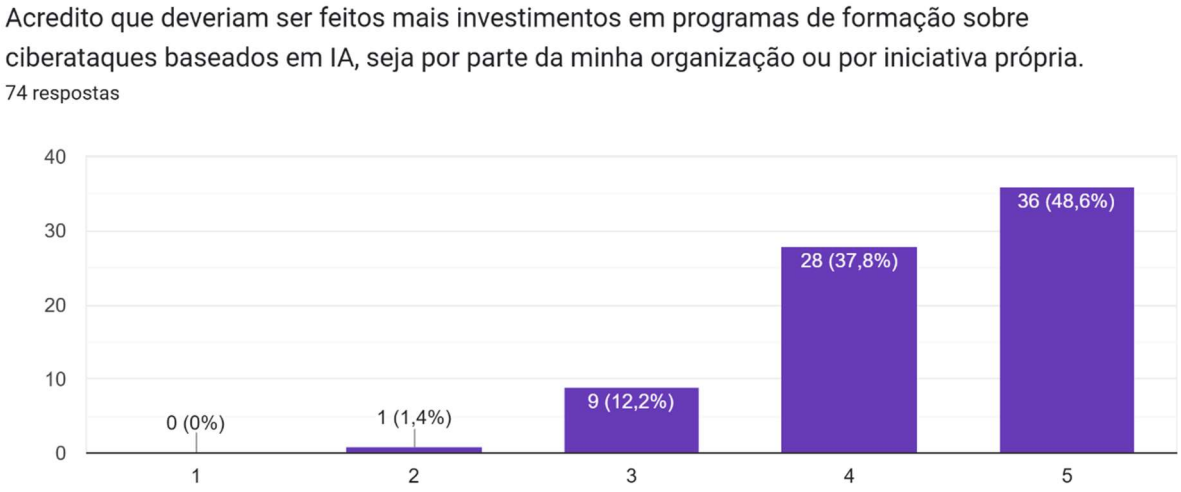
- **Reconhecimento da Essencialidade da Formação Contínua:** Uma esmagadora maioria dos participantes (somando as categorias 4 e 5, que representam 31,1% + 55,4% = **86,5%**) considera que formações regulares em cibersegurança são essenciais ou muito essenciais para se manterem atualizados sobre ciberataques baseados em IA.
- **Consciência da Dinâmica da Ameaça:** Este resultado reforça a perceção (já observada em gráficos anteriores) de que os ciberataques baseados em IA são uma ameaça em constante evolução e que o conhecimento estático não é suficiente para combatê-los.

- **Importância da Educação Contínua:** Há um claro reconhecimento da necessidade de um compromisso contínuo com a aprendizagem e atualização de conhecimentos para enfrentar os desafios colocados pela IA no cenário da cibersegurança.

Em suma, o gráfico demonstra um consenso muito forte entre os participantes de que a formação contínua e regular em cibersegurança é crucial para acompanhar a evolução dos ciberataques baseados em IA.

A Figura 32, apresenta a Perceção sobre a Necessidade de Investimento em Formação sobre Ciberataques Baseados em IA

Figura 32 - Perceção sobre a Necessidade de Investimento em Formação sobre Ciberataques Baseados em IA



Fonte: Dados do questionário da pergunta n.º 31 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a perceção dos participantes sobre a necessidade de mais investimentos em programas de formação sobre ciberataques baseados em Inteligência Artificial (IA), quer por parte da sua organização, quer por iniciativa própria. A pergunta específica da investigação foi "Acredito que deveriam ser

feitos mais investimentos em programas de formação sobre ciberataques baseados em IA, seja por parte da minha organização ou por iniciativa própria.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não acredita que deveriam ser feitos mais investimentos.
- **2 (Discordo):** A pessoa acredita que deveriam ser feitos poucos investimentos adicionais.
- **3 (Neutro):** A pessoa tem uma opinião neutra ou incerta sobre a necessidade de mais investimentos.
- **4 (Concordo):** A pessoa concorda que deveriam ser feitos mais investimentos.
- **5 (Concordo totalmente):** A pessoa concorda totalmente que deveriam ser feitos muitos mais investimentos.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 0 respostas (0%) – Nenhum dos participantes discorda totalmente, o que indica um consenso de que investimentos adicionais são, no mínimo, relevantes.
- **Nível 2 (Discordo):** 1 resposta (1,4%) – Uma minoria muito pequena não vê a necessidade de mais investimentos.
- **Nível 3 (Neutro):** 9 respostas (12,2%) – Uma pequena percentagem dos inquiridos está neutra.
- **Nível 4 (Concordo):** 28 respostas (37,8%) – Um número considerável de participantes concorda que deveriam ser feitos mais investimentos.
- **Nível 5 (Concordo totalmente):** 36 respostas (48,6%) – Esta é a categoria dominante, com quase metade dos inquiridos a concordar totalmente que deveriam ser feitos muitos mais investimentos em formação.

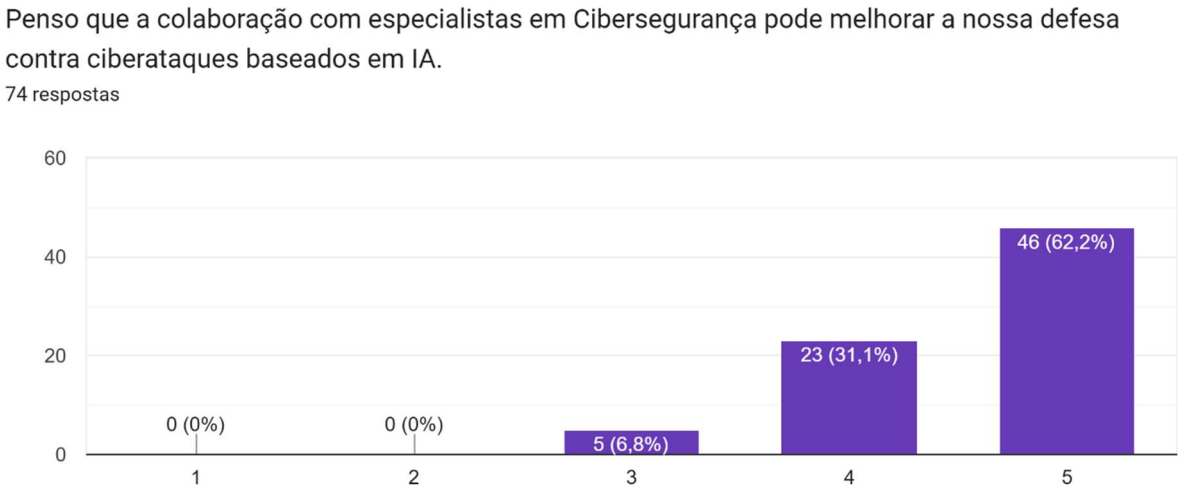
Conclusões Principais:

- **Forte Procura por Mais Investimento em Formação:** Uma esmagadora maioria dos participantes (somando as categorias 4 e 5, que representam 37,8% + 48,6% = **86,4%**) acredita que deveriam ser feitos mais investimentos em programas de formação sobre ciberataques baseados em IA.
- **Reconhecimento da Necessidade de Recursos:** Este resultado reforça a perceção de que o conhecimento atual e as defesas existentes podem não ser suficientes para lidar com a ameaça da IA na cibersegurança, e que é preciso mais recursos para capacitação.
- **Implicação para Organizações e Indivíduos:** A disposição para que os investimentos sejam feitos "seja por parte da minha organização ou por iniciativa própria" demonstra uma dupla responsabilidade percebida. As organizações são incentivadas a investir, mas os indivíduos também estão dispostos a tomar a iniciativa para se capacitarem.

Em suma, o gráfico revela um desejo claro e generalizado por mais investimento em formação sobre ciberataques baseados em IA, destacando a importância percebida da educação e preparação para enfrentar esta ameaça em evolução.

A Figura 33, apresenta a Perceção da Relevância da Colaboração Técnica na Defesa contra Ciberataques Baseados em IA

Figura 33 - Perceção da Relevância da Colaboração Técnica na Defesa contra Ciberataques Baseados em IA



Fonte: Dados do questionário da pergunta n.º 32 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a perceção dos participantes sobre o quanto a colaboração com especialistas em Cibersegurança pode melhorar a defesa contra ciberataques baseados em Inteligência Artificial (IA). A pergunta específica da investigação foi "Penso que a colaboração com especialistas em Cibersegurança pode melhorar a nossa defesa contra ciberataques baseados em IA.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não acredita que a colaboração com especialistas melhore a defesa.
- **2 (Discordo):** A pessoa tem pouca convicção de que a colaboração seja benéfica.
- **3 (Neutro):** A pessoa tem uma opinião neutra ou incerta sobre o impacto da colaboração.

- **4 (Concordo):** A pessoa concorda que a colaboração com especialistas pode melhorar a defesa.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação, indicando uma forte crença no benefício da colaboração.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 0 respostas (0%) – Nenhum dos participantes discorda totalmente, o que sugere um consenso de que a colaboração tem, no mínimo, algum valor.
- **Nível 2 (Discordo):** 0 respostas (0%) – Ninguém discorda, reforçando a ideia de que a colaboração é vista de forma positiva.
- **Nível 3 (Neutro):** 5 respostas (6,8%) – Uma minoria muito pequena dos inquiridos está neutra.
- **Nível 4 (Concordo):** 23 respostas (31,1%) – Um número considerável de participantes concorda que a colaboração com especialistas pode melhorar a defesa.
- **Nível 5 (Concordo totalmente):** 46 respostas (62,2%) – Esta é a categoria dominante, com a maioria esmagadora dos inquiridos a concordar totalmente com a afirmação, indicando uma fortíssima crença na utilidade da colaboração.

Conclusões Principais:

- **Elevadíssima Valorização da Colaboração:** A grande maioria dos participantes (somando as categorias 4 e 5, que representam 31,1% + 62,2% = **93,3%**) acredita que a colaboração com especialistas em Cibersegurança é benéfica ou muito benéfica para melhorar a defesa contra ciberataques baseados em IA.
- **Reconhecimento da *Expertise* Externa:** Os resultados demonstram um claro reconhecimento de que a complexidade dos ciberataques baseados em IA exige o conhecimento e a experiência de especialistas.

- **Abertura para Parcerias e Conhecimento Compartilhado:** Há uma forte indicação de que as organizações e indivíduos estão abertos a procurar e estabelecer parcerias com especialistas em cibersegurança para fortalecer as suas defesas.

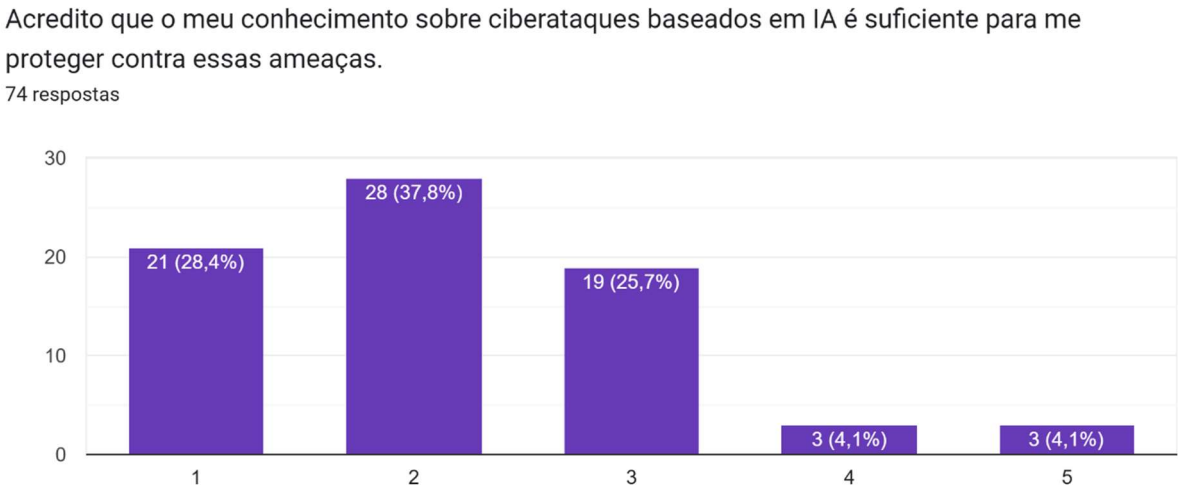
Em suma, este gráfico revela um consenso esmagador de que a colaboração com especialistas em cibersegurança é vista como um fator crucial e altamente eficaz para melhorar a defesa contra os desafios impostos pelos ciberataques baseados em IA.

5.6 Impacto das ameaças: examinar como o nível de conhecimento afeta a vulnerabilidade dos utilizadores a ciberataques.

Num ambiente digital em constante evolução, onde os ciberataques se tornam cada vez mais sofisticados, o conhecimento dos utilizadores desempenha um papel crucial na sua capacidade de se protegerem. Este subcapítulo tem como objetivo examinar a relação entre o nível de literacia em cibersegurança e a vulnerabilidade dos indivíduos face a ameaças digitais, com especial destaque para os ciberataques baseados em inteligência artificial. Através da análise de dados recolhidos, pretende-se compreender de que forma a falta de conhecimento pode aumentar o risco de exposição, e como a formação adequada pode mitigar esse risco. Esta abordagem permite identificar lacunas críticas na preparação dos utilizadores e fundamentar estratégias educativas mais eficazes para fortalecer a resiliência digital.

A Figura 34, apresenta a Perceção da Suficiência do Conhecimento para Enfrentar Ciberataques com IA

Figura 34 - Perceção da Suficiência do Conhecimento para Enfrentar Ciberataques com IA



Fonte: Dados do questionário da pergunta n.º 33 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou o nível de autoconfiança dos participantes em relação à suficiência do seu conhecimento sobre ciberataques baseados em Inteligência Artificial (IA) para se protegerem contra essas ameaças. A pergunta específica da investigação foi "Acredito que o meu conhecimento sobre ciberataques baseados em IA é suficiente para me proteger contra essas ameaças.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não acredita que o seu conhecimento seja suficiente.
- **2 (Discordo):** A pessoa tem pouca confiança na suficiência do seu conhecimento.
- **3 (Neutro):** A pessoa tem uma opinião neutra ou incerta sobre a suficiência do seu conhecimento.

- **4 (Concordo):** A pessoa concorda que o seu conhecimento é suficiente para se proteger.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação, indicando uma forte confiança na suficiência do seu conhecimento.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 21 respostas (28,4%) – Uma parte significativa dos inquiridos discorda totalmente, o que aponta para uma forte perceção de que o seu conhecimento é insuficiente.
- **Nível 2 (Discordo):** 28 respostas (37,8%) – Esta é a categoria mais frequente, indicando que a maioria dos participantes não se sente com conhecimento suficiente.
- **Nível 3 (Neutro):** 19 respostas (25,7%) – Uma parcela considerável está neutra, o que pode indicar incerteza ou uma perceção de conhecimento apenas razoável, mas não suficiente.
- **Nível 4 (Concordo):** 3 respostas (4,1%) – Uma minoria muito pequena acredita ter conhecimento suficiente.
- **Nível 5 (Concordo totalmente):** 3 respostas (4,1%) – Um número igualmente pequeno de pessoas tem total confiança no seu conhecimento.

Conclusões Principais:

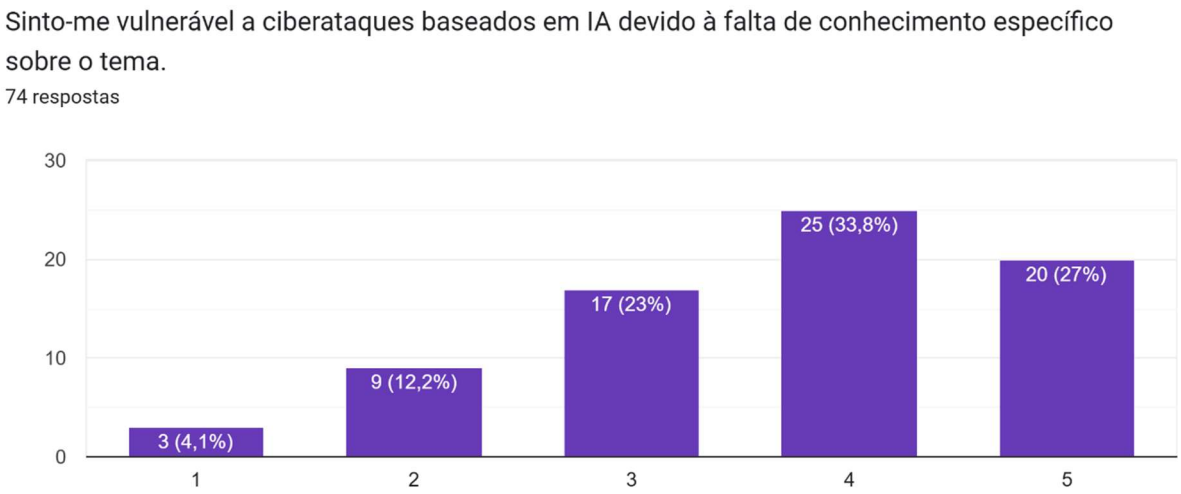
- **Baixa Autoconfiança no Conhecimento Atual:** Uma esmagadora maioria dos participantes (somando as categorias 1, 2 e 3, que representam 28,4% + 37,8% + 25,7% = **91,9%**) não acredita que o seu conhecimento atual sobre ciberataques baseados em IA seja suficiente para se protegerem.
- **Contraste com a Perceção da Ameaça:** Este resultado contrasta com a alta perceção da ameaça que foi observada em outros gráficos (por exemplo, no gráfico "Acredito que os ciberataques baseados em IA são uma ameaça significativa para a segurança digital."), indicando que, embora as pessoas reconheçam o perigo, não se sentem adequadamente preparadas.

- **Necessidade Urgente de Capacitação:** A baixa autoconfiança no próprio conhecimento reforça a necessidade de programas de formação e recursos educativos para capacitar os indivíduos a lidar com ciberameaças baseadas em IA.

Em suma, o gráfico revela que a maioria dos inquiridos não considera que o seu conhecimento atual sobre ciberataques baseados em IA seja suficiente para se protegerem, o que aponta para uma lacuna significativa na preparação e uma forte necessidade de investimento em educação e treinamento nessa área.

A Figura 35, apresenta Perceção de Vulnerabilidade a Ciberataques com IA por Falta de Conhecimento

Figura 35 - Perceção de Vulnerabilidade a Ciberataques com IA por Falta de Conhecimento



Fonte: Dados do questionário da pergunta n.º 34 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou o sentimento de vulnerabilidade dos participantes a ciberataques baseados em Inteligência Artificial (IA), atribuindo essa vulnerabilidade à falta de conhecimento específico sobre o tema. A pergunta específica da investigação foi "Sinto-me vulnerável a ciberataques baseados em IA devido à falta de conhecimento específico sobre o tema.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não se sente vulnerável devido à falta de conhecimento.
- **2 (Discordo):** A pessoa tem pouca vulnerabilidade percebida devido à falta de conhecimento.
- **3 (Neutro):** A pessoa tem uma opinião neutra ou incerta sobre a sua vulnerabilidade relacionada à falta de conhecimento.
- **4 (Concordo):** A pessoa concorda que se sente vulnerável devido à falta de conhecimento específico sobre o tema.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação, indicando um forte sentimento de vulnerabilidade devido à falta de conhecimento.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 3 respostas (4,1%) – Uma pequena minoria não se sente vulnerável pela falta de conhecimento.
- **Nível 2 (Discordo):** 9 respostas (12,2%) – Um grupo pequeno discorda, mas ainda representa uma minoria.
- **Nível 3 (Neutro):** 17 respostas (23%) – Uma parte significativa dos inquiridos está neutra, o que pode indicar alguma incerteza ou uma vulnerabilidade moderada.
- **Nível 4 (Concordo):** 25 respostas (33,8%) – Um número considerável de participantes concorda que se sente vulnerável devido à falta de conhecimento.
- **Nível 5 (Concordo totalmente):** 20 respostas (27%) – Uma parte expressiva dos inquiridos concorda totalmente, indicando um alto nível de preocupação e reconhecimento da falta de preparo.

Conclusões Principais:

- **Elevado Sentimento de Vulnerabilidade:** Uma grande maioria dos participantes (somando as categorias 4 e 5, que representam 33,8% + 27% = **60,8%**) sente-se

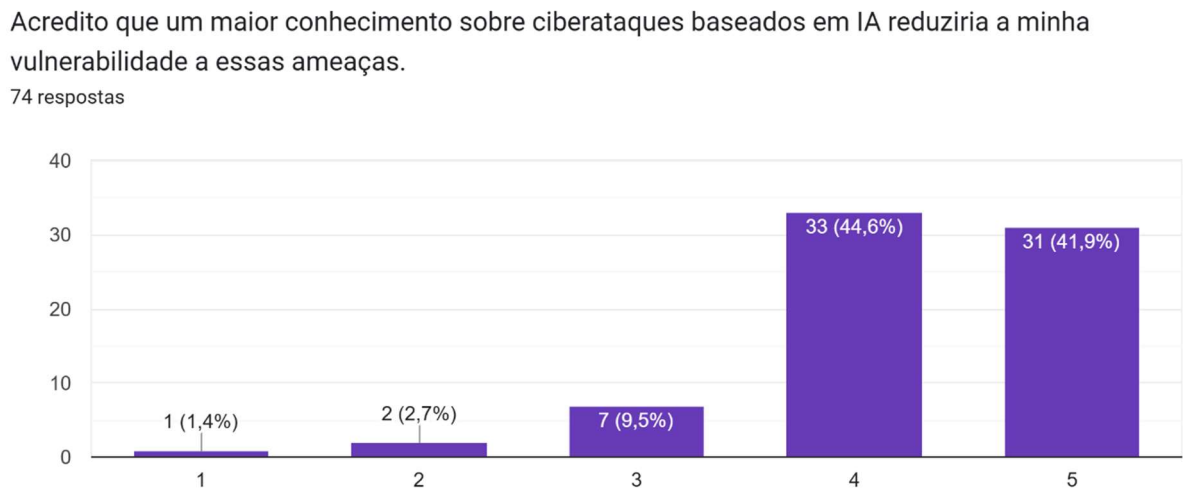
vulnerável a ciberataques baseados em IA devido à falta de conhecimento específico. Se incluirmos os neutros, que podem ter alguma incerteza, o valor sobe para 83,8% (60,8% + 23%).

- **Ligação entre Conhecimento e Segurança:** O gráfico estabelece uma clara ligação na mente dos inquiridos entre a falta de conhecimento sobre ciberataques baseados em IA e o seu sentimento de vulnerabilidade.
- **Motivação para a Formação:** Este sentimento de vulnerabilidade pode ser um forte motivador para a procura de formação e recursos educativos, como observado em gráficos anteriores. As pessoas reconhecem que o conhecimento é uma defesa fundamental.

Em suma, o gráfico demonstra que uma parte significativa dos inquiridos se sente vulnerável a ciberataques baseados em IA, e atribui essa vulnerabilidade diretamente à sua perceção de falta de conhecimento específico sobre o tema, sublinhando a importância da educação e capacitação nesta área.

A Figura 36, apresenta a Perceção sobre a Redução da Vulnerabilidade com Aumento do Conhecimento em Ciberataques com IA

Figura 36 - Perceção sobre a Redução da Vulnerabilidade com Aumento do Conhecimento em Ciberataques com IA



Fonte: Dados do questionário da pergunta n.º 35 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a perceção dos participantes sobre como um maior conhecimento acerca de ciberataques baseados em Inteligência Artificial (IA) poderia impactar a sua vulnerabilidade a essas ameaças. A pergunta específica da investigação "Acredito que um maior conhecimento sobre ciberataques baseados em IA reduziria a minha vulnerabilidade a essas ameaças.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não acredita que mais conhecimento reduziria a sua vulnerabilidade.
- **2 (Discordo):** A pessoa tem pouca convicção de que mais conhecimento seria eficaz na redução da vulnerabilidade.
- **3 (Neutro):** A pessoa tem uma opinião neutra ou incerta sobre a relação entre mais conhecimento e redução da vulnerabilidade.
- **4 (Concordo):** A pessoa concorda que um maior conhecimento reduziria a sua vulnerabilidade.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação, indicando uma forte crença no poder do conhecimento para reduzir a vulnerabilidade.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 1 resposta (1,4%) – Uma minoria ínfima não vê ligação entre conhecimento e vulnerabilidade.
- **Nível 2 (Discordo):** 2 respostas (2,7%) – Um número muito pequeno de inquiridos discorda.
- **Nível 3 (Neutro):** 7 respostas (9,5%) – Uma pequena percentagem dos inquiridos está neutra.
- **Nível 4 (Concordo):** 33 respostas (44,6%) – Um número expressivo de participantes concorda que mais conhecimento reduziria a vulnerabilidade.

- **Nível 5 (Concordo totalmente):** 31 respostas (41,9%) – Esta é a categoria dominante, com uma grande parte dos inquiridos a concordar totalmente que um maior conhecimento é crucial para reduzir a vulnerabilidade.

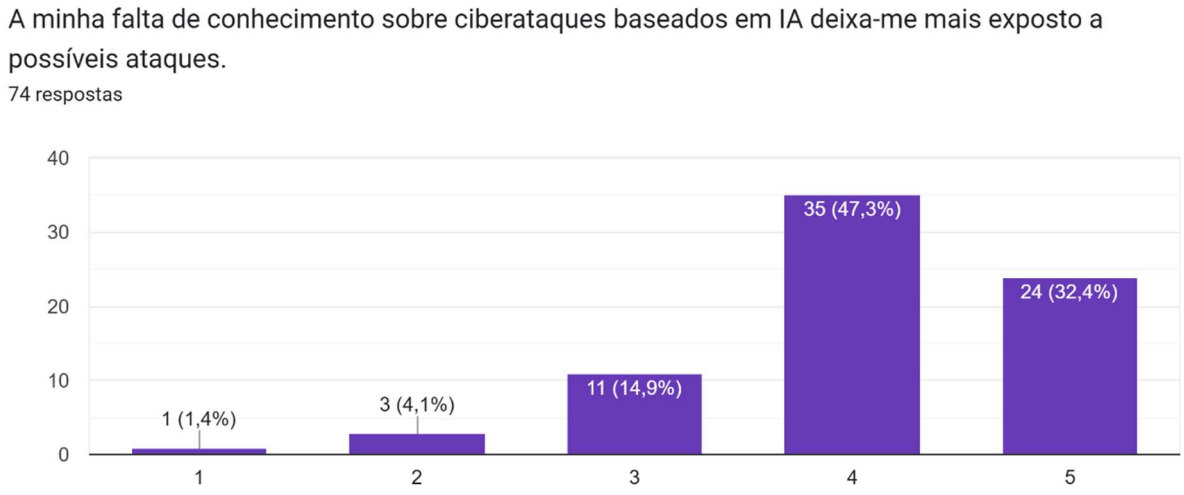
Conclusões Principais:

- **Alto Reconhecimento do Valor do Conhecimento:** Uma esmagadora maioria dos participantes (somando as categorias 4 e 5, que representam 44,6% + 41,9% = **86,5%**) acredita fortemente que um maior conhecimento sobre ciberataques baseados em IA é fundamental para reduzir a sua vulnerabilidade.
- **Consciência da Educação como Defesa:** Os resultados indicam uma clara perceção de que a educação e a aquisição de conhecimento são aspetos-chave na estratégia de defesa pessoal e profissional contra as ameaças de cibersegurança impulsionadas pela IA.
- **Implicação para Programas de Formação:** Este gráfico reforça a importância de investir e desenvolver programas de formação acessíveis e eficazes, pois há uma clara procura e reconhecimento do seu impacto na segurança individual e organizacional.

Em suma, o gráfico demonstra um consenso muito forte entre os participantes de que o aumento do conhecimento sobre ciberataques baseados em IA é um caminho direto e eficaz para diminuir a sua própria vulnerabilidade a essas ameaças.

A Figura 37, apresenta a Perceção de Exposição a Ciberataques com IA Devido à Falta de Conhecimento

Figura 37 - Perceção de Exposição a Ciberataques com IA Devido à Falta de Conhecimento



Fonte: Dados do questionário da pergunta n.º 36 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a perceção dos participantes sobre como a sua própria falta de conhecimento específico sobre ciberataques baseados em Inteligência Artificial (IA) os expõe a possíveis ataques. A pergunta específica da investigação "A minha falta de conhecimento sobre ciberataques baseados em IA deixa-me mais exposto a possíveis ataques.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não acredita que a sua falta de conhecimento a exponha mais a ataques.
- **2 (Discordo):** A pessoa tem pouca convicção de que a falta de conhecimento aumente a exposição.

- **3 (Neutro):** A pessoa tem uma opinião neutra ou incerta sobre a relação entre a falta de conhecimento e a exposição a ataques.
- **4 (Concordo):** A pessoa concorda que a sua falta de conhecimento a deixa mais exposta a possíveis ataques.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação, indicando uma forte crença de que a falta de conhecimento aumenta significativamente a sua exposição.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 1 resposta (1,4%) – Uma minoria ínfima não vê a falta de conhecimento como um fator de exposição.
- **Nível 2 (Discordo):** 3 respostas (4,1%) – Um número muito pequeno de inquiridos discorda.
- **Nível 3 (Neutro):** 11 respostas (14,9%) – Uma percentagem razoável de inquiridos está neutra.
- **Nível 4 (Concordo):** 35 respostas (47,3%) – Quase metade dos participantes concorda que a sua falta de conhecimento os torna mais expostos.
- **Nível 5 (Concordo totalmente):** 24 respostas (32,4%) – Uma parte substancial dos inquiridos concorda totalmente com a afirmação, evidenciando uma forte preocupação.

Conclusões Principais:

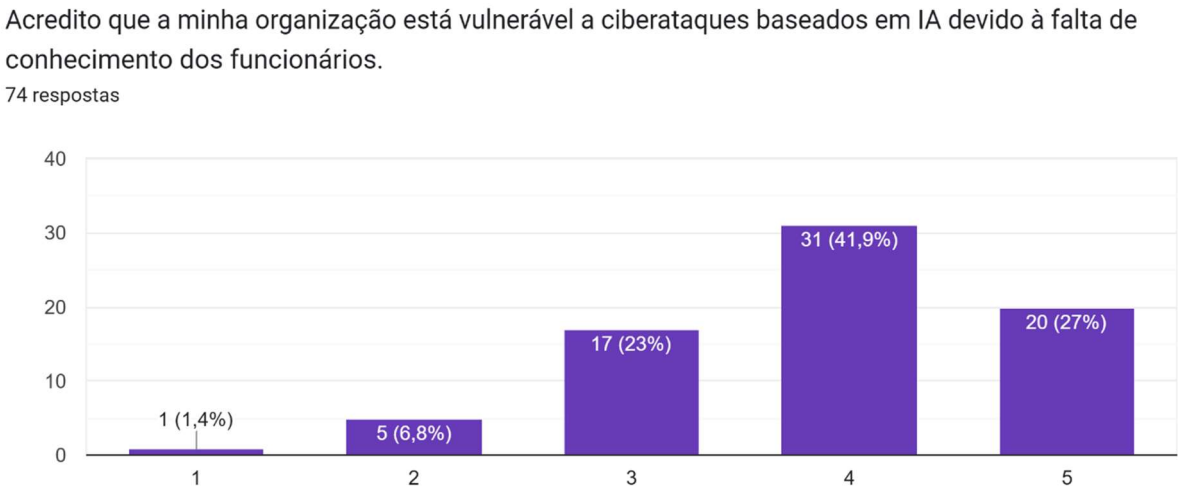
- **Reconhecimento da Exposição Devido à Falta de Conhecimento:** Uma vasta maioria dos participantes (somando as categorias 4 e 5, que representam 47,3% + 32,4% = **79,7%**) acredita que a sua falta de conhecimento sobre ciberataques baseados em IA os deixa mais expostos a possíveis ataques. Se incluirmos os neutros, que podem ter alguma incerteza, o valor sobe para 94,6% (79,7% + 14,9%).

- **Consciência do Risco Pessoal:** Os resultados indicam uma forte consciência individual sobre como a lacuna de conhecimento em um domínio tão crítico como a cibersegurança baseada em IA pode levar a vulnerabilidades reais.
- **Impulso para a Aprendizagem e Proteção:** Esta perceção de maior exposição é um motivador claro para que os indivíduos procurem mais conhecimento e treino, o que está alinhado com as conclusões de outros gráficos que indicam uma procura por formação.

Em suma, o gráfico demonstra um consenso muito forte entre os participantes de que a sua falta de conhecimento específico sobre ciberataques baseados em IA é um fator direto que aumenta a sua exposição a ameaças, reforçando a urgência da capacitação nesta área.

A Figura 38, apresenta a Perceção de Vulnerabilidade Organizacional a Ciberataques com IA Devido à Falta de Conhecimento dos Funcionários

Figura 38 - Perceção de Vulnerabilidade Organizacional a Ciberataques com IA Devido à Falta de Conhecimento dos Funcionários



Fonte: Dados do questionário da pergunta n.º 37 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a perceção dos participantes sobre a vulnerabilidade da sua própria organização a ciberataques baseados em Inteligência Artificial (IA), atribuindo essa vulnerabilidade à falta de conhecimento dos funcionários. A pergunta específica da investigação "Acredito que a minha organização está vulnerável a ciberataques baseados em IA devido à falta de conhecimento dos funcionários.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não acredita que a organização esteja vulnerável pela falta de conhecimento dos funcionários.
- **2 (Discordo):** A pessoa tem pouca convicção de que a organização seja vulnerável por esse motivo.
- **3 (Neutro):** A pessoa tem uma opinião neutra ou incerta sobre a vulnerabilidade da organização devido à falta de conhecimento dos funcionários.
- **4 (Concordo):** A pessoa concorda que a sua organização está vulnerável devido à falta de conhecimento dos funcionários.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação, indicando uma forte crença na vulnerabilidade da organização por essa razão.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 1 resposta (1,4%) – Uma minoria ínfima não vê a falta de conhecimento dos funcionários como um fator de vulnerabilidade para a organização.
- **Nível 2 (Discordo):** 5 respostas (6,8%) – Um pequeno grupo de inquiridos discorda.
- **Nível 3 (Neutro):** 17 respostas (23%) – Uma parcela considerável dos inquiridos está neutra, o que pode indicar incerteza ou uma perceção moderada da vulnerabilidade organizacional ligada ao conhecimento dos funcionários.

- **Nível 4 (Concordo):** 31 respostas (41,9%) – Um número expressivo de participantes concorda que a sua organização está vulnerável devido à falta de conhecimento dos funcionários.
- **Nível 5 (Concordo totalmente):** 20 respostas (27%) – Uma parte significativa dos inquiridos concorda totalmente, evidenciando uma forte preocupação com a segurança da organização devido à capacitação dos seus colaboradores.

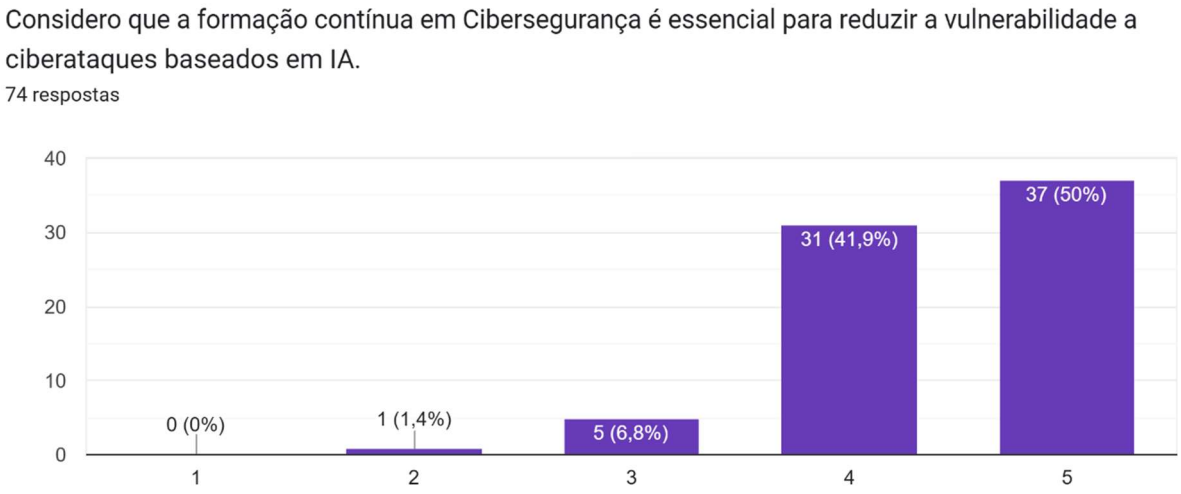
Conclusões Principais:

- **Elevada Perceção de Vulnerabilidade Organizacional:** Uma grande maioria dos participantes (somando as categorias 4 e 5, que representam 41,9% + 27% = **68,9%**) acredita que a sua organização está vulnerável a ciberataques baseados em IA devido à falta de conhecimento dos funcionários. Se incluirmos os neutros, que podem ter alguma incerteza ou considerar uma vulnerabilidade moderada, o valor sobe para 91,9% (68,9% + 23%).
- **Reconhecimento do Fator Humano na Segurança:** Este resultado sublinha o entendimento de que os funcionários representam um ponto crítico na cadeia de segurança, e que a sua falta de conhecimento específico sobre ameaças de IA pode ser explorada.
- **Implicação para Treinamento Corporativo:** O gráfico indica uma clara necessidade de investimento por parte das organizações em programas de treino e consciencialização em cibersegurança, focados em IA, para os seus colaboradores. A capacitação dos funcionários é vista como essencial para fortalecer as defesas corporativas.

Em suma, o gráfico demonstra um forte reconhecimento por parte dos inquiridos de que a falta de conhecimento dos funcionários sobre ciberataques baseados em IA representa uma vulnerabilidade significativa para as suas organizações, destacando a importância crucial do treino contínuo para a segurança empresarial.

A Figura 39, apresenta a Perceção sobre o Papel da Formação Contínua na Prevenção de Ciberataques com IA

Figura 39 - Perceção sobre o Papel da Formação Contínua na Prevenção de Ciberataques com IA



Fonte: Dados do questionário da pergunta n.º 38 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a perceção dos participantes sobre a essencialidade da formação contínua em Cibersegurança para reduzir a vulnerabilidade a ciberataques baseados em Inteligência Artificial (IA). A pergunta específica da investigação "Considero que a formação contínua em Cibersegurança é essencial para reduzir a vulnerabilidade a ciberataques baseados em IA.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não considera a formação contínua essencial para reduzir a vulnerabilidade.
- **2 (Discordo):** A pessoa considera a formação contínua pouco essencial.
- **3 (Neutro):** A pessoa tem uma opinião neutra ou incerta sobre a essencialidade da formação contínua para reduzir a vulnerabilidade.
- **4 (Concordo):** A pessoa concorda que a formação contínua é essencial para reduzir a vulnerabilidade.

- **5 (Concordo totalmente):** A pessoa concorda totalmente que a formação contínua é muito essencial para reduzir a vulnerabilidade.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 0 respostas (0%) – Nenhum dos participantes discorda totalmente, indicando um consenso de que a formação contínua é, no mínimo, algo importante.
- **Nível 2 (Discordo):** 1 resposta (1,4%) – Uma minoria muito pequena não considera a formação contínua essencial.
- **Nível 3 (Neutro):** 5 respostas (6,8%) – Uma pequena percentagem dos inquiridos está neutra.
- **Nível 4 (Concordo):** 31 respostas (41,9%) – Um número considerável de participantes concorda que a formação contínua é essencial.
- **Nível 5 (Concordo totalmente):** 37 respostas (50%) – Esta é a categoria dominante, com metade dos inquiridos a concordar totalmente que a formação contínua é muito essencial.

Conclusões Principais:

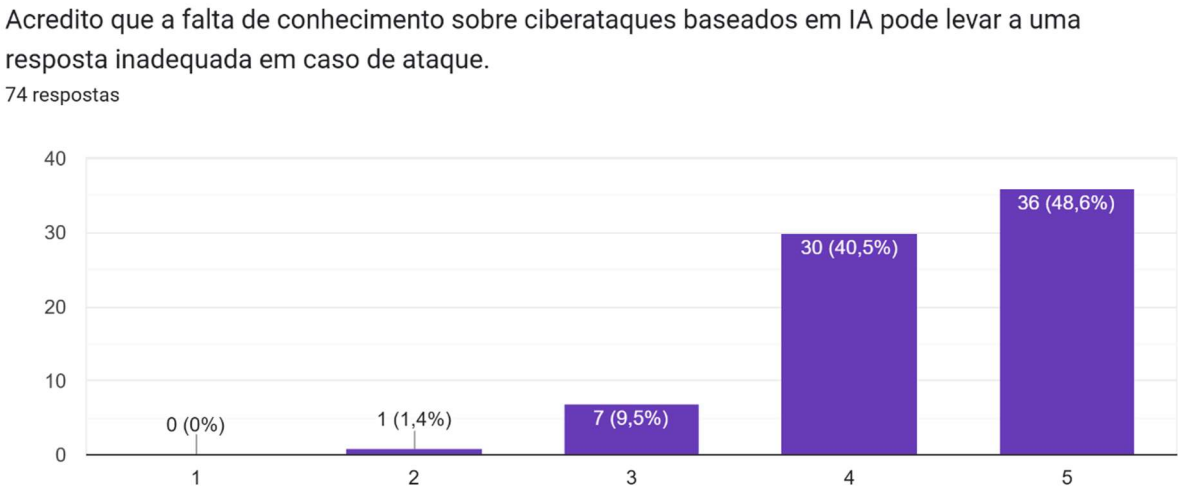
- **Elevado Reconhecimento da Essencialidade da Formação Contínua:** Uma esmagadora maioria dos participantes (somando as categorias 4 e 5, que representam 41,9% + 50% = **91,9%**) considera que a formação contínua em cibersegurança é essencial ou muito essencial para reduzir a vulnerabilidade a ciberataques baseados em IA.
- **Consciência da Dinâmica da Ameaça:** Este resultado reforça a perceção de que os ciberataques baseados em IA são uma ameaça em constante evolução, exigindo uma atualização constante de conhecimentos para manter as defesas eficazes.
- **Importância da Educação Contínua para Redução de Vulnerabilidade:** Há um claro reconhecimento da necessidade de um compromisso contínuo com a aprendizagem e atualização de conhecimentos como um meio direto para diminuir a vulnerabilidade

percebida (como visto em gráficos anteriores, por exemplo, "A minha falta de conhecimento sobre ciberataques baseados em IA deixa-me mais exposto a possíveis ataques." e "Sinto-me vulnerável a ciberataques baseados em IA devido à falta de conhecimento específico sobre o tema.").

Em suma, o gráfico demonstra um consenso muito forte entre os participantes de que a formação contínua em cibersegurança é crucial para acompanhar a evolução das ameaças e, consequentemente, reduzir a vulnerabilidade a ciberataques baseados em IA.

A Figura 40, apresenta a Perceção sobre as Consequências da Falta de Conhecimento em Ciberataques com IA

Figura 40 - Perceção sobre as Consequências da Falta de Conhecimento em Ciberataques com IA



Fonte: Dados do questionário da pergunta n.º 39 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a crença dos participantes sobre se a falta de conhecimento específico acerca de ciberataques baseados em Inteligência Artificial (IA) pode resultar numa resposta inadequada em caso de ataque. A pergunta específica da investigação "Acredito que a falta de conhecimento sobre ciberataques baseados em IA pode levar a uma resposta inadequada em caso de ataque.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não acredita que a falta de conhecimento leve a uma resposta inadequada.
- **2 (Discordo):** A pessoa tem pouca convicção de que a falta de conhecimento prejudicaria a resposta.
- **3 (Neutro):** A pessoa tem uma opinião neutra ou incerta sobre a relação entre a falta de conhecimento e a qualidade da resposta a um ataque.
- **4 (Concordo):** A pessoa concorda que a falta de conhecimento pode levar a uma resposta inadequada.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação, indicando uma forte crença de que a falta de conhecimento resultará numa resposta inadequada.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 0 respostas (0%) – Nenhum dos participantes discorda totalmente, o que sugere um consenso de que a falta de conhecimento, no mínimo, não é inofensiva.
- **Nível 2 (Discordo):** 1 resposta (1,4%) – Uma minoria ínfima não acredita que a falta de conhecimento prejudique a resposta.
- **Nível 3 (Neutro):** 7 respostas (9,5%) – Uma pequena percentagem dos inquiridos está neutra.
- **Nível 4 (Concordo):** 30 respostas (40,5%) – Um número significativo de participantes concorda que a falta de conhecimento pode levar a uma resposta inadequada.
- **Nível 5 (Concordo totalmente):** 36 respostas (48,6%) – Esta é a categoria dominante, com quase metade dos inquiridos a concordar totalmente que a falta de conhecimento resultaria numa resposta inadequada.

Conclusões Principais:

- **Forte Ligação entre Conhecimento e Resposta Efetiva:** Uma esmagadora maioria dos participantes (somando as categorias 4 e 5, que representam 40,5% + 48,6% = **89,1%**) acredita que a falta de conhecimento sobre ciberataques baseados em IA pode levar a uma resposta inadequada em caso de ataque.
- **Reconhecimento da Importância da Preparação:** Este resultado sublinha a consciência de que a capacidade de resposta a um incidente de cibersegurança depende diretamente do nível de conhecimento e preparação prévia.
- **Implicação para Treino e Planos de Resposta:** O gráfico destaca a necessidade crítica de treinar indivíduos e organizações para garantir que tenham o conhecimento necessário para responder de forma eficaz a ataques de IA, minimizando danos e interrupções.

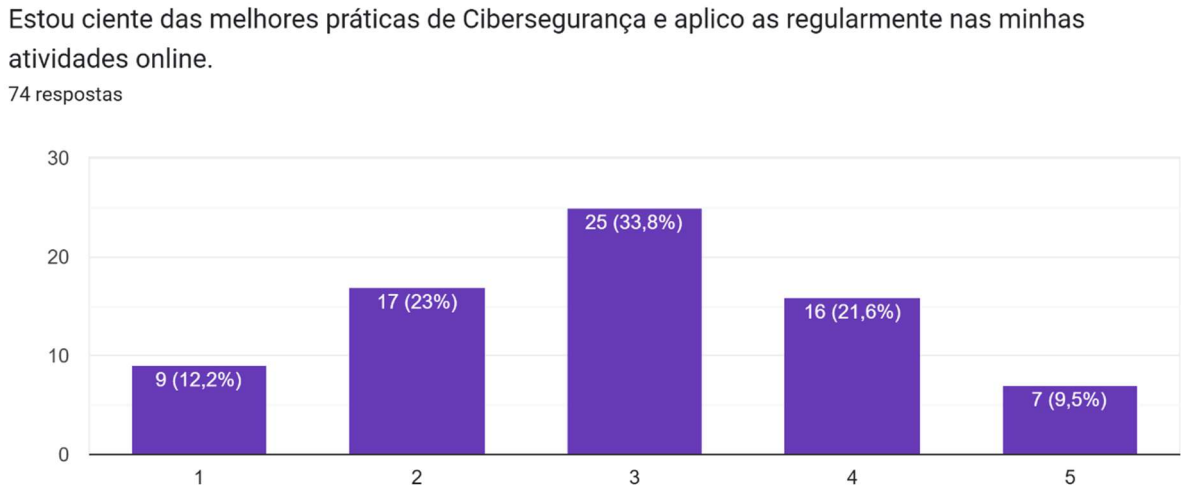
Em suma, o gráfico revela um consenso muito forte de que a falta de conhecimento em ciberataques baseados em IA é um fator determinante para uma resposta ineficaz, realçando a importância da capacitação para a resiliência a essas ameaças.

5.7 Consciencialização e comportamento: investigar como a consciencialização sobre cibersegurança influencia as práticas e o comportamento online dos utilizadores.

Num contexto digital cada vez mais vulnerável a ameaças cibernéticas, a consciencialização em cibersegurança emerge como um fator determinante na formação de comportamentos *online* seguros. Este subcapítulo tem como objetivo investigar de que forma o grau de conhecimento e sensibilização dos utilizadores sobre riscos digitais influência as suas atitudes, decisões e práticas no ambiente virtual. Através da análise de dados empíricos, procura-se compreender se uma maior consciencialização se traduz em comportamentos mais prudentes, como a adoção de boas práticas de segurança, a utilização de ferramentas de proteção ou a resistência a técnicas de engenharia social. Esta abordagem permite não só avaliar o impacto da literacia digital na segurança individual, mas também identificar oportunidades para reforçar a cultura de cibersegurança entre os utilizadores.

A Figura 41, apresenta a Perceção e Aplicação das Melhores Práticas de Cibersegurança no Comportamento Digital dos Utilizadores

Figura 41 - Perceção e Aplicação das Melhores Práticas de Cibersegurança no Comportamento Digital dos Utilizadores



Fonte: Dados do questionário da pergunta n.º 40 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou o nível de consciência e aplicação das melhores práticas de Cibersegurança pelos participantes nas suas atividades online. A pergunta específica da investigação "Estou ciente das melhores práticas de Cibersegurança e aplico-as regularmente nas minhas atividades online.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não está ciente das melhores práticas ou não as aplica.
- **2 (Discordo):** A pessoa tem pouca consciência ou aplicação das melhores práticas.
- **3 (Neutro):** A pessoa tem uma consciência moderada ou aplica as práticas de forma inconsistente.

- **4 (Concordo):** A pessoa concorda que está ciente e aplica as melhores práticas regularmente.
- **5 (Concordo totalmente):** A pessoa concorda totalmente, indicando alta consciência e aplicação consistente.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 9 respostas (12,2%) – Uma parcela significativa dos inquiridos admite não estar ciente ou aplicar as melhores práticas.
- **Nível 2 (Discordo):** 17 respostas (23%) – Um grupo considerável sente que tem pouca consciência ou aplicação.
- **Nível 3 (Neutro):** 25 respostas (33,8%) – Esta é a categoria mais frequente, indicando que a maior parte dos inquiridos tem uma compreensão moderada ou uma aplicação inconsistente das melhores práticas.
- **Nível 4 (Concordo):** 16 respostas (21,6%) – Uma minoria concorda que está ciente e aplica as práticas regularmente.
- **Nível 5 (Concordo totalmente):** 7 respostas (9,5%) – Uma pequena parcela tem total confiança na sua consciência e aplicação.

Conclusões Principais:

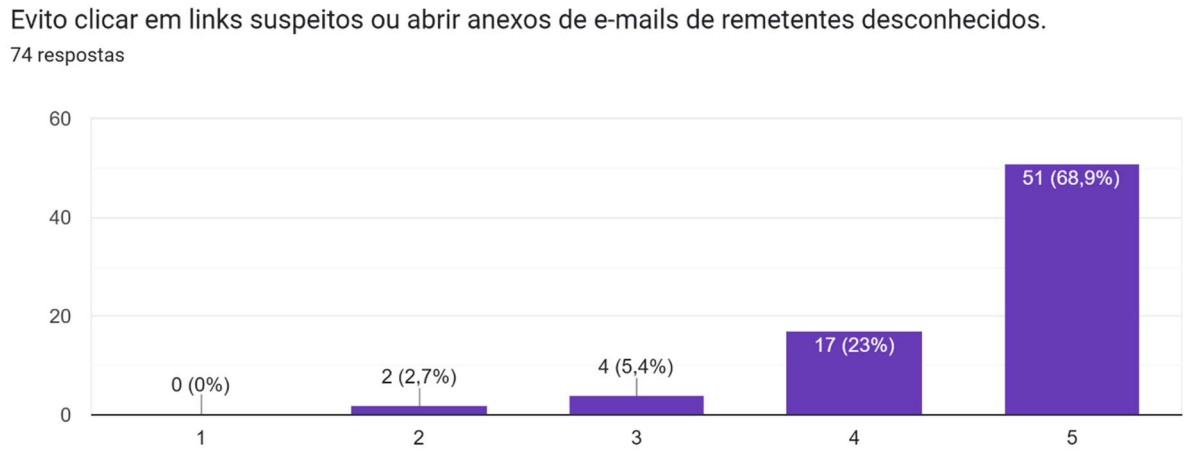
- **Lacuna na Aplicação de Melhores Práticas:** A maioria dos inquiridos (somando as categorias 1, 2 e 3, que representam 12,2% + 23% + 33,8% = **69%**) não se sente totalmente confiante em estar ciente e aplicar regularmente as melhores práticas de cibersegurança. A maior concentração está na categoria neutra, sugerindo que muitos podem ter algum conhecimento, mas não o suficiente para uma aplicação consistente.
- **Desafio na Adoção Comportamental:** Apesar de gráficos anteriores indicarem uma alta preocupação com ciberataques de IA e a necessidade de formação, este gráfico mostra que a tradução desse reconhecimento em práticas diárias efetivas ainda é um desafio para a maioria.

- **Necessidade de Sensibilização e Ferramentas Práticas:** Há uma clara indicação de que são necessários mais esforços para educar os indivíduos não apenas sobre os riscos e a importância da cibersegurança, mas também sobre as ações práticas e as "melhores práticas" a serem implementadas no dia a dia, e possivelmente, ferramentas que facilitem essa aplicação.

Em suma, o gráfico revela que, embora possa haver alguma consciência, uma parcela significativa dos participantes ainda não aplica as melhores práticas de cibersegurança de forma consistente nas suas atividades online, o que sublinha a necessidade de programas de sensibilização e formação prática para fechar essa lacuna de comportamento.

A Figura 42, apresenta Práticas de Segurança: Evitar Links e Anexos de Remetentes Desconhecido

Figura 42 - Práticas de Segurança: Evitar Links e Anexos de Remetentes Desconhecido



Fonte: Dados do questionário da pergunta n.º 41 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a frequência com que os participantes evitam clicar em *links* suspeitos ou abrir anexos de *e-mails* de remetentes desconhecidos, uma prática fundamental de cibersegurança. A pergunta específica

da investigação "Evito clicar em *links* suspeitos ou abrir anexos de e-mails de remetentes desconhecidos.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não evita ou raramente evita tais ações.
- **2 (Discordo):** A pessoa evita essas ações com pouca frequência.
- **3 (Neutro):** A pessoa evita essas ações ocasionalmente ou de forma inconsistente.
- **4 (Concordo):** A pessoa concorda que evita tais ações.
- **5 (Concordo totalmente):** A pessoa concorda totalmente, indicando que evita essas ações de forma muito consistente.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 0 respostas (0%) – Ninguém discorda totalmente, o que é um bom indicador de que a importância dessa prática é reconhecida.
- **Nível 2 (Discordo):** 2 respostas (2,7%) – Uma minoria muito pequena ainda não adota essa prática consistentemente.
- **Nível 3 (Neutro):** 4 respostas (5,4%) – Uma pequena percentagem dos inquiridos está neutra, o que pode indicar alguma inconsistência na aplicação da prática.
- **Nível 4 (Concordo):** 17 respostas (23%) – Um número considerável de participantes concorda que evita essas ações.
- **Nível 5 (Concordo totalmente):** 51 respostas (68,9%) – Esta é a categoria dominante, com uma esmagadora maioria dos inquiridos a concordar totalmente que evita clicar em links suspeitos ou abrir anexos de *e-mails* de remetentes desconhecidos.

Conclusões Principais:

- **Alta Adoção de Práticas Básicas de Segurança:** A maioria esmagadora dos participantes (somando as categorias 4 e 5, que representam 23% + 68,9% = **91,9%**) afirma evitar clicar em *links* suspeitos ou abrir anexos de *e-mails* de remetentes

desconhecidos. Este é um resultado muito positivo, pois indica que uma das práticas mais básicas e eficazes de cibersegurança é amplamente adotada.

- **Base Sólida para Consciencialização:** Este gráfico sugere que, embora possa haver lacunas em conhecimentos mais avançados sobre ciberataques baseados em IA (como visto em gráficos anteriores), a consciencialização sobre as ameaças mais comuns de *phishing* e *malware* via *e-mail* é alta.
- **Área de Força em Segurança Comportamental:** A consistência elevada na adoção desta prática demonstra um bom nível de disciplina e cautela nas atividades *online* entre os inquiridos.

Em suma, o gráfico revela que a grande maioria dos participantes adota consistentemente a prática de evitar *links* e anexos suspeitos, indicando um alto nível de consciência sobre essa forma comum de ataque e uma forte adesão às melhores práticas básicas de cibersegurança.

A Figura 43, apresenta o Uso de Senhas Fortes e Únicas nas Contas Online: Perceção dos Utilizadores

Figura 43 - Uso de Senhas Fortes e Únicas nas Contas Online: Perceção dos Utilizadores

Fonte: Dados do questionário da pergunta n.º 42 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a frequência com que os participantes utilizam senhas fortes e únicas para as suas contas online, uma prática fundamental de cibersegurança. A pergunta específica da investigação "Utilizo senhas fortes e únicas para cada uma das minhas contas online.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não utiliza senhas fortes ou únicas.
- **2 (Discordo):** A pessoa utiliza senhas fortes/únicas com pouca frequência.
- **3 (Neutro):** A pessoa tem uma aplicação inconsistente de senhas fortes e únicas.
- **4 (Concordo):** A pessoa concorda que utiliza senhas fortes e únicas.
- **5 (Concordo totalmente):** A pessoa concorda totalmente, indicando que utiliza senhas fortes e únicas de forma muito consistente.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 3 respostas (4,1%) – Uma pequena minoria não adere a esta prática.
- **Nível 2 (Discordo):** 5 respostas (6,8%) – Um grupo pequeno não utiliza consistentemente senhas fortes e únicas.
- **Nível 3 (Neutro):** 16 respostas (21,6%) – Uma parcela considerável dos inquiridos tem uma aplicação inconsistente ou neutra em relação a esta prática.
- **Nível 4 (Concordo):** 20 respostas (27%) – Um número razoável de participantes concorda que utiliza senhas fortes e únicas.
- **Nível 5 (Concordo totalmente):** 30 respostas (40,5%) – Esta é a categoria dominante, com uma parte significativa dos inquiridos a concordar totalmente que utiliza senhas fortes e únicas de forma muito consistente.

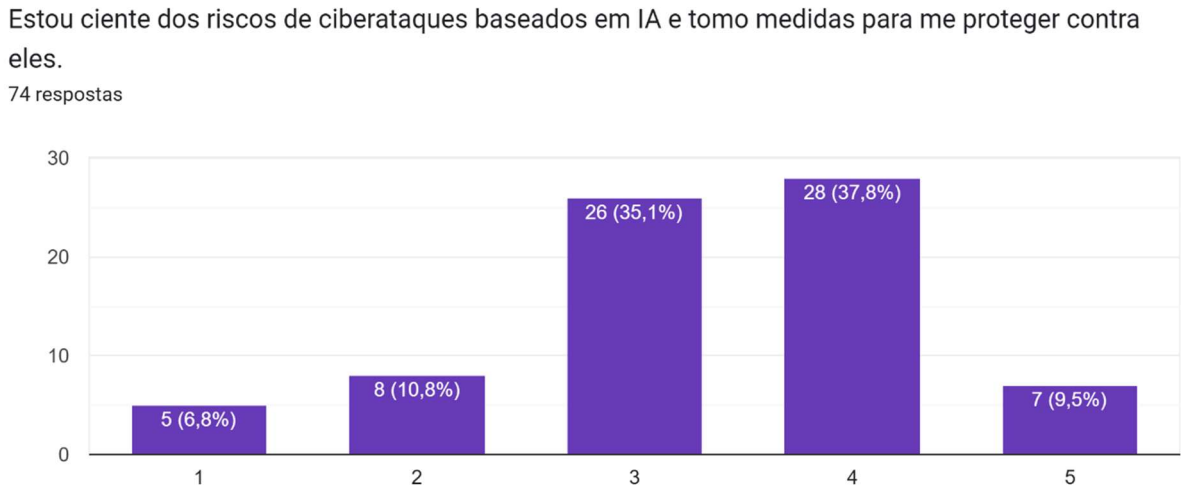
Conclusões Principais:

- **Boa, mas Não Total, Adoção de Práticas de Senha:** A maioria dos participantes (somando as categorias 4 e 5, que representam 27% + 40,5% = **67,5%**) afirma utilizar senhas fortes e únicas. Embora este seja um bom indicador de consciencialização e prática, ainda há uma parcela considerável (cerca de 32,5% somando as categorias 1, 2 e 3) que não segue esta prática consistentemente.
- **Espaço para Melhoria:** Comparado com o alto nível de adesão à prática de evitar *links* suspeitos (91,9% nas categorias 4 e 5), a utilização de senhas fortes e únicas, apesar de maioritária, ainda apresenta um desafio para uma porção relevante dos inquiridos.
- **Importância da Educação Contínua:** Este gráfico reforça a necessidade de campanhas de sensibilização e formação que enfatizem a importância das senhas fortes e únicas como uma camada fundamental de defesa contra ciberataques, incluindo aqueles potencializados por IA.

Em suma, o gráfico mostra que, embora muitos participantes já adotem a prática de usar senhas fortes e únicas, ainda existe uma oportunidade significativa para melhorar a adesão a esta prática essencial de cibersegurança entre todos os inquiridos.

A Figura 44, apresenta a Perceção dos Utilizadores sobre Riscos e Ações de Defesa contra Ciberataques Baseados em IA

Figura 44 - Perceção dos Utilizadores sobre Riscos e Ações de Defesa contra Ciberataques Baseados em IA



Fonte: Dados do questionário da pergunta n.º 43 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou o nível de consciência dos participantes sobre os riscos de ciberataques baseados em Inteligência Artificial (IA) e as medidas que tomam para se proteger contra eles. A pergunta específica da investigação "Estou ciente dos riscos de ciberataques baseados em IA e tomo medidas para me proteger contra eles.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não está ciente dos riscos ou não toma medidas.
- **2 (Discordo):** A pessoa tem pouca consciência dos riscos ou toma poucas medidas.
- **3 (Neutro):** A pessoa tem uma consciência moderada dos riscos e toma algumas medidas, mas talvez de forma inconsistente.

- **4 (Concordo):** A pessoa concorda que está ciente dos riscos e toma medidas para se proteger.
- **5 (Concordo totalmente):** A pessoa concorda totalmente, indicando alta consciência e aplicação consistente de medidas de proteção.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 5 respostas (6,8%) – Uma pequena minoria não se sente ciente nem protetora.
- **Nível 2 (Discordo):** 8 respostas (10,8%) – Um grupo um pouco maior discorda, indicando falta de consciência ou de ação protetora.
- **Nível 3 (Neutro):** 26 respostas (35,1%) – Esta é a categoria mais frequente, sugerindo que uma parte significativa dos inquiridos tem uma consciência e/ou aplicação de medidas de proteção apenas moderada ou inconsistente.
- **Nível 4 (Concordo):** 28 respostas (37,8%) – Um número considerável de participantes concorda que está ciente e toma medidas.
- **Nível 5 (Concordo totalmente):** 7 respostas (9,5%) – Uma pequena parcela tem total confiança na sua consciência e capacidade de proteção.

Conclusões Principais:

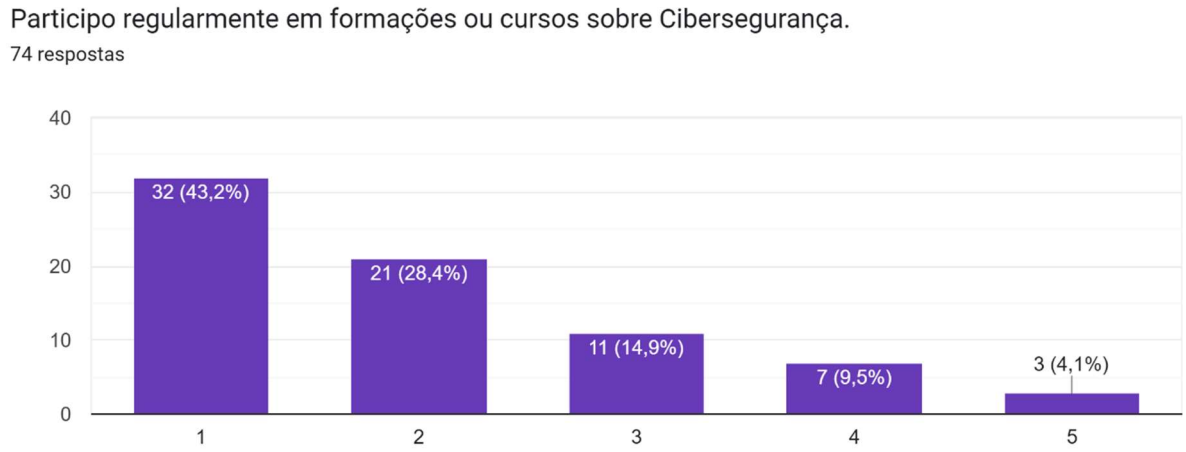
- **Consciência Moderada e Ação Inconsistente:** Embora 47,3% (37,8% + 9,5%) dos participantes concordem que estão cientes e tomam medidas, a maior concentração de respostas está na categoria "Neutro" (35,1%). Isso sugere que, para uma parcela significativa, a consciência e as ações de proteção contra ciberataques baseados em IA podem não ser totalmente consistentes ou abrangentes.
- **Contraste com a Perceção de Ameaça:** Apesar de muitos gráficos anteriores mostrarem uma alta perceção de que os ciberataques baseados em IA são uma ameaça significativa (por exemplo, "Acredito que os ciberataques baseados em IA são uma ameaça significativa para a segurança digital."), este gráfico revela que essa perceção nem sempre se traduz em um alto nível de autoproteção percebida.

- **Necessidade de Traduzir Consciência em Ação:** Há uma lacuna entre o reconhecimento do risco e a adoção efetiva e consistente de medidas de proteção. Isso indica a necessidade de programas de formação que não apenas informem sobre os riscos, mas também capacitem os indivíduos com ações práticas e fáceis de implementar para se protegerem.

Em suma, o gráfico indica que, embora muitos estejam cientes dos riscos de ciberataques baseados em IA, uma parte considerável dos inquiridos tem uma postura apenas moderada ou inconsistente na tomada de medidas de proteção, sublinhando a necessidade de fortalecer a ligação entre a consciência e a ação prática de cibersegurança.

A Figura 45, apresenta a Regularidade na Participação em Cursos de Cibersegurança pelos Utilizadores

Figura 45 - Regularidade na Participação em Cursos de Cibersegurança pelos Utilizadores



Fonte: Dados do questionário da pergunta n.º 44 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a frequência com que os participantes participam regularmente em formações ou cursos sobre

Cibersegurança. A pergunta específica da investigação: "Participo regularmente em formações ou cursos sobre Cibersegurança.", e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não participa ou raramente participa em formações.
- **2 (Discordo):** A pessoa participa com pouca frequência em formações.
- **3 (Neutro):** A pessoa participa ocasionalmente ou de forma inconsistente em formações.
- **4 (Concordo):** A pessoa concorda que participa regularmente em formações.
- **5 (Concordo totalmente):** A pessoa concorda totalmente, indicando que participa muito regularmente em formações.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 32 respostas (43,2%) – Esta é a categoria mais frequente, indicando que uma grande parte dos inquiridos não participa regularmente em formações ou cursos sobre Cibersegurança.
- **Nível 2 (Discordo):** 21 respostas (28,4%) – Um grupo considerável tem pouca participação em formações.
- **Nível 3 (Neutro):** 11 respostas (14,9%) – Uma parte dos inquiridos participa ocasionalmente ou de forma inconsistente.
- **Nível 4 (Concordo):** 7 respostas (9,5%) – Uma minoria muito pequena concorda que participa regularmente.
- **Nível 5 (Concordo totalmente):** 3 respostas (4,1%) – Apenas uma minoria ínfima participa muito regularmente.

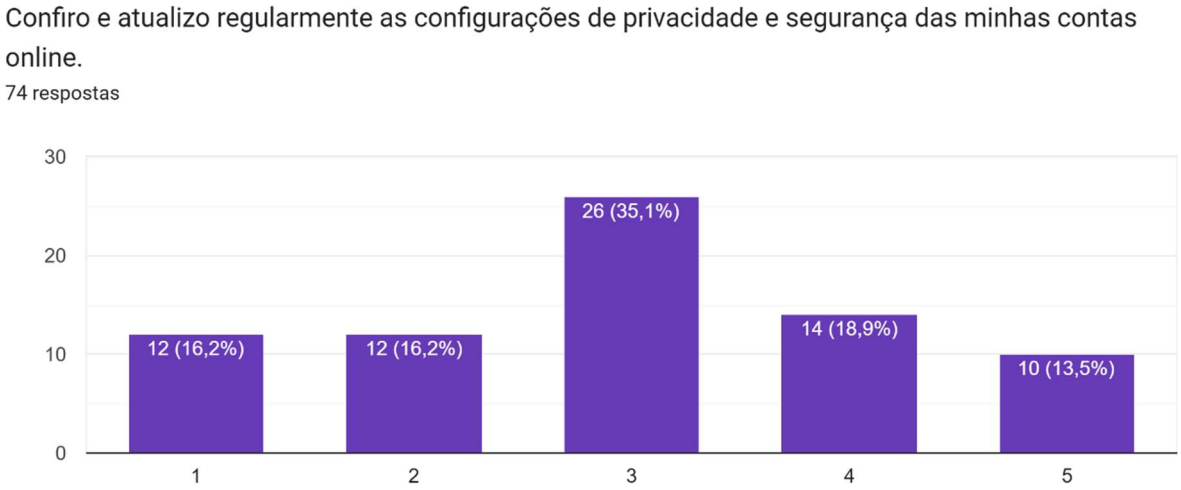
Conclusões Principais:

- **Baixa Participação em Formações de Cibersegurança:** Uma esmagadora maioria dos participantes (somando as categorias 1, 2 e 3, que representam 43,2% + 28,4% + 14,9% = **86,5%**) não participa regularmente em formações ou cursos sobre Cibersegurança.
- **Contraste com a Perceção de Necessidade:** Este resultado contrasta fortemente com as conclusões de outros gráficos, que mostraram uma alta perceção da ameaça dos ciberataques baseados em IA, um alto reconhecimento da necessidade de mais investimentos em formação e da essencialidade da formação contínua para reduzir a vulnerabilidade. Embora a vontade e o reconhecimento estejam presentes, a participação efetiva é baixa.
- **Lacuna entre Intenção e Ação:** Há uma clara lacuna entre a intenção ou o reconhecimento da necessidade de formação e a participação ativa em programas de cibersegurança. Isso pode ser devido a barreiras como falta de tempo, custo, falta de ofertas adequadas ou falta de incentivo.
- **Implicação para Fornecedores de Formação e Organizações:** Há uma grande oportunidade e uma necessidade premente de tornar a formação em cibersegurança mais acessível, atraente e incentivada, tanto por iniciativa própria dos indivíduos quanto por parte das organizações, para que a alta perceção da ameaça se traduza em maior capacitação.

Em suma, o gráfico revela que, apesar de reconhecerem a importância da formação em cibersegurança para as ameaças de IA, a maioria dos participantes não participa regularmente em tais programas, indicando uma barreira significativa entre a consciência da necessidade e a ação de capacitação.

A Figura 46, apresenta as Práticas de Revisão de Segurança Digital pelos Utilizadores

Figura 46 - Práticas de Revisão de Segurança Digital pelos Utilizadores



Fonte: Dados do questionário da pergunta n.º 45 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a frequência com que os participantes conferem e atualizam regularmente as configurações de privacidade e segurança das suas contas online. A pergunta específica da investigação: "Confiro e atualizo regularmente as configurações de privacidade e segurança das minhas contas online." e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não confere nem atualiza as configurações.
- **2 (Discordo):** A pessoa raramente confere ou atualiza.
- **3 (Neutro):** A pessoa confere ou atualiza ocasionalmente/inconsistentemente.
- **4 (Concordo):** A pessoa concorda que confere e atualiza regularmente.
- **5 (Concordo totalmente):** A pessoa concorda totalmente, indicando uma prática muito consistente.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 12 respostas (16,2%) – Uma parcela significativa dos inquiridos não adota esta prática de segurança fundamental.
- **Nível 2 (Discordo):** 12 respostas (16,2%) – Um grupo igualmente grande discorda, reforçando que muitos não estão a gerir ativamente as suas configurações.
- **Nível 3 (Neutro):** 26 respostas (35,1%) – Esta é a categoria mais frequente, sugerindo que a maioria dos participantes é inconsistente ou passiva em relação à gestão das configurações de segurança e privacidade.
- **Nível 4 (Concordo):** 14 respostas (18,9%) – Uma minoria concorda que confere e atualiza regularmente.
- **Nível 5 (Concordo totalmente):** 10 respostas (13,5%) – Apenas uma pequena minoria tem total confiança na sua prática regular.

Conclusões Principais:

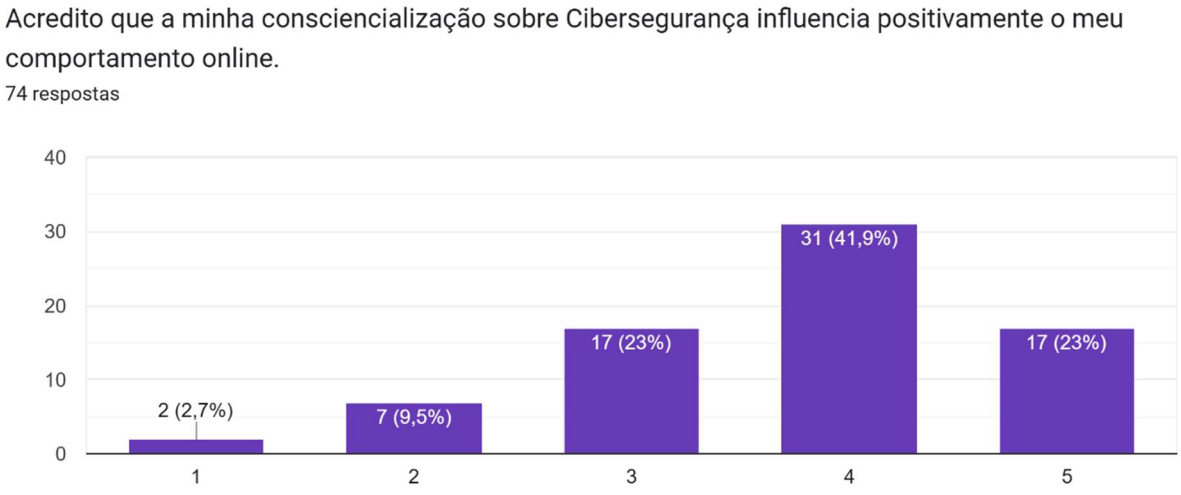
- **Baixa Adoção de Gestão Ativa de Segurança:** A maioria dos participantes (somando as categorias 1, 2 e 3, que representam 16,2% + 16,2% + 35,1% = **67,5%**) não demonstra uma prática regular e consistente de conferir e atualizar as configurações de privacidade e segurança das suas contas *online*.
- **Contraste com Outras Práticas:** Ao contrário da alta adesão a evitar *links* suspeitos (91,9%) ou, em menor grau, o uso de senhas fortes e únicas (67,5%), a gestão proativa das configurações de privacidade/segurança parece ser uma área onde a ação é menos frequente. Isso pode indicar que essa prática é percebida como mais complexa, menos urgente ou menos compreendida pelos utilizadores.
- **Risco Subjacente:** A falta de gestão ativa das configurações de privacidade e segurança pode deixar os utilizadores e as suas contas *online* vulneráveis a ataques, incluindo aqueles potencializados por IA que podem explorar configurações padrão ou desatualizadas.

- **Necessidade de Sensibilização e Simplificação:** Este gráfico sugere uma necessidade de campanhas que não apenas expliquem a importância de gerir estas configurações, mas também que simplifiquem o processo para os utilizadores.

Em suma, o gráfico revela que uma parcela significativa dos participantes não confere e atualiza regularmente as configurações de privacidade e segurança das suas contas online, o que representa uma lacuna importante na adoção de melhores práticas de cibersegurança e um potencial ponto de vulnerabilidade.

A Figura 47, apresenta o Impacto da Consciencialização em Cibersegurança no Comportamento Online dos Utilizadores

Figura 47 - Impacto da Consciencialização em Cibersegurança no Comportamento Online dos Utilizadores



Fonte: Dados do questionário da pergunta n.º 46 (Anexo 1)

Este gráfico de barras apresenta os resultados de uma investigação que avaliou a crença dos participantes sobre o impacto da sua própria consciencialização em Cibersegurança no seu comportamento online. A pergunta específica da investigação: "Acredito que a minha

consciencialização sobre Cibersegurança influencia positivamente o meu comportamento online." e foram recolhidas 74 respostas.

A escala utilizada para as respostas é a seguinte:

- **1 (Discordo totalmente):** A pessoa não acredita que a consciencialização influencie positivamente o seu comportamento.
- **2 (Discordo):** A pessoa tem pouca convicção de que a consciencialização seja um fator positivo.
- **3 (Neutro):** A pessoa tem uma opinião neutra ou incerta sobre a influência da consciencialização no seu comportamento online.
- **4 (Concordo):** A pessoa concorda que a sua consciencialização influencia positivamente o seu comportamento *online*.
- **5 (Concordo totalmente):** A pessoa concorda totalmente com a afirmação, indicando uma forte crença na influência positiva da consciencialização.

Análise dos Resultados:

- **Nível 1 (Discordo totalmente):** 2 respostas (2,7%) – Uma minoria muito pequena não vê a consciência como um fator positivo.
- **Nível 2 (Discordo):** 7 respostas (9,5%) – Um pequeno grupo de inquiridos discorda.
- **Nível 3 (Neutro):** 17 respostas (23%) – Uma parcela considerável dos inquiridos está neutra.
- **Nível 4 (Concordo):** 31 respostas (41,9%) – Esta é a categoria mais frequente, com uma parte significativa dos participantes a concordar que a sua consciencialização influencia positivamente o seu comportamento.
- **Nível 5 (Concordo totalmente):** 17 respostas (23%) – Um número expressivo de inquiridos concorda totalmente, evidenciando uma forte crença na relação entre consciência e comportamento seguro.

Conclusões Principais:

- **Forte Crença na Relação Consciência-Comportamento:** Uma grande maioria dos participantes (somando as categorias 4 e 5, que representam 41,9% + 23% = **64,9%**) acredita que a sua consciencialização sobre Cibersegurança influencia positivamente o seu comportamento online. Se incluirmos os neutros, que podem ter alguma incerteza, mas não negam a influência, o valor sobe para 87,9% (64,9% + 23%).
- **Perceção de Agência Pessoal:** Os resultados indicam que os indivíduos sentem que o seu próprio conhecimento e consciência são ferramentas eficazes para moldar as suas ações de segurança online.
- **Relevância de Campanhas de Sensibilização:** Este gráfico reforça a importância das campanhas de sensibilização em cibersegurança, pois os participantes percebem que o aumento da consciência leva a comportamentos mais seguros.

Em suma, o gráfico demonstra que a maioria dos participantes acredita que a sua consciencialização em cibersegurança tem um impacto positivo no seu comportamento *online*, validando a eficácia da educação e sensibilização como ferramentas para promover práticas mais seguras.

6. CONCLUSÃO

6.1 Síntese dos Resultados

A presente investigação permitiu aferir, de forma sistemática e fundamentada, o grau de literacia dos utilizadores relativamente aos ciberataques potenciados por Inteligência Artificial (IA), evidenciando um conjunto de tendências, perceções e lacunas que carecem de atenção estratégica no domínio da cibersegurança.

Os dados recolhidos e analisados revelam uma perceção generalizada da gravidade e da crescente sofisticação dos ciberataques com recurso a IA sendo que a maioria dos inquiridos reconhece o seu impacto potencial sobre a segurança digital, tanto a nível pessoal como organizacional. Contudo, esta perceção não se traduz, de forma proporcional, em conhecimento técnico aprofundado ou em práticas de proteção consistentes. A maioria dos participantes demonstrou sentir-se vulnerável devido à insuficiência de conhecimento específico, e apenas uma minoria revelou confiança na sua capacidade de identificar, compreender e mitigar este tipo de ameaças.

Verificou-se, ainda, que embora práticas básicas de segurança — como evitar *links* suspeitos ou utilizar palavras-passe robustas — sejam relativamente bem adotadas, outras medidas essenciais, como a revisão periódica das configurações de segurança ou a participação regular em formações especializadas, continuam a ser negligenciadas por uma parte significativa da amostra. Esta dissociação entre a perceção do risco e a adoção de comportamentos preventivos evidencia a necessidade de reforçar a componente educativa e formativa no âmbito da cibersegurança.

Importa sublinhar o elevado interesse manifestado pelos inquiridos em participar em iniciativas formativas, como *workshops*, cursos online e simulações práticas, bem como a valorização da colaboração com especialistas em cibersegurança. Estes dados apontam para uma oportunidade concreta de intervenção, que deve ser capitalizada por instituições de ensino, entidades públicas e privadas, e organismos reguladores, no sentido de promover uma cultura de cibersegurança mais robusta, inclusiva e adaptada aos desafios emergentes.

Em suma, conclui-se que a mitigação eficaz dos riscos associados aos ciberataques baseados em IA exige uma abordagem holística, que combine soluções tecnológicas avançadas com

estratégias educativas contínuas e adaptativas. O conhecimento, a consciencialização e a capacitação dos utilizadores constituem pilares fundamentais para a construção de um ecossistema digital mais seguro, resiliente e preparado para enfrentar as ameaças do presente e do futuro.

6.2 Limitações do Estudo

Apesar da relevância dos resultados obtidos, este estudo apresenta algumas limitações que devem ser reconhecidas. Em primeiro lugar, a amostra utilizada foi composta por 74 participantes, o que, embora suficiente para uma análise exploratória, não permite generalizar plenamente as conclusões para toda a população. Em segundo lugar, a recolha de dados foi realizada exclusivamente através de questionários online, o que pode ter condicionado a diversidade dos inquiridos e introduzido viés de autorresposta, dado que os participantes mais interessados em Cibersegurança tendem a responder com maior frequência. Além disso, o estudo concentrou-se no contexto português, limitando a comparação com outras realidades internacionais. Por fim, a natureza descritiva e exploratória da investigação não permite estabelecer relações causais entre o nível de conhecimento dos utilizadores e a sua vulnerabilidade a ciberataques, restringindo-se à identificação de padrões e perceções. Estas limitações, contudo, abrem espaço para trabalhos futuros que possam ampliar a amostra, diversificar os métodos de recolha de dados e adotar abordagens comparativas e longitudinais.

6.3 Trabalhos Futuros

Para além dos resultados obtidos, este estudo abre caminho para futuras investigações que poderão aprofundar a análise do impacto da Inteligência Artificial nos ciberataques e na consciencialização dos utilizadores. Recomenda-se a realização de estudos longitudinais que permitam avaliar a evolução do conhecimento e das perceções ao longo do tempo, bem como a aplicação de metodologias comparativas entre diferentes grupos profissionais e contextos geográficos. Adicionalmente, seria pertinente explorar o desenvolvimento de programas educacionais específicos e ferramentas de simulação baseadas em IA, capazes de preparar os utilizadores para enfrentar cenários de ataque realistas. A integração de abordagens interdisciplinares, envolvendo áreas como psicologia, sociologia e ciência da computação, poderá também enriquecer a compreensão sobre o comportamento humano perante ameaças digitais e contribuir para a criação de estratégias de defesa mais eficazes e adaptativas.

REFERÊNCIAS BIBLIOGRÁFICAS

1. Almeida, J. E. (2020). Cibersegurança: da prevenção do risco à gestão de incidentes. Revista Ibérica de Sistemas e Tecnologias de Informação.
2. Borba, G. L., & Mota, L. F. A. (2024). Análise dos riscos da inteligência artificial nos ciberataques. Revista Científica ACERTTE. https://doi.org/10.63026/acertte.v4i4.182
3. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., … & Amodei, D. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Oxford: Future of Humanity Institute. https://arxiv.org/abs/1802.07228
4. Callegari, F., Sirianni, A., & Ceravolo, R. (2016). Advanced Persistent Threats: A Survey. Computers & Security, 57, 18–41.
5. Centro Nacional de Cibersegurança (CNCS). (2024). Relatório de Cibersegurança em Portugal 2024. Lisboa: CNCS. https://www.cncs.gov.pt/docs/relatorio-ciberseguranca-2024.pdf
6. Centro Nacional de Cibersegurança (CNCS). (2025). Relatório de Cibersegurança em Portugal – Riscos & Conflitos (6.ª edição). Lisboa: CNCS. https://www.cncs.gov.pt/docs/rel-riscosconflitos2024-obcibercncs.pdf
7. CloudTarget. (2024). A importância da inteligência de ameaças na defesa cibernética. CloudTarget. https://cloudtarget.com.br/a-importancia-da-inteligencia-de-ameacas-na-defesa-cibernetica/
8. Compete 2030. (2025). Portugal aposta em inteligência artificial para liderar inovação e sustentabilidade. Lisboa: Governo de Portugal. https://www.compete2030.gov.pt/comunicacao/portugal-aposta-em-inteligencia-artificial-para-liderar-inovacao-e-sustentabilidade/
9. Conceito.de. (n.d.). Cibersegurança - O que é, origem, influência e na internet. Retrieved from https://www.conceito.de

10. Costa da Conceição, I. G. (2023). Ameaças Cibernéticas e os Seus Impactos na Segurança Humana [Dissertação de Mestrado, Universidade Autónoma de Lisboa].

11. Cruz, J. V. D. S., Casemiro, J. V., Gallizzi, J. E. S., & Kalili, R. M. (2024). Inteligência artificial e Cibersegurança: análise de ameaças emergentes e estratégias defensivas. Revista Delos. https://doi.org/10.47283/244670492021090225

12. Cruz, J. V. D. S., Casemiro, J. V., Gallizzi, J. E. S., & Kalili, R. M. (2024). Inteligência artificial e Cibersegurança: análise de ameaças emergentes e estratégias defensivas. REVISTA DELOS, 17(61), e2954. https://doi.org/10.55905/rdelosv17.n61-193

13. Cruz, R., Casemiro, J., Gallizzi, R., & Kalili, R. (2024). Artificial Intelligence in Cybersecurity: Phishing, Deepfakes and Emerging Threats. Journal of Information Security, 12(3), 45–62.

14. De Almeida Souza, J. P., & De Moraes, M. J. (2021). Fortalezas e fragilidades no uso da inteligência artificial na Cibersegurança. Revista Tecnológica da Fatec Americana. https://doi.org/10.47283/244670492021090225

15. European Union Agency for Cybersecurity (ENISA). (2021). Cybersecurity training and awareness raising. ENISA. Disponível em: https://www.enisa.europa.eu/publications/cybersecurity-training-and-awareness-raising

16. European Union Agency for Cybersecurity (ENISA). (2023). ENISA Threat Landscape 2023. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

17. Ferreira, M. (2025, 30 de novembro). Inteligência artificial e descuido dos utilizadores aumentam riscos de segurança online. O Mirante. Disponível em: https://omirante.pt/sociedade/2025-11-30-inteligencia-artificial-e-descuido-dos-utilizadores-aumentam-riscos-de-seguranca-online-02b2d95e

18. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press. https://doi.org/10.1038/nature14539

19. Hadnagy, C. (2010). Social Engineering: The Art of Human Hacking. John Wiley & Sons.

20. Indra Group. (2025). Innovation Telescope – Portugal: Investimento em Inteligência Artificial, Cibersegurança, Computação Quântica e 5G. Madrid: Indra. https://www.indracompany.com/sites/default/files/20251103_innovation_telescope_-_zoom_portugal.pdf

21. Jakkal, V. (2021). Como a IA está transformando a cibersegurança: abordando o aumento das ameaças cibernéticas. Microsoft Source. https://news.microsoft.com/source/latam/features/seguranca/como-a-ia-esta-transformando-a-ciberseguranca-abordando-o-aumento-das-ameacas-ciberneticas

22. Jurafsky, D., & Martin, J. H. (2023). Speech and language processing (3rd ed.). Draft online edition.

23. Laroche Borba, G., & Araújo Mota, L. F. (2024). Análise dos riscos da inteligência artificial nos ciberataques. Revista Científica ACERTTE, 4(4), e44182. https://doi.org/10.63026/acertte.v4i4.182

24. Microsoft. (2024). Como a IA está transformando a cibersegurança: abordando o aumento das ameaças cibernéticas.

    https://news.microsoft.com/source/latam/features/seguranca/como-a-ia-esta-transformando-a-ciberseguranca-abordando-o-aumento-das-ameacas-ciberneticas/?lang=pt-br

25. Mirkovic, J., & Reiher, P. (2004). A survey of research on denial of service attack and defense. UCLA CSD Technical Report, 04001.

26. Mitchell, T. M. (1997). Machine learning. McGraw-Hill.

27. Morais, V. M. S. (2022). O Ecossistema de Cibersegurança em Portugal [Dissertação de Mestrado, Instituto Politécnico de Leiria].

28. Observatório de Cibersegurança. (2024). Estudo sobre a Educação para a Cibersegurança no Ensino Básico e Secundário em Portugal. Lisboa: CNCS. https://www.cncs.gov.pt/docs/estudo-ensino-bas-sec-obcibercncs.pdf

29. Prosegur Cipher. (2025). Ciberataques a infraestruturas críticas em alta: setor da energia em alerta. Prosegur. https://www.prosegur.pt/artigos/sala-de-imprensa/ciberataques-infraestruturas-setor-energia-alerta

30. PwC Portugal. (2025). IA lidera investimentos em cibersegurança num cenário de risco crescente. PwC Global Digital Trust Insights 2026. https://www.pwc.pt/pt/sala-imprensa/artigos-opiniao/2025/ia-lidera-investimentos-ciberseguranca-cenario-risco-crescente.html

31. Raff, E., Sylvester, J., & Nicholas, C. (2017). Malware detection by eating a whole exe. In Proceedings of the 14th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 99–119). Springer.

32. RAUSCHER, K. F., & YASCHENKO, V. (Eds.). (2011). Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations. East-West Institute & Information Security Institute of Moscow State University. http://www.ewi.info/system/files/reports/RussiaU%20S%20%20bilateral%20on%20terminology%20v76%20%282%29.pdf

33. Russell, S. J., & Norvig, P. (2020). Artificial Intelligence: A Modern Approach (4th ed.). Pearson. https://doi.org/10.1016/B978-0-12-385057-7.00001-9

34. Russell, S., & Norvig, P. (2021). Artificial intelligence: A modern approach (4th ed.). Pearson.

35. SciELO Brasil. (2021). Inteligência Artificial e Sociedade: Avanços e Riscos.

36. Shaikh, F. A., & Siponen, M. (2024). Organizational Learning from Cybersecurity Performance: Effects on Cybersecurity Investment Decisions. Information Systems Frontiers, 26(3), 1109–1120. https://doi.org/10.1007/s10796-023-10404-7

37. Silva, S., & Glória Júnior, I. (2023). Ransomware: A Evolução Dos Ataques Na Contemporaneidade e Seus Desafios para a Segurança Digital. Journal of Technology & Information, 3(2). http://www.jtni.com.br/index.php/JTnI/article/view/84

38. Souza, J., & Morais, M. (2021). Fortalezas e fragilidades no uso da inteligência artificial na cibersegurança. Revista Tecnológica da Fatec Americana, 9(2).

39. Szeliski, R. (2022). Computer vision: Algorithms and applications (2nd ed.). Springer.

40. Tecnoblog. (n.d.). O que é Cibersegurança? Saiba o que significa o conceito e entenda sua importância. Retrieved from https://tecnoblog.net

41. Universidade de Coimbra & Indra Group. (2025). IA e Cibersegurança: O Desafio da Confiança Digital. Coimbra: UC. https://www.itsecurity.pt/news/analysis/universidade-de-coimbra-expoe-riscos-criticos-sobre-seguranca-dos-modelos-de-ia

42. Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. Science, 359(6380), 1146–1151.

APÊNDICES

APÊNDICE – QUESTIONÁRIO ONLINE

"Análise do Conhecimento dos Utilizadores sobre Ciberataques Baseados em Inteligência Artificial"

Consentimento informado, livre e esclarecido para participação em investigação de acordo com a Declaração de Helsínquia e a Convenção de Oviedo.

O presente questionário online tem como objetivo recolher informação sobre o nível de conhecimento dos utilizadores sobre ciberataques que utilizam inteligência artificial (IA). Pretende-se identificar o grau de familiaridade dos questionados com os conceitos e práticas relacionadas a esses tipos de ciberataques, bem como avaliar a perceção deles sobre os riscos e as medidas de segurança associadas. As informações recolhidas serão utilizadas para desenvolver estratégias de consciencialização e formação que visem melhorar a segurança cibernética dos utilizadores. A informação obtida destina-se unicamente a ser usada em investigação científica pela comunidade académica.

Está a ser convidada/o a responder a este inquérito na condição de residente em Portugal e maior de idade. A sua participação é voluntária e anónima.

O questionário estará disponível até 31 de maio de 2025 e o seu preenchimento demorará cerca de 10/15 minutos. As suas respostas são confidenciais. Não será recolhida qualquer informação identificativa como nome, morada ou contactos. A confidencialidade dos dados recolhidos será assegurada de acordo com a legislação em vigor. Poderá desistir de participar em qualquer momento do questionário ou retirar a autorização para utilizar os seus dados, de acordo com a lei de proteção de dados pessoais portuguesa Nº 58/2019.

As questões a que irá responder pretendem avaliar:

1. Quais são os níveis de conhecimento e perceção dos utilizadores sobre os riscos e métodos de prevenção de ciberataques baseados em inteligência artificial?

2. Como o nível de conhecimento dos utilizadores afeta a sua vulnerabilidade a ciberataques?

O inquérito enquadra-se num projeto de investigação do aluno Valdemar António Pacheco, nº 20131810, no âmbito da Unidade Curricular Gestão de Sistemas e Tecnologias de Informação, do 2º ano do Mestrado em GSTI da Atlântica – Instituto Universitário, sob a orientação da Prof. Doutora Carla Sofia Rocha da Silva e foi aprovado pela Comissão de Ética da Atlântica – Instituto Universitário. Em caso de dúvidas pode contactar o investigador responsável através do e-mail carlasilva@uatlantica.pt.

Foi estabelecido um sistema de anonimização eficaz que não permite a identificação posterior do sujeito. No uso que se realize dos resultados do estudo, com fins de ensino, investigação e/ou publicação, respeitar-se-á sempre a devida anonimização dos dados de caráter pessoal, de modo que os sujeitos da investigação não serão identificados ou identificáveis.

Ao escolher a opção "Concordo" abaixo estará a indicar que tomou conhecimento da informação acima, que reside em Portugal, é maior de idade e que está de acordo em participar voluntariamente neste estudo.

Caso não concorde feche o presente questionário.

Obrigado

Prof. Doutora Carla Silva

Concordo ☐

Dados Demográficos:

1. **Idade:**
   - Qual é a sua idade?
     - ( ) 18-24 anos
     - ( ) 25-34 anos
     - ( ) 35-44 anos
     - ( ) 45-54 anos
     - ( ) 55-64 anos
     - ( ) 65 anos ou mais
2. **Género:**
   - Qual é o seu género?
     - ( ) Masculino
     - ( ) Feminino
     - ( ) Outro
     - ( ) Prefiro não responder
3. **Nível de Educação:**
   - Qual é o seu nível de educação mais alto concluído?
     - ( ) Ensino Básico
     - ( ) Ensino Secundário
     - ( ) Licenciatura
     - ( ) Pós-graduação
     - ( ) Mestrado
     - ( ) Doutoramento
     - ( ) Outro
4. **Área de Atuação:**
   - Em qual área você atua profissionalmente?
     - ( ) Tecnologia da Informação e da Comunicação
     - ( ) Serviços públicos ou Administração
     - ( ) Recursos Humanos
     - ( ) Negócios ou consultadoria
     - ( ) Outro

Objetivo_01: Avaliar o Conhecimento Atual: Medir o nível de conhecimento dos utilizadores sobre ciberataques baseados em IA.

Questionário: Avaliação do Conhecimento sobre Ciberataques Baseados em IA

Instruções: Por favor, indique o seu nível de concordância com as seguintes afirmações, utilizando a escala de 1 a 5, onde 1 significa "Discordo totalmente" e 5 significa "Concordo totalmente".

1. **Estou familiarizado com o conceito de ciberataques baseados em IA.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
2. **Sei identificar diferentes tipos de ciberataques que utilizam IA.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
3. **Entendo como a IA pode ser utilizada para automatizar ciberataques.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
4. **Estou ciente das medidas de segurança que podem ser implementadas para proteger contra ciberataques baseados em IA.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
5. **Acredito que estou preparado(a), ou que a minha organização está preparada para lidar com ciberataques baseados em IA.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)

- 4 (Concordo)
- 5 (Concordo totalmente)

6. **Tenho conhecimento sobre casos reais de ciberataques que utilizaram IA.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
7. **Sei onde procurar informações atualizadas sobre ciberataques baseados em IA.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)

Objetivo_02: Identificar Lacunas de Conhecimento: Descobrir áreas onde os utilizadores têm menos compreensão ou estão mais vulneráveis.

Questionário: Identificação de Lacunas de Conhecimento sobre Ciberataques Baseados em IA

Instruções: Por favor, indique o seu nível de concordância com as seguintes afirmações, utilizando a escala de 1 a 5, onde 1 significa "Discordo totalmente" e 5 significa "Concordo totalmente".

1. **Tenho dificuldade em entender como a IA pode ser utilizada para realizar ataques de phishing.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
2. **Não estou familiarizado com as técnicas de deteção de ciberataques baseados em IA.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
3. **Tenho pouca compreensão sobre como a IA pode ser usada para explorar vulnerabilidades em sistemas de segurança.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
4. **Não sei como a IA pode ser utilizada para criar malware avançado.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
5. **Tenho dificuldade em identificar sinais de ciberataques que utilizam IA.**
    - 1 (Discordo totalmente)

- 2 (Discordo)
- 3 (Neutro)
- 4 (Concordo)
- 5 (Concordo totalmente)

6. **Não estou ciente das melhores práticas para proteger contra ciberataques baseados em IA.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
7. **Tenho pouca compreensão sobre como a IA pode ser usada para realizar ataques de negação de serviço (*DDoS*).**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)

Objetivo_03: Analisar Perceções: Compreender como os utilizadores percebem a gravidade e a frequência dos ciberataques.

Questionário: Análise das Perceções sobre Ciberataques Baseados em IA

Instruções: Por favor, indique o seu nível de concordância com as seguintes afirmações, utilizando a escala de 1 a 5, onde 1 significa "Discordo totalmente" e 5 significa "Concordo totalmente".

1. **Acredito que os ciberataques baseados em IA são uma ameaça significativa para a segurança digital.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
2. **Considero que a frequência dos ciberataques baseados em IA está a aumentar.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
3. **Estou preocupado com o impacto potencial dos ciberataques baseados em IA na minha vida pessoal e profissional.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
4. **Acredito que os ciberataques baseados em IA são mais difíceis de detetar do que os ciberataques tradicionais.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
5. **Penso que a minha organização está vulnerável a ciberataques baseados em IA.**

- 1 (Discordo totalmente)
- 2 (Discordo)
- 3 (Neutro)
- 4 (Concordo)
- 5 (Concordo totalmente)

6. **Acredito que os ciberataques baseados em IA podem causar danos significativos às infraestruturas críticas.**

- 1 (Discordo totalmente)
- 2 (Discordo)
- 3 (Neutro)
- 4 (Concordo)
- 5 (Concordo totalmente)

7. **Estou ciente de que os ciberataques baseados em IA podem evoluir rapidamente e tornar-se mais sofisticados.**

- 1 (Discordo totalmente)
- 2 (Discordo)
- 3 (Neutro)
- 4 (Concordo)
- 5 (Concordo totalmente)

Objetivo_04: Propor Soluções Educacionais: Desenvolver métodos para melhorar o conhecimento e a preparação dos utilizadores contra essas ameaças.

Questionário: Propostas Educacionais para Melhorar o Conhecimento sobre Ciberataques Baseados em IA

Instruções: Por favor, indique o seu nível de concordância com as seguintes afirmações, utilizando a escala de 1 a 5, onde 1 significa "Discordo totalmente" e 5 significa "Concordo totalmente".

1. **Gostaria de participar em workshops sobre Cibersegurança focados em ciberataques baseados em IA.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
2. **Acredito que cursos online sobre ciberataques baseados em IA seriam úteis para aumentar o meu conhecimento.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
3. **Penso que simulações práticas de ciberataques baseados em IA ajudariam a melhorar a minha preparação.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
4. **Acredito que materiais educativos, como guias e tutoriais, seriam benéficos para entender melhor os ciberataques baseados em IA.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)

5. **Considero que formações regulares sobre Cibersegurança são essenciais para manter-me atualizado sobre ciberataques baseados em IA.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
6. **Acredito que deveriam ser feitos mais investimentos em programas de formação sobre ciberataques baseados em IA, seja por parte da minha organização ou por iniciativa própria.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
7. **Penso que a colaboração com especialistas em Cibersegurança pode melhorar a nossa defesa contra ciberataques baseados em IA.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)

Objetivo_05: Impacto das Ameaças: Examinar como o nível de conhecimento afeta a vulnerabilidade dos utilizadores a ciberataques.

Questionário: Impacto das Ameaças de Ciberataques Baseados em IA

Instruções: Por favor, indique o seu nível de concordância com as seguintes afirmações, utilizando a escala de 1 a 5, onde 1 significa "Discordo totalmente" e 5 significa "Concordo totalmente".

1. **Acredito que o meu conhecimento sobre ciberataques baseados em IA é suficiente para me proteger contra essas ameaças.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
2. **Sinto-me vulnerável a ciberataques baseados em IA devido à falta de conhecimento específico sobre o tema.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
3. **Acredito que um maior conhecimento sobre ciberataques baseados em IA reduziria a minha vulnerabilidade a essas ameaças.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
4. **A minha falta de conhecimento sobre ciberataques baseados em IA deixa-me mais exposto a possíveis ataques.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
5. **Acredito que a minha organização está vulnerável a ciberataques baseados em IA devido à falta de conhecimento dos funcionários.**

- 1 (Discordo totalmente)
- 2 (Discordo)
- 3 (Neutro)
- 4 (Concordo)
- 5 (Concordo totalmente)

6. **Considero que a formação contínua em Cibersegurança é essencial para reduzir a vulnerabilidade a ciberataques baseados em IA.**

    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)

7. **Acredito que a falta de conhecimento sobre ciberataques baseados em IA pode levar a uma resposta inadequada em caso de ataque.**

    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)

Objetivo_06: Consciencialização e Comportamento: Investigar como a consciencialização sobre Cibersegurança influencia as práticas e o comportamento online dos utilizadores.

Questionário: Consciencialização e Comportamento em Cibersegurança

Instruções: Por favor, indique o seu nível de concordância com as seguintes afirmações, utilizando a escala de 1 a 5, onde 1 significa "Discordo totalmente" e 5 significa "Concordo totalmente".

1. **Estou ciente das melhores práticas de Cibersegurança e aplico as regularmente nas minhas atividades online.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
2. **Evito clicar em links suspeitos ou abrir anexos de e-mails de remetentes desconhecidos.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
3. **Utilizo senhas fortes e únicas para cada uma das minhas contas online.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
4. **Estou ciente dos riscos de ciberataques baseados em IA e tomo medidas para me proteger contra eles.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
5. **Participo regularmente em formações ou cursos sobre Cibersegurança.**
    - 1 (Discordo totalmente)

- 2 (Discordo)
- 3 (Neutro)
- 4 (Concordo)
- 5 (Concordo totalmente)

6. **Confiro e atualizo regularmente as configurações de privacidade e segurança das minhas contas online.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)
7. **Acredito que a minha consciencialização sobre Cibersegurança influencia positivamente o meu comportamento online.**
    - 1 (Discordo totalmente)
    - 2 (Discordo)
    - 3 (Neutro)
    - 4 (Concordo)
    - 5 (Concordo totalmente)