INSTITUTO POLITÉCNICO DE BRAGANÇA
Escola Superior de Tecnologia e Gestão

A Cibersegurança e Tendências Emergentes

Arnilde Rita Costa Fernandes

Dissertação apresentada à Escola Superior de Tecnologia e Gestão para obtenção do Grau de Mestre em Engenharia Eletrotécnica de Computadores

Trabalho realizado sob a orientação de:

Professora Dr.ª Isabel Maria Lopes

Bragança

Outubro de 2025

Dedicatória

Dedico este projeto a todas as pessoas que me apoiaram ao longo do caminho. Primeiramente, a Deus, aos meus familiares, que estiveram sempre do meu lado, oferecendo incentivo e compreensão durante este percurso acadêmico. Aos amigos, que proporcionaram momentos de descontração e alívio nos momentos de tensão. Ao meu namorado pelo incentivo e pela força nos momentos mais difíceis. A minha orientadora, pelo suporte e sabedoria compartilhada, que me guiou na realização deste projeto de dissertação. A todos os professores e colegas que contribuíram para a minha formação e enriqueceram a minha jornada académica. Esta conquista não seria possível sem o apoio e o carinho de cada um de vocês.

Agradecimentos

Gostaria de expressar os meus sinceros agradecimentos pela oportunidade de realizar esta dissertação. Fico grata pela oportunidade de aplicar os meus conhecimentos neste trabalho.

Gostaria também de agradecer por todo o apoio e incentivo que me foram fornecidos ao longo do processo. Agradeço a todos aqueles que deram o seu apoio e contribuíram para o sucesso desta dissertação.

Muito obrigada!

Resumo

Num mundo onde a tecnologia tem estado em constante evolução de forma exponencial, seguido do aumento de aparelhos conectados, a sociedade tem se mostrado submissa as tecnologias, e vê-se um grande aumento da vulnerabilidade da cibersegurança por parte das pessoas e entidades, constituindo assim um número acrescido de ciberataques por parte dos hackers, uma vez que não sabem como se proteger devidamente contra esses ataques, tornando-se assim alvos principais. Desta forma, torna-se importante encontrar uma forma de mitigar esses ataques, implementando assim tendências emergentes como a Inteligência Artificial, Blockchain e Internet das Coisas, para poder de alguma forma mitigar a vulnerabilidade da segurança.

Com esse intuito, esta dissertação tem como principal objetivo, fazer a análise do panorama atual da cibersegurança, explorar as tendências emergentes que podem ser mais eficazes para mitigar os riscos cibernéticos, e avaliar os desafios que vêm com a implementação da cibersegurança nas organizações.

A metodologia de pesquisa utilizada foi a mista, sendo qualitativa com base na revisão bibliográfica, através de artigos científicos, relatórios e fontes de domínio público, quantitativa com base num inquérito que foi dirigido a um determinado grupo de pessoas e posteriormente aplicação de técnicas de Machine learning, especificamente o algoritmos de árvore de decisão para análise preditiva dos dados recolhidos.

Os resultados foram tratados e analisados de forma a contextualizar as respostas com o facto das pessoas e profissionais de TI se encontrarem informadas sobre as principais ameaças cibernéticas e como se devem proteger das mesmas, e analisar como os mesmos percebem os desafios e soluções da segurança digital.

Palavras-Chave: Cibersegurança, Inteligência Artificial, Tendências emergentes, Internet das coisas, Machine Learning.

Abstract

In a world where technology has been constantly evolving exponentially, followed by an increase in connected devices, society has shown itself to be submissive to technology, and there has been a significant increase in cybersecurity vulnerability on the part of individuals and entities, thus constituting an increased number of cyberattacks by hackers, since they do not know how to properly protect themselves against these attacks, thus becoming prime targets. Therefore, it is important to find a way to mitigate these attacks by implementing emerging trends such as Artificial Intelligence, Blockchain, and the Internet of Things to somehow mitigate security vulnerabilities.

To this end, the main objective of this dissertation is to analyze the current cybersecurity landscape, explore emerging trends that may be most effective in mitigating cyber risks, and assess the challenges that come with implementing cybersecurity in organizations.

The research methodology used was mixed, being qualitative based on a literature review, through scientific articles, reports, and public domain sources, and quantitative based on a survey that was directed at a specific group of people and subsequently applied machine learning techniques, specifically decision tree algorithms for predictive analysis of the collected data.

The results were processed and analyzed in order to contextualize the responses with the fact that people and IT professionals are informed about the main cyber threats and how to protect themselves from them, and to analyze how they perceive the challenges and solutions of digital security.

Keywords: Cybersecurity, Artificial Intelligence, Emerging Trends, Internet of Things, Machine Learning.

Índice Geral

Lista de Siglas/Abreviaturas

(APT) Advanced Persistent Threats

(CNCS) Centro Nacional de Cibersegurança

(IA) Inteligência Artificial

(IoT) Internet das Coisas

(ITU) International Telecommunication Union

(ML) Machine Learning

(NIST) Instituto Nacional de Padrões e Tecnologia

Índice de Figuras

Capítulo 1 Introdução

Neste capítulo será abordado contextualizado o tema, focando-se na cibersegurança, objetivo do trabalho, justificação do estudo e estrutura do relatório.

1.1. Contextualização

A cibersegurança tem-se tornado cada vez mais fundamental na nossa sociedade digital. Ela defende-nos contra diversas ameaças virtuais, protegendo os nossos computadores, servidores, dispositivos móveis e redes de ataques maliciosos [1].

Nos últimos anos, especialmente após a pandemia que impactou o mundo inteiro, a nossa vida tornou-se cada vez mais digitalizada. A internet, agora, é parte essencial do nosso quotidiano, trazendo muitas oportunidades e vantagens. Porém, essa mudança também trouxe riscos, como os ciberataques, que visam roubar dados, espionar e causar outros problemas.

Segundo o Centro Nacional de Cibersegurança (CNCS), em Portugal, a criminalidade cibernética aumentou em 2023, mesmo que o número total de incidentes de segurança tenha se estabilizado segundo alguns indicadores.

Ao longo desta dissertação, serão exploradas as dificuldades e desafios da cibersegurança, além de discutir as principais medidas e tendências que estão surgindo para enfrentar essas ameaças.

1.2. Objetivos

O objetivo desta dissertação é examinar o panorama atual da cibersegurança, identificando as principais ameaças que surgem com o crescimento da internet na vida das pessoas. Além disso, serão analisadas as tendências mais relevantes que estão emergindo em resposta ao aumento dessas ameaças e às necessidades das empresas para proteger os seus ativos e sistemas.

1.3. Justificação do Estudo

À medida que a tecnologia avança e a necessidade de compartilhar informações digitalmente cresce, ficamos mais vulneráveis a ataques cibernéticos. Diante desse cenário, é essencial estudar tendências emergentes na cibersegurança que possam ajudar a mitigar esses riscos e atender às necessidades de proteção das organizações.

Neste estudo, serão exploradas as tendências como Inteligência Artificial (IA), Blockchain e Internet das Coisas (IoT), analisando como essas tecnologias podem impactar e trazer benefícios no mundo digital.

1.4. Estrutura do relatório

O presente documento está organizado em cinco capítulos, conforme descrito abaixo:

Capítulo 1: Introdução, onde será apresentada uma breve introdução abordando o contexto, os objetivos do estudo e a justificação para a sua realização.

Capítulo 2: Revisão bibliográfica, que busca fornecer uma visão sobre os principais estudos, conceitos e tendências relacionados à cibersegurança e às novas tecnologias que estão surgindo. Para isso, foram consultadas diversas fontes acadêmicas, artigos científicos e relatórios, a fim de entender o estado atual da pesquisa e identificar áreas que precisam de mais investigação para direcionar estudos futuros.

Capítulo 3: Metodologia, onde serão explorados os métodos que foram utilizados durante o processo da pesquisa, como a metodologia mista, permitindo assim obter uma visão ampla das principais ameaças e desafios enfrentados pelas organizações e não só na área da cibersegurança.

Capítulo 4: Análise e Discussão de Resultados, onde será apresentada uma análise completa com base nos dados obtidos pelo inquérito, permitindo assim entender o nível de conhecimento e perceções das pessoas no ramo da cibersegurança.

Capítulo 5: Conclusão, onde serão apresentadas as considerações finais, bem como uma visão geral sobre os resultados da pesquisa. Além de abordar sugestões para trabalhos futuros e melhorias nas aplicações desenvolvidas.

Capítulo 2 Revisão Bibliográfica

Este capítulo aborda a revisão bibliográfica sobre os fundamentos da cibersegurança, baseada em artigos científicos, livros e trabalhos acadêmicos de diversos autores, com o objetivo de analisar diferentes perspetivas e a contribuição dos diversos autores, possibilitando melhor compreensão sobre o tema em estudo.

.

2.1. Introdução ao Panorama atual da Cibersegurança

Com o grande crescimento e dependência das tecnologias e da internet no nosso quotidiano, a cibersegurança acaba por se tornar um elemento-chave no mundo digital. Os dispositivos computacionais vêm se tornando muito populares através da IoT e de tecnologia de comunicação, e isso faz com que sejam disponibilizados diversos serviços pelas redes, fazendo com que mais e mais dados sejam gerados, e haja uma grande dependência das pessoas e empresas nas tecnologias digitais [2].

Com a crescente "dependência da tecnologia em nossas vidas diárias, os riscos e as consequências dos ciberataques tornaram-se mais severos e abrangentes" [3].

A cibersegurança é considerada como um tema complexo, pois envolve muitos fatores e aspetos, e exige respostas diversas para lidar com diferentes tipos de ameaças [4]. Resumidamente, podemos definir o conceito de segurança informática, ou usualmente denominado de cibersegurança, como "a capacidade de proteger as redes e sistemas informáticos, bem como os dados que nestes circulam, de forma a assegurar a respetiva disponibilidade, autenticidade, integridade e confidencialidade" [5]. A cibersegurança também pode ser definida como:

> A coleção de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, abordagens de gestão de riscos, ações, treinamentos, melhores práticas, garantias e tecnologias que podem ser usadas para proteger o ambiente cibernético e os ativos da organização e do utilizador. Os ativos da organização e do utilizador incluem dispositivos de computação conectados, pessoal, infraestrutura, aplicativos, serviços, sistemas de telecomunicações e a totalidade das informações transmitidas e/ou armazenadas no ambiente cibernético [6].

O papel da cibersegurança tem se tornado extremamente importante, na proporção em que a sociedade se torna gradualmente mais conectada e submissa de tecnologias consolidadas e emergentes [7].

Como uma preocupação significativa no campo da cibersegurança, ‘’ameaças cibernéticas como phishing e ransomware evoluíram para formas sofisticadas de ataques que podem devastar tanto indivíduos quanto organizações ‘’ [8].

O panorama de ameaças continua em constante desenvolvimento, e isso faz com que a segurança digital se torne um desafio cada vez mais enigmático. Dos potenciais riscos, temos o malware, ataques de phishing, engenharia social[1] e outras ameaças cibernéticas aprimoradas, que sondam as fragilidades tecnológicas e humanas. Nesse contexto, torna-se essencial acompanhar as tendências emergentes em segurança cibernética, implementando medidas preventivas e soluções modernas para salvaguardar informações sensíveis e reduzir as chances de ataques [3].

2.2. Principais Ameaças Cibernéticas

Como os ciberataques se estão tornando progressivamente mais aprimorado e passando despercebidos pelas vítimas, fica difícil saber quando sofremos um ataque e só se apercebe depois de algum tempo, quando os dados e segredos empresarial foram desviados pelos atacantes [9]. Na figura 1, podemos observar os diferentes tipos de Ameaças Cibernéticas [10].

[1] A engenharia social pode ser definida como um processo utilizado pelos cibercriminosos para manipular pessoas, de modo que estas realizem involuntariamente ações do interesse do manipulador, explorando a falta de consciencialização e conhecimento das pessoas. Geralmente, estas ações causam danos, ou aumentam a probabilidade de causar danos futuros, à confidencialidade, integridade e disponibilidade dos recursos ou ativos da organização.

Figura 1: Esquema de tipos de ataques cibernéticos. Fonte: Abrahams et al.

2.2.1. Phishing

Phishing é uma ameaça significativa, uma vez que a partir de técnicas de engenharia socias, engana os utilizadores e faz com que os demais divulguem a sua informação sensível, como credencias de login ou outros dados [3]. Torna-se notório de que, phishing prossegue sendo uma ameaça dominante, nomeadamente em departamentos como a saúde, em consequência da pandemia COVID-19 que intensificou as vulnerabilidades [8].

Considerando que os ataques phishing exploram a psicologia humana constantemente e tendem a ser extremamente específicos e avançados, tornam-se mais propensos a serem difíceis de defender. Ataques de ‘’engenharia social em geral, incluindo phishing, estão tornando-se cada vez mais comuns e representam uma ameaça séria para organizações e indivíduos’’ [3].

2.2.2. Insider Threats (Ameaças internas)

Segundo o US-CERT (United States Computer Emergency Readiness Team), inside threat é uma ameaça que se refere a um funcionário, seja ele atual ou antigo, contratado ou parceiro que teve acesso autorizado a sistemas, redes ou dados da organização e que, intencionalmente, ultrapassou ou abusou desse acesso. Isso pode comprometer a confidencialidade, integridade ou disponibilidade das informações e sistemas da empresa. Os principais motivos que levam a ações de insiders maliciosos incluem: ganho

financeiro, descontentamento no trabalho, sensação de posse, ideologia ou influência externa. As consequências dessas ações podem variar bastante, incluindo fraude, sabotagem, espionagem e roubo ou perda de informações sensíveis. Essas ameaças são frequentemente vistas como um dos maiores riscos de cibersegurança para empresas, organizações e órgãos governamentais [11].

2.2.3. Ameaças Persistentes Avançadas (APT)

Segundo o Instituto Nacional de Padrões e Tecnologia (NIST), uma APT (Ameaça Persistente Avançada) é um adversário extremamente capacitado e com recursos consideráveis. Essa ameaça consegue explorar vários métodos de ataque, como ações cibernéticas, físicas e estratégias de dissimulação, para alcançar seus objetivos. Frequentemente, esses objetivos envolvem infiltrar-se e consolidar um acesso na infraestrutura de TI de organizações escolhidas, buscando extrair informações, comprometer operações essenciais, ou preparar-se para futuras ações [12].

As principais características de uma APT são:

1. **Persistência** – o adversário busca seus objetivos ao longo do tempo, mantendo presença no sistema.
2. **Adaptação** – ele ajusta suas táticas conforme os mecanismos de defesa que são aplicados.
3. **Determinação** – mantém o nível de empenho necessário para alcançar os seus objetivos.

Embora os ataques APT não exijam necessariamente tecnologias de ponta, a abordagem organizada e em múltiplas camadas que eles adotam torna muito difícil neutralizá-los [46].

2.2.4. Malware

Malware é conhecido como ‘’software malicioso’’, e é arquitetado para conseguir aceder ao computador, ou mesmo ser instalado sem aviso prévio dos utilizadores, de forma a poder efetuar ações prejudiciais com o intuito de beneficiar os criadores do malware. Os vários tipos de malware que existem podem comprometer seriamente a performance do

equipamento; outros, por mais simples que sejam, também podem servir como distração para o utilizador, e até os mais complexos que se apoderam dos dados sensíveis do aparelho do utilizador [13].

Códigos maliciosos (malware) "são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador" [14]. Várias das formas como um computador pode ser comprometido pelos códigos maliciosos são [14]:

- Exploração de vulnerabilidade existentes nos programas instalados;
- Autoexecução em mídias removíveis infetadas, como pen-drives;
- Acesso a páginas web maliciosas, com o uso de navegadores vulneráveis;
- Ação direta de atacantes que colocam ficheiros corrompidos depois de invadirem o computador;
- Execução de arquivos infetados.

Uma vez instalados, "os códigos maliciosos passam a ter acesso aos dados armazenados no computador e podem executar ações em nome do utilizador, de acordo com as permissões de cada utilizador" [14].

2.2.4.1. Tipos de Malware

- **Vírus**: Um programa malicioso, que tem a função de danificar o computador do utilizador, ao apagar ou anexar ficheiros, ocupando o armazenamento do computador, diminuindo o desempenho do computador e outros. Pode-se alastrar através de anexos de e-mail, pen-drives, etc. Desde que o utilizador não execute o ficheiro, o vírus não pode ser ativado, ou seja, sem intervenção humana não pode ser ativado [13].
- **Worm:** Programa capaz de se replicar automaticamente, e difere do vírus por não necessitarem de intervenção humana para propagar pela rede e espalhar do equipamento infetado para a rede toda. Consomem muitos recursos como espaço, largura de banda e, consequentemente, afetam o funcionamento de redes e o uso de computadores [13, 14].

- **Cavalo de troia[2] (Trojan):** "Os Trojans se disfarçam, parecendo ser algo legítimo. Os Trojans geralmente destroem dados ou tentam extrair informações confidenciais, incluindo dados financeiros e senhas" [15]. Uma vez que o ficheiro parece ser legítimo, o utilizador faz o download, isto não só provoca danos no computador como abre uma porta dos fundos que permite que o utilizador seja controlado por um computador remoto, e os trojans não infetam os outros computadores da rede e não se multiplicam [13].

- **Ransomware:** Em inglês "ransom", que significa resgate, exigir resgate ou pagar para resgatar, é uma classe de malware por resgate que é instalada no computador do utilizador pelo atacante, usada para práticas de extorsão virtual, ameaçando as vítimas e exigindo um pagamento para o resgate [16,17]. Em 1989 Josep Popp desenvolveu o primeiro ransomware de nome AIDS, e exigindo um resgate após a infestação [18]. É conhecido como Síndrome da Imunodeficiência Adquirida (AIDS) ou Trojan-PC Cyborg e se alastrou numa conferência dobre AIDS através de vinte mil disquetes infetados que foram distribuídos aos integrantes [19]. "Ele permanece silencioso no sistema e é ativado após 90 reinicializações do sistema. Ao ser ativado, ele ou criptografa os arquivos ou oculta os diretórios [19]. Podem ser classificados em duas categorias com base no seu modo de atuar: "Cryptoransomware" que codifica os arquivos e "lockerransomware" que restringe o acesso completo do utilizador ao sistema [20].

- **Bot e botnet:** são programas que permitem ao atacante controlar remotamente computadores infetados sem o consentimento do utilizador, enquanto botnet é uma rede composta por inúmeros computadores que permitem potencializar as ações danosas executadas pelos bots. Podem ser efetuadas ações maliciosas como ataques de negação de serviço, propagação de códigos maliciosos, coleta de dados de inúmeros computadores, envio de spam, entre outros [14].

- **Syware:** São programas que ficam de olho nas atividades do sistema e mandam informações recolhidas para terceiros. O uso pode ser legítimo quando às vezes, o próprio dono do computador instala para monitorizar as atividades e evitar que o computador seja usado de forma inadequada. Mas também pode ser usado de

[2] O "Cavalo de Troia", segundo a mitologia grega, foi uma grande estátua, utilizada como instrumento de guerra pelos gregos para obter acesso ` a cidade de Troia. A estátua do cavalo foi recheada com soldados que, durante a noite, abriram os portões da cidade possibilitando a entrada dos gregos e a dominação de Troia.

forma maliciosa, e neste caso spyware compromete a sua privacidade e segurança ao capturar dados como navegação na web, credenciais de login e outras informações sensíveis. Existem alguns tipos de spyware como o Keylogger, que regista tudo o que digitamos, geralmente é ativado quando acedemos sites de bancos. Temos o Screenlogger que grava cliques do rato do computador e imagens do ecrã, utilizado muitas vezes para roubar credenciais de teclados virtuais. E Adware que mostra anúncios, que podem ser legítimos (ajudando a financiar serviços gratuitos) ou maliciosos (exibindo propagandas direcionadas sem que você tenha dado permissão) [14].

2.2.5. Denial of service (DoS)

DoS é um ataque que tem como finalidade interromper a execução de um serviço, e torna inacessível o acesso aos utilizadores autorizados. São simples de executar e tem a capacidade de gerar danos graves, podem paralisar os serviços de uma empresa, deixando-a inoperante globalmente. No caso dos ataques DDoS "Distributed Denial of service" em inglês, que é uma variante do DoS, recorre-se a múltiplos dispositivos para efetuar ataques simultâneos a um alvo [6]. Ataques DoS "exploram vulnerabilidades na arquitetura do sistema que está sob ataque. Em alguns casos, ele explora a fraqueza de muitos protocolos comuns da Internet, como o protocolo de mensagem de controle da Internet (ICMP)'' [6].

2.2.6. Ataques a Dispositivos IoT

Internet das coisas (IoT), é um ecossistema que compõe dispositivos físicos interligados entre si, com a capacidade de recolher e partilhar informações através da internet. Qualquer objeto pode se conectar, não se limitando apenas aos computadores e tablets tradicionais [21]. A Agência da União Europeia para a Cibersegurança (ENISA), define a IoT como um conceito emergente que envolve um vasto ecossistema de dispositivos e serviços conectados, incluindo sensores, objetos inteligentes, veículos, equipamentos industriais e de saúde [22]. A palavra "coisas" em IoT é conhecida como dispositivos IoT [23].

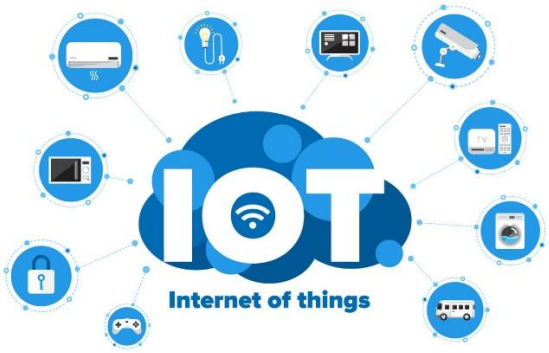

Figura 2: Internet das coisas. Fonte: GlobalSign Blog

A IoT facilita a interligação entre diferentes dispositivos, como smartphones, eletrodomésticos inteligentes, veículos, sensores internos e externos, entre outros. Diversas abordagens são aplicadas para garantir a boa gestão da inclusão de uma vasta gama de dispositivos inteligentes à internet [24, 25].

Os dispositivos IoT têm diversas aplicações, desde o uso doméstico, setores industriais e de saúde, como mostra na figura 3 [23].

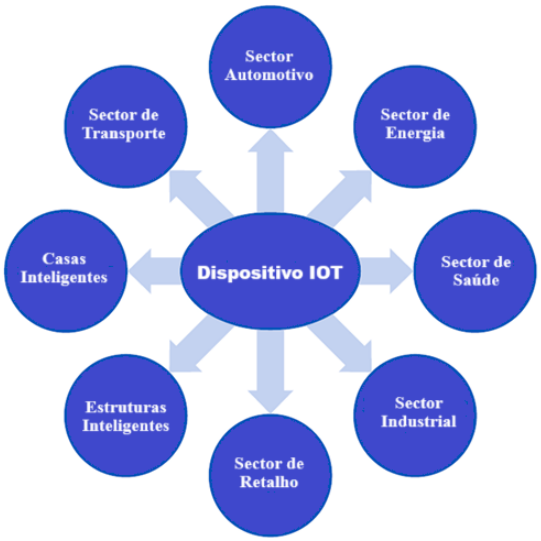

Figura 3: Aplicações de IoT; Adaptado de Cyber Resilience Act 2022

De acordo com o relatório *State of IoT Summer 2024* da IoT Analytics, havia cerca de 16,6 bilhões de dispositivos IoT conectados até o final de 2023. Isso representa um crescimento de 15% em relação ao ano anterior. Para 2024, a previsão era que esse número aumentaria em mais 13%, chegando a 18,8 bilhões de dispositivos. É verdade que algumas circunstâncias, como inflação, altas taxas de juros, falta de chipsets e conflitos geopolíticos, reduziram um pouco esse crescimento. Apesar desses desafios,

51% das empresas estão pensando em aumentar seus orçamentos para IoT no próximo ano. E olhando para o futuro, estima-se que o total de dispositivos conectados possa alcançar 40 bilhões até 2030. No entanto, essa previsão foi ajustada um pouco devido a novas tendências no mercado [26].

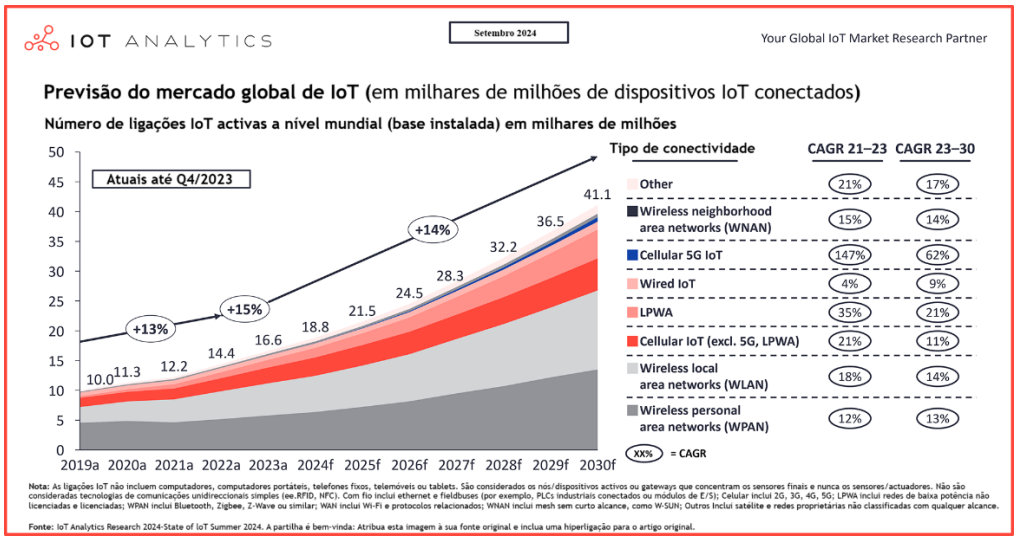

Figura 4: Previsão do mercado global de IoT. Adaptado de IoT Analytics Research 2024

2.2.6.1. Funcionamento da IoT

A IoT opera como um sistema de componentes interconectados, permitindo que eles trabalhem juntos para coletar, analisar e agir sobre dados de maneira contínua [27]. Na figura 4, demonstra-se como os componentes básicos da IoT podem ser interligados como forma de fornecer soluções simples.

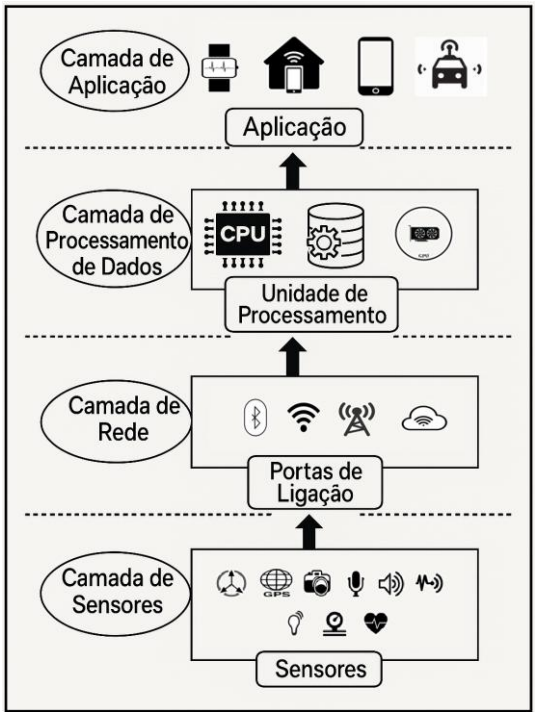

Figura 5: Os 4 componentes da IoT. Adaptado de Researchgate.

- **Camada de Sensores (Sensing Layer):** Os sensores são responsáveis por captar várias informações, como a temperatura e o movimento. Já os atuadores utilizam esses dados para realizar ações automáticas, como aumentar ou diminuir a temperatura do ar condicionado [27].
- **Camada de Conectividade (Network Layer):** Para enviar as informações que recolhem, os dispositivos IoT conectam-se a redes sem fios, podendo ser Wi-Fi, Bluetooth ou até mesmo redes móveis [27].
- **Camada de Processamento de Dados (Data Processing Layer):** Os dados são enviados para processamento, que pode ocorrer em servidores locais ou na nuvem. Lá, algoritmos estão prontos para analisar tudo e gerar insights bem úteis [27].
- **Camada de Aplicação (Application Layer):** As pessoas conseguem visualizar e controlar os seus dispositivos IoT por meio de aplicativos e painéis de controle, podendo personalizar as suas preferências e receber alertas. Além disso, a automação faz com que esses dispositivos reajam automaticamente a certos eventos [27].

2.2.6.2. Ataques comuns à IoT

Por motivos de limitação de recursos computacionais, a vasta gama de dispositivos IoT utilizados nas redes empresariais é vulnerável a ciberataques, o que dificulta a execução

de mecanismos tradicionais de segurança convencionais como antivírus e firewall, podendo levar ao aumento de fugas de dados e acessos não autorizados [28].

Como os dispositivos IoT são produzidos por diversos produtores, eles seguem diferentes princípios e padrões organizacionais. Por isso, manter uma consistência de segurança em todos os dispositivos produzidos torna-se complicado. A vulnerabilidade nesses dispositivos, pode permitir ataques que comprometam a integridade dos dados na plataforma. Desta forma, torna-se essencial a importância de projetar e desenvolver métodos de segurança alternativos para mitigar esses riscos [28].

Questões como a falta de correção das vulnerabilidades, a falta de soluções de segurança adequadas e senhas inalteradas ou inseguras, fazem com que os dispositivos sejam considerados como vulneráveis [29]. Ataques como DDoS e ataques de malware, têm se tornado uma tendência e andam cada vez mais direcionados aos dispositivos IoT. Alguns ataques comuns que atacam os dispositivos IoT são:

- **Ataques Man-in-the-Middle (MITM)**: é um ataque que permanece sendo uma ameaça constante na cibersegurança. Os cibercriminosos conseguem aceder, modificar e até mesmo se passarem pelos utilizadores legítimos. As áreas de Wi-Fi gratuito são muito vulneráveis, porque os pacotes que não são criptografados podem ser acedidos facilmente. Os hackers muitas vezes redirecionam o tráfego da rede pela conexão deles, o que permite que capturem informações sensíveis, como dados pessoais ou senhas. Isso mostra como é importante usar conexões seguras, especialmente em Wi-Fi público, e adotar a criptografia para proteger os seus dados enquanto eles estão em trânsito. Ter consciência sobre segurança e agir de forma responsável online é fundamental. Usar software licenciado, ferramentas de antivírus e antispyware, manter firewalls pessoais e criar senhas fortes são maneiras eficazes de proteger seus sistemas. Também é prudente evitar downloads de fontes desconhecidas, ter cuidado com anexos de e-mail e evitar sites suspeitos. A incorporação de máquinas virtuais pode adicionar uma camada extra de segurança. No cenário em constante mudança das ameaças cibernéticas, ser proativo e bem informado é a chave para proteger os seus sistemas de computador e informações pessoais [30].

- **Espionagem**: Os cibercriminosos interceptam o tráfego de rede e obtêm as credenciais ou dados confidenciais que os dispositivos IoT transmitem pelas redes

corporativas, caso exista uma conexão fraca entre dispositivos IoT e um servidor [29].

- **Ataques de senha de força bruta**: A segurança dos dispositivos IoT muitas vezes não é levada em conta nas empresas, o que os torna alvos fáceis para possíveis ataques cibernéticos. Esses ataques podem ser do tipo força bruta ou de dicionário. Muitas vezes, as senhas desses dispositivos são deixadas como estavam de fábrica ou definidas com senhas bem simples. Isso permite que os cibercriminosos realizem ataques de força bruta ou dicionário para conseguir acesso aos dispositivos [29].

- **Sequestro de firmware**: Atualmente, com tantas marcas e produtos de IoT, cada um vem com seu próprio software e atualizações. Essa diversidade pode ser um prato cheio para agentes mal-intencionados, que acabam enviando atualizações ou drivers falsos pela internet. Assim, se os drivers dos dispositivos de IoT não forem devidamente verificados, existe o risco de que invasores possam sequestrar o dispositivo e instalar software nocivo [29].

- **Injeção de nó malicioso**: Como o nome sugere, os invasores inserem fisicamente nós maliciosos entre nós legítimos em uma rede IoT durante esse tipo de ataque. Dessa forma, esses nós maliciosos conseguem ter controle sobre os dados que circulam entre os nós conectados [29].

- **Adulterações físicas**: As ameaças físicas estão por aí, especialmente quando se trata de dispositivos IoT que podem ser acedidos de fora. É um desafio para as empresas controlar quem tem acesso a eles. Agentes de ameaças podem explorar dispositivos IoT que não estão bem protegidos fisicamente ou instalar malware [29].

2.3. Tendências Emergentes em Cibersegurança

O ameaçador panorama das ciberameaças está em constante transformação. Isso torna indispensável a contínua criação e implementação de excelentes soluções na área da cibersegurança. Nos últimos anos, diversas tendências emergentes têm mostrado um grande potencial para proporcionar cada vez mais segurança no ambiente digital e para reduzir a quantidade e a gravidade de incidentes na área [31].

2.3.1. Inteligência Artificial e Aprendizado de Máquina (ML)

A inteligência artificial (IA) e o aprendizado de máquina (ML) na cibersegurança, trouxeram avanços significativos, fazendo com que as empresas e organizações consigam respostas mais rápidas e eficazes, que visam melhorar a identificação e respostas a ameaças mais eficientes em tempo real. Com a IA, as soluções de cibersegurança podem analisar grandes conjuntos de dados, identificar padrões e descobrir anomalias que possam ser ameaças cibernéticas. Com técnicas de aprendizado não supervisionado, a IA consegue adaptar-se aos novos tipos de ataques malware que possam surgir, proporcionando uma proteção mais eficaz. Para além disso, outra tendência, a automação de processos, melhora a gestão de incidentes, permitindo que as equipas de segurança possam dedicar-se a desafios mais elaborados e serem mais eficazes e eficientes. [3,31].

Como tudo, o uso da IA na cibersegurança também traz algumas complicações. E como exemplo, os desvios nos algoritmos é uma preocupação crescente, uma vez que os modelos de IA replicam as vezes e até amplificam os desvios humanos. Outra questão, é o facto de os sistemas que são alimentados pela IA requerem enormes quantidades de dados para poderem treinar modelos de aprendizado de máquina, o que pode ser um problema para as empresas com escassez de dados. Um dos campos onde a IA vem ganhando destaque é na segurança de redes, onde são usadas ferramentas de análise de tráfego de rede (NTA) que usam algoritmos para poder permitir as equipas identificarem e responderem rapidamente as ameaças, monitorizando e detetando padrões de ameaças em tempo real [3].

2.3.2. Blockchain

A tecnologia Blockchain é vista como uma solução para desafios da cibersegurança, fornecendo uma estrutura descentralizada e segura para armazenamento e partilha de dados. A aplicação dessa tecnologia no setor propõe a criação de identidades digitais seguras, o rastreamento da proveniência das informações e a manutenção de registos que, por definição, são imutáveis, de eventos de segurança. Para além disso, as soluções que têm o blockchain como base estão se inserindo em outros ambientes como o da gestão de identidade, comunicação segura e crítica, reduzindo a vulnerabilidade e perda de dados. Uma das suas grandes vantagens, é a sua robustez contra adulterações e a capacidade de fornecer um registo claro e confiável de operações. Mas os seus promissores recursos, tais como o funcionamento sem uma autoridade central, a transparência e a resistência à fraude, não garantem que as tecnologias baseadas em blockchain sejam adotadas na cibersegurança. As razões principais para essa falta de adoção incluem desafios de escalabilidade, interoperabilidade e questões de governação. Para contornar esses percalços, estudiosos da área estão a buscar novas maneiras de tornar o uso do blockchain mais eficiente, garantindo a integração do sistema com os já existentes e otimizando, sob a luz da pesquisa, as condições para se implantar um sistema seguro baseado nessa nova tecnologia [3,31].

2.3.3. Computação Quântica

Na computação quântica, a evolução ocorre a nível de hardware, particularmente os processadores. Ao contrário dos computadores tradicionais, que trabalham com bits digitais que só podem estar em um estado fixo de 0 ou 1, os computadores quânticos utilizam qubits. Esses qubits têm a incrível capacidade de estar em múltiplos estados ao mesmo tempo. Isso é algo que a gente pode entender melhor com o famoso exemplo do gato de Schrödinger[3], e é isso que permite um processamento de dados muito mais potente e paralelo [32].

A computação quântica tem o potencial de resolver problemas complexos de maneira mais eficiente do que os computadores que usamos hoje. Mas essa mesma capacidade

[3] O **gato de Schrödinger** é um experimento mental de 1935 que ilustra o paradoxo de aplicar as leis da Mecânica Quântica a sistemas macroscópicos. No experimento, um gato em uma caixa pode estar vivo e morto ao mesmo tempo até que uma medição defina seu estado.

traz desafios, especialmente quando falamos sobre a segurança da informação. Algoritmos de criptografia que hoje parecem seguros podem, no futuro, ser vulneráveis por causa do avanço da computação quântica. Por exemplo, métodos de criptografia que estão protegendo dados sensíveis agora podem ser facilmente quebrados por computadores quânticos, colocando em risco informações confidenciais. Para evitar esses riscos, é fundamental que empresas e governos comecem a adotar algoritmos de criptografia que sejam resistentes à computação quântica [32].

A introdução da computação quântica no campo da IA promete trazer várias mudanças. Com novas técnicas, é possível melhorar o desempenho dos algoritmos de aprendizagem automática. A superposição quântica, por exemplo, permite que sejam processados milhares de informações ao mesmo tempo, o que acelera bastante o treinamento dos modelos e traz vantagens em relação aos métodos convencionais. Além disso, a computação quântica pode dar um empurrãozinho para avanços na aprendizagem por reforço e na tomada de decisões em situações complexas. Essa capacidade de lidar com enormes volumes de dados pode levar à criação de sistemas de IA mais inteligentes, que replicam processos do nosso cérebro e se adaptam melhor a diferentes desafios [33]. Adaptar-se de forma proativa a essa nova realidade tecnológica é muito importante para garantir a segurança e a privacidade das informações no futuro [32].

2.3.4. Cloud Security (Segurança na nuvem)

Cloud security, ou também conhecida como computing security, é uma área complexa que se encontra em constante evolução, exigindo combinação de técnicas e administrativos para lidar com os desafios cibernéticos. A criptografia entra como uma peça-chave nesse cenário, garantindo que os nossos dados fiquem seguros, tanto quando estão guardados quanto enquanto estão sendo enviados. Ela ajuda a bloquear acessos indesejados e a evitar que informações preciosas se espalhem. Mas, nem sempre é fácil de usar criptografia na nuvem. Existem desafios, especialmente quando se trata de entender como gerenciar chaves e aplicar as técnicas corretas de criptografia. Uma alternativa interessante que vem ganhando atenção é a criptografia homomórfica, que nos permite processar dados sem ter de descriptografá-los, o que proporciona mais segurança [3].

2.3.5. Internet das Coisas (IoT)

O crescimento da IoT, trouxe consigo diversas vulnerabilidades, pois, as conexões de dispositivos estão cada vez mais propensas a se tornarem alvos de ataques cibernéticos [31]. Além disso, a privacidade de dados torna-se muito preocupante, uma vez que a recolha em grande escala de informações pode resultar em violações, o que torna essencial ter uma boa encriptação e controle de acesso. A integração com sistemas que já existem pode ser complexa, porque as diferenças nos protocolos e na compatibilidade dificultam a comunicação entre eles. Outra questão é a escalabilidade que, com o crescimento da IoT, é preciso ter redes mais rápidas e eficientes para garantir que tudo funcione da melhor maneira [34]. A gestão de dispositivos é outra dificuldade que exige atualizações constantes e manutenções para evitar falhas e que as tecnologias fiquem ultrapassadas. E, para completar, a quantidade imensa de dados gerados pode causar uma sobrecarga, dificultando a análise e a extração de perspetivas que são importantes [34].

Como forma de mitigar esses riscos, as tecnologias emergentes da cibersegurança para IoT focam-se na proteção dos dispositivos, dos protocolos de comunicação, e da transmissão de dados. Estratégias como a autenticação de dispositivos, inicialização segura e atualizações remotas são essenciais para mitigar ataques botnets e acessos não autorizados a infraestruturas críticas [31].

A evolução da IoT está sendo acelerada por várias tendências tecnológicas. Com a chegada do 5G e do Edge Computing, a velocidade de conexão melhora consideravelmente e a latência diminui, o que é ótimo para coisas como veículos autônomos e cidades inteligentes que precisam reagir rapidamente. Ao mesmo tempo, a preocupação com a segurança aumenta, levando a melhorias em criptografia, autenticação e regulamentações para a proteção de dados sensíveis [34].

A integração da IA na IoT traz uma nova dimensão às operações, tornando-as mais inteligentes e eficientes. Isso se reflete em aplicações práticas, como a manutenção preditiva e a personalização dos cuidados de saúde. Além disso, a sustentabilidade e o gerenciamento de energia também são beneficiados pela IoT, ajudando a otimizar recursos e a reduzir desperdícios em redes inteligentes e infraestruturas urbanas. No campo da saúde, a IoT está desempenhando um papel cada vez mais importante na monitorização remota de pacientes, permitindo tratamentos mais eficazes e

diminuindo a necessidade de consultas presenciais. Essas mudanças destacam como a IoT está impulsionando a inovação e a transformação digital em diferentes setores [34].

2.4. Desafios para as organizações

No mundo de hoje, cada vez mais conectado e dependente da tecnologia, a cibersegurança é uma preocupação que não dá para ignorar. Todas as empresas, sejam grandes ou pequenas, precisam ficar atentas a isso. Com o uso crescente das tecnologias de informação e comunicação, surgem novos desafios e riscos. Por isso, proteger-se contra ameaças cibernéticas é fundamental para garantir a continuidade e o sucesso de qualquer organização [35].

Uma das maiores ameaças que as empresas enfrentam são os chamados insider threat (ameaças internas). que é literalmente o membro que faz parte da organização, ou seja, é considerado um "agente de confiança". O funcionário tendo um nome de utilizador e uma palavra-passe autêntico, convive de forma constante com os ativos de informação da organização, e podem provocar problemas a confidencialidade, integridade ou disponibilidade dos sistemas de informação (SI), através de ações intencionais como um funcionário insatisfeito ou espionagem, ou a falha em seguir as políticas de segurança pode acontecer por vários motivos, como negligência, falta de treinamento adequado ou simplesmente desinteresse em manter a integridade e a privacidade das informações sensíveis da organização, parceiros e clientes [36].

O CNCS em Portugal, afirma que: "Há uma atitude positiva a respeito da cibersegurança por parte das organizações, mas estas ainda têm falta de recursos internos" [37]. O CNCS desenvolveu o Quadro Nacional de Referência para a Cibersegurança (ENRCS), que reúne um conjunto de técnicas com o objetivo de reduzir os riscos associados a ciberameaças nas organizações contendo as bases para que qualquer entidade possa, de uma forma voluntária, cumprir os requisitos mínimos de segurança das redes e sistemas de informação [38].

Os principais desafios que as organizações hoje enfrentam são:

- **Sofisticação das técnicas de ameaças digitais**: Ameaças como Malware, Phishing, Ataques de força bruta e outros estão numa constante evolução, o que os torna mais sofisticados e difícil de detetar [39].

- **Inexistência de planos de resposta a incidentes:** As empresas não têm um plano bem estruturado, testado e alinhado as necessidades dos ativos que necessitam de ser protegidos, para o caso de acontecerem incidentes, o que compromete a uma resposta aos ciberataques [39].

- **Treinamento inadequado das equipas:** É necessário que os funcionários estejam devidamente treinados e capacitado, de modo a responder de forma rápida e eficiente aos ataques cibernéticos, a falta desta preparação dificulta a implementação de ações rápidas durante as crises [39].

- **Foco reativo, não preventivo:** As organizações limitam-se em combater e mitigar ataques que já aconteceram, ao invés de adotarem uma postura preventiva e proativa, dificultando a antecipação dos riscos [39].

- **Escassez de especialistas em Cibersegurança:** Ainda é um grande desafio para as empresas lidar com a falta de profissionais qualificados, o que acaba tornando difícil a implementação de controles e soluções de segurança de forma eficaz [39].

- **Desalinhamento com as estratégias de negócios:** Muitas empresas têm dificuldade em integrar a cibersegurança nas suas estratégias e objetivos de negócio. Isso faz com que suas defesas sejam inconsistentes e pouco eficazes. Para superar esses desafios, é crucial ter um planeamento sólido, oferecer formação contínua e realizar simulações realistas que ajudem a reforçar a preparação e a resiliência organizacional [39].

2.4.1. Escassez de Profissionais

A escassez de profissionais capacitados em cibersegurança é um verdadeiro desafio global. Por isso, é fundamental que invistamos na formação e qualificação nessa área. Para que possamos criar uma cultura de cibersegurança sólida, é essencial incluir esse assunto nos currículos escolares desde cedo e promover iniciativas educativas e de sensibilização que alcancem toda a sociedade [40].

Segundo a CNCS, as organizações em Portugal estão cada vez mais conscientes da importância da cibersegurança e têm trabalhado em estratégias para implementá-la. No entanto, muitas delas enfrentam dificuldades devido à falta de recursos internos, e a escassez de profissionais qualificados é ainda maior do que a média na União Europeia. A Administração Pública, por sua vez, identifica uma necessidade urgente de habilidades nessa área. Como resultado, é cada vez mais comum que as organizações optem por contratar serviços externos de cibersegurança para preencher essas lacunas [37].

Segundo o International Information System Security Certification Consortium (ISC2), houve um aumento de talento na área da cibersegurança ano de 2023, mas não foi o suficiente para suprir a necessidade, de modo que se verificou que no ano de 2023 houve uma escassez de quatro milhões de profissionais na área no mundo todo. Pelos dados do ISC2, com o aumento dos ataques cibernéticos, 75% dos profissionais de cibersegurança acredita que o cenário atual das ameaças vem sendo um grande desafio nos últimos cinco anos [41].

A falta de profissionais qualificados em cibersegurança tem gerado problemas sérios para a segurança das empresas. Segundo o relatório "Global Cybersecurity Skills Gap Report" da Fortinet, quase 90% das organizações enfrentaram pelo menos uma violação de segurança no último ano por causa dessa lacuna. Essa escassez de mão de obra aumenta os riscos cibernéticos, e 70% das empresas admitem que isso contribui para riscos adicionais. Estima-se que é preciso quatro milhões de profissionais para preencher essa crescente lacuna na força de trabalho da cibersegurança. As certificações em cibersegurança são muito valorizadas pelos empregadores como um sinal de que o profissional tem os conhecimentos e habilidades necessários. Para enfrentar os riscos e combater as ameaças mais complicadas, é essencial que adotemos uma abordagem colaborativa que una tecnologia de segurança adequada, formação contínua dos profissionais e uma sensibilização geral sobre a importância da cibersegurança. Aumento na frequência de ciberataques caros, juntamente com as possíveis consequências severas para executivos, está forçando as empresas a reforçarem suas defesas contra esses ataques. Consequentemente, as organizações estão se concentrando em uma abordagem que combina treinamento, conscientização e tecnologia para lidar com os desafios atuais [42].

2.4.2. Conformidade com o RGPD

O Regulamento Geral de Proteção de Dados, conhecido como RGPD, é uma importante legislação da União Europeia (UE 2016/679) que estabelece regras para proteger, processar e garantir a livre circulação de dados pessoais entre os Estados-Membros. Esta legislação encontra-se em vigor desde o dia 25 de maio de 2018, e aplica-se aos organismos e entidades que integram a administração pública. O Regulamento Geral de Proteção de Dados (RGPD) é algo que todos devem cumprir uma vez que garante a cada cidadão uma série de direitos sobre os seus dados pessoais. Esses direitos podem ser facilmente exercidos junto das entidades que lidam com a recolha e o armazenamento dessas informações [43].

Estar em conformidade é basicamente seguir as normas e regulamentos que orientam as ações no quotidiano. Para garantir a conformidade, é necessário que as empresas conheçam as legislações e regras que lhes competem, garantindo o conhecimento jurídicos especializados. Dessa maneira, podem definir políticas e procedimentos para garantir o seu cumprimento, como treinar os funcionários, acompanhar o que acontece internamente e ter formas de relatar e resolver problemas que possam surgir. Além disso, fazer auditorias e avaliações periódicas é fundamental para ter certeza de que tudo está funcionando bem e que a organização está atualizada com as regulamentações [44].

Para as empresas estarem em conformidade com o RGPD, devem sensibilizar os seus colaboradores sobre a importância de cuidar dos dados. Isso envolve investir em ferramentas adequadas, como software de segurança, designar um responsável pela proteção de dados (EPD) e revisar as práticas de gestão de dados em uso. É fundamental criar um inventário detalhado dos dados, atualizar as políticas de privacidade, reforçar os mecanismos de consentimento e estabelecer protocolos para atender a solicitações de dados. Também é muito importante treinar os funcionários e preparar um plano de resposta a possíveis violações, garantindo que as partes afetadas e as autoridades reguladoras sejam notificadas rapidamente [44].

No que diz respeito às organizações, o RGPD exige que adotem medidas, tanto técnicas quanto organizacionais, para se alinharem às normas de proteção de dados e para respeitar os direitos dos cidadãos. Desde que o regulamento entrou em vigor, o Instituto de Gestão Financeira e Equipamentos da Justiça, I.P. (IGFEJ) tem tomado todas as providências necessárias para garantir que está em conformidade e que os mecanismos de proteção de

dados funcionam corretamente. O IGFEJ também disponibiliza aos titulares dos dados os meios que eles precisam para exercer seus direitos, garantindo transparência e conformidade através da sua Política de Privacidade e Proteção de Dados Pessoais. Nesse cenário, o Encarregado de Proteção de Dados (DP) do IGFEJ fica responsável por monitorar o cumprimento das regras e por manter a comunicação com os titulares dos dados, oferecendo esclarecimentos e servindo como ponto de contato com a Comissão Nacional de Proteção de Dados (CNPD) [43].

2.5. Lacunas na Literatura

A literatura sobre cibersegurança tem avançado rapidamente para acompanhar novas ameaças e tecnologias que surgem no nosso dia a dia. No entanto, ainda existem algumas lacunas que dificultam a eficácia das soluções disponíveis e a capacidade das organizações de se protegerem contra riscos emergentes.

Uma dessas lacunas é o uso da IA na defesa cibernética. Apesar dos progressos na deteção de ameaças, muitas empresas ainda encontram dificuldades para implementar essas tecnologias. Um estudo da Kaspersky mostrou que 19% das empresas europeias não têm ferramentas de cibersegurança baseadas em IA e cerca de 40% enfrentam uma escassez de profissionais qualificados nessa área. Além disso, nota-se uma falta significativa de formações específicas sobre a aplicação da IA na segurança digital, o que dificulta a adoção eficaz dessas soluções [45].

Outra lacuna importante está relacionada ao papel do machine learning (ML) na segurança da IoT. Embora o ML seja visto como uma abordagem promissora para detetar e mitigar ataques cibernéticos, ainda faltam estudos que mostrem sua aplicabilidade em situações reais. A maioria das pesquisas foca em modelos teóricos, sem abordar detalhadamente desafios práticos, como a adaptação de algoritmos a diferentes tipos de dispositivos IoT e a gestão da grande quantidade de dados gerados por essas redes [46].

Por fim, a crescente adoção de dispositivos IoT tem colocado as organizações frente a riscos significativos, e a literatura ainda não fornece soluções abrangentes para mitigar essas vulnerabilidades. Muitos dispositivos IoT têm falhas de segurança que podem ser facilmente exploradas. A grande quantidade de dados gerados torna seu monitoramento

e proteção um verdadeiro desafio. Embora existam recomendações gerais, como a atualização regular de firmware e a troca de senhas padrões, ainda há uma carência de estudos que proponham estratégias concretas e escaláveis para garantir a segurança das redes IoT em ambientes corporativos [47].

Todas essas lacunas mostram a necessidade de mais pesquisas e iniciativas para fortalecer a cibersegurança e assegurar que as organizações estejam preparadas para enfrentar as ameaças que estão por vir.

Capítulo 3 Metodologia

Este capítulo tem como objetivo descrever os principais métodos de investigação que foram utilizados para realizar a pesquisa. Foram utilizadas as metodologias mistas, ou seja, possuem uma abordagem qualitativa com base na revisão bibliográfica e uma abordagem quantitativa com base num inquérito aplicado a um determinado grupo de participantes. Adicionalmente utilizaram-se técnicas de IA, em específico o algoritmo de árvore de decisão. Desta maneira, é possível conseguir uma visão ampla das principais ameaças, das inovações tecnológicas, dos desafios que as organizações enfrentam na área de cibersegurança e obter uma análise empírica e preditiva aos dados obtidos.

3.1. Tipo de pesquisa

Para a realização deste trabalho, adotou-se a metodologia mista, em que foram combinadas as abordagens qualitativas e quantitativas. A abordagem qualitativa fundamentou-se na revisão bibliográfica, que facilitou a compreensão do estado atual da cibersegurança e das tendências emergentes. A abordagem quantitativa, em contrapartida, fundamentou-se na análise dos dados recolhidos por intermédio do inquérito aplicado, cujas perguntas usadas encontram-se no Anexo A.

Como complemento, foram aplicadas técnicas de IA, especificamente Aprendizado de Máquina (ML), como forma de investigar os resultados e identificar padrões significativos nos dados obtidos. Uma vez que esta pesquisa tenta compreender um fenômeno que se encontra em constante avanço, é descrita como de carácter exploratório, envolvendo a coleta de dados e o uso da IA para identificar padrões e relações nos dados.

3.2. Procedimento de Recolha de Dados

Através da ferramenta Google Forms, criou-se um questionário online, como forma de entender melhor como as empresas, estudantes, profissionais na área e os utilizadores da internet veem este mundo da cibersegurança. Neste estudo, o termo utilizadores de internet refere-se ao público geral que, embora não possua formação ou atividade profissional específica em cibersegurança, faz uso cotidiano da internet para fins pessoais, sociais ou profissionais. Neste estudo, o questionário foi destinado a todas as pessoas de diferentes faixas etárias, sem restrição de idade, permitindo variedade na amostra; desta maneira, as respostas abrangem desde participantes mais jovens até os mais velhos. A divulgação do questionário foi feita em diferentes redes sociais, como o LinkedIn e outras, fóruns temáticos e alguns grupos profissionais relacionados com a área de tecnologia e segurança de informação. Também foi divulgado para os estudantes e alguns docentes do Instituto Politécnico de Bragança. O questionário tratava-se de um link aberto no Google Forms, o que impediu o cálculo da percentagem de respostas em função do questionário enviado, assim sendo, obteve-se um total de 143 respostas correspondendo à amostra final para o estudo. Como foi referido anteriormente, o objetivo foi de recolher e avaliar as perceções tanto de utilizadores comuns, com um total de 128 respostas, quanto de profissionais na área de cibersegurança, com um total de 15 respostas, totalizando as 143 respostas do estudo.

3.2.1. Inquérito por Questionário

Este questionário foi constituído por perguntas fechadas, ou seja, perguntas de escolha múltipla e de escala de Likert para medir a opinião e atitude dos participantes, e também uma pergunta aberta no final do inquérito. As questões foram divididas em quatro grupos principais:

- Perfil do Participante;
- Perceção e Experiência com cibersegurança;
- Tecnologia e tendências Emergentes (composto por duas partes);
- Medidas de segurança e Regulamentação

Com as informações adquiridas, foi permitido compreender as perceções atuais da sociedade e dos profissionais sobre os desafios e riscos, e também das soluções emergentes no campo da cibersegurança.

3.3. Métodos de Análise de Dados

Após a recolha dos dados, eles foram organizados e analisados com o auxílio de ferramentas como Google Forms, Google Sheets e Microsoft Excel. As respostas quantitativas foram tratadas usando estatísticas descritivas, incluindo cálculos de frequências absolutas e percentuais, e apresentadas por diversos tipos de gráficos. O objetivo foi identificar padrões de comportamento, níveis de conhecimento e perceções dos participantes sobre cibersegurança. Por outro lado, as respostas qualitativas, especialmente a questão aberta ao final do questionário, passaram por uma análise temática. Essas respostas foram classificadas em categorias como formação e conscientização, boas práticas, capacitação de idosos, uso de tecnologias específicas e fortalecimento da literacia digital. Essa abordagem ajudou a complementar os dados numéricos, oferecendo uma visão mais detalhada e subjetiva sobre as preocupações e sugestões dos participantes. Combinar os dados quantitativos e qualitativos contribuiu para uma compreensão mais completa do tema, fortalecendo as interpretações à luz da revisão da literatura.

Capítulo 4 Análise e Discussão de Resultados

Neste capítulo serão apresentados os resultados obtidos no âmbito da dissertação, organizados de forma a responder aos objetivos definidos anteriormente. Primeiramente, serão apresentados os dados recolhidos, e depois recorrendo às representações gráficas para facilitar a análise. Em seguida, procede-se à discussão dos resultados, relacionando-os com os aspetos teóricos apresentados nos capítulos anteriores e destacando as principais implicações para o estudo.

4.1. Análise de Dados e Discussão dos Resultados

A amostra deste estudo apresenta 143 respostas completas do inquérito, que se dividem em 128 respostas de utilizadores comuns da internet e 15 de profissionais na área. O inquérito foi estruturado em 5 secções principais, que correspondem a: (i) Perfil de participante; (ii) Perceção e experiência com cibersegurança; (iii) Tecnologia e Tendências emergentes (para utilizadores e estudantes); (iv) Tecnologia e tendências emergentes (para empresas e profissionais de TI); e por fim, (v) Medidas de segurança e regulamentação.

Os dados coletados foram tratados pela plataforma Google Forms, ferramenta onde foi disponibilizado o inquérito online, e este inquérito pode ser visualizado no anexo A. De seguida, esses dados foram analisados como forma de identificar padrões de perceção, conhecimento, práticas de segurança e os principais desafios enfrentados por indivíduos e organizações nos domínios da cibersegurança.

4.1.1. Perfil dos Participantes

Na figura 6 abaixo, pode-se comprovar que a amostra é de um total de 143 pessoas, com idades que variam desde menores de 18 anos, até pessoas com mais de 50 anos. É composto maioritariamente por participantes com idade compreendida entre os 18 e 25 anos. Com base nos dados recolhidos, isto demonstra que a amostra é constituída predominantemente por jovens adultos, que demonstram interesse em tecnologia, o que pode influenciar na sua visão em relação aos riscos na cibersegurança.

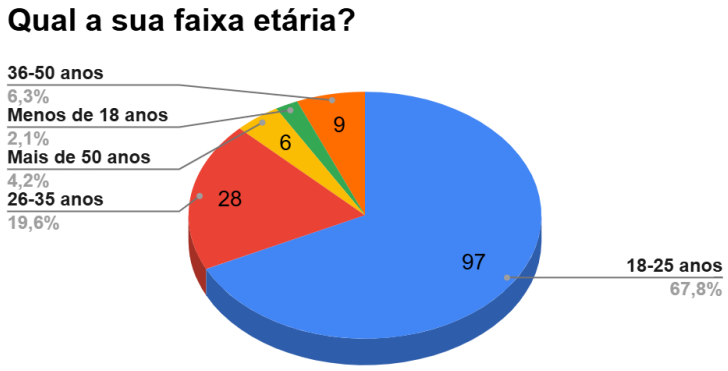

Figura 6: Faixa etária.

Na figura 7, podemos observar que dos participantes, 74 são do gênero feminino e 66 do gênero masculino, sendo que 3 participantes preferiram não expor o seu gênero.

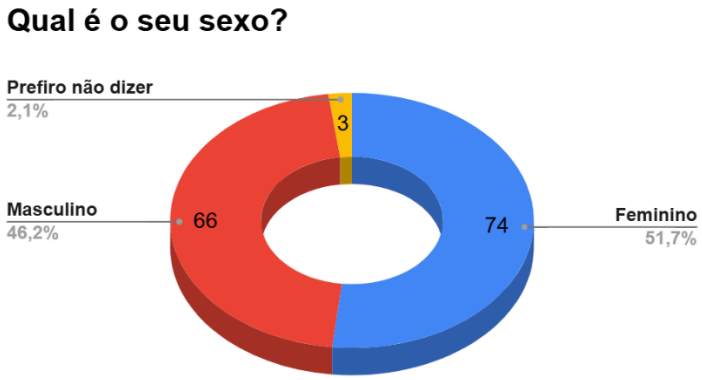

Figura 7: Identificação do sexo.

Relativamente ao parâmetro do nível de escolaridade, a figura 8 mostra-nos que, a grande maioria respondeu como sendo a Licenciatura (com um total de 72 resposta), seguido de Ensino Secundário (com 41 respostas), e por fim Mestrado (23 respostas). Com esta questão, podemos observar que ter ou não um nível de habilitação elevado, não garante que as pessoas tenham um maior conhecimento sobre segurança informática, uma vez que não necessariamente as formações são ligadas a área de segurança de informação. Posteriormente, será comprovado sobre o mesmo com os dados adquiridos.

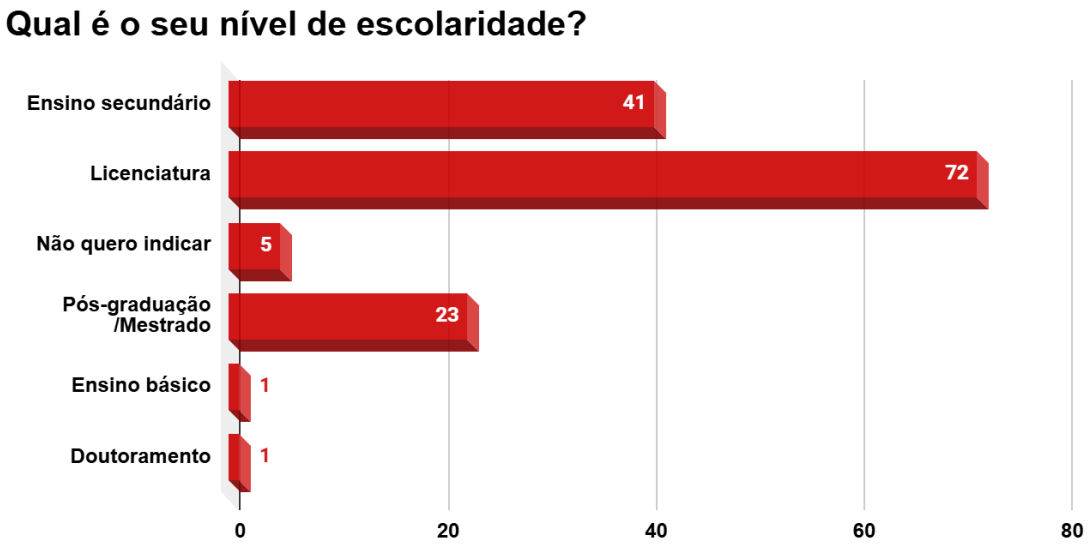

Figura 8: Identificação do nível de escolaridade.

Pelo gráfico da figura 9, percebe-se que neste estudo, o maior grupo é representado por estudantes (108 respostas), seguido de profissionais de TI (16 respostas) e de utilizadores de internet (14 respostas), diferente das outras categorias que apresentam escassas respostas. Deste modo, as perceções que obteremos serão a maior parte do ponto de vista dos estudantes.

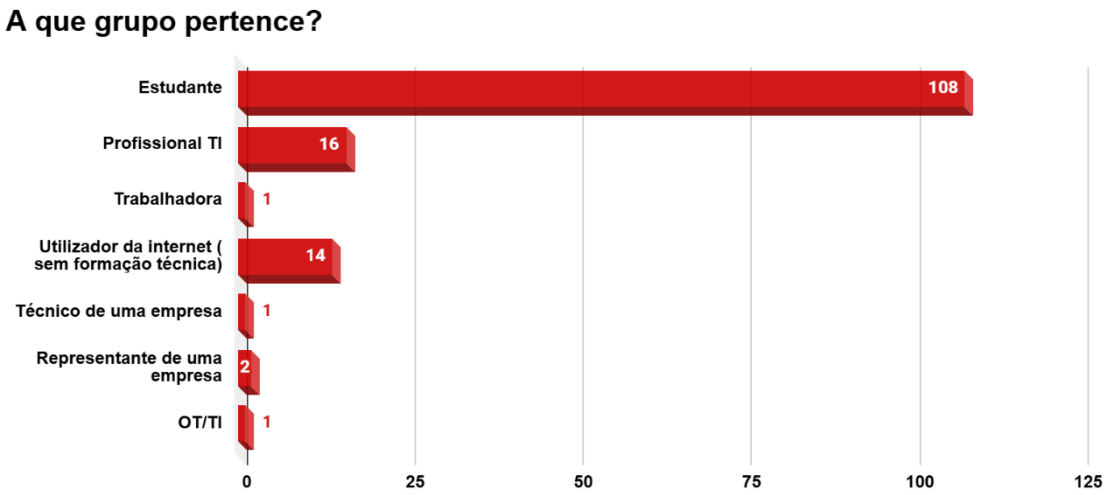

Figura 9:Perfil dos participantes.

A figura 10 abaixo explora o nível de conhecimento dos participantes no que diz respeito à cibersegurança, e verificou-se que a maioria absoluta (76 pessoas) afirmou ter conhecimentos básicos sobre a cibersegurança. De seguida, 31 pessoas afirmam ter um conhecimento intermédio e 10 afirmam ter conhecimento avançado. Por outro lado, 26 pessoas afirmaram não possuir nenhum conhecimento sobre cibersegurança. Esses dados demonstram que, embora haja um número significativo de pessoas que possuem competência em cibersegurança, ainda existe uma minoria em que nota-se um baixo nível de conhecimento nesta área. Embora 76 pessoas afirmaram ter conhecimento básico, não quer dizer que possuem um baixo nível de escolaridade, assim como afirmar ter conhecimento avançado não significa possuir um alto nível de escolaridade. Esta questão será esclarecida na figura 11.

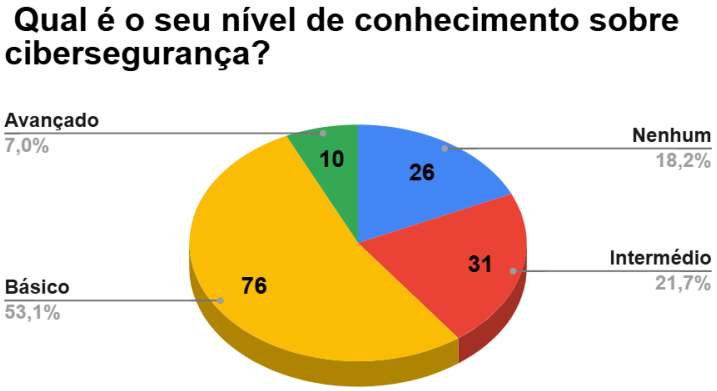

Figura 10: Nível de conhecimento sobre cibersegurança.

Na figura 11 abaixo, no nível básico, cerca de 50% das pessoas que afirmam ter algum conhecimento possuem uma licenciatura (41 respostas), seguidas pela escolaridade do ensino secundário (22 respostas). No nível intermédio, os números estão mais equilibrados, com destaque para quem tem licenciatura (12 respostas) e ensino secundário (11 respostas). Já no nível avançado, há uma menor quantidade de respostas, mas ainda assim aparece a licenciatura (3 respostas), pós-graduação ou mestrado (4 respostas) e até doutorado (1 resposta). Por fim, no nenhum, a maior concentração também está entre os participantes com licenciatura (16 respostas), o que mostra que ter um grau acadêmico mais alto não garante necessariamente mais conhecimento em cibersegurança.

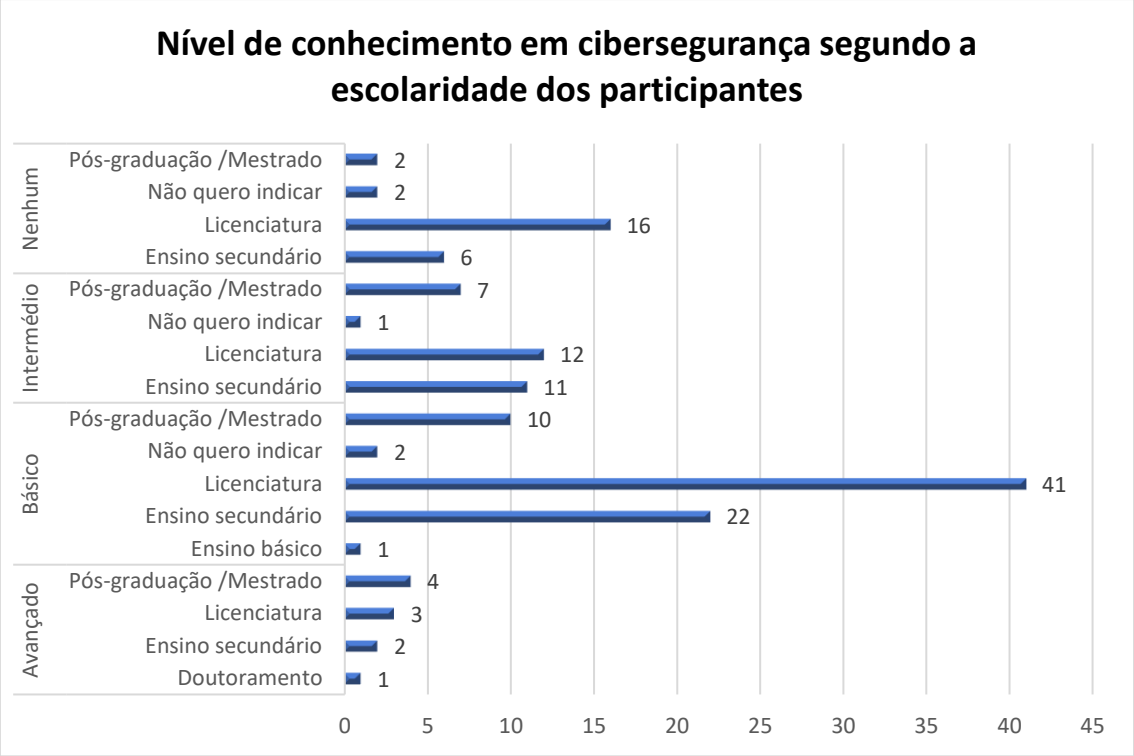

Figura 11: Nível de conhecimento em cibersegurança segundo a escolaridade dos participantes.

Na figura 12, nota-se que ao questionar sobre o uso de software antivírus ou firewall, a maior parte (77 pessoas) disseram que usam, mas apenas no computador. De seguida temos 43 pessoas que dizem usar em todos os dispositivos e 21 pessoas que não usam nenhum mecanismo de proteção. Estes dados mostram que, embora muitas pessoas se preocupem com a segurança digital, ainda há uma tendência a subestimar os riscos ligados aos dispositivos móveis, que fazem parte do nosso dia a dia na internet. Não ter uma proteção completa deixa os utilizadores vulneráveis a diversos perigos, o que torna essencial investir em educação digital e incentivar boas práticas de segurança, como as recomendadas pela ENISA [48]. Além disso, uma parte significativa das pessoas não

utiliza nenhuma ferramenta de proteção, o que reforça a necessidade de promover iniciativas educativas acessíveis que permitem conscientizar sobre a importância de agir de forma antecipada na proteção online.

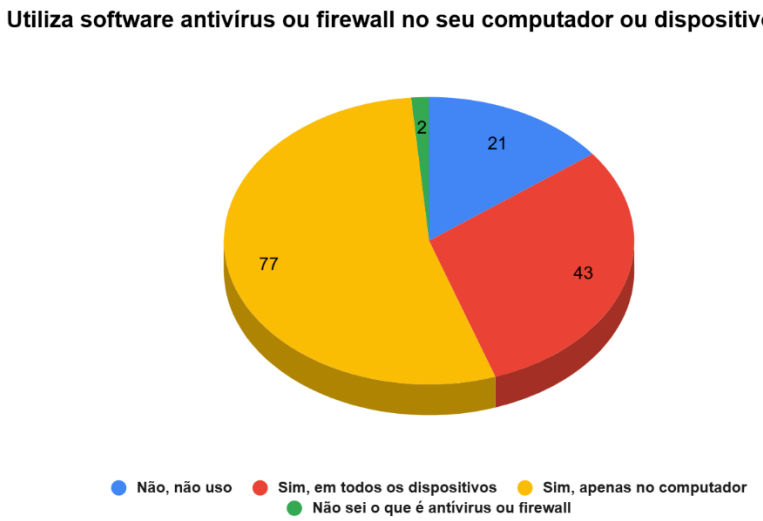

Figura 12: Uso de antivírus ou firewall.

Analisando a amostra, na figura 13, pode-se constatar que das duas pessoas que dizem não saber o que é antivírus, não possuem qualquer conhecimento sobre segurança de informação e possuem habilitação em licenciatura, e isto confirma que, mesmo tendo uma qualificação de nível superior, sem foco nesta área, não garante total conhecimento em cibersegurança e consequentemente não asseguram competências para combater as ameaças.

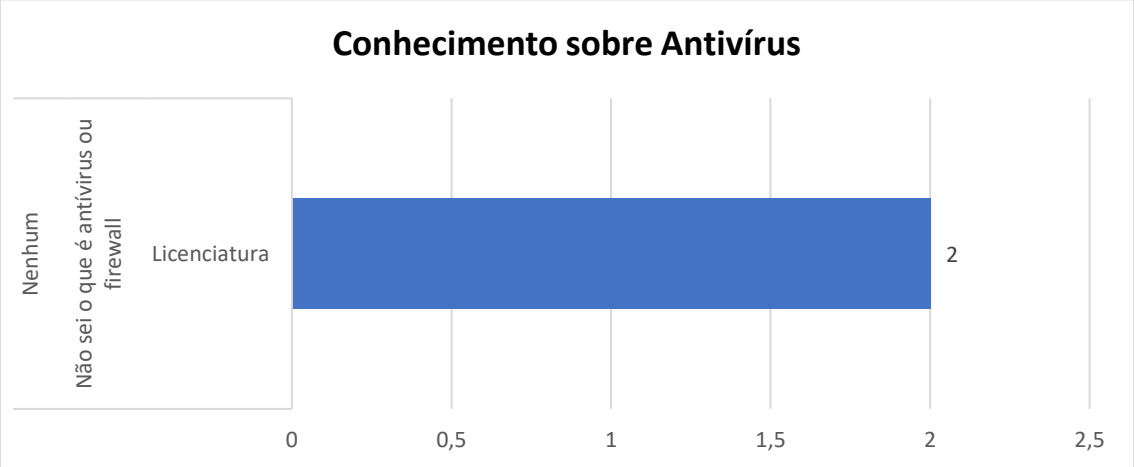

Figura 13: Conhecimento sobre antivírus.

4.1.2. Perceções e Experiência com Cibersegurança

Esta parte possui o objetivo de avaliar a perceção geral das pessoas sobre segurança digital, ameaças e boas práticas.

Quando foi perguntado aos participantes se já sofreram algum tipo de ataque, representado na figura 14, a maioria dos participantes, 44,8% afirmou que não sofreu nenhum tipo de ataque, em contrapartida, 37,1% diz já ter sofrido algum tipo de ataque e 18,2% diz não saber se já sofreu ou não um ataque cibernético. Isto demonstra que possivelmente a grande maioria possui um bom conhecimento sobre os ataques e sobre as consequências que podem surgir caso não se preparem adequadamente para a sua proteção. Ao mesmo tempo, nota-se uma falta de conhecimento no grupo que não sabe se já foi vítima de algum tipo de ataque, o que reforça a importância da implementação da educação digital nesta área como forma de passar o conhecimento e manter as pessoas mais preparadas.

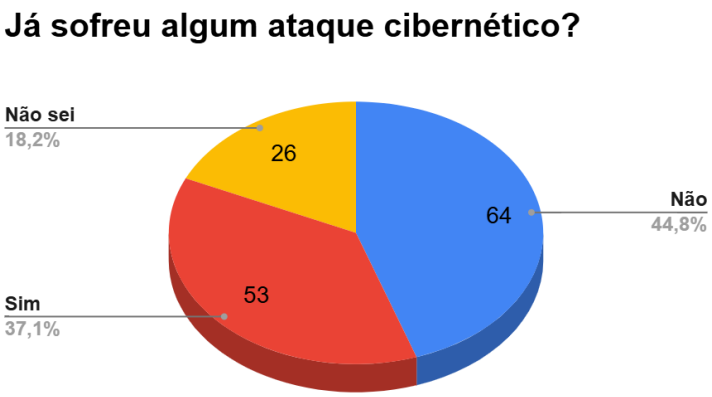

Figura 14: Ocorrência de ataques cibernéticos.

Na figura 15, tentou-se perceber melhor quais são os outros tipos de ataques que os participantes possam ter experienciado, então, foi deixado no questionário uma opção em aberto, no qual podiam dizer quais foram os ataques que já sofreram, e assim houve algumas respostas como: code injection, Denial of service, engenharia social, roubo de cartão de débito, cartão bancário pirateado, DDos e emails falsos que se enquadram na categoria de ataque phishing. Fazendo uma análise geral, o ataque mais comum é o phishing, seguido de roubo de credenciais. Assim podemos reforçar que estes resultados se encontram em conformidade com estudos anteriores, como foi referido pelo autor D.

Jerbi [3], que apontam o phishing como sendo uma ameaça dominante e cada vez mais comum.

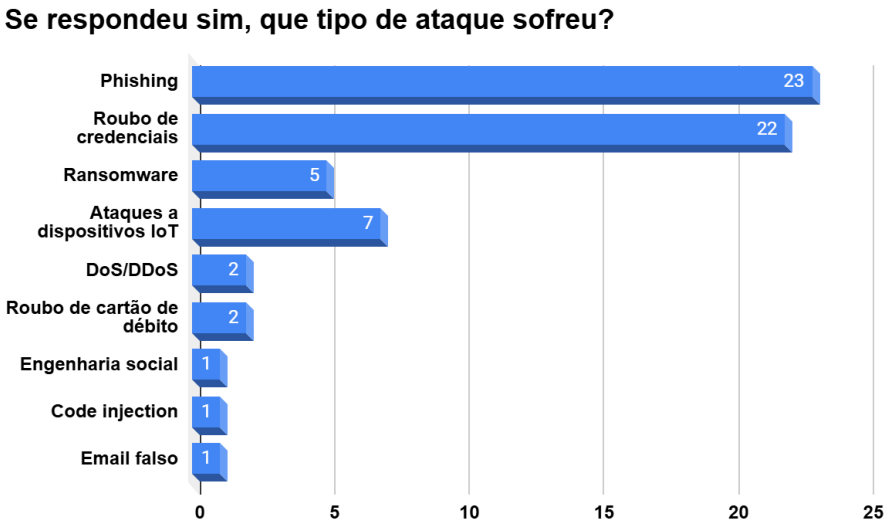

Figura 15: Tipos de ataques sofrido.

Na figura 16, encontra-se a opinião dos participantes relativamente ao quão seguros e confortáveis se sentem navegando na internet. Do mesmo modo que 46 dos participantes se sentem um pouco seguros, outros 46 se sentem neutros em relação à sua segurança online. De seguida, 28 pessoas afirmaram sentirem segurança ao navegar na internet, e apenas 6 relataram sentir-se muito seguros. Todavia, 17 participantes demonstraram muita insegurança. Estes resultados demonstram uma situação de incerteza no geral, ou de uma limitação de confiança por parte dos participantes. Embora não se sintam completamente expostos ao perigo, também não sentem um conforto em relação à proteção digital. Isto pode-se dar pelo facto de experiências de ameaças como phishing e outros vivida pelos mesmos, ou também devido a exposição a nóticias sobre ataques cibernéticos.

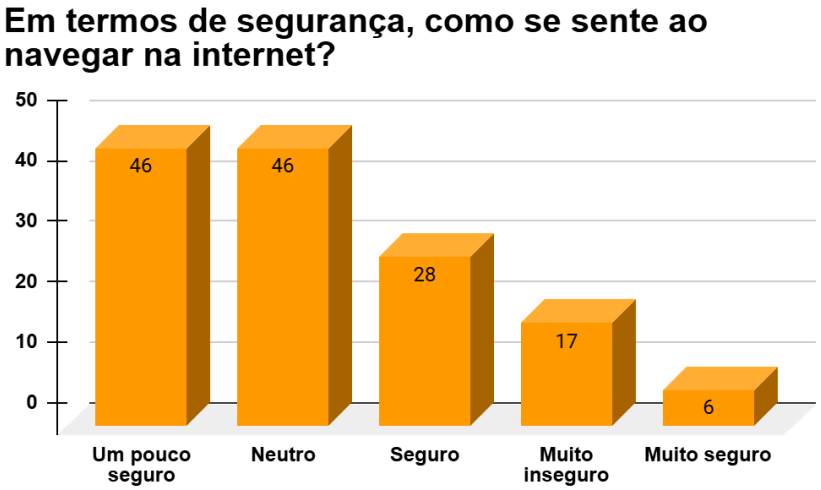

Figura 16: Percepção de segurança ao navegar na internet.

Na figura 17, foi analisado como forma de perceber quais dispositivos os participantes acham mais propensos a sofrerem ataques, e a grande maioria (55 participantes) acredita que os smartphones são mais prováveis de sofrerem ataques, seguida dos computadores (51 participantes). Enquanto isso, 18 pessoas disseram que os dispositivos de infraestrutura empresarial são os mais vulneráveis e 19 pessoas disseram ser os dispositivos IoT. Isto demonstra que os smartphones e os computadores são os alvos favoritos dos cibercriminosos, pelo facto de serem os mais utilizados para fins pessoais e profissionais, armazenamento de dados sensíveis e conexão em redes públicas e privadas. Dispositivos de IoT e infraestruturas empresariais receberam uma menor indicação, provavelmente porque há uma sensação de maior proteção. No entanto, estudos recentes indicam que tanto IoT quanto redes corporativas estão tornando-se alvos cada vez mais frequentes, o que reforça a importância de estabelecer políticas de segurança sólidas para todos os dispositivos.

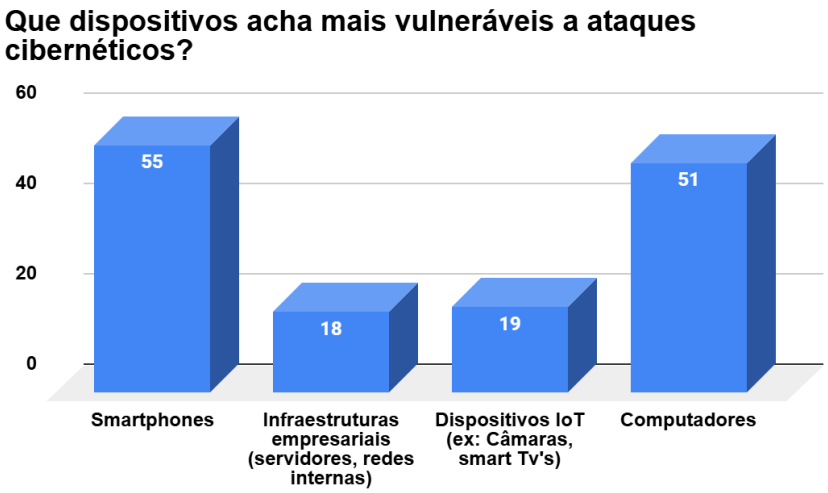

Figura 17: Dispositivos vulneráveis a ataques cibernéticos.

Colocou-se a questão aos participantes, de quais eram as ameaças que consideravam como mais preocupantes atualmente, podendo escolher mais respostas, como pode ser observado na figura 18. A maioria, 48, respondeu que não sabia qual era a ameaça mais preocupante, isto revela o défice de conhecimento destes participantes, o que torna importante a educação digital neste contexto. No segundo caso, 41 pessoas responderam phishing como a ameaça mais preocupante, o que entra em concordância com o relatório da CNCS [37], que a destacou como sendo uma ameaça muito relevante.

Outros 22 participantes destacaram os ataques a dispositivos de Internet das Coisas (IoT), enquanto 15 enfatizaram o ransomware e 14 mencionaram ataques de negação de serviço (DDoS). Além disso, três respostas indicaram preocupações adicionais, como a falta de conhecimento, o próprio usuário e a quebra no controle de acesso, o que aponta para a vulnerabilidade humana.

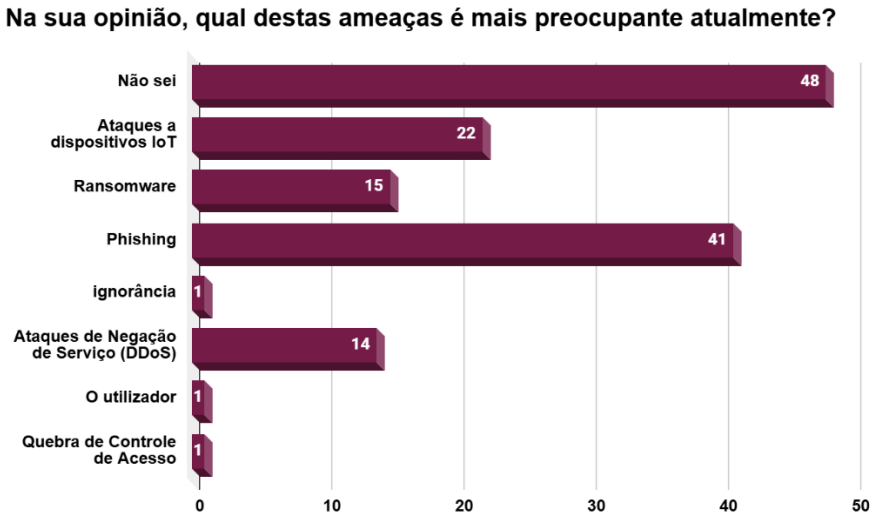

Figura 18: Ameaças cibernéticas mais preocupantes.

A questão 12 identificada na figura 19 procura avaliar como as pessoas se encontram preparadas, caso tenham de experienciar um ciberataque. A maioria (74 pessoas) diz estar pouco preparada e o segundo maior grupo (55) diz estar muito despreparada. Isto demonstra uma preocupação enorme, uma vez que com uma preparação relativamente boa ou uma boa preparação como os outros afirmam (10 e 4 pessoas), podem se proteger sem preocupações caso sofram algum tipo de ciberataque.

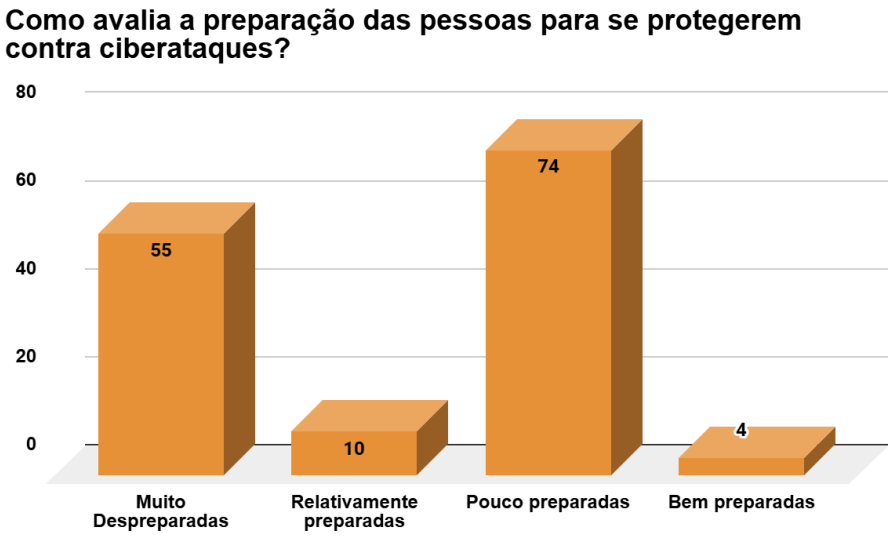

Figura 19: Avaliação de preparação contra ciberataque.

A questão abaixo, representada na figura 20, buscou entender como as empresas se encontram preparadas caso sofram um ciberataque, e para a amostra em questão, 65 pessoas não trabalham numa empresa, então não são consideradas como alvo para esta

questão. Podemos afirmar que 35 pessoas dizem que as suas empresas se encontram bem preparadas e 13 afirmam estar extremamente preparadas. Isto mostra que as empresas se preocupam na defesa dos seus dados e dos seus clientes. Em contrapartida, 23 afirmam que a empresa se encontra pouco preparada e 7 dizem que está muito mal preparada. Apesar de ser a minoria, de qualquer forma isto mostra o quão perigoso pode ser. Com um grande número de tecnologias surgindo e os riscos que surgem com elas, as organizações e empresas devem investir em prol da proteção contra ameaças como forma de certificar a eficácia organizacional [35].

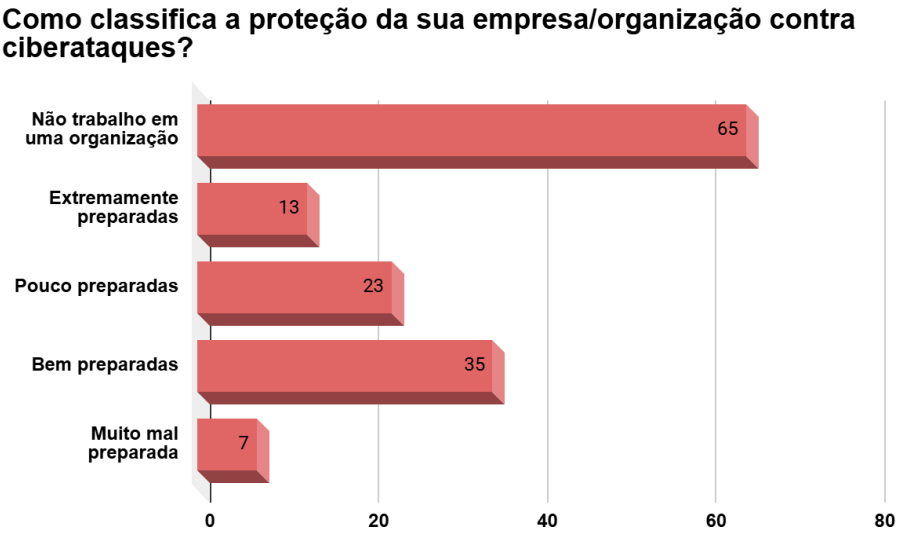

Figura 20: Avaliação de proteção de empresas/organizações contra ciberataques.

A próxima questão busca entender com que frequência as pessoas atualizam as suas palavras-passe. Na figura 21, podemos observar que 88 pessoas afirmam que só alteram a senha quando são solicitadas, 13 declaram que atualizam de 1 em 1 ano, 12 dizem que atualizam de 6 em 6 meses, 19 atualizam a cada 3 meses e 11 afirmam que nunca mudam a sua senha. Como foi reforçado na revisão bibliográfica, a falta de alteração das palavras-passe ou o uso de senhas muito fracas faz com que os dispositivos se tornem vulneráveis, o que faz com que os ataques comprometam a integridade dos dados [28, 29].

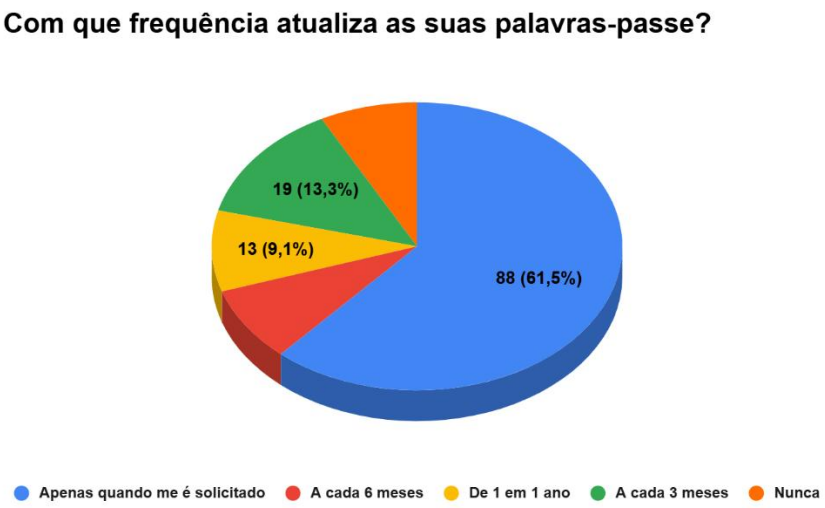

Figura 21: Frequência de atualização de palavras-passe.

A figura 22, retrata o impacto que os participantes demonstram ter caso sofressem um ataque cibernético, e os resultados mostram uma grande preocupação das 88 pessoas que afirmam a perda de dados pessoais e financeiros como um grande impacto na sua vida e assim, esta noção esta em conformidade com os perigos mais comuns a ataques como phishing, malware e ransomware. Em seguida, 21 pessoas dizem ser perda de acesso a serviços essenciais, o que retrata o aumento da dependência digital. De seguida, 17 pessoas dizem ser roubo de identidade, que é também relevante uma vez que o roubo de identidade está associado à usurpação de perfil, fraude online e outros. Posteriormente, 10 pessoas dizem ser danos à reputação pessoal/profissional, o que, apesar de ser pouco frequente, pode trazer danos irreversíveis, principalmente em profissões de exposição pública. No final, 7 pessoas respondem como nenhum impacto relevante, o que pode revelar falha na literacia digital e subestimação dos riscos, e isso demonstra o quão importante é investir na educação digital.

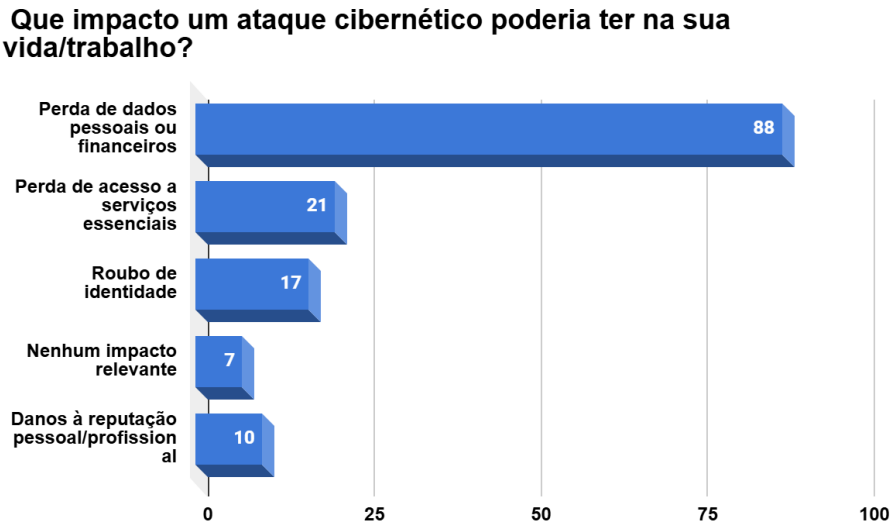

Figura 22: Impacto de um ataque cibernético (pessoal e profissional).

A questão seguinte, representada na figura 23, buscou determinar, segundo os participantes, o que pode se considerar como sendo o maior desafio na cibersegurança nos dias de hoje, e a maior parte da amostra (89 pessoas) afirmou que a falta de conhecimento por parte dos utilizadores representa um grande desafio. Isto demonstra que a falta de conhecimento dos utilizadores os torna um alvo fácil de sofrer ataques pela internet. O fator humano é um aspeto crítico e continua sendo um componente vulnerável, já que a ausência de literacia digital faz com que os utilizadores se tornem vulneráveis a ataques como phishing e outras formas de engenharia social [49]. Por isso, a importância de investir na educação e priorizar a conscientização dos utilizadores relativamente aos riscos e boas práticas de segurança digital. Por outro lado, 27 participantes afirmaram que o maior desafio é o crescimento das novas tecnologias sem proteção adequada. Se essas tecnologias como IoT, IA e outros não forem providenciadas com a proteção necessária desde a fase de planeamento, a sua superfície de ataque aumenta e a probabilidade de cibercriminosos conseguirem explorar a vulnerabilidade desses sistemas é extremamente elevada.

Houve também respostas em menor escala, que consideravam como desafio a falta de investimento nas empresas (11 respostas) e falta de profissionais na área (10 respostas). A falta de investimento adequado por parte das organizações pode causar problemas na execução de sistemas de defesas atualizados, nas auditorias e na contratação de profissionais qualificados [44]. Sem esse investimento, muitas empresas continuam vulneráveis ou usam sistemas que já estão ultrapassados. A falta de profissionais na área já é uma realidade que vemos em todo o mundo. A procura por especialistas nessa área só cresce, mas ainda há poucos profissionais disponíveis. Essa escassez de talentos dificulta às empresas responderem bem às novas ameaças [37]. Por fim, 6 pessoas afirmaram que a falta de regulamentação eficaz é a maior dificuldade. Sem regras claras, que acompanhem o ritmo acelerado da tecnologia, fica difícil montar estratégias de proteção bem coordenadas e com responsabilidades bem definidas, especialmente quando as ameaças atravessam fronteiras e acontecem em contextos internacionais.

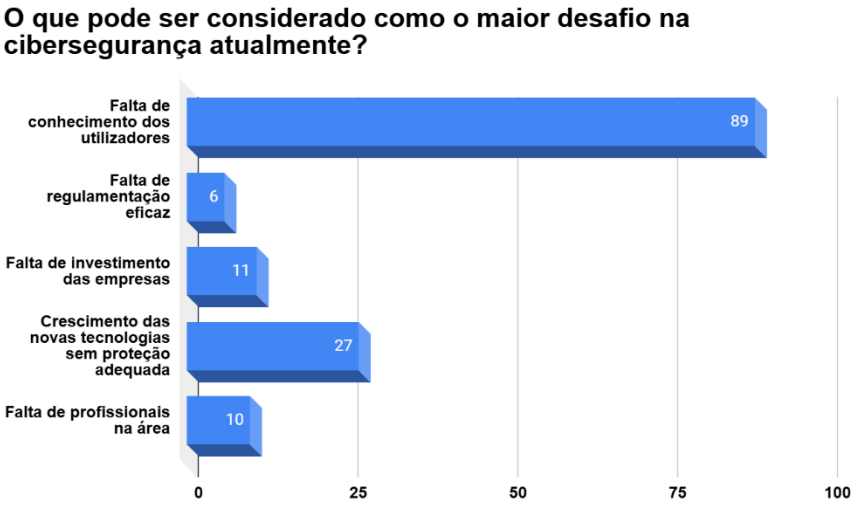

Figura 23: Maior desafio atual na cibersegurança.

A figura 24, mostra-nos a diferença de conhecimento entre pessoa que trabalham na área da cibersegurança e as que não trabalham, onde dos 143 participantes, 128 (85,5%) não trabalham diretamente com a segurança de informação e apenas 15 (10.5%) trabalham. No entanto, na figura 9 que pedia a indicação de qual grupo os participantes pertenciam, 16 pessoas afirmaram pertencer ao grupo de profissionais de TI, o que diverge da informação atual. Esta diferença pode ser devido a diferentes interpretações das questões ou possíveis variações na amostra. Ainda assim, este pequeno desvio não afeta os resultados geral da análise de forma significativa.

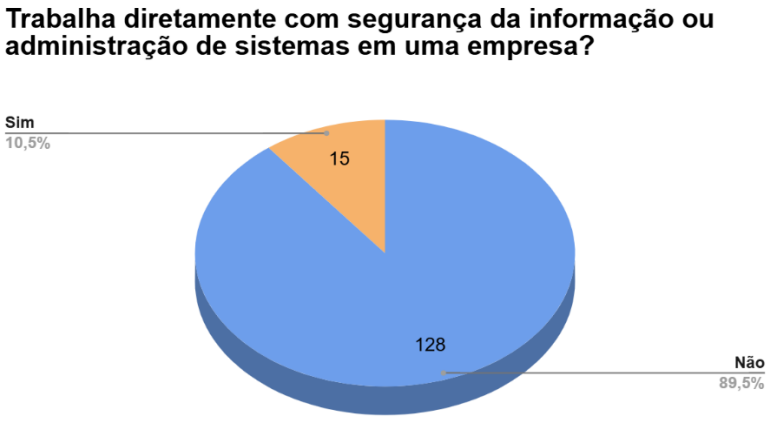

Figura 24: Atuação em segurança da informação ou administração de sistemas.

4.1.3. Tecnologia e Tendências Emergentes

Esta secção será dividida em duas partes, uma para utilizadores da internet e estudantes e outra para empresas e profissionais de TI. Esta divisão tem como objetivo explorar a área de conhecimento de cada parte tanto em conteúdos mais complexos quanto nos mais simples.

4.1.3.1. Parte 1 – Para utilizadores da internet e estudantes

Nesta primeira parte, dedicada a um grupo de participantes (128), os participantes foram analisados com base no conhecimento que possuem sobre a cibersegurança.

A pergunta 18 da figura 25 buscou perceber até que ponto os participantes conhecem ou já ouviram falar sobre a utilização da IA no contexto da cibersegurança e a grande maioria (77 pessoas) afirmou possuir um conhecimento básico, o que demonstra uma perceção inicial, porém ainda limitada, sobre a implementação prática da IA neste campo. Contudo, 42 pessoas afirmaram não ter nenhum conhecimento sobre esta relação entre IA e cibersegurança, salientando a falta de conhecimento de forma significativa. Por fim, apenas 9 pessoas alegaram ter um bom conhecimento, indicando familiaridade mais profunda e técnica ou profissional com o tema. Estes resultados demonstraram que, mesmo que a noção da IA esteja presente no discurso tecnológico, o seu uso prático no âmbito da cibersegurança não é totalmente compreendido pela maioria dos utilizadores.

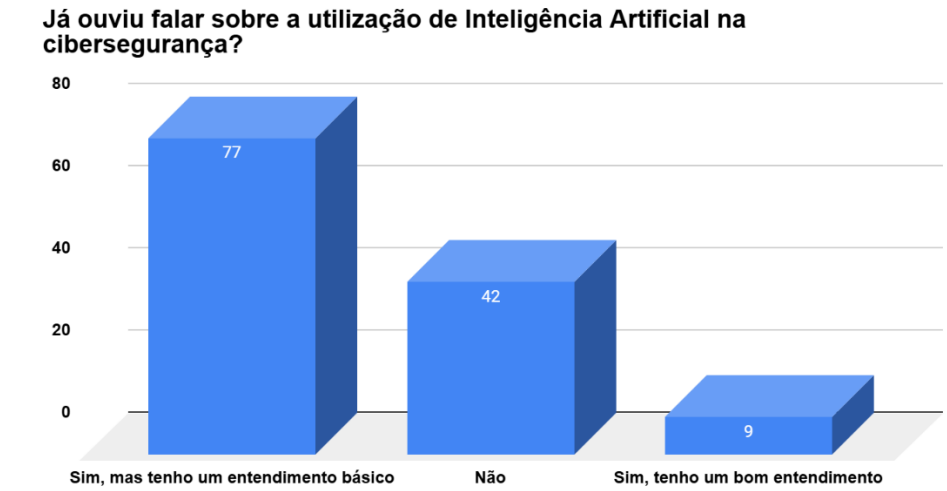

Figura 25: Familiaridade com a IA na cibersegurança.

A questão 19, representada na figura 26, visava compreender com que tendência a IA seria usada, para defesas ou ataques. Segundo os participantes, 33 acreditam que a IA será mais usada para efetuar ataques e apenas 16 acreditam que será usada para contribuir com a defesa. Por outro lado, 56 acreditam que a IA será usada tanto para efetuar ataques como defesas e 23 dizem não saber. A verdade é que com o rápido desenvolvimento das tendências emergentes, a IA tem se tornado muito eficaz no combate às ameaças e no fortalecimento da segurança digital, mas em contrapartida os cibercriminosos também aproveitam da IA para o seu próprio benefício, explorando-a para fins maliciosos. Portanto, é importante e crucial que as organizações possam implementar medidas de controlo rigorosas de forma a assegurar que a IA se torna uma aliada e não uma ameaça [50].

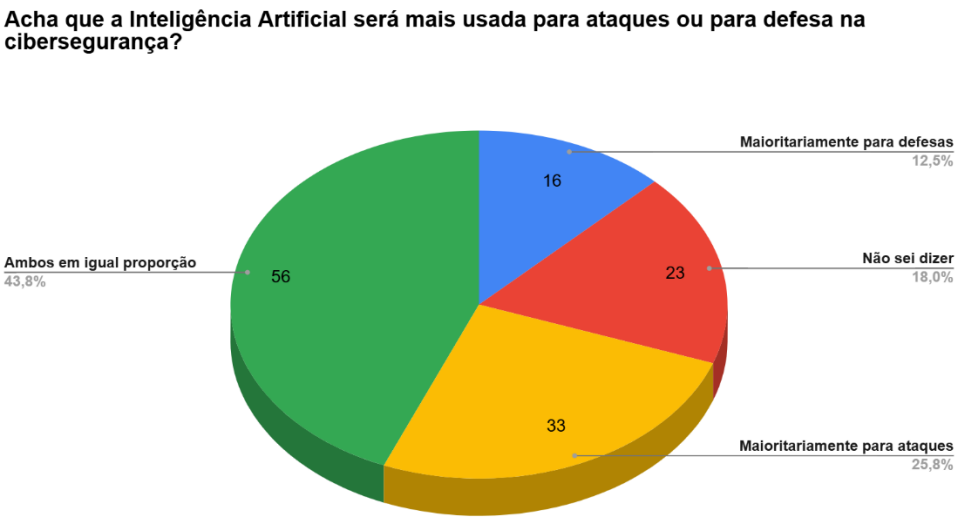

Figura 26: Percepção sobre o uso da IA: ataques vs. defesa na cibersegurança.

Relativamente à questão 20 representada na figura 27 do inquérito, empenhou-se em entender o nível de compreensão dos participantes em relação a esta tendência emergente "Blockchain". A maioria, 56 pessoas, afirmou não saber se essa tecnologia pode ser considerada como uma solução eficaz para a segurança digital, demonstrando uma falta de conhecimento técnico sobre o assunto e baixa compreensão pelo público em geral. Por outro lado, 45 participantes afirmaram que não acham que esta tendência é uma solução eficaz para a segurança digital, enquanto apenas 25 pessoas acreditam que a blockchain pode ser uma possível resposta no reforço da segurança.

Não obstante essa visão, os estudos mostram que a Blockchain dispõe de características com grande potencial para aperfeiçoar a segurança cibernética. Medidas de segurança como estrutura descentralizada, transparente e imutável ajudam na redução de riscos de manipulação de dados e reforçam a confiança em transações digitais [51]. Estas tecnologias carregam inúmeras vantagens como criptografia forte, prevenção de ataques DDos, eficiência de custos e outros, e também contribuem para a proteção de dados, permitindo que apenas haja a visualização e participação de redes confiáveis nas transações. A blockchain também se torna promissora na proteção contra ciberataques, nomeadamente em setores como áreas de direito de propriedade e saúde [52].

Esses dados mostram que, mesmo que o conhecimento sobre Blockchain ainda não seja algo que a maioria das pessoas conhece bem, há um consenso na literatura de que essa

tecnologia tem um papel importante na criação de sistemas digitais mais seguros e confiáveis.

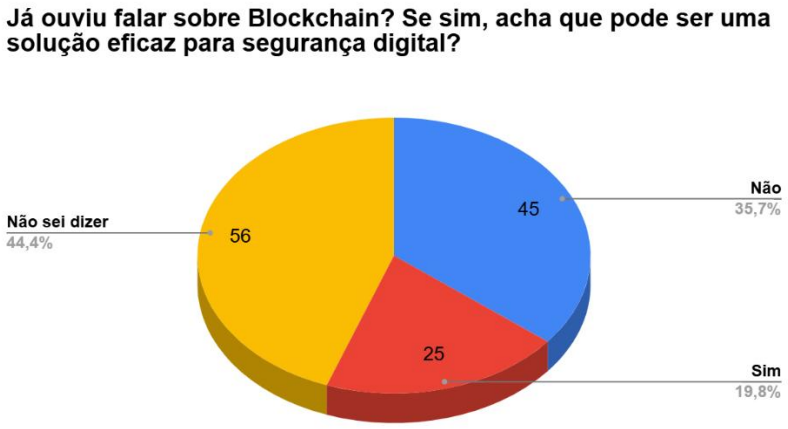

Figura 27: Avaliação da eficácia do Blockchain na segurança digital.

A ilustração da figura 28 abaixo resume as escolhas dos participantes relativamente a como avaliam o impacto da IoT na cibersegurança. Dos participantes, 21 pessoas afirmaram que o impacto da IoT traz mais riscos do que benefícios e 15 disseram que traz mais benefícios do que riscos.

Por outro lado, a maioria, 62 participantes, afirmaram que dependendo da implementação, pode ter um impacto positivo ou negativo, e de facto, a literatura reforça que a grande escala crescente de dispositivos abre margem para ataques cibernéticos e a escassez de segurança em diversos dispositivos IoT, contribui com vulnerabilidade a invasões [31], mas também cria oportunidades para a melhoria da eficiência e a segurança em vários setores, como foi referido na literatura [34].

Outros 30 disseram não saber como avaliar este impacto, o que demonstra falta de conhecimento sobre o assunto em específico e mostra o quão importante seria investir na educação da cibersegurança.

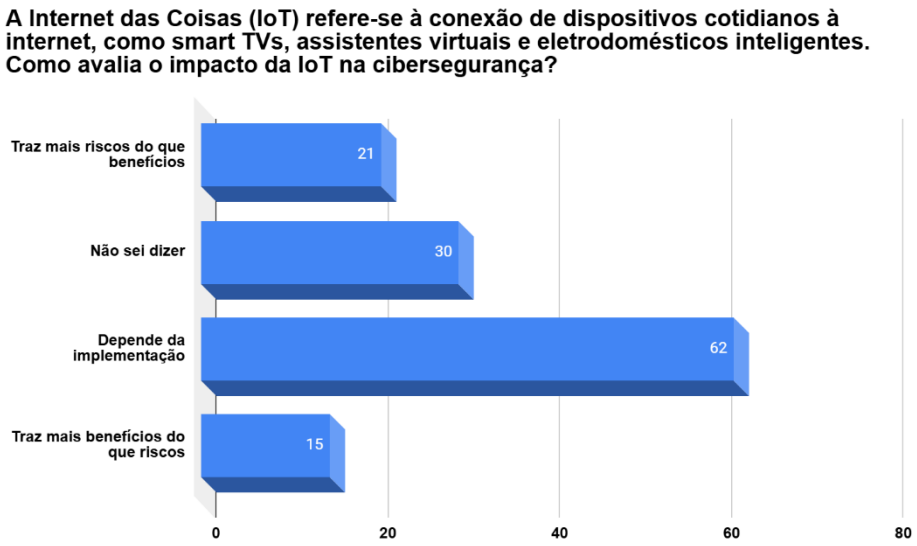

Figura 28: Avaliação do impacto da IoT na cibersegurança.

Na figura 29, é questionado aos participantes se os mesmos usam serviços de armazenamento em nuvem para o armazenamento de informações. O resultado que se obteve foi que 50 participantes afirmaram usar regularmente, 46 afirmaram usar ocasionalmente. O armazenamento em nuvem funciona como um data center virtual e possui muitos benefícios, desde a grande capacidade de armazenamento e custos baixos, e a possibilidade de poder aceder os nossos dados a partir de qualquer lugar e a qualquer momento, e isto mostra que esta tecnologia possui várias vantagens, o que explica o porquê de muitos participantes fazerem o seu uso [53].

Por outro lado, 24 pessoas afirmaram não usar o armazenamento em nuvem, e isto provavelmente deve-se ao facto de que esta tecnologia também possui desvantagens que impulsionam ao não uso deste serviço. Desvantagens como, a necessidade de estar conectado a internet uma vez que, sem ela o acesso a esses dados torna-se impossível, dificuldade na migração uma vez que depois de usar um provedor de armazenamento específico, a migração de dados para outro provedor torna-se muito difícil e também o que se pode considerar como um grande fator, é a problemática da segurança e da privacidade, já que isso implica fornecer o controle de informações privadas a uma empresa terceirizada e caso a empresa tenha más intenções ou devido alguma falha pode acontecer o vazamento de dados, oque pode causar prejuízos [53]. Por fim, apenas 8 pessoas afirmaram não saber se usam ou não, isto pode acontecer por falta de conhecimento sobre o assunto.

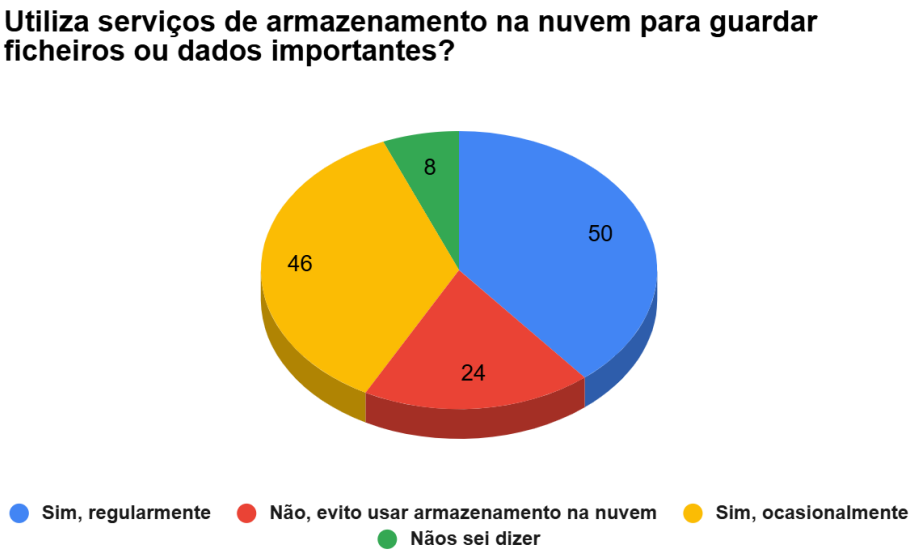

Figura 29: Uso de serviços de armazenamento na nuvem.

Nos resultados da figura 30, onde busca entender o nível de confiança das pessoas nos serviços de armazenamento, a grande parte dos participantes (71) responderam que confiam na segurança dos serviços, mas com alguma precaução, de seguida, houve 28 pessoas que afirmaram que não confiam muito e apenas 4 disseram que não confiam nada na segurança, o que mostra muita desconfiança e medo relativamente proteção dos dados e a privacidade. Esses resultados podem indicar que apesar de manterem a sua confiança nesses serviços, estão conscientes de que existem riscos associados a estas plataformas, e existem desvantagens que podem trazer prejuízos para pessoas [53].

De seguida, 25 participantes afirmaram que confiam totalmente nesses serviços, revelando um número pequeno de pessoas mais confiantes na credibilidade dessas plataformas.

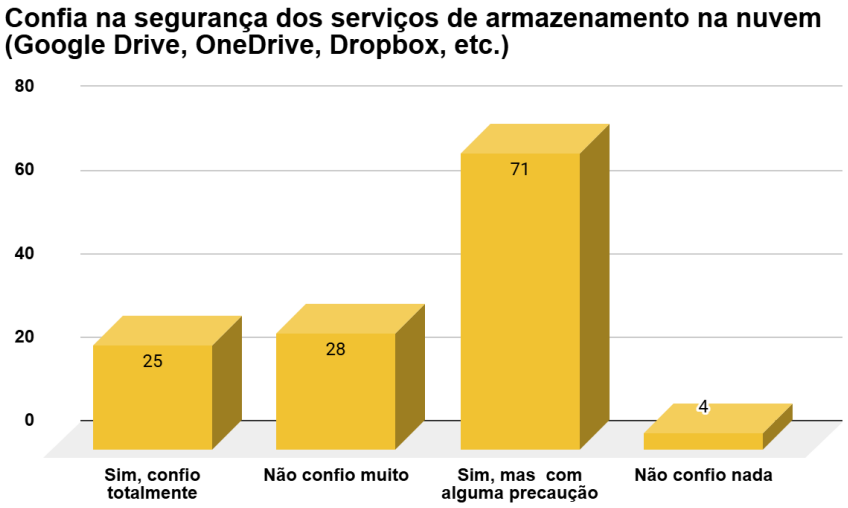

Figura 30: Nível de confiança nos serviços de armazenamento na nuvem.

Para melhor entender as medidas consideradas mais eficazes na proteção de dados armazenados na nuvem, temos a figura 31 abaixo, com o objetivo de fazer esta análise, em que os participantes podiam escolher até duas opções. A grande maioria, 69 participantes, afirmaram que a encriptação de dados antes de fazer o armazenamento de dados é a melhor medida, diminui os riscos de os dados serem expostos em uma violação, pois, a encriptação de dados permite que as informações sejam consultadas apenas por aqueles que possuem a chave correta de criptografia, que é capaz de tornar os conteúdos acessíveis e compreensíveis a quem os possuí, e isto é uma forma de garantir a privacidade e segurança dos dados [52].

Por outro lado, 61 pessoas afirmaram que evitar armazenar dados sensíveis na nuvem era a melhor opção, demonstrando ter cautela e pouca confiança no que se refere aos seus dados. A autenticação multifator (2FA), com 41 escolhas dos participantes, aparece como uma medida relevante, mas por ser pouco familiarizada com o público, é menos priorizada comparada às outras ou também pode haver uma percepção de que as outras medidas são mais eficazes. De acordo com a All Tech Magazine, a MFA acrescenta uma camada extra de segurança importante, dificultando bastante que alguém acesse as informações sem permissão, mesmo que a senha seja roubada [54].

Por fim, fornecedores com certificação de segurança foram votados por 27 participantes, provando que, por mais que seja uma medida importante, não é uma prioridade como preocupação, e isto provavelmente deve-se à dificuldade de verificar certificações ou também à confiança entre as marcas. Apesar de ainda não ser tão comum, essa abordagem

é bastante valorizada pela Financial Times, que reforça a importância de verificar cuidadosamente esses fornecedores e a confiabilidade dos auditores responsáveis pelas certificações [55].

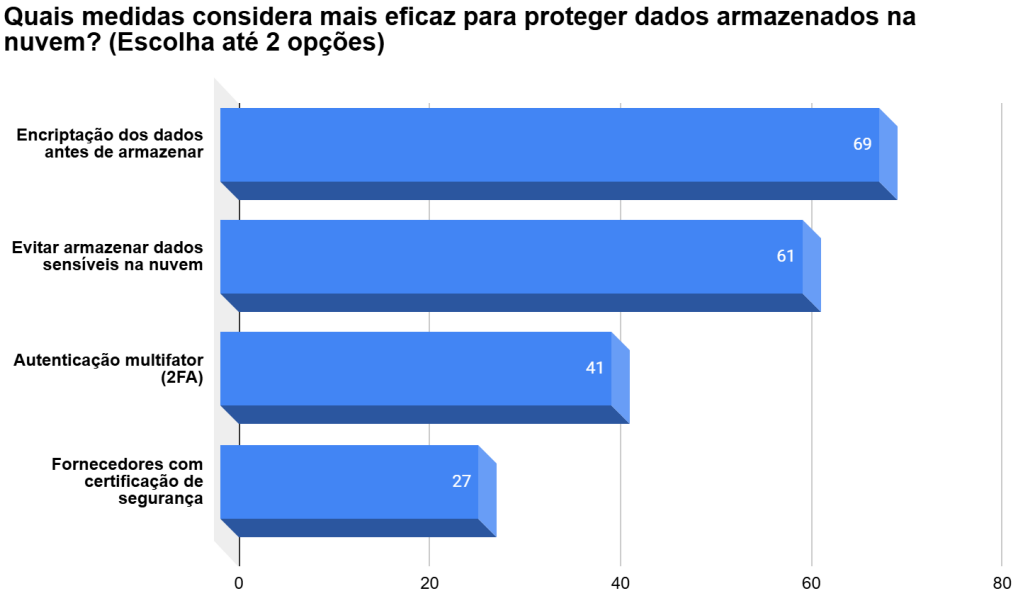

Figura 31: Medidas eficazes para proteção de dados armazenados na nuvem.

4.1.3.2. Parte 2 - Para empresas e profissionais de TI

Nesta segunda parte, o objetivo continua sendo o mesmo, mas desta vez serão analisadas as respostas de um grupo menor de participantes (15), e mais uma vez, os participantes foram analisados com base no conhecimento que possuem sobre a cibersegurança.

A análise dos dados representados na figura 32 ilustra as opiniões dos participantes, relativamente ao conhecimento da computação quântica, e dos 15 participantes, 6 demonstraram ter um bom conhecimento sobre esta tendência, 7 disseram já ter ouvido falar, mas não possuem muito conhecimento sobre ela, e apenas 2 afirmaram não ter conhecimento sobre esta tendência aplicada na cibersegurança. Isto mostra que, apesar da computação quântica ser uma inovação relativamente recente, já há um investimento no conhecimento dos profissionais e nas empresas, como pode ser observado nas respostas dos 6 participantes, e isto deve-se ao facto de esta tendência ser reconhecida pelos seus impactos potenciais tecnológicos que tendem a ser promissoras para o futuro.

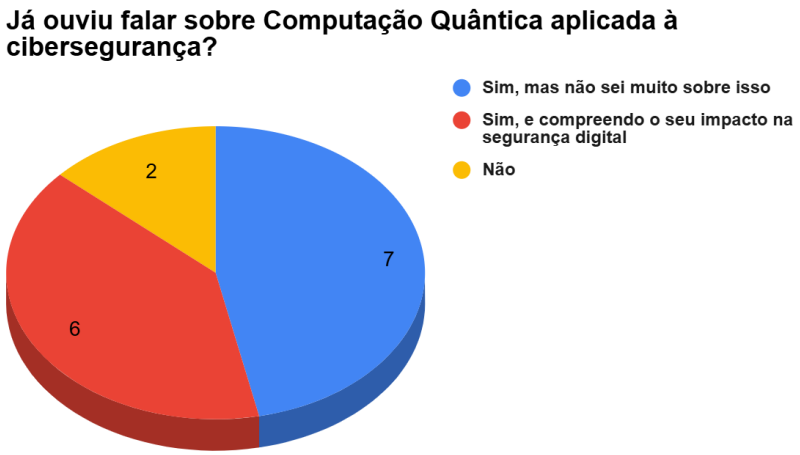

Figura 32: Conhecimento sobre Computação Quântica na cibersegurança.

A figura 33 procurou entender, segundo os participantes, o que a computação quântica representava (risco ou solução) para a cibersegurança, e verificou-se que 7 pessoas afirmaram que esta tendência representava tanto um risco, como solução na cibersegurança, 4 pessoas disseram que representava uma solução para reforço da segurança, apenas uma pessoa afirmou que a tendência representava um risco e 3 pessoas não souberam responder. Isto mostra que alguns acreditam na mudança que esta nova tendência pode proporcionar e outros tendem a ter mais cautela devido ao risco que pode surgir. De facto, a computação quântica é uma tecnologia de grande potencial no âmbito da cibersegurança, abrindo portas para novas estratégias de proteção de dados diante das ameaças futuras. Um avanço fundamental reside nas técnicas de correção de erros quânticos, essenciais para assegurar a estabilidade e a confiabilidade dos sistemas quânticos utilizados em criptografia [56].

Contudo, apesar do seu promissor horizonte, essa tecnologia ainda encontra obstáculos significativos, como a necessidade de dispositivos extremamente precisos e os desafios na implementação em larga escala. O desenvolvimento de sistemas quânticos viáveis para comunicação digital requer não só progressos técnicos, mas também uma revisão aprofundada dos protocolos de segurança atualmente empregados. Dessa forma, a computação quântica pode tanto representar uma solução inovadora quanto um novo vetor de riscos, ressaltando a importância de uma abordagem cautelosa e equilibrada na sua aplicação no campo da segurança digital [56].

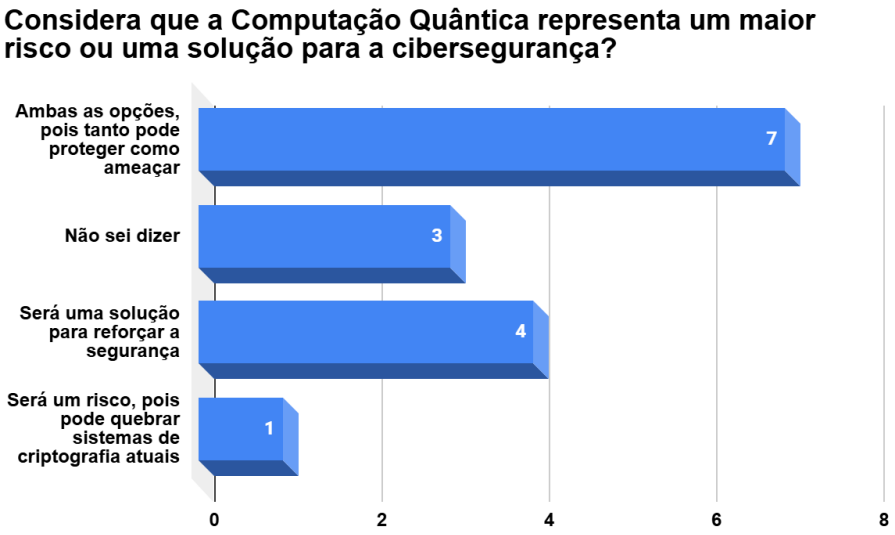

Figura 33: Percepção da Computação Quântica: riscos e soluções em cibersegurança.

A seguinte figura 34, apresenta a perceção dos participantes relativamente a quão preparadas as empresas estão para se protegerem de ataques cibernéticos usando as tendências emergentes, e o que podemos concluir é que 9 pessoas de 15 acredita que as empresas estão longe de estarem preparadas para este tipo de defesa, 3 pessoas acreditam que as empresas se encontram capacitadas para lidarem com este tipo de situação e 3 não souberam responder. Este resultado revela uma clara falta de confiança nas capacidades organizacionais, o que pode estar relacionado tanto com a complexidade das tecnologias emergentes como com a ausência de profissionais especializados e com a insuficiência de estratégias de segurança robustas. Como salienta Souza [57], a tecnologia, por si só, não garante a segurança digital. É imprescindível investir na capacitação contínua das equipas, bem como na implementação de políticas e infraestruturas adaptadas às novas ameaças. Dessa forma, a sinergia entre tecnologia e o fator humano torna-se indispensável para um sistema de cibersegurança eficaz.

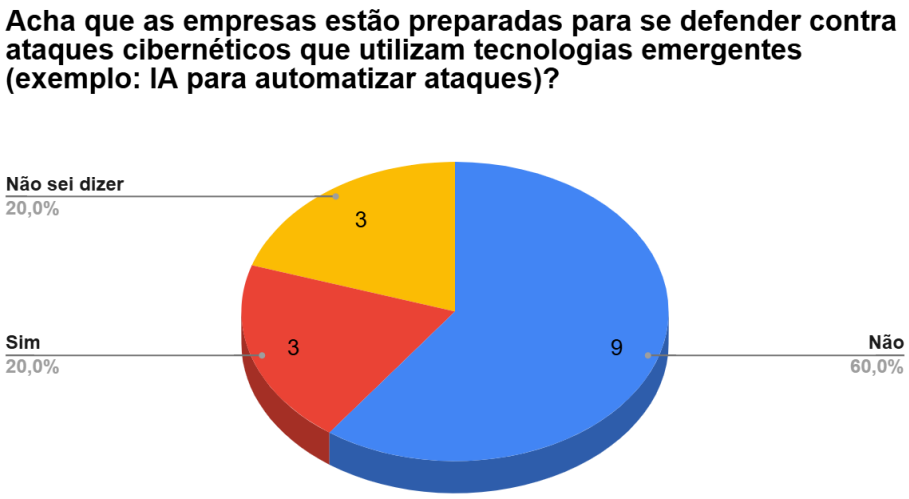

Figura 34: Avaliação da preparação das empresas contra ataques com tecnologias emergentes.

Nesta pergunta da figura 35, os participantes foram questionados se as empresas nas quais se encontram inseridas utilizam alguma tecnologia emergente como IA, blockchain e outras para reforçar a cibersegurança. A maioria dos participantes, equivalente a 8 pessoas, responderam afirmativamente, indicando que as suas empresas já utilizam este tipo de tecnologia. Por outro lado, 2 pessoas responderam que as suas empresas não usam, e 5 pessoas afirmaram não saber. Os resultados revelam uma tendência encorajadora na incorporação de tecnologias emergentes voltadas ao fortalecimento da segurança digital, evidenciando que mais da metade das empresas consultadas já estão investindo nesse tipo de inovação. Segundo o CNCS, tecnologias emergentes como IA, computação em nuvem e outras, estão cada vez mais presentes nas práticas de segurança digital em Portugal [58].

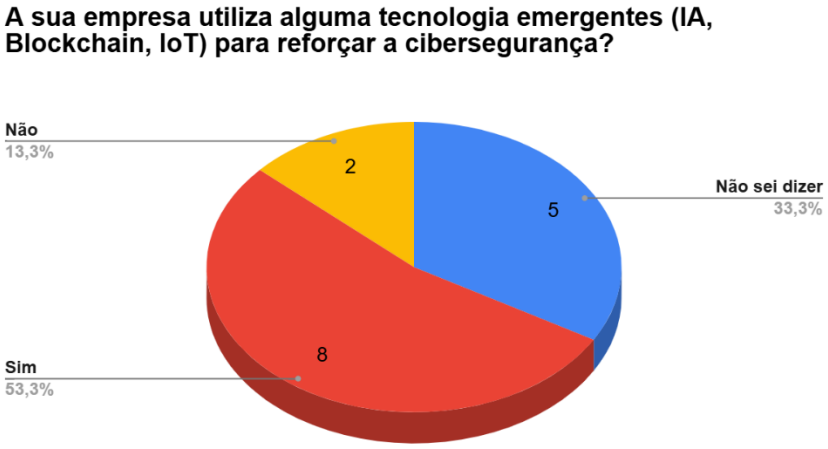

Figura 35: Utilização empresarial de tecnologias emergentes (IA, Blockchain, IoT) em cibersegurança.

O gráfico da figura 36 procurou entender se as empresas realizavam testes regularmente para a identificação de possíveis vulnerabilidades. Dos participantes, 5 afirmaram que as suas empresas realizam algumas vezes por ano, 5 afirmaram que as empresas realizam os testes mensalmente, 2 afirmaram que os testes são realizados apenas quando existem atualizações importantes e outros 2 afirmaram que não fazem testes de penetração. Os resultados demonstram, de uma forma geral, que as empresas estão a investir nesta prática como forma de se protegerem de possíveis riscos cibernéticos. É muito importante que as empresas invistam nestes testes de penetração, pois possibilitam verificar as defesas de segurança, simulando ataques reais, como forma de descobrir pontos fracos dos sistemas, permitindo assim melhorar as medidas de segurança, identificar as vulnerabilidades antes que sejam exploradas pelos cibercriminosos, e garantir a conformidade com requisitos regulatórios [59].

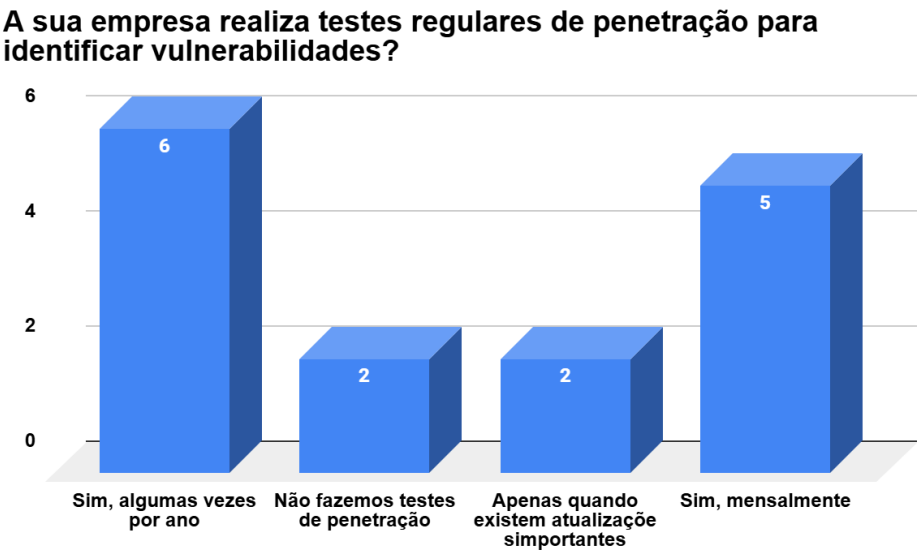

Figura 36: Realização de testes regulares de penetração.

Conforme apresentado na figura 37, foi perguntado se as empresas deveriam se preparar para a era da computação quântica, e 9 dos participantes afirmara que é essencial que as empresas comecem sim a desenvolver sistemas de criptografia resistentes a quântica, e outras 3 pessoas também disseram que as empresas devem começar a preparar-se, mas que ainda estamos longe de ver um impacto real do mesmo, e 3 pessoas não souberam responder. Estes resultados indicam que há uma crescente conscientização sobre o quão importante é estar preparado. Com o avanço tecnológico exponencial, principalmente na área da computação quântica, é notória a importância de refletir os sistemas de segurança digital da atualidade. Como especialistas já destacaram, a computação quântica tem o potencial de resolver problemas bem complicados de forma muito eficiente. No entanto, ela também pode representar uma ameaça séria à segurança da informação, pois pode quebrar os algoritmos de criptografia usados atualmente [32]. De acordo com a IT Insight [60], quanto mais a computação quântica se desenvolve, os métodos criptográficos tradicionais podem se tornar vulneráveis, o que reforça a necessidade de as empresas investirem em soluções de segurança quântica, como a criptografia pós-quântica. Não se trata apenas de acompanhar as inovações, mas de antecipar riscos e garantir que os dados sensíveis não fiquem expostos a novas formas de ataque.

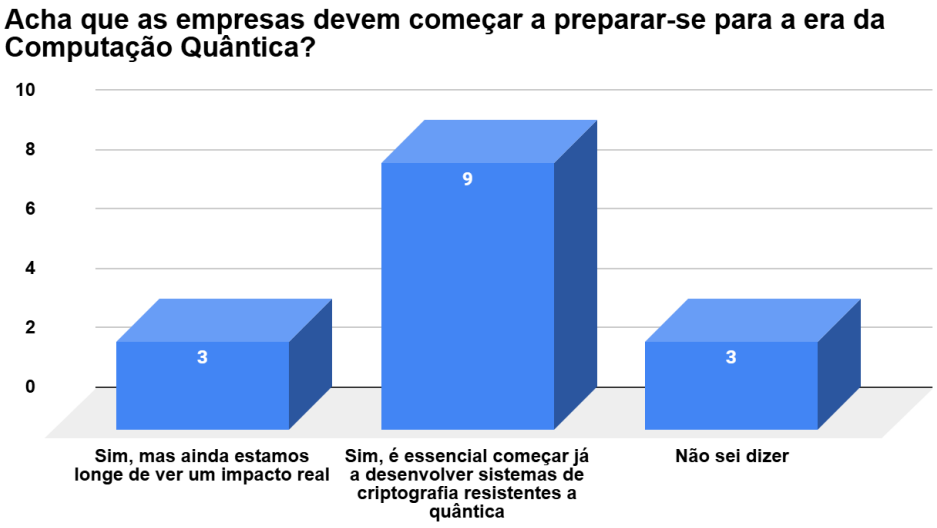

Figura 37: Opinião sobre a necessidade de preparação empresarial para a era Quântica.

Na figura 38, foi questionado se as empresas se encontram preparadas para lidar com os ataques a serviços na nuvem. A maioria (10 participantes) disse que algumas estão preparadas e outras não, enquanto 4 disseram que não e que a maioria ainda possui falhas de segurança, e por fim, apenas 1 pessoa considerou que as empresas estão bem preparadas. Estes dados demonstram, embora haja algum nível de preparação, muitas empresas/organizações ainda apresentam lacunas significativas no que diz respeito à cibersegurança. Essa perceção está alinhada com os desafios apontados na literatura especializada. Segundo Jain et al., os principais riscos associados à computação em nuvem incluem falhas de configuração, ausência de políticas de acesso seguras, violação de dados e baixa maturidade dos sistemas de defesa [61]. Além disso, a Kaspersky destaca que a proteção inadequada das credenciais de acesso, a falta de monitoramento contínuo e a má gestão de permissões são fatores críticos que aumentam a vulnerabilidade a ciberataques [62]. Dessa forma, os dados obtidos nesta investigação reforçam a ideia de que apenas uma parte das empresas está efetivamente preparada para enfrentar ameaças relacionadas à nuvem, sendo fundamental que haja um investimento contínuo não só em tecnologia, mas também em formação, políticas de segurança e cultura organizacional.

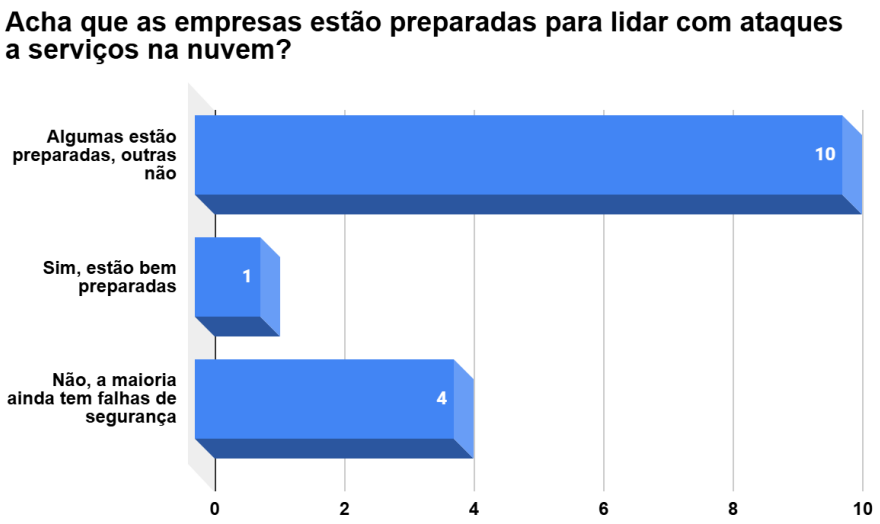

Figura 38: Avaliação de preparação de empresas contra ataques em serviços na nuvem.

A Figura 39 focou em compreender as medidas de segurança que os participantes implementam para manter a sua segurança e de seus dados. Dos 15, 9 participantes afirmaram que utilizam encriptação de dados, outros 4 afirmaram que utilizam o modelo Zero Trust, 2 afirmaram que utilizam firewall, 2 afirmaram que utilizam auditorias de segurança e apenas 1 afirmou que utiliza uma VPN como defesa. Entretanto, dois participantes afirmaram que não tomavam quaisquer precauções de segurança. Esses resultados mostram um grau respeitável de compreensão sobre a necessidade da proteção de dados na nuvem. O facto da criptografia e o Zero Trust terem sido mencionados na maioria das respostas indica que os participantes estão de alguma forma cientes dos procedimentos de segurança. Mesmo no caso de uma violação, a criptografia é uma precaução essencial para garantir a confidencialidade dos dados [62].

De outro modo, o modelo Zero Trust exige verificação contínua, pois pressupõe que nenhuma entidade, interna ou externa, é inerentemente confiável [63]. Auditorias frequentes ajudam a localizar e corrigir vulnerabilidades antes que elas sejam usadas contra você [64]. Entretanto, pelo facto de 2 pessoas não tomarem qualquer precaução, surgem preocupações relacionadas à literacia digital e à divulgação de práticas sólidas de segurança cibernética entre os utilizadores de serviços em nuvem.

Figura 39: Medidas adotadas para segurança na nuvem.

A representação abaixo na figura 40 questionou aos participantes se as suas empresas implementaram a IA para detetar ameaças cibernéticas. Verificaram-se 8 respostas afirmando que sim e 7 respostas afirmando que não. Estes dados indicam que, apesar de algumas empresas já começarem com a implementação da IA, ainda existe um grupo relevante que ainda não adotou esta tecnologia. Para as empresas que já fazem uso desta tecnologia, encontram-se bem capacitadas, podendo analisar grandes quantidades de dados, identificar padrões e detetar anomalias, conforme explorado na literatura [3, 31]. A IA, especialmente quando emprega técnicas de aprendizado de máquina não supervisionado, permite que os sistemas se ajustem a novas ameaças, incluindo variantes desconhecidas de malware. Além disso, automatizar processos ajuda a tornar as equipes de segurança mais eficientes, liberando tempo para lidar com problemas mais complexos.

No entanto, o uso de IA também traz desafios. A literatura destaca questões como jogadores nos algoritmos que podem reproduzir ou amplificar preconceitos existentes, além da necessidade de grandes volumes de dados para treinar modelos eficazes, o que pode dificultar organizações com recursos limitados [3]. Uma das áreas em que a IA tem mostrado maior eficácia é na análise de tráfego de rede (Network Traffic Analysis – NTA), permitindo monitorar continuamente e em tempo real padrões de comportamento suspeitos. Portanto, os dados confirmam as discussões existentes: a IA é uma ferramenta poderosa, mas requer preparação técnica, dados de alta qualidade e supervisão cuidadosa para ser eficaz na proteção contra ameaças cibernéticas.

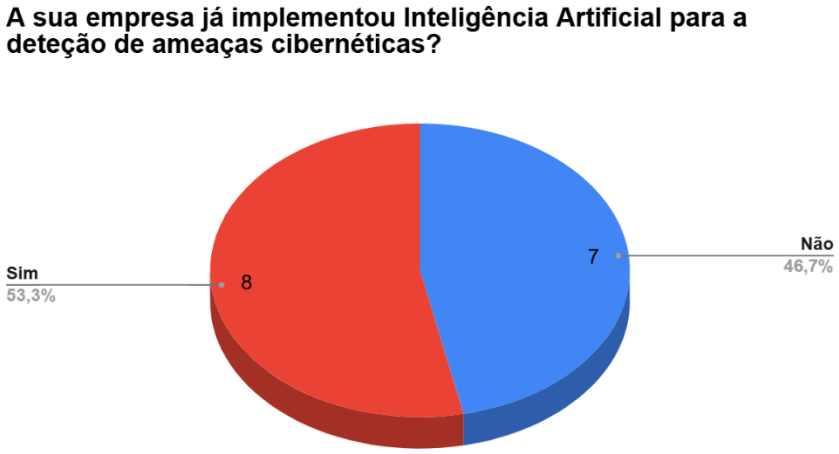

Figura 40: Implementação de IA nas empresas para a deteção de ameaças cibernéticas.

Na questão seguinte, apresentada na figura 41, buscou entender na perspetiva dos participantes qual das 4 tecnologias apresentadas terá maior impacto na cibersegurança nos próximos anos. Grande parte (11) afirmou que seria a IA, 2 afirmaram que seria computação quântica, 1 afirmou que seria segurança na nuvem e 1 afirmou que seria a IoT. Os resultados mostram uma tendência significativa de que a IA será uma ferramenta essencial para o futuro da cibersegurança. Encontra-se de acordo com estudos recentes, que ressaltam a sua capacidade de detetar ameaças em tempo real, automatizar respostas e aprender continuamente com os dados disponíveis.

Ainda assim, o fato de outras tecnologias também terem sido mencionadas, embora com menor frequência, reforça a importância de uma abordagem que envolve várias áreas do conhecimento. A computação quântica pode representar tanto uma ameaça quanto uma oportunidade, especialmente na criação e quebra de sistemas de criptografia. Sua capacidade de processamento inovadora é uma ferramenta poderosa que pode impulsionar avanços em muitas áreas diferentes, como na saúde, no setor energético e no de transportes, e com novos sistemas de encriptação mais avançados, a segurança digital será ainda mais forte, ajudando a proteger melhor informações pessoais, dados financeiros e serviços essenciais contra-ataques cibernéticos [32].

Além disso, a segurança na nuvem e a IoT continuam sendo áreas críticas, devido ao crescimento acelerado de dados e dispositivos conectados. Por isso, embora a IA seja destaque atualmente, é essencial que as organizações acompanhem o desenvolvimento de

todas essas tecnologias para manter sua resistência frente aos novos desafios de segurança digital.

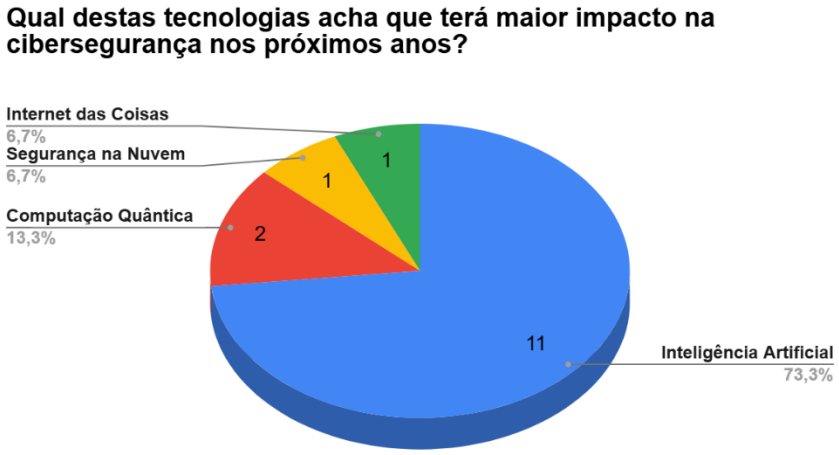

Figura 41: Tecnologias com maior impacto na cibersegurança futuramente.

O gráfico ilustrado na figura 42, questionou qual é o impacto mais significativo de um ataque cibernético em uma pequena empresa na opinião dos participantes, e das opções disponibilizadas, a maioria (7 participantes) afirmaram que seria interrupções das operações, 4 afirmaram que seria perda de dados sensíveis, 3 afirmaram que seria perda financeira e 1 afirmou que seria danos a reputação. Esse resultado mostra uma visão alinhada com estudos atuais sobre segurança cibernética em pequenas e médias empresas, que apontam a interrupção operacional como uma das consequências mais críticas dos ataques.

Segundo o relatório da IBM "Cost of a Data Breach 2023" [65], quando as operações são interrompidas, pode haver paralisações longas, queda na produtividade e atrasos na cadeia de suprimentos, que são fatores que impactam diretamente a sustentabilidade de pequenas empresas, que muitas vezes têm recursos limitados para lidar com esses problemas. Além disso, a perda de dados sensíveis também foi apontada como uma das preocupações mais importantes. De acordo com o relatório da ENISA "Threat Environment 2023" [48], perder dados pode levar a penalizações legais, como as relacionadas ao RGPD, e prejudicar a confiança dos clientes. Mesmo que menos participantes tenham mencionado perdas financeiras ou danos à reputação, esses impactos continuam sendo importantes e frequentemente estão ligados aos demais. Esses dados reforçam a necessidade de adotar medidas preventivas que priorizem a continuidade das operações e a proteção dos dados,

especialmente em pequenas empresas, que normalmente são mais vulneráveis a ataques cibernéticos por terem recursos técnicos e humanos mais limitados.

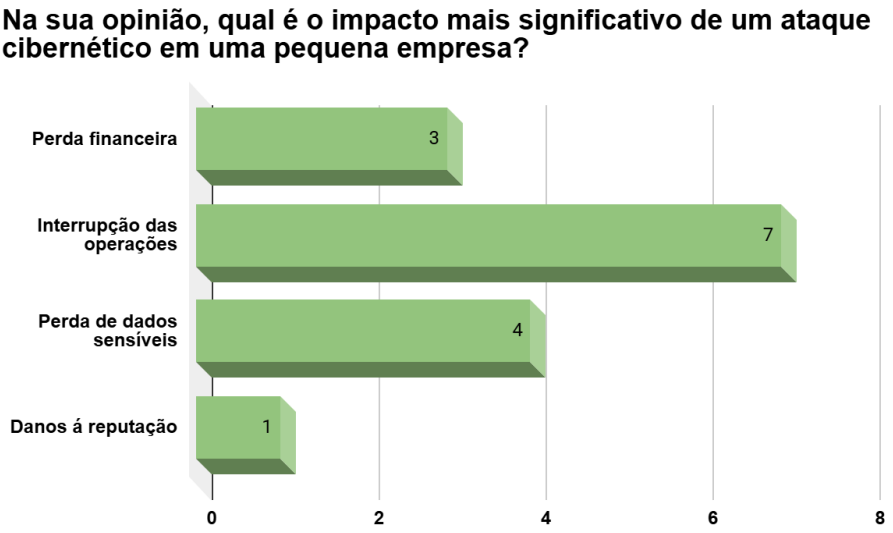

Figura 42: Impacto mais significativo de ataques cibernéticos em pequenas empresas.

4.1.4. Perceção e Experiência com Cibersegurança

Esta secção tem o objetivo de avaliar a adoção de boas práticas, regulamentações e desafios na proteção de dados e sistemas. Para esta parte, os números de participantes a considerar foram a amostra total de 143.

Na tentativa de entender o nível de conhecimento dos participantes sobre alguma regulamentação de proteção de dados, como o Regulamento Geral de Proteção de Dados (RGPD), a figura 43 representa os dados adquiridos na visão dos participantes. A maior parte das pessoas (69) afirmou que não conhece o RGPD, enquanto 52 disseram que têm uma compreensão superficial, e apenas 21 se consideraram bem informados sobre a regulamentação. Esses números indicam uma grande lacuna no entendimento das regras essenciais de proteção de dados pessoais, o que é especialmente preocupante num momento em que ataques cibernéticos aumentam e os dados pessoais se tornam cada vez mais estratégicos. Ainda assim, o fato de muitas pessoas terem algum grau de familiaridade, mesmo que superficial, pode ser visto também como um sinal positivo de interesse e disposição para aprender mais.

Segundo a Agência Europeia para a Cibersegurança (ENISA), a falta de conhecimento sobre a regulamentação é um dos principais obstáculos enfrentados por empresas e

indivíduos ao tentar implementar políticas eficazes de cibersegurança. A escassez de treinamentos contínuos sobre o RGPD, especialmente para pequenas empresas e profissionais não técnicos, aumenta a vulnerabilidade tanto do ponto de vista técnico quanto legal. Assim, esses resultados reforçam a importância de investir em programas de conscientização e capacitação contínua em proteção de dados, ajudando a diminuir riscos de incidentes, melhorar a conformidade legal e fortalecer uma cultura de segurança digital [48].

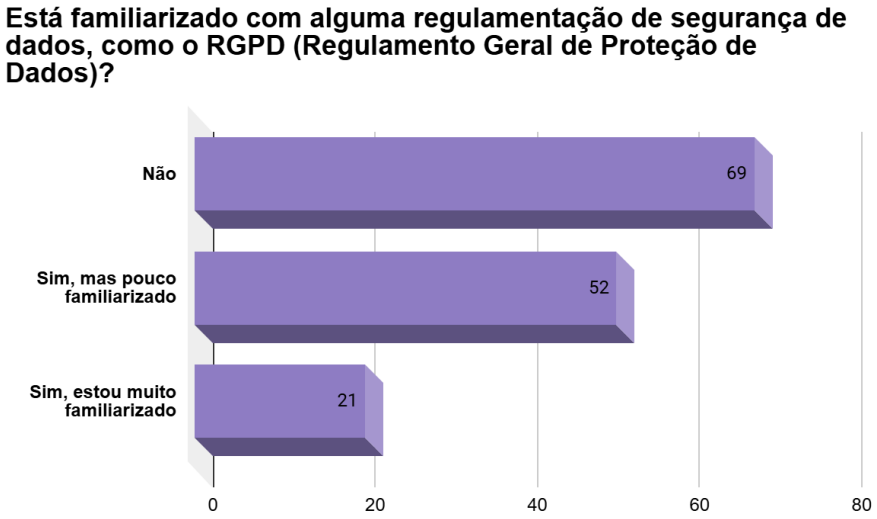

Figura 43: Familiaridade com Regulamento Geral de Proteção de Dados (RGPD).

Para entender se as organizações seguem as normas do RGPD, a figura 44 apresenta os dados dos participantes, onde 64 afirmaram não saber dizer se as empresas seguiam ou não as normas, 37 não se aplicam neste caso, 34 afirmaram que as empresas estão a seguir as normas e apenas 8 afirmaram que não. Este estudo mostra de forma clara que há uma grande falta de conhecimento sobre como é aplicado o RGPD no ambiente empresarial. Essa situação pode indicar uma comunicação interna pouco eficaz nas empresas e uma necessidade maior de formação dos colaboradores. Quase metade dos participantes não soube responder às perguntas, reforçando a importância de investir em ações de conscientização, treinamentos e maior transparência sobre as práticas de proteção de dados. Como reforçado na literatura, as empresas devem estar em conformidade com os regulamentos, permitindo assim definir políticas e procedimentos para garantir o seu cumprimento, como treinar os funcionários, acompanhar o que acontece internamente e ter formas de relatar e resolver problemas que possam surgir,

assim como devem sensibilizar os seus colaboradores da importância dos dados [44]. Conhecer bem o RGPD deve ser uma preocupação de toda a organização.

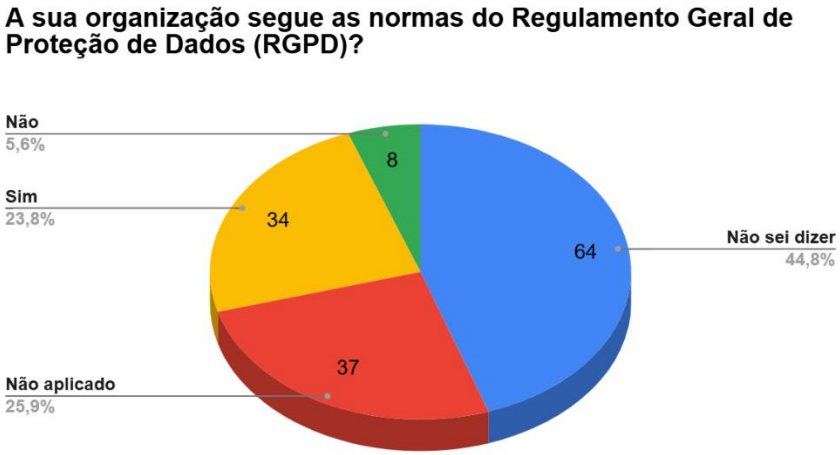

Figura 44: Conformidade da organização com as normas do RGPD.

A figura 45, teve o intuito de saber a opinião dos participantes, relativamente se consideram que o RGPD tem sido eficaz na proteção dos dados dos utilizadores. Grande parte (76) pessoas afirmaram que não sabem dizer se tem sido eficaz, 46 pessoas disseram que sim, mas que ainda existem falhas, 13 pessoas afirmaram que tem sido eficaz e protege bem os dados e 8 pessoas afirmaram que não tem sido muito eficaz. Em geral os resultados transmitem que há uma confiança no que diz respeito a eficácia da RGPD, mas existe também uma grande lacuna relativamente ao conhecimento e compreensão sobre como funciona na prática. Mais da metade dos participantes, não souberam opinar sobre o tema, o que indica que, mesmo com a existência de regras e regulamentações, muitas pessoas ainda não percebem claramente como elas funcionam ou quais são seus efeitos.

Essa situação pode ser resultado de vários fatores, como a falta de uma comunicação clara por parte das instituições responsáveis sobre como o regulamento é aplicado, o pouco conhecimento ou de sensibilização das pessoas sobre seus direitos e responsabilidades no que diz respeito à proteção de dados, e também a complexidade do próprio regulamento, que muitas vezes parece técnico demais e longe do dia a dia da maioria. Segundo a literatura, após a entrada em vigor do regulamento, medida foram tomadas para garantir a conformidade e que os mecanismos de proteção dos dados funcionem corretamente. Garantindo a conformidade nas empresas, fazendo auditorias, investindo nas ferramentas

adequadas e com bom treinamento dos funcionários, os dados dos utilizadores estarão protegidos [44].

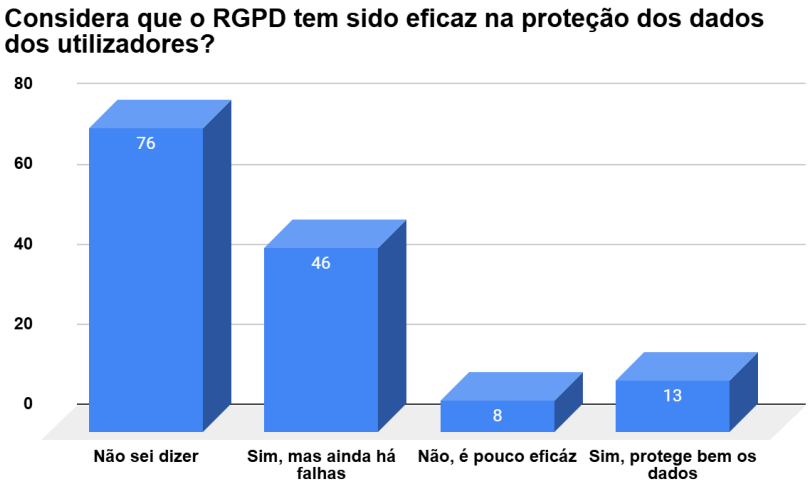

Figura 45: Percepção da eficácia do RGPD na proteção de dados.

A figura 46 teve o intuito de avaliar se os participantes já receberam algum alerta sobre um possível ataque cibernético na conta pessoal ou profissional. A maioria, 71 participantes, afirmaram que já receberam alerta e tomaram as medidas necessárias, e isto mostra que estão conscientes em relação aos riscos que possam surgir caso não tomem nenhuma atitude antecipadamente. Por outro lado, 52 participantes afirmaram que nunca receberam qualquer alerta, o que pode significar que já adotam boas práticas de segurança ou que ainda não foram alvo de tentativas visíveis de ataque.

No entanto, como evidencia a ENISA, a falta de alertas não garante uma proteção completa, podendo também gerar uma falsa sensação de segurança ou refletir ausência de ferramentas eficazes de monitoramento [49]. Por outro lado, 20 pessoas relataram que receberam alerta, mas não tomaram nenhuma precaução, o que se torna preocupante. Este cenário está alinhado com as recomendações do NIST, que ressaltam a importância de oferecer formação contínua aos utilizadores e estabelecer procedimentos claros para lidar com incidentes. Dessa forma, é possível diminuir os riscos e incentivar uma cultura de prevenção [66].

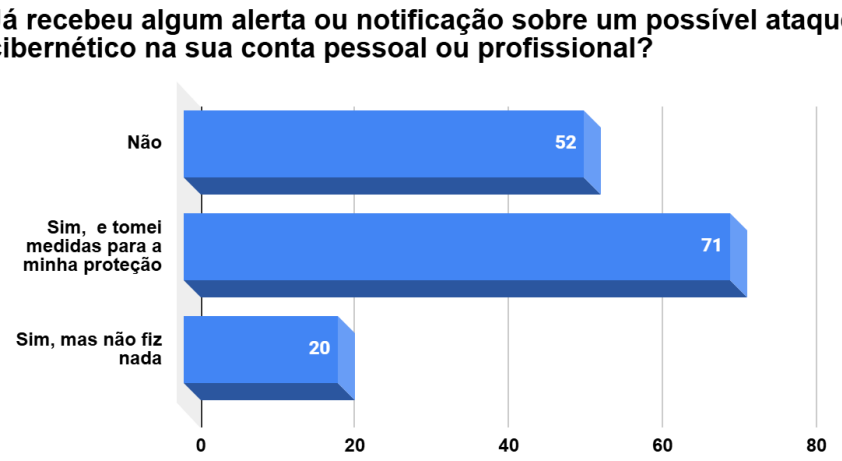

Figura 46: Receção de alertas/notificação de ataques cibernéticos.

O gráfico a seguir, procurou entender como os participantes percebem a falta de profissionais qualificados em cibersegurança, e a maioria (79), afirmou que sim, existe falta de pessoas qualificadas, 11 pessoas disseram que não e 53 não souberam responder. Esses resultados, reforçam a preocupação global com a escassez de profissionais qualificados, como já destacado na literatura.

Segundo o relatório do ISC2 [41], em 2023, o déficit mundial de profissionais de cibersegurança ultrapassava quatro milhões, o que representa um grande desafio diante do aumento dos ataques cibernéticos. Em Portugal, dados da CNCS mostram que a situação é ainda mais grave do que a média da União Europeia, afetando até mesmo a administração pública, que tem buscado serviços externos como alternativa. Esses números ressaltam a importância de investir na formação técnica, promovendo a inclusão de disciplinas relacionadas à cibersegurança nos currículos escolares e campanhas de conscientização pública. Além disso, organizações como a Fortinet indicam que cerca de 90% das empresas já enfrentaram incidentes de segurança atribuídos à falta de profissionais qualificados, o que demonstra que essa escassez não é apenas um problema técnico, mas um risco real para a segurança das organizações e da sociedade como um todo [42].

Figura 47: Percepção de falta de profissionais qualificados em cibersegurança.

Nesta questão seguinte representada na figura 48, os participantes tiveram que escolher um total de medidas de segurança que achavam ser mais eficazes para a proteção de dados e sistemas. A maior parte das pessoas (97) considerou como medida eficaz a formação contínua dos utilizadores e este resultado reforça a importância do fator humano na cibersegurança, como destacado pela ENISA [49], considerando-o um dos aspetos mais críticos. A conscientização e o treinamento dos usuários são estratégias fundamentais para reduzir os riscos.

De seguida, 85 escolheram a encriptação de dados, alinhando com o estudo que indica a encriptação de dados como, um grande fator na confidencialidade e na segurança dos dados [62]. A autenticação multifator foi escolhida por 66 pessoas como medida eficaz, refletindo a importância de usar métodos extras para garantir um controle melhor de quem consegue acessar os sistemas, esta medida possui uma camada de segurança que impede o acesso das informações, independentemente de ter a senha roubada [54]. Posteriormente, 49 pessoas citaram a auditorias e testes regulares, indicando que muitos reconhecem que fazer revisões constantes ajuda a descobrir vulnerabilidades. E como foi mencionado na literatura, as auditorias de rotina permitem encontrar e corrigir vulnerabilidades, antes que sejam usadas contra nós mesmos [64].

Por fim, 48 respostas destacaram que investir em tecnologia também é importante, revelando que os usuários reconhecem que soluções tecnológicas avançadas precisam estar aliadas ao treinamento de pessoas e à implementação de processos eficazes. Esses resultados reforçam a ideia internacional de que a cibersegurança depende de uma responsabilidade compartilhada entre pessoas, procedimentos e tecnologia. Não só a

capacitação contínua, mas também as constantes atualizações são essenciais para a prevenção [49].

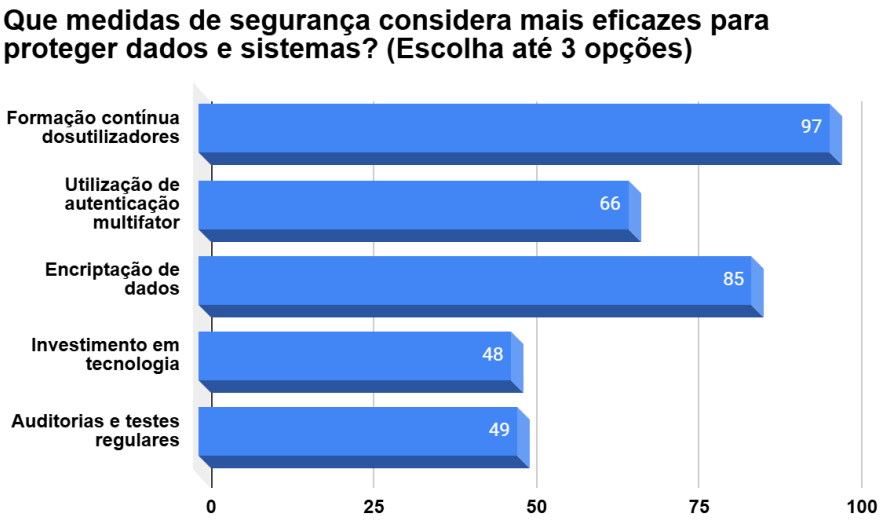

Figura 48: Medidas de segurança consideradas mais eficazes.

Nesta última questão (Figura 49), foi uma questão aberta para que os participantes pudessem compartilhar suas recomendações pessoais sobre como melhorar a segurança digital. No total, foram recebidas 42 respostas, o que proporcionou uma visão mais detalhada das perceções de cada um. Entre as sugestões mais comuns, destacou-se a importância de capacitar os utilizadores, especialmente os mais idosos, que muitas vezes não têm conhecimentos suficientes para identificar ou evitar ameaças online. A conscientização contínua e a educação digital foram apontadas como passos essenciais para desenvolver uma cultura sólida de cibersegurança. Outros participantes reforçaram a necessidade de praticar boas medidas de segurança, como usar autenticação multifator (MFA), criar senhas fortes, usar gerenciadores de senhas e adotar ferramentas de defesa contra ameaças virtuais. Também houve menção ao uso de IA na deteção de comportamentos suspeitos, mostrando que uma parte dos participantes reconhece o potencial dessas tecnologias emergentes para ajudar na segurança digital. Além disso, mencionaram soluções de segurança proativas, que não apenas identificam ataques em tempo real, mas também evitam incidentes antes que eles aconteçam. Isso revela uma maior consciência sobre a importância de prevenir, ao invés de apenas reagir a problemas. Resumindo, as respostas abertas reforçam os dados das perguntas de múltipla escolha, principalmente quanto à necessidade de formação contínua e ao uso de tecnologias

eficazes. Ao mesmo tempo, demonstram que a fraqueza humana ainda é uma das maiores vulnerabilidades na cadeia da segurança digital, como foi dito por um dos participantes:

"Os utilizadores ainda são o elo mais fraco na segurança por recorrer à senhas repetidas e fracas para muitos acessos sem autenticação em multi-etapas, além de fazer acesso à portais suspeitos ou pirataria para obter algum tipo de privilégio."

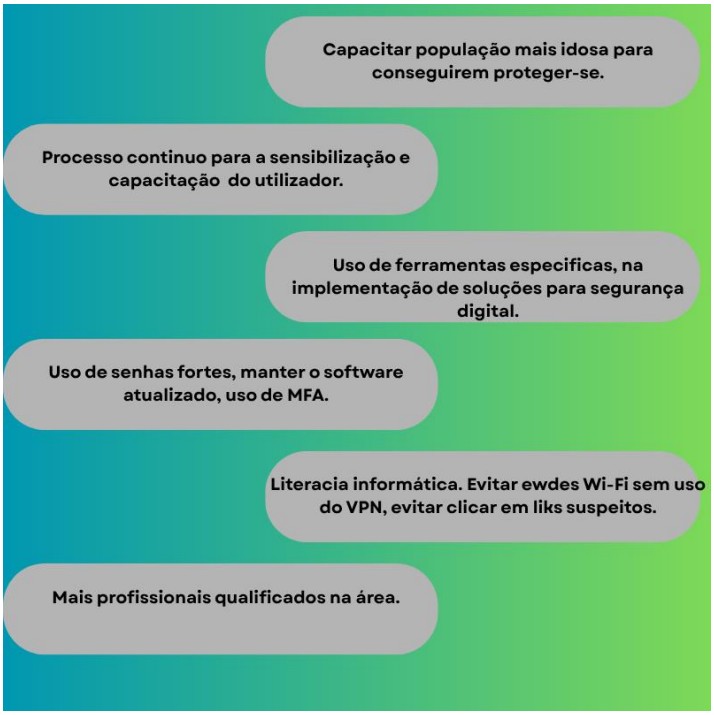

Figura 49: Recomendações sugeridas como forma de melhorar a segurança digital.

4.2. Análise de Dados baseada em técnicas de IA

Nesta secção, serão aplicadas as técnicas de IA, especificamente algoritmo de ML, nas amostras recolhidas através do inquérito. O código utilizado na criação da árvore pode ser consultado no anexo B. O objetivo é buscar padrões, identificar as relações entre as variáveis e prever alguns comportamentos e perceções dos participantes com relação à cibersegurança.

Foi utilizado o modelo preditivo supervisionado, precisamente a técnica da Árvore de Decisão. Este é um método de fácil compreensão e que mostra como diferentes fatores podem influenciar o resultado. É uma técnica que facilita a visualização das regras de decisão, que ajudam a entender os resultados das pesquisas e fornecem uma visão preditiva de quais variáveis são mais relevantes. Os nós dividem os dados em ramificações com base nos valores das características até chegar ao "nós folha" que representa o resultado ou previsão final [67].

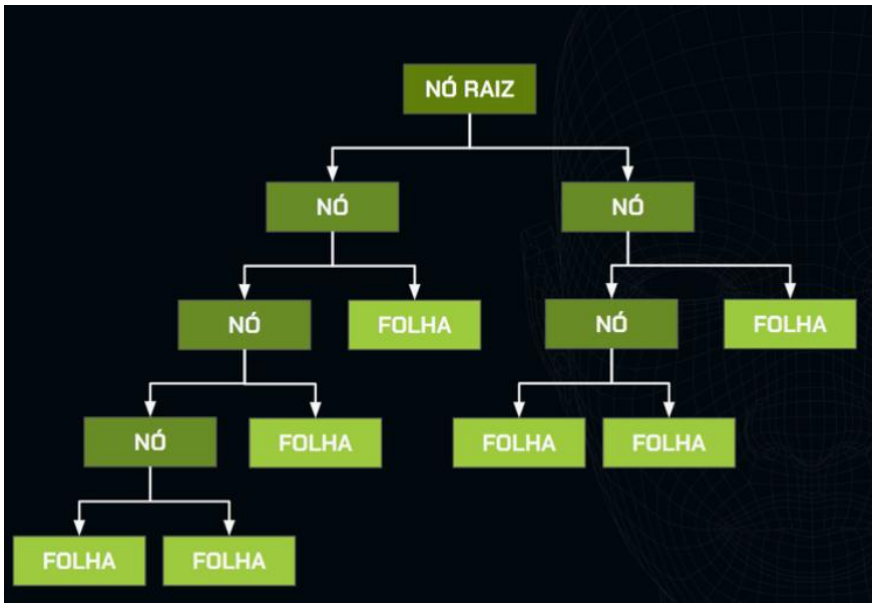

Figura 50: Estruturação de uma Árvore de Decisão com seus nós de decisão e os nós folha. Fonte: Alura.

Existem alguns parâmetros importantes, como é o caso do max_depth, que define a profundidade da árvore, permitindo assim uma melhor visualização limitando a mesma, e o decision_tree, que pode ser de regressão ou de classificação (que é o nosso caso), e outros [68]. As *decisionTrees* possuem hiperparâmetros importantes, que permitem a árvore fazer a separação considerando o atributo. Esses hiperparâmetros são o *criterion*

que é o gini por padrão e o splitter, que já vem definido. Em outras palavras, ela busca fazer a divisão de forma a diminuir ao máximo o coeficiente de gini, da melhor forma possível. O *gini* mede a heterogeneidade dos dados buscando reduzir a impureza no próximo ramo, variando de 0 (puro) a 1 (totalmente impuro). Se usarmos a opção entropy, o foco passa a ser aumentar o ganho de informação, ou seja, reduzir a entropia na próxima camada de divisão. Outros hiperparâmetros a serem considerados são: *sample* que é o número da amostra, e *value* que é o número de registros que tem cada classe na amostra [68].

O trabalho foi desenvolvido a partir da ferramenta Google Colab e recorreu à linguagem de programação Python. As bibliotecas utilizadas foram *pandas, numpy, scikit-learn e matplotlib* para o tratamento, treino e visualização dos dados.

4.2.1. Preparação dos Dados

Antes de mais, os dados precisavam estar preparados de forma que não causassem erro durante o treino. Foram selecionadas quatro questões principais para serem as variáveis alvos das quais temos:

- Q6. Nível de familiaridade com ataques cibernéticos?
- Q7. Já sofreu algum ataque?
- Q9. Em termos de segurança, como se sente ao navegar na internet'
- Q40. Falta de profissionais em cibersegurança?

Para cada uma das questões anteriores, foram selecionadas algumas das variáveis preditivas que ajudam a prever melhor cada uma das variáveis alvos escolhidas, que são as seguintes:

- Q1. Qual a sua faixa etária?
- Q2. Qual o seu sexo?
- Q3. Qual o seu nível de escolaridade?
- Q4. A que grupo pertence?

- Q5. Qual o seu nível de conhecimento sobre cibersegurança?
- Q6. Utiliza software ou firewall no seu computador ou dispositivos?
- Q7. Já sofreu algum ataque cibernético?

Normalmente durante o treinamento do modelo ML, os dados categóricos ou os dados em formatos de texto não são aceites pela maioria dos algoritmos, logo houve a necessidade de fazer essa conversão usando uma técnica de pré-processamento de dados, uma vez que grande parte dos dados estava em formato de texto ou categórica. Na figura 51, temos a representação dos dados antes da conversão e para fazer a conversão, utilizou-se o LabelEncoder da biblioteca SciKit Learning [69].

	1. Qual a sua faixa etária?	2. Qual é o seu sexo?	3. Qual é o seu nível de escolaridade?	4. A que grupo pertence?	5. Qual é o seu nível de conhecimento sobre cibersegurança?	6. Utiliza software antivírus ou firewall no seu computador ou dispositivos?	7. Já sofreu algum ataque cibernético?
0	18-25 anos	Feminino	Ensino secundário	Estudante	Nenhum	Não, não uso	Não
1	26-35 anos	Feminino	Licenciatura	Estudante	Intermédio	Sim, em todos os dispositivos	Não
2	18-25 anos	Masculino	Ensino secundário	Estudante	Básico	Sim, apenas no computador	Sim
3	18-25 anos	Feminino	Licenciatura	Profissional TI	Básico	Sim, apenas no computador	Sim
4	18-25 anos	Masculino	Licenciatura	Profissional TI	Intermédio	Sim, apenas no computador	Sim

Figura 51: Dados antes da conversão com o LabelEncoder.

A partir daí, criaram-se variáveis, cujo objetivo foi armazenar os valores novos após a conversão. O LabelEncoder tem o papel de fazer a transformação desses valores categóricos em numéricos. O LabelEncoder se enquadra neste caso uma vez que as variáveis a serem convertidas seguem uma ordem implícita como é recomendada. Após a transformação, obtemos os resultados observados na figura 52.

	1. Qual a sua faixa etária?	2. Qual é o seu sexo?	3. Qual é o seu nível de escolaridade?	4. A que grupo pertence?	5. Qual é o seu nível de conhecimento sobre cibersegurança?	6. Utiliza software antivírus ou firewall no seu computador ou dispositivos?	7. Já sofreu algum ataque cibernético?
0	0	0	2	0	3	1	0
1	1	0	3	0	2	3	0
2	0	1	2	0	1	2	2
3	0	0	3	2	1	2	2
4	0	1	3	2	2	2	2

Figura 52: Dados depois da conversão com o LabelEncoder.

Após a conversão, cada variável ficou com os respectivos valores numéricos, como pode ser visto na figura 53.

1. Qual a sua faixa etária?':
18-25 anos - 0
26-35 anos - 1
36-50 anos - 2
Mais de 50 anos - 3
Menos de 18 anos - 4

2. Qual é o seu sexo?
Feminino - 0
Masculino - 1
Prefiro não dizer - 2

3. Qual é o seu nível de escolaridade?
Doutoramento - 0
Ensino básico - 1
Ensino secundário - 2
Licenciatura - 3
Não quero indicar - 4
Pós-graduação /Mestrado - 5

4. A que grupo pertence?
Estudante - 0
OT/TI - 1
Profissional TI - 2
Representante de uma empresa - 3
Trabalhadora - 4
Técnico de uma empresa - 5
Utilizador da internet (sem formação técnica) - 6

5. Qual é o seu nível de conhecimento sobre cibersegurança?
Avançado - 0
Básico - 1
Intermédio - 2
Nenhum - 3

6. Utiliza software antivírus ou firewall no seu computador ou dispositivos?
Não sei o que é antívirus ou firewall - 0
Não, não uso - 1
Sim, apenas no computador - 2
Sim, em todos os dispositivos - 3

7. Já sofreu algum ataque cibernético?
Não - 0
Não sei - 1
Sim - 2

Figura 53: Conversão de variáveis categóricas para variáveis numéricas.

4.2.2. Construção da árvore de decisão

Para fazer a construção deste algoritmo de ML usando o Google Colab, primeiramente devemos importar as bibliotecas necessárias: *pandas e sklearn.* Com elas, podemos dar início à construção das árvores. De seguida, é feito o carregamento dos dados em formato CSV, e é feita a conversão das variáveis categóricas para numéricas, e define-se que variáveis serão alvos e quais serão as explicativas.

Durante o processo, é necessário passar por duas etapas: a de aprendizado, onde se baseia nos dados de treino fornecidos, e a de previsão, que é usada para previsão das respostas. Os dados são divididos em dois grupos: de treino e de teste, recorrendo ao uso da função *train_test_split().* Para que haja a classificação correta dos dados, é necessário selecionar bons atributos nos nós, onde em cada nó será selecionado um atributo pelo algoritmo que separa melhor os dados, e depois disso acontece a divisão recursiva, em que os dados serão separados em subconjuntos, criando nós e ramos até que seja atingida a condição de paragem [70].

Após efetuar todos os processos necessários, obtemos as árvores geradas e recorremos a algumas métricas de avaliação como: acurácia, precisão, Recall e Fi-score. Essas métricas ajudam a avaliar a capacidade de erro e acerto do modelo de ML.Na figura abaixo, mostra-se como funciona a geração da árvore da decisão.

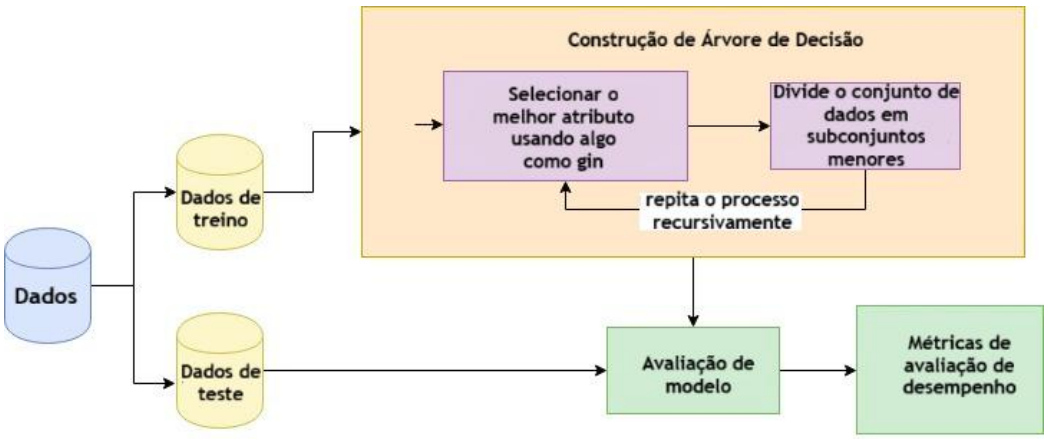

Figura 54: Funcionamento do algoritmo de árvore de decisão. Adaptado de Datacamp.

Acurácia é a métrica que ajuda a descobrir o desempenho do modelo numa tarefa de classificação [71].

$$Acurácia = \frac{Previsões\ Corretas}{\text{Total de previsões}}$$

Esta métrica, F1-score, é a média harmônica entre a precisão e o recall [71].

$$F1\ Score = 2 * \frac{Precisões * Recall}{Precisõe + Recall}$$

Esta métrica, a precisão, nos diz quanto podemos confiar num modelo quando ele faz a previsão de pertença a uma determinada classe, ou seja, das previsões positivas quanto acertou [71].

$$Precisão = \frac{Previsões\ Positivas\ Corretas}{\text{Total de positivas}}$$

O recall, também conhecido como taxa de deteção, nos dá a informação de todos os exemplos que o modelo poderia detetar, quantos realmente conseguiu detetar [71].

$$Recall = \frac{Previsões\ Positivas\ Corretas}{\text{Exemplos Positivos}}$$

A matriz da confusão é uma ferramenta muito útil, simples e de fácil compreensão, que permite avaliar a performance do modelo ML. Ela mostra o número de previsões corretas e incorretas que o modelo faz para cada classe [72]. A partir dela podemos calcular as métricas referidas anteriormente. Na figura 55, temos a estrutura básica da matriz da confusão.

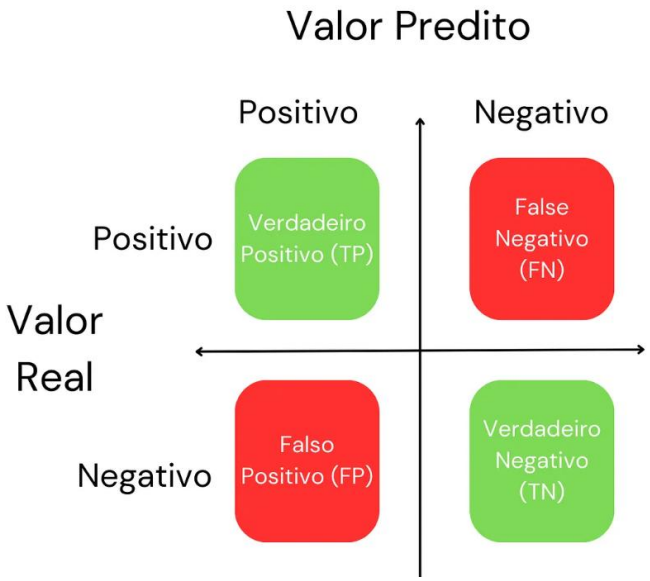

Figura 55: Estrutura da matriz da confusão. Fonte: Medium.

4.2.3. Resultados e Interpretações

Para cada uma das quatro questões ou variáveis-alvo, serão feitas as suas análises e interpretações das suas árvores de decisão. Para responder à pergunta Q6, na qual a variável-alvo, as perguntas selecionadas como variáveis explicativas foram Q1, Q3, Q5 e Q7.

Primeiramente temos a árvore de decisão que foi gerada para a questão Q6 representada na figura 56, onde buscou entender quais os fatores que mais induzem ao uso dos mecanismos de defesa entre os participantes. Para este caso utilizou-se 70% dos dados para treino e 30% para teste e este modelo foi desenvolvido com base em variáveis que ajudam a entender o nível de conhecimento sobre cibersegurança, incluindo fatores como escolaridade, faixa etária, o grupo a que pertencem e a experiência prévia com ataques cibernéticos, que são as variáveis explicativas.

No nó raiz, ocorre uma divisão na variável "nível de conhecimento sobre cibersegurança", evidenciando que esta é a variável principal que melhor ajuda a prever o comportamento dos utilizadores na adoção de ferramentas de segurança. Para as pessoas que demonstraram ter conhecimento avançado (<= 0.5 True) costumam recorrer mais aos softwares de proteção, enquanto para as que demonstraram ter conhecimento básico, intermédio ou nenhum (>0.5 False) demonstraram menor adesão a esta prática. Este

resultado mostra claramente que a familiaridade das pessoas com o mundo digital é fundamental para que elas adotem medidas de prevenção. De seguida, a variável "já sofreu algum ataque cibernético" também teve o seu impacto, evidenciando que pessoas que já foram vítimas de ataques costumam recorrer mais aos softwares de proteção, mostrando que sofrer um ataque as leva a adotar mecanismos de segurança.

A faixa etária teve o seu papel relevante, em que se constatou que pessoas mais jovens, entre 18 e 35 anos, têm maior probabilidade de usar antivírus e firewalls, uma vez que elas podem estar mais familiarizadas com tecnologia e mais presentes em ambientes digitais. Pessoas de idade mais avançada normalmente usam menos essas proteções. Isso pode ser por menor contato com práticas mais recentes de cibersegurança. Resumindo, a análise mostra que o conhecimento e a experiência prática com ameaças digitais são fatores mais importantes para usar ferramentas de segurança. Os resultados indicam que é preciso investir em educação e conscientização. Assim, podemos promover comportamentos de proteção mais consistentes, independentemente da idade ou da escolaridade.

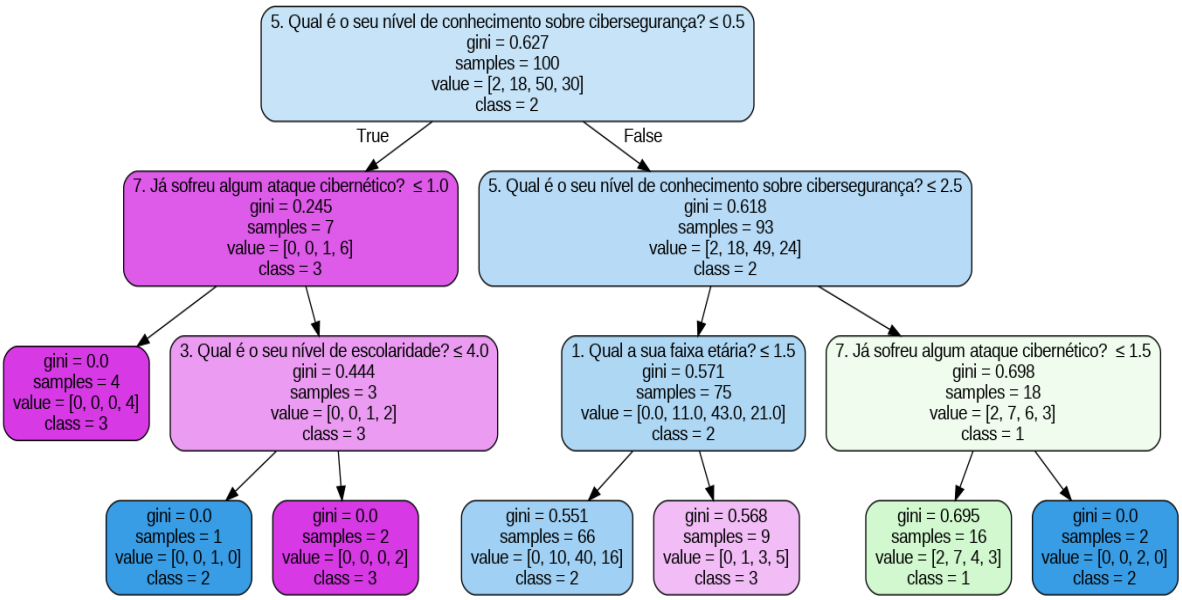

Figura 56: Árvore de decisão referente à utilização de antivírus / firewall.

Para avaliar o desempenho do modelo, foram utilizadas métricas de avaliação. A acurácia foi de 53,49%, o que significa que o modelo acertou cerca de metade das previsões; a precisão foi de 40,02%, indicando que, entre as previsões de usar antivírus ou firewall, aproximadamente 40% estavam corretas. O recall de 49,48% mostra que o modelo

conseguiu identificar quase metade dos participantes que realmente usam essas ferramentas e o F1-score de 42,59% mostra um equilíbrio moderado entre a precisão e o recall. A matriz de confusão indica que o modelo teve um desempenho adequado para uma amostra pequena e com classes desiguais, entretanto, o modelo ainda tem dificuldades em fazer previsões corretas de forma geral.

Esses números mostram que o modelo consegue detectar alguns padrões simples, mas, para melhorar os resultados, precisamos de mais respostas e também é importante que as respostas estejam mais equilibradas entre diferentes categorias.

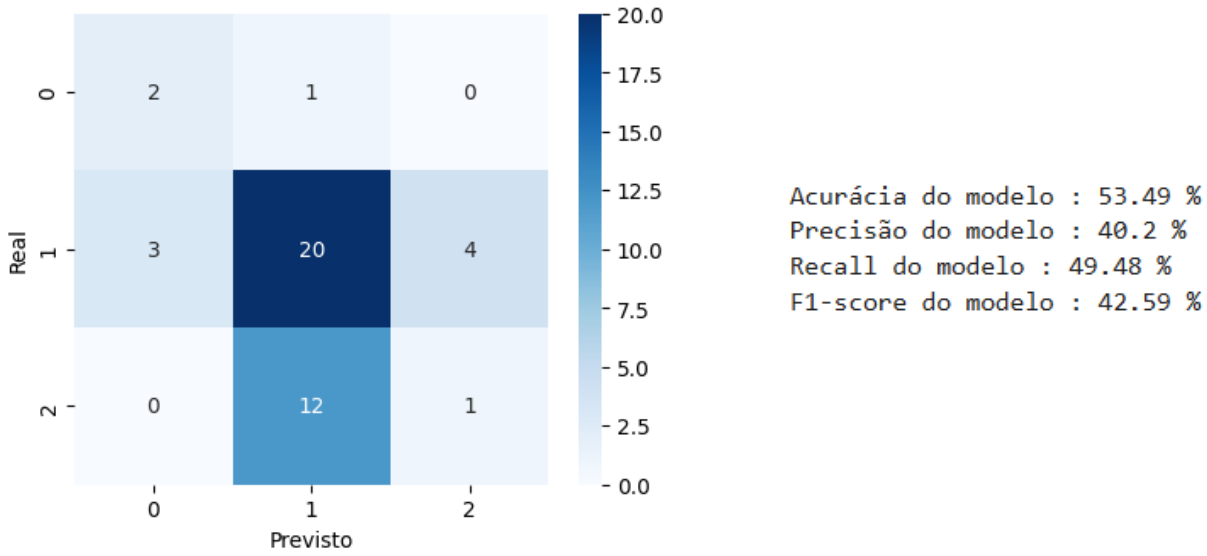

Figura 57: Matriz da confusão e métricas de avaliação Q6

Para a figura 58, podemos observar a árvore de decisão da questão Q7 "já sofreu algum ataque cibernético" cujo objetivo é identificar que variáveis explicam qual é a probabilidade de um utilizador ser alvo de ataque cibernético. Para este caso utilizaram-se 80% dos dados para treino e 20% para teste, e as variáveis explicativas foram: Faixa etária, sexo, grupo pertencente e uso de software/firewall. Neste caso, a variável-alvo mais significativa para prever quando ocorrem ataques cibernéticos é o uso de software antivírus/firewall. Isto indica que existe uma relação entre o uso ou não das ferramentas de proteção digital e experiências com incidentes de segurança na internet.

Nota-se que pessoas que não usam o antivírus ou firewall (<=1.5 True) têm mais chance de ter sido vítimas de ataques e esta constatação reforça a importância de adotar medidas de proteção que fazem diferença no que diz respeito à prevenção de ameaças. Entre aqueles que confirmaram usar algum tipo de software de proteção, o modelo apontou que

o grupo profissional e o sexo influenciam as chances de sofrer um ataque. Os participantes que pertencem ao grupo "profissional de TI" tendem a sofrer menos ataque, provavelmente porque têm mais conhecimento técnico e seguem práticas mais rígidas de segurança. Por outro lado, o sexo masculino mostrou um pouco mais de casos de ataques, o que pode estar relacionado ao fato de que eles usam mais plataformas e serviços digitais, embora essa diferença não seja estatisticamente significativa dentro da amostra analisada.

Com base na faixa etária, a análise indica que pessoas com menos de 35 anos têm uma leve tendência de sofrer mais ataques, talvez por estarem mais expostos online e usarem de forma excessiva as redes socias, e por outro lado, grupos com mais de 35 anos mostraram uma ocorrência de menores incidentes, o que pode estar ligado ao uso mais cuidadoso das tecnologias.

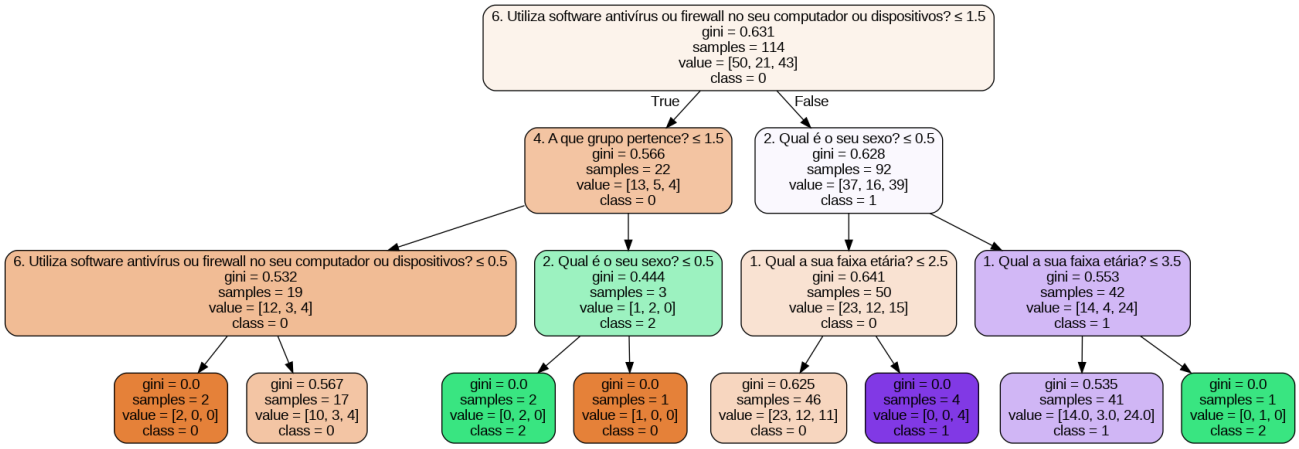

Figura 58: Árvore de decisão Q7

Quanto ao desempenho do modelo, a acurácia de 44,83% indica que acertou cerca de 45% dos casos, a precisão de 30,39%, recall de 37,62% e F1-score de 32,67% sugerem uma capacidade moderada de previsão, o que é esperado, dado o pequeno número de amostras e o carácter social e comportamental das variáveis. De modo geral, mesmo com limitações técnicas devido ao volume de dados, a análise permitiu entender o comportamento e perfis dos utilizadores. Os resultados reforçam que investir em formação em cibersegurança e usar softwares de proteção continua sendo fundamental para diminuir a vulnerabilidade digital.

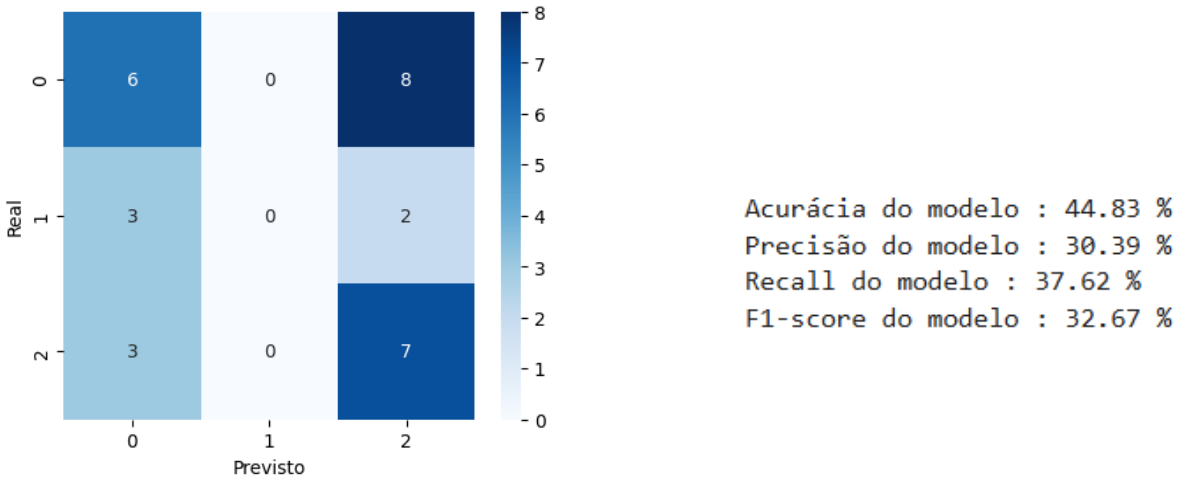

Figura 59: Matriz da confusão e métrica de avaliação Q7

A figura 60 representa a árvore de decisão da questão Q9 "Em termos de segurança, como se sente ao navegar na internet?", que procura entender como os utilizadores se sentem na internet em termos de segurança, e as variáveis explicativas que foram consideradas são: sexo, nível de escolaridade, grupo pertencente e o nível de conhecimento sobre cibersegurança. Os dados foram divididos em 30% teste e 70% treino. Neste caso, a variável "Qual é o seu sexo" é a mais relevante na divisão dos dados, mostrando que o gênero tem influência na percepção das pessoas sobre sua segurança digital.

Temos a ramificação esquerda (True) representa principalmente as participantes do gênero feminino, enquanto a da direita (False) inclui, maioritariamente, os do sexo masculino e os que não quiseram se identificar. De modo geral, percebe-se que as mulheres costumam sentir-se menos seguras ou apenas um pouco seguras ao navegar na internet, especialmente quando têm níveis de escolaridade mais baixos. Por outro lado, entre as pessoas com formação superior ou pós-graduação, há uma maior sensação de confiança, principalmente quando combinada com um conhecimento intermediário ou avançado sobre cibersegurança.

Entre os homens, a percepção de segurança está mais ligada ao nível de conhecimento sobre cibersegurança e ao grupo profissional. Quem trabalha em áreas ligadas à tecnologia ou demonstra maior familiaridade com práticas de segurança digital tende a se sentir seguro ou muito seguro ao usar a internet. Por outro lado, aqueles com menos contato com temas de cibersegurança percebem sua segurança online de forma mais neutra. De modo geral, a árvore de decisão indica que o nível de escolaridade e

o conhecimento sobre cibersegurança são fatores determinantes na forma como as pessoas avaliam sua segurança digital. Quanto mais conhecimento e formação, maior a sensação de proteção e confiança ao usar a internet.

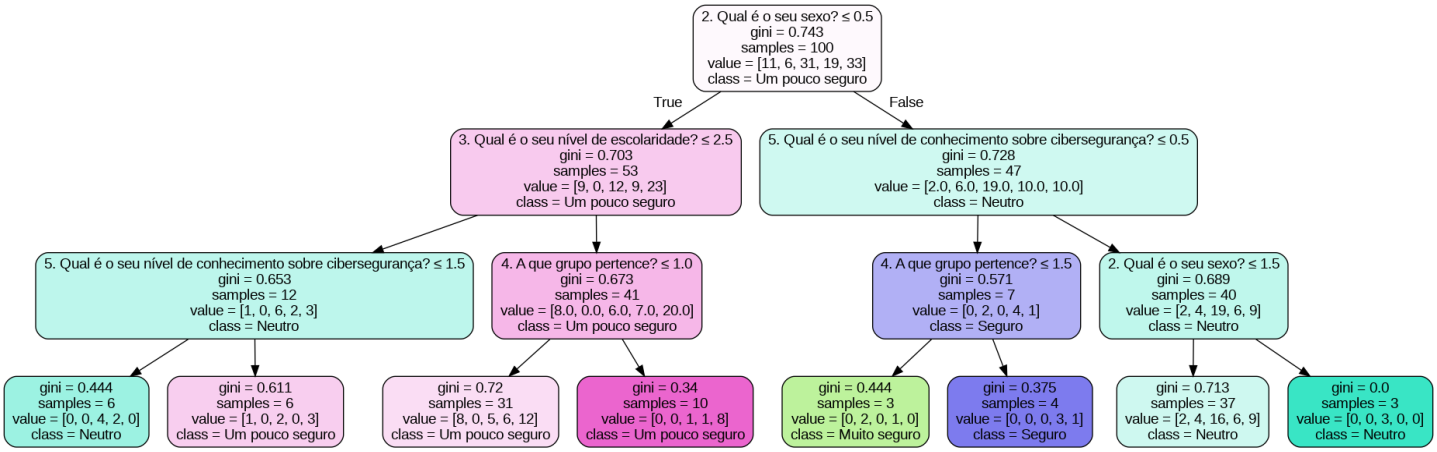

Figura 60: Arvore de decisão Q9

Relativamente ao desempenho do modelo, a acurácia de 39,53%, precisão de 17,02%, recall de 24,31% e F1-score de 20,03% indicam que, apesar de sua baixa capacidade preditiva, devido ao tamanho limitado da amostra e à diversidade das respostas, ele fornece uma análise interpretativa útil. Essa análise ajuda a identificar as variáveis que mais influenciam a percepção de segurança digital, contribuindo para uma compreensão melhor do comportamento dos usuários frente aos riscos cibernéticos.

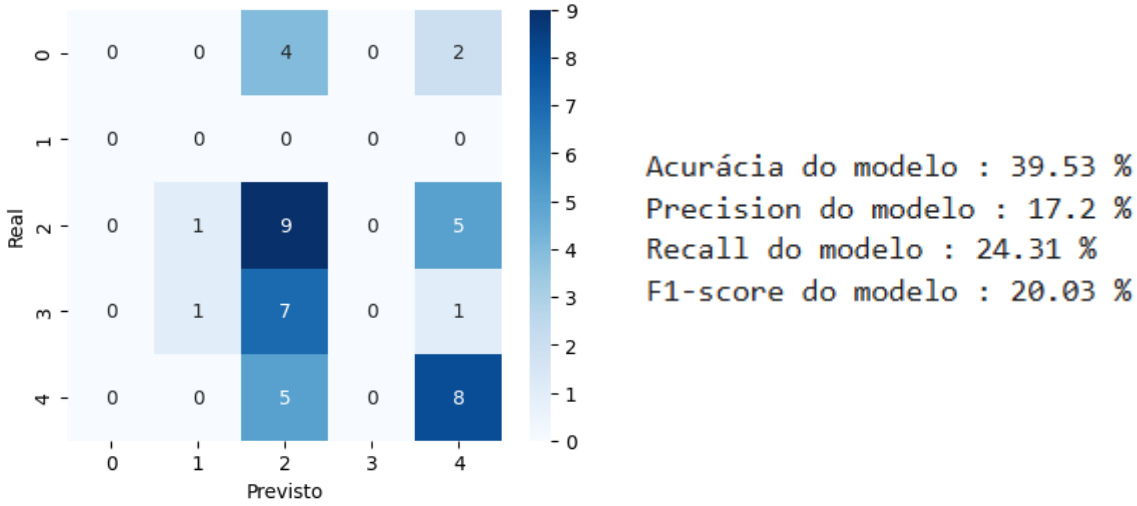

Figura 61: Matriz da confusão e métricas de avaliação Q9

Na figura 62, a árvore de decisão buscou entender quais são os fatores que mais influenciam a percepção dos participantes sobre a escassez de profissionais qualificados na área da cibersegurança, e as variáveis explicativas selecionadas foram: nível de escolaridade, grupo pertencente e conhecimento sobre cibersegurança. Neste caso, os dados foram utilizados: 80% para treino e 20% para teste. Podemos observar que neste caso, a variável "Qual é o seu nível de conhecimento?" foi a mais relevante na divisão dos dados.

O valor de corte definido pelo modelo foi <= 2.5 que separa os participantes que possuem conhecimento (avançado, básico e intermédio) dos que não possuem nenhum conhecimento em cibersegurança. Os participantes que afirmaram ter um conhecimento básico ou intermediário foram os que mais perceberam a falta de profissionais qualificados, demonstrando uma visão mais crítica sobre a situação atual do setor. Esse resultado faz sentido, pois pessoas com algum grau de familiaridade na área compreendem melhor as exigências técnicas e a escassez de especialistas que o mercado enfrenta. No entanto, para pessoas com baixo nível de escolaridade ou conhecimento limitado sobre cibersegurança, a resposta mais comum foi "Não sei dizer", indicando menor consciência sobre o cenário profissional na área. Já entre aqueles com formação mais avançada (licenciatura, mestrado ou pós-graduação), há maior concordância de que, de facto, há uma carência de profissionais, refletindo uma compreensão mais sólida da realidade do mercado.

A variável "A que grupo pertence" também influenciou. Profissionais de TI e estudantes de áreas tecnológicas tendem a reconhecer a escassez de especialistas, enquanto utilizadores comuns da internet ou indivíduos de áreas não técnicas costumam ficar mais indecisos ou neutros em suas respostas. Resumindo, os resultados indicam que a percepção sobre a falta de profissionais na cibersegurança está fortemente relacionada ao nível de conhecimento técnico e ao contexto de atuação dos respondentes. Quanto mais contato os indivíduos têm com temas ou práticas da área, maior a consciência da escassez de especialistas, o que está alinhado com relatórios internacionais e com a realidade global do setor.

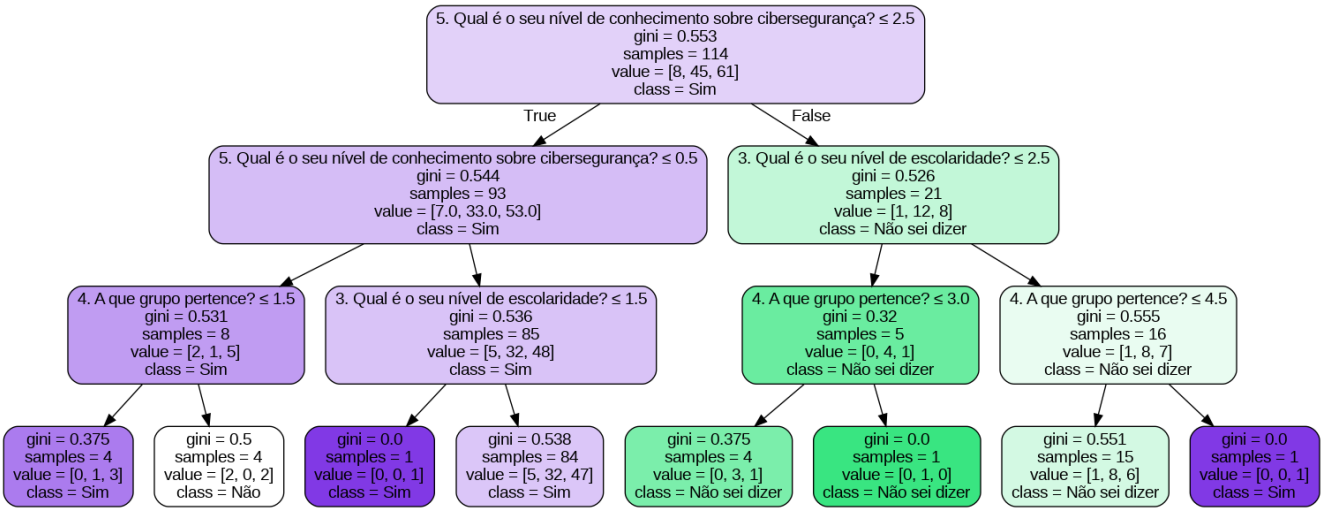

Figura 62: Árvore de decisão Q40

Relativamente ao desempenho do modelo, ele atingiu uma acurácia de 65,52%, o que indica uma boa capacidade de previsão, especialmente considerando o tamanho limitado da amostra. As métricas de precisão (47,22%) e recall (42,13%) mostram que o modelo conseguiu captar tendências reais nos dados, embora ainda existam variações naturais entre os grupos analisados.

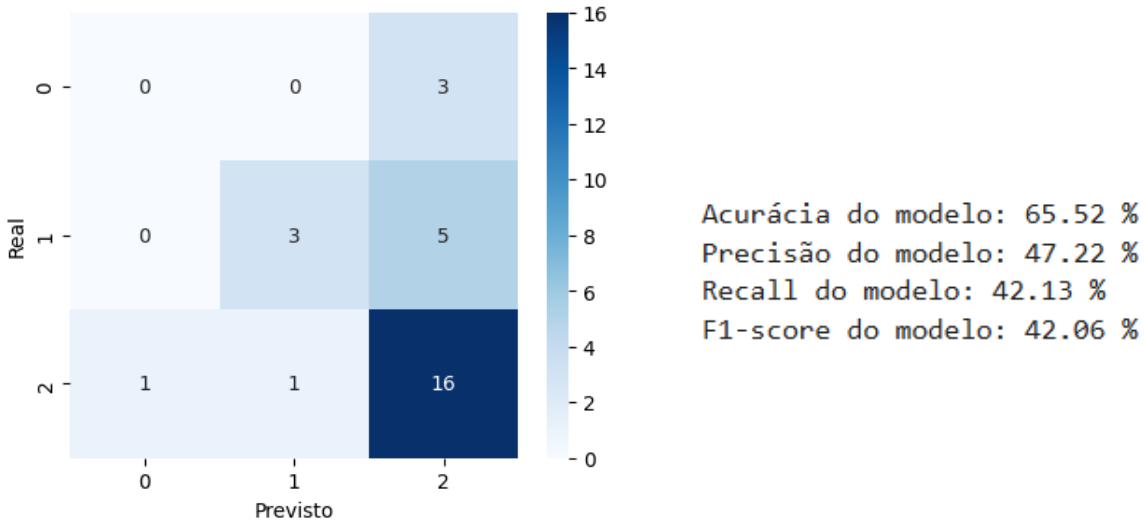

Figura 63: Matriz da confusão e métrica de avaliação Q40.

Em resumo, o uso da árvore de decisão ajudou a identificar que o nível de conhecimento sobre segurança cibernética, a formação acadêmica e o grupo profissional são os principais fatores que influenciam a forma como os participantes percebem e se comportam em relação à segurança digital. Embora algumas previsões tenham apresentado menor precisão devido ao pequeno tamanho da amostra, os resultados gerais revelaram padrões significativos, mostrando que um maior conhecimento geralmente se

correlaciona com práticas mais seguras e uma percepção mais consciente dos riscos cibernéticos.

Concluindo, o uso da Árvore de Decisão ajudou a identificar que o nível de conhecimento sobre cibersegurança, a escolaridade e o grupo profissional são os principais fatores que influenciam as perceções e comportamentos dos participantes em relação à segurança digital. Mesmo que algumas previsões tenham tido baixa precisão devido ao número limitado de participantes, os resultados mostraram padrões importantes, sugerindo que quanto maior o conhecimento, mais provável é que as pessoas adotem práticas mais seguras e tenham uma compreensão mais clara dos riscos cibernéticos. Esta conclusão se alinha com o relatório do NIST, onde sublinham a importância de formações aos utilizadores, como maneira de se sentirem mais capazes de lidar com riscos cibernéticos [66].

Capítulo 5 Conclusões

Esta dissertação teve como objetivo central analisar o cenário atual da cibersegurança, identificar as principais tendências que estão surgindo e compreender os principais desafios que as organizações enfrentam ao tentar implementar estratégias eficazes de proteção digital. Para isso, foi adotada uma abordagem mista que combina revisão bibliográfica com um levantamento através de questionários e posteriormente, a integração de técnicas de IA baseadas no aprendizado de máquina (ML), especificamente o algoritmo de Árvore de Decisão para a análise preditiva da amostra recolhida.

Os resultados mostram que, apesar do aumento na conscientização sobre a importância da cibersegurança, ainda existe uma grande lacuna no conhecimento teórico e na aplicação prática de medidas de proteção, especialmente entre os utilizadores comuns. Atitudes inseguras, como o desconhecimento de ameaças como o phishing, o uso de senhas fracas ou inadequadas e pouca familiaridade com o RGPD, continuam sendo comuns e evidenciam a necessidade urgente de investir em educação digital. Além disso, a análise revelou que o nível de conhecimento técnico, a escolaridade e o grupo profissional influenciam bastante como as pessoas lidam com a adoção de práticas de segurança, algo que foi confirmado pela análise da Árvore de Decisão.

A utilização da IA neste estudo ajudou a identificar padrões importantes e fatores que mais afetam a percepção e o comportamento dos participantes, mostrando que pessoas com maior nível de alfabetização digital e experiência prévia em cibersegurança tendem a seguir práticas mais seguras. Apesar de algumas limitações, como um tamanho de amostra menor, o uso de aprendizado de máquina mostrou ser útil para evidenciar o potencial da IA como ferramenta de apoio na análise e previsão de comportamentos relacionados à segurança digital.

Resumindo, melhorar a cibersegurança exige mais do que apenas soluções tecnológicas: é preciso desenvolver competências humanas, investir em formação contínua e criar políticas que envolvam pessoas, processos e tecnologia. É fundamental que escolas, empresas e órgãos públicos promovam a educação digital e incentivem o uso responsável e seguro da tecnologia.

Por fim, recomenda-se que futuras pesquisas explorem outras técnicas de aprendizado de máquina, como Random Forest ou Redes Neuronais, usando amostras maiores e mais variadas, para melhorar a capacidade preditiva desses modelos. Além disso, é importante aprofundar os estudos sobre a eficácia de tecnologias emergentes, como IA, Blockchain e Computação Quântica, no fortalecimento da segurança digital e na redução das vulnerabilidades humanas e organizacionais. Essas linhas de pesquisa podem complementar os resultados deste trabalho e ajudar a construir uma sociedade digital mais segura, resistente e consciente.

Bibliografia

[1] Kaspersky, “What is cyber security?”, Kaspersky, 2023. [Online]. Available: https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security. [Accessed: Jan. 6, 2025].

[2] L. Borges and M. Nogueira, "Introdução à Ciência de Dados em Cibersegurança," Anais Estendidos do XXXVIII Simpósio Brasileiro de Bancos de Dados, Belo Horizonte, MG, 2023, pp. 183-188, doi: 10.5753/sbbd_estendido.2023.25634.

[3] D. Jerbi, "Beyond Firewalls: Navigating the Jungle of Emerging Cybersecurity Trends," *J Curr Trends Comp Sci Res*, vol. 2, no. 2, pp. 191-195, 2023.

[4] D. Brinkman, “Principles of cybersecurity,” in *Principles of Cybersecurity*, 2021, pp. 93–127. [Online]. Available: https://doi.org/10.1002/9781119070740.ch3. [Accessed: Fev. 10, 2025].

[5] S. de V. Casimiro, "Cibersegurança – Aspetos Legais", Comunicação oral apresentada na Segurança da Informação e Gestão do Risco na 3a Plataforma, Lisboa, 2014. Available: http://www.afceaportugal.pt/2014/eventos/12h10-Vieira_de_Almeida__Associados_s.pdf.

[6] ITU, “Recommendation ITU-T X.1205. Series X: data networks, open system communications and security,” 2008. [Online]. Available: https://www.itu.int/rec/T-REC-X.1205-200804-I. [Accessed: Feb. 10, 2025].

[7] A. Schaeffer-Filho, “Segurança cibernética 2030: experiências, desafios e oportunidades,” 2023, pp. 141–166. [Online]. Available: https://doi.org/10.5753/sbc.13058.5.7. [Accessed: Fev. 10, 2025].

[8] B. Naqvi and C. Ardito, "Coping with changing contexts: a healthcare security perspective," *pp. 139-146*, 2022. [Online]. Available: https://doi.org/10.1007/978-3-030-98388-8_13. [Accessed: Fev. 11, 2025].

[9] K. K. R. Choo, "The cyber threat landscape: Challenges and future research directions," *Computers & security*, vol. 30, no. 8, pp. 719-731, 2011.

[10] Abrahams et al., "Cybersecurity awareness and education programs: A review of employee engagement and accountability," *Computer science & IT research journal*, vol. 5, no. 1, 2024, doi: 10.51594/csitrj.v5i1.708.

[11] G. Mazzarolo e A. D. Jurcut, "Insider threats in Cyber Security: The enemy within the gates," *arXiv preprint*, 2019. [Online]. Disponível em: https://arxiv.org/abs/1911.09575. [Accessed: 18 abr. 2025].

[12] J. Chen, C. Su, K.-H. Yeh e M. Yung, "Special Issue on Advanced Persistent Threat," *Future Generation Computer Systems*, vol. 79, parte 1, pp. 243-246, 2018. doi: 10.1016/j.future.2017.11.005.

[13] J. Pande, Introduction to Cyber Security. [Online]. Available: https://uou.ac.in/sites/default/files/slm/Introduction-cyber-security.pdf. [Accessed: 17 Fev. 2025].

[14] Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), Cartilha de Segurança para Internet. [Online]. Available: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. [Accessed: 11 Fev. 2025].

[15] J. Joseph Bloun, "Adaptive rule-based malware detection employing learning classifier systems," *Thesis- Master of science in computer science*, Missouri University of Science and Technology, 2011.

[16] Candido et al., "Segurança da informação com foco na propagação iminente de ransomware nas corporações," *Revista foco*, vol. 16, no. 5, 2023, doi: 10.54751/revistafoco.v16n5-024.

[17] Fornasier et al., "Ransomware e cibersegurança: a informação ameaçada por ataques a dados," *Revista thesis juris*, vol. 9, no. 1, 2020, doi: 10.5585/rtj.v9i1.16739.

[18] J. Ferdous, R. Islam, A. Mahboubi and M. Z. Islam, "A Review of State-of-the-Art Malware Attack Trends and Defense Mechanisms," in *IEEE Access*, vol. 11, pp. 121118-121141, 2023, doi: 10.1109/ACCESS.2023.3328351.

[19] U. Zahoora, A. Khan, M. Rajarajan et al., "Ransomware detection using deep learning based unsupervised feature extraction and a cost sensitive Pareto Ensemble classifier," *Sci Rep*, vol. 12, p. 15647, 2022. Available: https://doi.org/10.1038/s41598-022-19443-7.

[20] Filho and Freitas, "Ransomware: origens, consequências e prevenção," *Studies in engineering and exact sciences*, vol. 4, no. 1, 2023, doi: 10.54021/seesv4n1-026.

[21] P. Leitão, "Internet das Coisas: Part 1 - Introduction and Basic Concepts," *Escola de Tecnologia e Gestão*, Instituto Politécnico de Bragança (IPB), 2023.

[22] ENISA, "ENISA Threat Landscape 2022," Oct. 2022. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022. [Accessed: 12 Mar. 2025].

[23] *Cyber Resilience Act 2022: A silver bullet for cybersecurity of IoT devices or a shot in the dark?* [Online]. Available: iot devices.pdf.

[24] E. N. de V. Gregório, F. A. A. Lins, and O. de O. Nóbrega, "Connectivity Transparency of Blockchain Services in IoT Systems: a proposed architecture," *RSD*, vol. 10, no. 12, p. e239101220273, Sep. 2021.

[25] T. A. Farias Júnior, "A utilização do blockchain para: um mapeamento sistemático," *Rev. Contemp.*, vol. 3, no. 10, pp. 18433–18448, Oct. 2023.

[26] *IoT Analytics*, "Number of Connected IoT Devices," *IoT Analytics*, 2025. [Online]. Disponível em: https://iot-analytics.com/number-connected-iot-devices/. [Accessed: 16 mar. 2025].

[27] Splashtop, "What is IoT?" [Online]. Available: https://www.splashtop.com/pt/blog/what-is-iot?srsltid=AfmBOooBQk7aobZKzxlph-skrcsq3dItpXwlkgE6WvbS5-CM_05NlWw2. [Accessed: 13 abr. 2023].

[28] N. M. Karie, N. M. Sahri, and P. Haskell-Dowland, "IoT threat detection advances, challenges and future directions," *2020 Workshop on Emerging Technologies for Security in IoT (ETSecIoT)*, Sydney, NSW, Australia, 2020, pp. 22-29, doi: 10.1109/ETSecIoT50046.2020.00009.

[29] Socradar, "Common IoT attacks that compromise security," [Online]. Available: https://socradar.io/common-iot-attacks-that-compromise-security/.

[30] *Navigating the Cybersecurity Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments*, [Online].

[31] H. U. Salvi and S. S. Surve, “Emerging trends and future prospects of cybersecurity technologies: Addressing challenges and opportunities,” *Int. J. Sci. Res. Sci. Technol.*, vol. 10, no. 4, pp. 399-406, Jul.-Aug. 2023. [Online]. Available: https://doi.org/10.32628/IJSRST52310432.

[32] *Correio Negócios*, “A revolução da computação quântica e a cibersegurança: desafios e oportunidades,” 2025, [Online]. Available: https://www.correionegocios.pt/2025/02/13/a-revolucao-da-computacao-quantica-e-a-ciberseguranca-desafios-e-oportunidades/.

[33] G. da S. Araújo, C. C. Favarato, A. J. R. Ambrozio, M. de P. Pompermayer, and J. S. dos Santos, “Além do horizonte digital: o fascínio da computação quântica,” *ARE*, vol. 7, no. 2, pp. 8015–8030, Feb. 2025, doi: 10.56238/arev7n2-202.

[34] Splashtop, “What is IoT?” [Online]. Available: https://www.splashtop.com/pt/blog/what-is-iot?srsltid=AfmBOooBQk7aobZKzxlph-skrcsq3dIt. [Accessed: 11 Mai. 2025].

pXwlkgE6WvbS5-CM_05NlWw2.

[35] *Samsic*, “A importância da cibersegurança nas organizações,” [Online]. Available: https://www.samsic.pt/blog/a-importancia-da-ciberseguranca-nas-organizacoes/.

[36] M. Warkentin and R. Willison, “Behavioral and policy issues in information systems security: The insider threat,” *Eur. J. Inf. Syst.*, vol. 18, no. 2, pp. 101-105, 2009.

[37] *CNCS*, “Relatório sobre riscos e conflitos 2024,” [Online]. Available: https://www.cncs.gov.pt/docs/rel-riscosconflitos2024-obcibercncs.pdf. [Accessed: 11 Mai. 2025].

[38] *CNCS*, “Guia de gestão dos riscos 11,” [Online]. Available: https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf. [Accessed: 11 Mai. 2025].

[39] *LinkedIn*, “Cibersegurança nas corporações: desafios e estratégias,” [Online]. Available: https://www.linkedin.com/pulse/ciberseguran%C3%A7a-nas-corpora%C3%A7%C3%B5es-desafios-e-estrat%C3%A9gias-keeggo-sb50f/. [Accessed: 17 Mai. 2025].

[40] *Relações Exteriores*, “Cibersegurança e relações internacionais,” [Online]. Available: https://relacoesexteriores.com.br/ciberseguranca-relacoes-internacionais/. [Accessed: 17 Mai. 2025].

[41] *Business-IT*, “Falta de profissionais de cibersegurança vai continuar a aumentar em 2024,” [Online]. Available: https://business-it.pt/2024/04/01/falta-de-profissionais-de-ciberseguranca-vai-continuar-a-aumentar-em-2024/. [Accessed: 22 Mai. 2025].

[42] *ITSecurity*, “Escassez de competências de cibersegurança leva a falhas de segurança,” [Online]. Available: https://www.itsecurity.pt/news/analysis/escassez-de-competencias-de-ciberseguranca-leva-a-falhas-de-seguranca. [Accessed: 9 Jun. 2025].

[43] *IGFEJ*, “Regulamento Geral de Proteção de Dados (RGPD),” [Online]. Available: https://igfej.justica.gov.pt/Sobre-o-IGFEJ/Regulamento-Geral-de-Protecao-de-Dados-RGPD. [Accessed: 9 Jun. 2025].

[44] *RGPD*, “Conformidade com o RGPD,” [Online]. Available: https://rgpd.com/pt-pt/conformidade/#elementor-toc__heading-anchor-0. [Accessed: 9 Jun. 2025].

[45] *IT Security*, "Estudo revela lacunas na cibersegurança das empresas europeias em relação à IA," *IT Security*, 2025. [Online]. Disponível em: https://www.itsecurity.pt/news/analysis/estudo-revela-lacunas-na-ciberseguranca-das-empresas-europeias-em-relacao-a-ia. [Accessed: 15 Jun. 2025].

[46] *T. S. AlSalem, M. A. Almaiah, e A. Lutfi,* "Cybersecurity Risk Analysis in the IoT: A Systematic Review," *Electronics*, vol. 12, nº 18, p. 3958, 2023. [Online]. Disponível em: https://doi.org/10.3390/electronics12183958.

[47] *RiskXchange*, "IT security gaps," *RiskXchange*, 2025. [Online]. Disponível em: https://riskxchange.co/1006837/it-security-gaps/. [Accessed: 15 Jun. 2025].

[48] ENISA, *Threat Landscape 2023*, European Union Agency for Cybersecurity, 2023. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023. Accessed: 6 jul. 2025].

[49] ENISA, “ENISA Threat Landscape 2022,” Oct. 2022. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022. [Accessed: 15-Ago-2025].

[50] 3structure, “Blockchain na segurança cibernética: quais os impactos da relação?”, *3structure*, 23 nov. 2023. [Online]. Disponível em: https://3structure.com.br/blockchain-na-seguranca-cibernetica-quais-os-impactos-da-relacao/. [Accessed: 6 Jul. 2025].

[51] R. Mendes, “IA: uma aliada da cibersegurança ou um desafio a ser gerido?”, *ECO – Economia Online*, 01 abr. 2024. [Online]. Disponível em: https://eco.sapo.pt/opiniao/ia-uma-aliada-da-ciberseguranca-ou-um-desafio-a-ser-gerido/. [Accessed: 10 Jul. 2025].

[52] “A A IMPORTÂNCIA DAS BLOCKCHAINS NA SEGURANÇA DE ATIVOS DIGITAIS”, *REMUNOM*, vol. 11, no. 1, Oct. 2024, doi: 10.61164/rmnm.v11i1.3010. Accessed: 16 jul. 2025].

[53] Infonova, “Armazenamento em nuvem: vantagens e desvantagens,” *Infonova*, 28-Jul-2022. [Online]. Available: https://infonova.com.br/armazenamento-em-nuvem-vantagens-e-desvantagens/. Accessed: 16 jul. 2025].

[54] Check Point Software Technologies, “What is cloud encryption?”, *Check Point – Cyber Hub*. [Online]. Available: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/what-is-cloud-encryption/ . [Accessed: 15 Ago. 2025].

[55] All Tech Magazine, “Two-factor authentication & cloud cybersecurity” (How-to article), *All Tech Magazine – How To*. [Online]. Available: https://alltechmagazine.com/how-to/two-factor-authentication-cybersecurity-cloud/ . [Accessed: 15 Ago. 2025].

[56] G. da S. . Araújo, C. C. . Favarato, A. J. R. . Ambrozio, M. de P. . Pompermayer, and J. S. . dos Santos, “BEYOND THE DIGITAL HORIZON: THE ALLURE OF QUANTUM COMPUTING”, *ARE*, vol. 7, no. 2, pp. 8015–8030, Feb. 2025, doi: 10.56238/arev7n2-202.

[57] L. P. de Souza, *O papel da cibersegurança na era digital: desafios, tendências e soluções globais: The role of cybersecurity in the digital age: global challenges, trends and solutions*, RCMOS - Revista Científica Multidisciplinar O Saber, vol. 1, no. 2, 2024. [Online]. Available: https://doi.org/10.51473/rcmos.v1i1.2025.1036

[58] Financial Times, “Why supplier security certifications matter” (artigo sobre certificações e confiança em fornecedores) , *Financial Times*. [Online]. Available: https://www.ft.com/content/8a79ab25-c902-4110-bcb8-be2fd422f6bf . [Accessed: 15 Ago. 2025].

[59] MSCyber, “Por que os testes de penetração são cruciais para a segurança de sua empresa?”, *MSCyber*, 27-Jun-2024. [Online]. Available: https://mscyber.co/pt/por-que-os-testes-de-penetracao-sao-cruciais-para-a-seguranca-de-sua-empresa/. [Accessed: 15 Ago. 2025].

[60] IT Insight, "As empresas devem preparar-se para a era quântica também do ponto de vista da segurança," IT Insight, 2023. [Online]. Available: https://www.itinsight.pt/news/seguranca/as-empresas-devem-preparar-se-para-a-era-quantica-tambem-do-ponto-de-vista-da-seguranca. [Accessed: 15 Ago. 2025].

[61] P. Jain, R. Kumar, V. G. Nair, and F. A. Yusuf, “Cloud Security Challenges and Solutions: A Review of Current Best Practices,” *International Journal of Multidisciplinary Research and Growth Evaluation*, vol. 6, no. 1, pp. 129–137, Jan.–Feb. 2025. [Online]. Available: https://www.researchgate.net/publication/387558426

[62] Kaspersky, “Cloud Security: Issues, Challenges and Best Practices,” *Kaspersky Resource Center*, 2024. [Online]. Available: https://www.kaspersky.com.br/resource-center/preemptive-safety/cloud-security-issues-challenges

[63] D. M. Silva, "Computação em Nuvem: Uma análise da adoção de medidas de segurança em empresas brasileiras," *Universidade Federal Rural do Semi-Árido (UFERSA)*, 2022. [Online]. Disponível em: https://repositorio.ufersa.edu.br/server/api/core/bitstreams/d1f7ad01-4c9c-43fc-b5ed-044288d0d866/content

[64] IBM Security, “Zero Trust: A framework for securing modern enterprises,” *IBM White Paper*, 2022. [Online]. Disponível em: https://www.ibm.com/security/zero-trust

[65] IBM, *Cost of a Data Breach Report 2023*. [Online]. Available: https://www.ibm.com/reports/data-breach

[66] NIST. *SP 800*-53 Rev. 5 – Security and Privacy Controls for Information Systems and Organizations. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final. Accessed: 20-Ago-2025.

[67] Alura, "Árvores de decisão: como funcionam e quando usar," *Alura*, 2025. [Online]. Available: https://www.alura.com.br/artigos/arvores-de-decisao. [Accessed: Set. 28, 2025].

[68] Sigmoidal, "Entendendo as Árvores de Decisão em Machine Learning," *Sigmoidal.ai*, 2025. [Online]. Available: https://sigmoidal.ai/entendendo-as-arvores-de-decisao-em-machine-learning/. [Accessed: Oct. 5, 2025].

[69] I.A. com Café, "Entendendo Label Encoding em Python," *IA com Café*, 2025. [Online]. Available: https://iacomcafe.com.br/entendendo-label-encoding-python/#google_vignette. [Accessed: Oct. 5, 2025].

[70] E. Terumi, "Árvore de decisão: como tomar decisões baseadas em dados," *Substack by Elisa Terumi*, 2025. [Online]. Available: https://elisaterumi.substack.com/p/arvore-de-decisao-como-tomar-decisoes. [Accessed: Oct. 11, 2025].

[71] M. Filho, "As métricas mais populares para avaliar modelos de Machine Learning," *MarioFilho.com*, 2025. [Online]. Available: https://mariofilho.com/as-metricas-mais-populares-para-avaliar-modelos-de-machine-learning/. [Accessed: Oct. 11, 2025].

[72] M. Filho, "O que é acurácia em Machine Learning," *MarioFilho.com*, 2025. [Online]. Available: https://mariofilho.com/o-que-e-acuracia-em-machine-learning/. [Accessed: Oct. 11, 2025].

Anexo A – Questionário Online

Metodologia Quantitativa – Inquérito online

Abrangido para amostras – Estudantes, Empresas, Profissionais de TI, Utilizadores de internet;

Secção 1 – Perfil do Respondente

1. Qual a sua faixa etária?
    a. Menos de 18 anos
    b. 18-25 anos
    c. 26-35 anos
    d. 36-50 anos
    e. Mais de 50 anos
2. Qual é o seu sexo?
    a. Feminino
    b. Masculino
    c. Não sei
3. Qual é o seu nível de escolaridade?
    a. Ensino básico
    b. Ensino secundário
    c. Licenciatura
    d. Pós-graduação/Mestrado
    e. Doutoramento
    f. Não quero indicar
4. A que grupo pertence?
    a. Estudante
    b. Utilizador da internet
    c. Representante de uma empresa
    d. Profissional de TI
    e. Outro:
5. Qual é o seu nível de conhecimento sobre cibersegurança?

a. Nenhum

b. Básico

c. Intermédio

d. Avançado

6. Utiliza software antivírus ou firewall no seu computador ou dispositivo?

a) Sim, em todos os dispositivos
b) Sim, apenas no computador
c) Não, não uso
d) Não sei o que é antivírus ou firewall

Secção 2 – Perceção e Experiência com Cibersegurança

7. Já sofreu algum ataque cibernético?

a. Sim

b. Não

c. Não sei

8. Se respondeu "Sim", que tipo de ataque sofreu?

d. Phishing

e. Ransomware

f. Roubo de credenciais

g. Ataque a dispositivo IoT

h. Outra

9. Em termos de segurança, como se sente ao navegar na internet?
   a. Muito inseguro
   b. Um pouco inseguro
   c. Neutro
   d. Seguro
   e. Muito seguro

10. Que dispositivos acha mais vulneráveis a ataques cibernéticos?
    a. Computadores
    b. Smartphones
    c. Dispositivos IoT (ex: câmaras, smart TVs)
    d. Infraestruturas empresariais (servidores, redes internas)

11. Na sua opinião, qual destas ameaças é mais preocupante atualmente?
    a. Phishing
    b. Ransomware
    c. Ataques a dispositivos IoT
    d. Ataques de Negação de Serviço (DDoS)
    e. Não sei
    f. Outra

12. Como avalia a preparação das pessoas para se protegerem contra ciberataques?
    a. Muito despreparadas
    b. Pouco preparadas
    c. Relativamente preparadas
    d. Bem preparadas

13. Como classifica a proteção da sua empresa/organização contra ciberataques?
    a. Muito mal preparada
    b. Pouco preparada
    c. Bem preparada
    d. Extremamente preparada
    e. Não trabalho em uma organização

14. Com que frequência atualiza as suas palavras-passe?
    a. A cada 3 meses

b. A cada 6 meses

c. Apenas quando me é solicitado

d. Nunca

15. Que impacto um ataque cibernético poderia ter na sua vida/trabalho?

a. Perda de dados pessoais ou financeiros

b. Roubo de identidade

c. Perda de acesso a serviços essenciais

d. Danos à reputação pessoal/profissional

e. Nenhum impacto relevante

16. O que pode ser considerado como o maior desafio na cibersegurança atualmente?

a. Falta de conhecimento dos utilizadores
b. Falta de investimento das empresas
c. Falta de regulamentação eficaz
d. Falta de profissionais na área
e. Crescimento das novas tecnologias sem proteção adequada

17. Trabalha diretamente com segurança da informação ou administração de sistemas em uma empresa?

a) Sim
b) Não

Secção 3 – Tecnologia e Tendências Emergentes – Para Utilizadores da internet e os Estudantes

18. Já ouviu falar sobre a utilização de Inteligência Artificial na cibersegurança?

a. Sim, tenho um bom entendimento

b. Sim, mas tenho um entendimento básico

c. Não

19. Acha que a Inteligência Artificial será mais usada para ataques ou para defesa na cibersegurança?
    a. Maioritariamente para ataques
    b. Maioritariamente para defesas
    c. Ambos em igual proporção
    d. Não sei dizer

20. Já ouviu falar sobre Blockchain? Se sim, acha que pode ser uma solução eficaz para segurança digital?
    1. Sim
    2. Não
    3. Não sei dizer

21. A internet das coisas (IoT) refere-se à conexão de dispositivos cotidianos à internet, como smart TVs, assistentes virtuais e eletrodomésticos inteligentes. Como avalia o impacto da IoT na cibersegurança?
    a) Traz mais benefícios do que riscos
    b) Traz mais riscos do que benefícios
    c) Depende da implementação
    d) Não sei diz

22. Utiliza serviços de armazenamento na nuvem para guardar ficheiros ou dados importantes?
    a) Sim, regularmente
    b) Sim, ocasionalmente
    c) Não, evito usar armazenamento na nuvem
    d) Nãos sei dizer

23. Confia na segurança dos serviços de armazenamento na nuvem (Google Drive, OneDrive, Dropbox, etc.)
    a) Sim, confio totalmente
    b) Sim, mas com alguma precaução
    c) Não confio muito

d) Não confio nada

24. Quais medidas considera mais eficazes para proteger dados armazenados na nuvem? *(Escolha até 2 opções)*

    a) Encriptação dos dados antes de os armazenar
    b) Utilização de autenticação multifator (2FA)
    c) Escolha de fornecedores com certificação de segurança
    d) Evitar armazenar dados sensíveis na nuvem

Secção 3 – Tecnologia e Tendências Emergentes – Para empresas e profissionais TI

25. Já ouviu falar sobre Computação Quântica aplicada à cibersegurança?

    a) Sim, e compreendo o seu impacto na segurança digital
    b) Sim, mas não sei muito sobre isso
    c) Não

26. Considera que a Computação Quântica representa um maior risco ou uma solução para a cibersegurança?

    a) Será uma solução para reforçar a segurança
    b) Será um risco, pois pode quebrar sistemas de criptografia atuais
    c) Ambas as opções, pois tanto pode proteger como ameaçar
    d) Não sei dizer

27. Acha que as empresas estão preparadas para se defender contra ataques cibernéticos que utilizam tecnologias emergentes (exemplo: IA para automatizar ataques)?

    a) Sim
    b) Não
    c) Não sei dizer

28. A sua empresa utiliza alguma tecnologia emergentes (IA, Blockchain, IoT) para reforçar a cibersegurança?

    a) Sim
    b) Não
    c) Não sei dizer

29. A sua empresa realiza testes regulares de penetração para identificar vulnerabilidades?

    a) Sim, mensalmente
    b) Sim, algumas vezes por ano
    c) Apenas quando existem atualizações importantes
    d) Não fazemos testes de penetração

30. Acha que as empresas devem começar a preparar-se para a era da Computação Quântica?

    a) Sim, é essencial começar já a desenvolver sistemas de criptografia resistentes a quântica
    b) Sim, mas ainda estamos longe de ver um impacto real
    c) Não, é demasiado cedo para isso
    d) Não sei dizer

31. Acha que as empresas estão preparadas para lidar com ataques a serviços na nuvem?

    a) Sim, estão bem preparadas
    b) Algumas estão preparadas, outras não
    c) Não, a maioria ainda tem falhas de segurança
    d) Não sei dizer

32. Que medidas adota para a segurança na nuvem?

    a) Zero trust
    b) Encriptação
    c) Firewalls
    d) Auditorias
    e) Nenhuma
    f) O uso de VPN

33. A sua empresa já implementou Inteligência Artificial para a deteção de ameaças cibernéticas?

    a) Sim
    b) Não

34. Qual destas tecnologias acha que terá maior impacto na cibersegurança nos próximos anos?

    a) Inteligência Artificial
    b) Blockchain
    c) Computação Quântica
    d) Segurança na Nuvem
    e) Internet das Coisas

35. Na sua opinião, qual é o impacto mais significativo de um ataque cibernético em uma pequena empresa?

    a) Perda financeira
    b) Danos á reputação
    c) Interrupção das operações
    d) Perda de dados sensíveis

Secção 4 – medidas de segurança e Regulamentação

36. Está familiarizado com alguma regulamentação de segurança de dados, como o RGPD (Regulamento Geral de Proteção de Dados)?

    a) Sim, estou muito familiarizado
    b) Sim, mas pouco familiarizado
    c) Não

37. A sua organização segue as normas do Regulamento Geral de Proteção de Dados (RGPD)?

    a) Sim
    b) Não
    c) Não sei dizer
    d) Não aplicado

38. Considera que o RGPD tem sido eficaz na proteção dos dados dos utilizadores?

    a) Sim, protege bem os dados
    b) Sim, mas ainda há falhas
    c) Não, é pouco eficaz
    d) Não sei dizer

39. Já recebeu algum alerta ou notificação sobre um possível ataque cibernético na sua conta pessoal ou profissional?

    a. Sim, e tomei medidas para a minha proteção
    b. Sim, mas não fiz nada
    c. Não

40. Acha que há falta de profissionais qualificados em cibersegurança?

    a. Sim
    b. Não
    c. Não sei

41. Que medidas de segurança considera mais eficazes para proteger dados e sistemas?

    a. Formação contínua dos utilizadores
    b. Utilização de autenticação multifator
    c. Encriptação de dados
    d. Investimento em tecnologia
    e. Auditorias e testes regulares
    f. Outra

42. Que recomendação sugere como melhoria na segurança digital? *(Resposta aberta)*

Anexo B – Código Google Colab

```
# -*- coding: utf-8 -*-
"""Dissertacao.ipynb

Automatically generated by Colab.

Original file is located at
    https://colab.research.google.com/drive/1XyZeJHLzduuvcHulgDYLMlXJbUCtyfCL
"""

#Importar do google drive
from google.colab import drive
drive.mount('/content/drive')

import pandas as pd
import numpy  as np

#bibliteca para machine learning
from sklearn import tree
from sklearn.preprocessing import LabelEncoder
from sklearn.model_selection import train_test_split
from sklearn import metrics
from sklearn.metrics import confusion_matrix
import seaborn as sns
import matplotlib.pyplot as plt
import graphviz
from sklearn.tree import export_graphviz
import graphviz
from sklearn.metrics import accuracy_score, precision_score, recall_score, f1_score, make_scorer, confusion_matrix
from sklearn.model_selection import train_test_split, cross_validate, StratifiedKFold

"""**Abrir os dados CSV**"""
```

```
#Abrir os dados

dados = pd.read_csv('/content/drive/MyDrive/Colab Notebooks/Ciberseguranca.csv', sep=';', on_bad_lines='skip') #erro de virgulas ;

#dados.head()


pd.set_option('display.max_rows', None) #abre os dados todos

display(dados) # ou simplesmente dados e mostrará tudo


dados.info(verbose=True) #mostra os tipos de dados da tabela


#Label Encoder

le_faixa = LabelEncoder()

dados["1. Qual a sua faixa etária?"] = le_faixa.fit_transform(dados["1. Qual a sua faixa etária?"])


le_sexo = LabelEncoder()

dados["2. Qual é o seu sexo?"] = le_sexo.fit_transform(dados["2. Qual é o seu sexo?"])


le_escolaridade = LabelEncoder()

dados["3. Qual é o seu nível de escolaridade?"] = le_escolaridade.fit_transform(dados["3. Qual é o seu nível de escolaridade?"])


le_grupo = LabelEncoder()

dados["4. A que grupo pertence?"] = le_grupo.fit_transform(dados["4. A que grupo pertence?"])


le_conhecimento = LabelEncoder()

dados["5. Qual é o seu nível de conhecimento sobre cibersegurança?"] = le_conhecimento.fit_transform(dados["5. Qual é o seu nível de conhecimento sobre cibersegurança?"])


le_firewall = LabelEncoder()

dados["6. Utiliza software antivírus ou firewall no seu computador ou dispositivos?"] = le_firewall.fit_transform(dados["6. Utiliza software antivírus ou firewall no seu computador ou dispositivos?"])


le_ataque = LabelEncoder()

dados["7. Já sofreu algum ataque cibernético? "] = le_ataque.fit_transform(dados["7. Já sofreu algum ataque cibernético? "])
```

```
le_segurança = LabelEncoder()

dados["9. Em termos de segurança, como se sente ao navegar na internet?"] = le_segurança.fit_transform(dados['9. Em termos de segurança, como se sente ao navegar na internet?'])


le_profissionais = LabelEncoder()

dados.iloc[:, 39] = le_profissionais.fit_transform(dados.iloc[:, 39])


#Display

display(dados["1. Qual a sua faixa etária?"])

display(dados["2. Qual é o seu sexo?"])

display(dados["3. Qual é o seu nível de escolaridade?"])

display(dados["4. A que grupo pertence?"])

display(dados["5. Qual é o seu nível de conhecimento sobre cibersegurança?"])

display(dados["6. Utiliza software antivírus ou firewall no seu computador ou dispositivos?"])

display(dados["9. Em termos de segurança, como se sente ao navegar na internet?"])

display(dados["36. Está familiarizado com alguma regulamentação de segurança de dados, como o RGPD (Regulamento Geral de Proteção de Dados)?"])

display(dados.iloc[:, 39])


"""**Q6 Nível de familiaridade com ataques cibernéticos**"""


#Q6 Nível de familiaridade com ataques cibernéticos


x6 = dados.iloc[:, [0, 2, 4, 6]]

y6 = dados.iloc[:, 5]


print("Valores únicos da variável alvo (antes da codificação):")

print(y6.unique())


# Aplicar LabelEncoder na variavel target y6

le_y6 = LabelEncoder()

y6_encoded = le_y6.fit_transform(y6)


print("\nValores únicos da variável alvo (depois da codificação):")
```

```
print(np.unique(y6_encoded))


# Dividir os dados em treino e teste
x6_train, x6_test, y6_train, y6_test = train_test_split(x6, y6_encoded, test_size=0.3, random_state=42)


#  Treinar o modelo de Árvore de Decisão
clf6 =  tree.DecisionTreeClassifier(max_depth=3, random_state=42)
clf6 = clf6.fit(x6_train,y6_train) # Changed clf to clf6


#  Fazer previsões e calcular precisão
y6_pred = clf6.predict(x6_test)
accuracy6 = metrics.accuracy_score(y6_test, y6_pred)
precision6 = metrics.precision_score(y6_test, y6_pred, average='macro', zero_division=0)
recall6 = metrics.recall_score(y6_test, y6_pred, average='macro', zero_division=0)
f1_6 = metrics.f1_score(y6_test, y6_pred, average='macro', zero_division=0)


print("\nAcurácia do modelo :", round(accuracy6 * 100, 2), "%")
print("Precisão do modelo :", round(precision6 * 100, 2), "%")
print("Recall do modelo :", round(recall6 * 100, 2), "%")
print("F1-score do modelo :", round(f1_6 * 100, 2), "%")


#  Matriz de confusão
cm6 = confusion_matrix(y6_test, y6_pred)
plt.figure(figsize=(5, 4))
sns.heatmap(cm6, annot=True, fmt='d', cmap='Blues')
plt.xlabel('Previsto')
plt.ylabel('Real')
plt.title('Matriz de Confusão - Q6: Utiliza software antivírus ou firewall no seu computador ou dispositivos?')
plt.show()


#clf = tree.DecisionTreeClassifier(max_depth=3, random_state=42)
dot_data6 = tree.export_graphviz(clf6,
                                 out_file=None,
```

```
                        feature_names=x6.columns, # Atualizar nomes de funcionalidades para corresponder a x6
                        class_names=[str(c) for c in le_y6.classes_], # Use as classes do LabelEncoder para nomes de classes
                        filled=True,
                        rounded=True,
                        special_characters=True)

graph = graphviz.Source(dot_data6)
#graph.render("arvore_decisao_Q6", format="png")  # salva em PNG
graph

"""**Q7. JÁ SOFREU ALGUM ATAQUE?**"""

# Pergunta alvo: "Já sofreu algum ataque cibernético?" (Q7)
x = dados.iloc[:, [0, 1, 3, 5]]  # variáveis explicativas
y = dados.iloc[:, 6]             # variável alvo (target)

print("Valores únicos da variável alvo:")
print(y.unique())

#  Dividir os dados em treino e teste

x_train, x_test, y_train, y_test = train_test_split(x, y, test_size=0.2, random_state=42)

# Treinar o modelo de Árvore de Decisão

clf = tree.DecisionTreeClassifier(max_depth=3, random_state=42)
clf = clf.fit(x_train, y_train)

# Fazer previsões e calcular precisão

y_pred = clf.predict(x_test)
accuracy = metrics.accuracy_score(y_test, y_pred)
precision = metrics.precision_score(y_test, y_pred, average='macro', zero_division=0)
```

```
recall = metrics.recall_score(y_test, y_pred, average='macro', zero_division=0)
f1 = metrics.f1_score(y_test, y_pred, average='macro', zero_division=0)

print("\nAcurácia do modelo :", round(accuracy * 100, 2), "%")
print("Precisão do modelo :", round(precision * 100, 2), "%")
print("Recall do modelo :", round(recall * 100, 2), "%")
print("F1-score do modelo :", round(f1 * 100, 2), "%")

# Matriz de confusão

cm = confusion_matrix(y_test, y_pred)
plt.figure(figsize=(5, 4))
sns.heatmap(cm, annot=True, fmt='d', cmap='Blues')
plt.xlabel('Previsto')
plt.ylabel('Real')
#plt.title('Matriz de Confusão - Q7: Já sofreu algum ataque cibernético?')
plt.show()

# Gerar e visualizar a árvore de decisão

dot_data = tree.export_graphviz(
    clf,
    out_file=None,
    feature_names=x.columns,
    class_names=[str(c) for c in y.unique()],
    filled=True,
    rounded=True,
    special_characters=True
)

graph = graphviz.Source(dot_data)
#graph.render("arvore_decisao_Q7", format="png")  # salva como imagem PNG
graph
```

```
"""**Q9 Em termos de segurança, como se sente ao navegar na internet?**"""

# Pergunta alvo: Em termos de segurança, como se sente ao navegar na internet? (Q9)
x9 = dados.iloc[:, 1:5]
y9=dados.iloc[:, 8]

print("Valores únicos da variável alvo:")
print(y9.unique())

#  Dividir os dados em treino e teste

x9_train, x9_test, y9_train, y9_test = train_test_split(x9, y9, test_size=0.3, random_state=42)

# Treinar o modelo de Árvore de Decisão

clf9 = tree.DecisionTreeClassifier(max_depth=3, random_state=42)
clf9 = clf9.fit(x9_train, y9_train)

#Fazer previsões e calcular precisão

y9_pred = clf9.predict(x9_test)
accuracy9 = metrics.accuracy_score(y9_test, y9_pred)
precision9 = metrics.precision_score(y9_test, y9_pred, average='macro', zero_division=0)
recall9 = metrics.recall_score(y9_test, y9_pred, average='macro', zero_division=0)
f1_9 = metrics.f1_score(y9_test, y9_pred, average='macro', zero_division=0)

print("\nAcurácia do modelo :", round(accuracy9 * 100, 2), "%")
print("Precision do modelo :", round(precision9 * 100, 2), "%")
print("Recall do modelo :", round(recall9 * 100, 2), "%")
print("F1-score do modelo :", round(f1_9 * 100, 2), "%")

#  Matriz de confusão

cm9 = confusion_matrix(y9_test, y9_pred)
```

```
plt.figure(figsize=(5, 4))
sns.heatmap(cm9, annot=True, fmt='d', cmap='Blues')
plt.xlabel('Previsto')
plt.ylabel('Real')
#plt.title('Matriz de Confusão - Q9: Em termos de segurança, como se sente ao navegar na internet?')
plt.show()

#  Gerar e visualizar a árvore de decisão

dot_data9 = tree.export_graphviz(
    clf9,
    out_file=None,
    feature_names=x9.columns,
    class_names=[str(c) for c in le_segurança.classes_], # Usa as classes do LabelEncoder existente
    filled=True,
    rounded=True,
    special_characters=True
)

graph9 = graphviz.Source(dot_data9)
#graph9.render("arvore_decisao_Q9", format="png")  # salva como imagem PNG
graph9

"""**Q40 – Falta de profissionais em cibersegurança**"""

x40 = dados.iloc[:, 2:5] # Seleciona colunas do índice 2 ao 4 (questões 3 a 5)
y40 = dados.iloc[:, 39]  # seleciona todas as linhas da 40ª coluna (índice 39)

# Converte y40 para tipo inteiro
y40 = y40.astype(int)

# Dividir os dados em treino e teste

x40_train, x40_test, y40_train, y40_test = train_test_split(x40, y40, test_size=0.2, random_state=42)
```

```
#Treinar o modelo de Árvore de Decisão

clf40 =  tree.DecisionTreeClassifier(max_depth=3, random_state=42)
clf40 = clf40.fit(x40_train,y40_train) # Converet y40 para int64

# Fazer previsões e calcular precisão

y40_pred = clf40.predict(x40_test)
accuracy40 = metrics.accuracy_score(y40_test, y40_pred)
precision40 = metrics.precision_score(y40_test, y40_pred, average='macro', zero_division=0)
recall40 = metrics.recall_score(y40_test, y40_pred, average='macro', zero_division=0)
f1_40 = metrics.f1_score(y40_test, y40_pred, average='macro', zero_division=0)

print("\nAcurácia do modelo:", round(accuracy40 * 100, 2), "%")
print("Precisão do modelo:", round(precision40 * 100, 2), "%")
print("Recall do modelo:", round(recall40 * 100, 2), "%")
print("F1-score do modelo:", round(f1_40 * 100, 2), "%")

#  Matriz de confusão

cm40 = confusion_matrix(y40_test, y40_pred)
plt.figure(figsize=(5, 4))
sns.heatmap(cm40, annot=True, fmt='d', cmap='Blues')
plt.xlabel('Previsto')
plt.ylabel('Real')
#plt.title('Matriz de Confusão - Q40: Acha que há falta de profissionais qualificados em cibersegurança?')
plt.show()

# Imprimir valores únicos em y40 para ajudar a identificar nomes de classes em falta
print("Unique values in y40:", y40.unique())

#Perguntas alvos: Em termos de segurança, como se sente ao navegar na internet?
import matplotlib.pyplot as plt
```

```
from sklearn.tree import export_graphviz
import graphviz
#clf = tree.DecisionTreeClassifier(max_depth=3, random_state=42)
dot_data40 = tree.export_graphviz(clf40,
                                  out_file=None,
                                   feature_names=x40.columns, # Atualiza nomes de funcionalidades para corresponder a x40
                                class_names=[str(x) for x in le_profissionais.classes_], # Usa as classes do LabelEncoder para class_names
                                  filled=True,
                                  rounded=True,
                                  special_characters=True)

graph = graphviz.Source(dot_data40)
#graph.render("arvore_decisao_Q40", format="png")  # salva em PNG
graph

# Mostra o mapeamento para cada LabelEncoder
print("Mapping for '1. Qual a sua faixa etária?':")
for i, item in enumerate(le_faixa.classes_):
    print(f"{item} - {i}")

print("\nMapping for '2. Qual é o seu sexo?':")
for i, item in enumerate(le_sexo.classes_):
    print(f"{item} - {i}")

print("\nMapping for '3. Qual é o seu nível de escolaridade?':")
for i, item in enumerate(le_escolaridade.classes_):
    print(f"{item} - {i}")

print("\nMapping for '4. A que grupo pertence?':")
for i, item in enumerate(le_grupo.classes_):
    print(f"{item} - {i}")
```

```
print("\nMapping for '5. Qual é o seu nível de conhecimento sobre cibersegurança?':")
for i, item in enumerate(le_conhecimento.classes_):
    print(f"{item} - {i}")

print("\nMapping for '6. Utiliza software antivírus ou firewall no seu computador ou dispositivos?':")
for i, item in enumerate(le_firewall.classes_):
    print(f"{item} - {i}")

print("\nMapping for '7. Já sofreu algum ataque cibernético?':")
for i, item in enumerate(le_ataque.classes_):
    print(f"{item} - {i}")

# A saída abaixo mostra o mapeamento do LabelEncoder antes do mapeamento manual.
print("\nMapping for column 39 (Q40):")
for i, item in enumerate(le_profissionais.classes_):
    print(f"{item} - {i}")
```