INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Inteligência artificial e segurança de informação: Influência da perceção de segurança nos comportamentos e sentimentos dos portugueses em relação à automação

Filipe Henderson Gonga Van-Dúnem

Mestrado em Gestão de Sistemas de Informação

Orientadora:
Doutora Inês Teixeira de Sousa Messias, Investigadora Associada, ISTAR-Iscte – Centro de Investigação em Ciências da Informação, Tecnologias e Arquitetura

Orientador:
Doutor Bráulio Alexandre Barreira Alturas, Professor Associado (com Agregação),
Iscte-Instituto Universitário de Lisboa

Outubro, 2025

TECNOLOGIAS
E ARQUITETURA

Departamento de Ciências e Tecnologias da Informação

Inteligência artificial e Segurança de informação: Influência da perceção de segurança nos comportamentos e sentimentos dos portugueses em relação a automação

Filipe Henderson Gonga Van-Dúnem

Mestrado em Gestão de Sistemas de Informação

Orientadora:
Doutora Inês Teixeira de Sousa Messias, Investigadora Associada, ISTAR-Iscte – Centro de Investigação em Ciências da Informação, Tecnologias e Arquitetura

Orientador:
Doutor Bráulio Alexandre Barreira Alturas, Professor Associado (com Agregação),
Iscte-Instituto Universitário de Lisboa

Outubro, 2025

Agradecimentos

Na realização da presente dissertação, gostaria de agradecer a todas as pessoas que de alguma forma estiveram presentes numa das fases mais importantes da minha vida e contribuíram para a concretização desta etapa.

Primeiramente, gostaria de agradecer à Professora Inês Messias e ao Professor Bráulio Alturas pela sua orientação e coorientação, respetivamente, pela disponibilidade, dedicação e todo o apoio que demonstraram ao longo desta etapa.

À minha família, em especial à minha irmã Andreza, à minha irmã Vanmira, á minha irmã Wanda, à minha mãe, e ao meu pai, por sempre acreditarem em mim e me apoiarem incondicionalmente.

Um agradecimento muito especial à Daniela, à Marta e ao João, por toda a motivação e por serem um pilar de apoio durante esta etapa.

Agradeço a Deus pela força e serenidade que me permitiram concluir este trabalho.

Deixo também um agradecimento especial a todos os participantes do questionário efetuado que, desta forma, contribuíram para que fosse possível tirar conclusões importantes para este estudo.

A todos os que enumerei o meu sincero “Obrigado”.

Resumo

A adoção de tecnologias de inteligência artificial nas empresas tem aumentado ao longo dos tempos, criando oportunidades de crescimento e de melhoria dos seus sistemas de informação e de segurança. Contudo, esta evolução tecnológica levanta, questões sobre a perceção de segurança da informação por parte dos utilizadores, nomeadamente quanto à confiança nos sistemas automatizados, e quanto à forma como os mesmos influenciam as práticas de proteção dos dados dos utilizadores. Assim, este estudo tem como principal objetivo analisar a perceção de segurança da informação na população portuguesa, mais especificamente, entender o quão relevante é para a população portuguesa permitir que um algoritmo de dados possa influenciar a sua perceção de segurança em relação aos seus dados informáticos. Para o efeito, foi desenvolvido um estudo de natureza quantitativa, através da aplicação de um questionário online de respostas fechadas. No total foram recolhidas 370 respostas, das quais 251 foram consideradas válidas para análise. Os dados recolhidos foram tratados e analisados com o recurso ao software IBM SPSS Statistics, utilizando técnicas de análise descritiva. De entre as várias conclusões deste trabalho, destaca-se que, de forma, geral os participantes apresentam uma perceção positiva de segurança da informação, embora se tenham verificado diferenças significativas em função do nível de literacia digital e da familiaridade com as tecnologias de inteligência artificial.

Palavras-Chave: perceção de segurança, inteligência artificial, segurança da informação, confiança tecnológica

Abstract

The adoption of artificial intelligence technologies in companies has increased over time, creating opportunities for growth and for improving their information and security systems. However, this technological evolution raises questions regarding user´s perception of information security, particularly concerning their trust in automated systems and how these systems influence users' data protection practices. Thus, the main objective of this study is to analyze the perception of information security within the Portuguese population, specifically aiming to understand how relevant it is for Portuguese individuals to allow a data algorithm to influence their perception of security regarding their digital information. To this end, a quantitative study was conducted through the administration of an online closed-end questionnaire. In total, 370 responses were collected, of which 251 were considered valid for analysis. The data collected was processed and analyzed using IBM SPSS Statistics software, applying descriptive analysis techniques. Among the various conclusions of this research, it stands out that, in general, participants demonstrated a positive perception of information security, although significant differences were observed according to the level of digital literacy and familiarity with artificial intelligence technologies.

Keywords: perception of security, artificial intelligence, information security, technological trust.

Índice Geral

Índice de Tabelas

Índice de Figuras

Glossário de Abreviaturas e Siglas

AGI – Inteligência Artificial Geral

ANI – Inteligência Artificial Estreita

ASI – Superinteligência Artificial

DESI – Índice de Digitalidade da Economia e da Sociedade

ES – Engenharia Social

IA – Inteligência Artificial

IBM – International Business Machines

ICI – Infraestrutura Critica de Informação

INE – Instituto Nacional de Estatística

IOT – Internet das Coisas

ISO – International Organization for Standardization

ISP – Política de Segurança da Informação

IUIPC – Internet User´s Information Privacy Concerns

PMT – Teoria da Proteção da Motivação

RCT – Teoria da Escolha Racional

SEM – Modelos de Equações Estruturais

SI – Sistemas de Informação

TAM – Technology Assessment Model

TI – Tecnologias de Informação

TIC – Tecnologia da Informação e Comunicação

TPB – Teoria do Comportamento Planeado

TRA – Teoria da Ação Racional

UE – União Europeia

UTAUT – Unified Theory of Acceptance and Use of Technology

UTAU2 – Unified Theory of Acceptance and Use of Technology 2

Capítulo 1 – Introdução

1.1. Enquadramento do tema

O século XXI tem como um dos seus marcos a quarta revolução industrial, acima de tudo uma etapa essencial do desenvolvimento tecnológico, sendo uma mudança de paradigma, que, influenciará, intrinsecamente, a sociedade e o modo como vivemos, interagimos e trabalhamos. Esta revolução tem impacto direto em diversos níveis: económico, político, ambiental, ético e social.

Para Rüßmann et al., (2015) a indústria 4.0 assenta em nove pilares fundamentais que sustentam a sua expansão: 1) Internet das Coisas; 2) Big Data e análise de dados; 3) Robots autónomos; 4) Simulação; 5) Integração Horizontal; 6) Serviços de *Cloud*; 7) Cibersegurança; 8) Produção aditiva; 9) Realidade Aumentada.

Segundo Kagermann et al., (2013) a indústria 4.0 apresenta um potencial altamente ambicioso, prometendo ganhos significativos de eficácia operacional, aumentos de produtividade, crescimento do volume de negócios, bem como um reforço da competitividade, levando ainda ao desenvolvimento de novos modelos de negócios, de novos serviços, e de novos produtos. Inclusive Kagermann et al., (2013) sublinha que a sua implementação efetiva requer a adoção de vários tipos de integração horizontal – relacionada com a cadeia de valor, e de integração digital, que consiste na introdução de mecanismos de engenharia digital ao longo de todo o ciclo de vida do produto e da sua cadeia de valor.

O autor Mccarthy (2004) define a inteligência artificial (IA) como a ciência e a engenharia de tornar as máquinas inteligentes, por outras palavras, usando os sistemas de informação para reproduzir a forma como opera a inteligência humana. Em todo o caso, a evolução da IA tem sido amplamente discutida por outros autores. Por exemplo, Kissinger et al., (2021, citados por Violante e Andrade, 2022) referem que "o seu funcionamento prevê progressos na busca da essência das coisas. (...) Todavia, como acontece com todas as tecnologias, a IA não tem a ver apenas com capacidades e promessas, mas também com o modo como é usada: para curar doenças e melhorar a educação, ou para propagar desinformação e opressão".

De acordo com estudos realizados pelo Eurobarómetro (2017), os dados indicam que 61% dos europeus têm uma perceção positiva em relação a inteligência artificial, porém, 88% defendem que estas tecnologias devem ser utilizadas e geridas com prudência.

Para Mercader Uguina (2017) a inteligência artificial tem o potencial de se vir a tornar num instrumento fundamental para a produção, em que a tomada de decisão é realizada considerando a coexistência de homens e máquinas.

Segundo Makridakis (2017, citado por Gessinger et al.,), a inteligência artificial está presente no quotidiano das pessoas e das empresas, através de recursos como reconhecimento de voz e de face ou sugestões de escrita presentes nos smartphones. Pan (2016, citado por Gessinger et al.,) acrescenta que, com esta popularização, a IA entrou num novo estágio evolutivo, por alguns designado como IA 2.0.

De acordo com Mendonça, Andrade e Neto (2018) a inteligência artificial é um vasto campo de investigação que compreende diversas abordagens, entre as quais se incluem a teoria *fuzzy*, as árvores de decisão e as redes neurais (Costa, 2006; Klashanov, 2016; Kornienko, Kornienko, Fofanov, & Chunik, 2015; Wolfert, Ge, Verdouw, & Bogaardt, 2017, citado por Mendonça, Andrade, e Neto, 2018).

Ainda segundo Mendonça, Andrade e Neto (2018), Pan (2016) salienta que a integração da IA nas demandas industriais provocou mudanças significativas na forma como os serviços são prestados. Exemplos citados incluem o robô de conversação Xiaobing, desenvolvido pela Microsoft, que transforma a interface gráfica tradicional numa interface interativa com compreensão natural e emocional; a aquisição do Linkedin pela Microsoft, com vista à reconstrução da comunidade usando IA, o sistema Watson da IBM, utilizado em hospitais para auxiliar na identificação de alternativas de diagnostico de cancro a partir de milhões de registos de pacientes; e a utilização da Baidu para traduções automáticas, processamento de linguagem natural e veículos inteligentes.

"Através da automatização, melhor dizendo, da realização de tarefas industriais sem o recurso à intervenção do homem, da evolução tecnológica e do desenvolvimento de máquinas e sistemas informatizados, a indústria sofre uma profunda transformação, criando-se espaço para a competitividade e eficácia" (Fonseca, 2020, p. 13).

1.2. Motivação e relevância do tema

A razão deste estudo, decorre do facto da temática escolhida ser atual e relevante para o contexto atual, devido a necessidade de compreender a adoção desta tecnologia, que cada vez mais faz parte do nosso quotidiano.

Irá também o presente estudo contribuir para ampliar a conscientização e a base de pesquisa para investigações futuras acerca de um tema pouco explorado a nível nacional.

Atualmente, as tecnologias de informação, nomeadamente os smartphones, tablets, computadores, entre outros, integram cada vez mais de maneira significativa o quotidiano, sendo que algumas de nossas responsabilidades são delegadas a esses dispositivos. No entanto, depositamos consideravelmente a confiança nesses aparelhos, sem questionar como isso pode impactar a segurança em relação aos dados que fornecemos, bem como as possíveis consequências ao cedermos a esses dispositivos o controle sobre as nossas vidas.

O índice digital da economia e da sociedade (DESI) é um relatório anual que resume os indicadores sobre o desempenho digital dos países da União Europeia, que é composto por quatro dimensões: capital humano, conexão, integração da tecnologia digital e os serviços públicos digitais.

De acordo com o relatório DESI a união europeia tem como meta equipar pelo menos 80% da população em geral com competências básicas de literacia digital e aumentar o número de especialistas em tecnologias de informação (TIC) para 20 milhões, com a convergência entre homens e mulheres até 2030.

A nível nacional, o Governo Português (2020, pp. 8-9) definiu o plano de ação para a transição digital, sustentado em três pilares fundamentais, bem como uma dimensão adicional de catalisação que cria as condições de base para uma aceleração digital do país:

1. Pilar I – Capacitação e inclusão digital das pessoas;
2. Pilar II- Transformação digital do tecido empresarial;
3. Pilar III- Digitalização do estado;
4. Catalisação da transição digital de Portugal.

A internet das Coisas (IOT) é uma ferramenta que irá permitir convergir os mundos físico e virtual, permitindo a criação de ambientes inteligentes, otimizando serviços. Todavia, o Internacional Data Corporation prevê que o número de dispositivos conectados à IOT instalados, aumente exponencialmente de cerca de 40 mil milhões em 2023 para 49 mil milhões em 2026, com uma taxa de crescimento anual de 7%.

A União Europeia está a financiar os Estados-Membros através do programa Horizonte Europa, que incentiva o desenvolvimento e a implementação de tecnologias de dados e de computação, bem como outras iniciativas inseridas no âmbito do cluster 4 «Digital, Indústria e Espaço».

1.3. Questões e objetivos de investigação

O tema desta investigação tem por base a perceção da segurança em relação à inteligência artificial. Pretende-se entender melhor a relação e a perceção da população portuguesa com a perceção de segurança.

O principal objetivo desta investigação será **perceber qual a influência da perceção de segurança da informação nos comportamentos e sentimentos da população portuguesa relativamente à automação**.

Como objetivos secundários foram definidos:

1. Identificar as expectativas, opiniões sobre a automação;
2. Determinar em que medida é que a segurança na automação é uma preocupação;
3. Conhecer a perceção dos comportamentos e sentimentos relativamente a automação;
4. Perceber em que medida a perceção de segurança se reflete nos comportamentos e sentimentos face a automação.

A função da investigação que se pretende seguir é compreender o modo como a população portuguesa perceciona a automação, em termos dos pensamentos e sentimentos que esta lhes suscita.

Decorrente da função de investigação, a questão a que se pretende dar resposta é: De que forma a perceção da segurança da informação influencia os comportamentos e sentimentos da população portuguesa relativamente à automação?

1.4. Abordagem metodológica

Tendo em consideração a função de pesquisa, será adotada uma metodologia quantitativa. Com base na revisão de literatura existente, sobre o tema em estudo, será elaborado um inquérito por questionário, que se constituirá como principal instrumento para a recolha de dados. Posteriormente, este inquérito será aplicado e divulgado através das redes sociais e partilhas realizadas por outros interessados.

Os dados obtidos serão tratados e analisados estatisticamente, utilizando os softwares IBM SPSS e Microsoft Excel, de modo a garantir a análise em conformidade com os objetivos traçados.

1.5.Estrutura e organização da dissertação

O presente estudo encontra-se estruturado em cinco capítulos, de modo a refletir as diferentes fases até à sua conclusão.

O primeiro capítulo introduz o tema da investigação, destacando as motivações e relevâncias do estudo, os objetivos definidos, tal como uma breve descrição da estrutura do trabalho.

O segundo capítulo aborda o enquadramento teórico, designado por Revisão da literatura.

O terceiro capítulo é dedicado à Metodologia, descrevendo o processo de recolha e tratamento de dados, o questionário utilizado, a amostra do estudo, bem como os métodos de análise aplicados.

O quarto capítulo apresenta a análise dos resultados obtidos e a discussão dos resultados obtidos, de acordo com a metodologia adotada.

Por fim, o quinto capítulo sintetiza as conclusões do estudo, realçando recomendações, limitações e sugestões para trabalhos futuros.

Capítulo 2 – Revisão da Literatura

2.1. Inteligência Artificial e Segurança da Informação

2.1.1. Definição de Inteligência Artificial

De acordo com Veiga e Pires (2023), e McCarthy (1963), citados por Veiga e Pires, 2023) a inteligência artificial (IA) pode definir-se como um ramo da ciência da computação que procura elaborar sistemas que simulam a capacidade humana de racionar, perceber, tomar decisões e resolver problemas. Ou seja, é a "capacidade que uma máquina tem para reproduzir competências semelhantes às humanas como é o caso do raciocínio, da aprendizagem, do planeamento e da criatividade" (Alturas, 2022).

A inteligência artificial pode ser dividida em inteligência artificial geral (AGI), inteligência artificial estreita (ANI) e superinteligência artificial (ASI) (Antonov, 2011; Gill, 2016). A inteligência artificial estreita inclui sistemas modernos de IA, tais como softwares de reconhecimento de voz (ex. Siri da Apple), que auxilia os utilizadores através da machine learning e não pode transferir conhecimento entre sistemas ou tarefas (Mclean et al., 2021; Salmon et al., 2021). Atualmente a inteligência artificial geral é um conceito teórico que será capaz de atingir metas de forma autónoma e transferir aprendizagens dentro de uma vasta gama de cenários (Mclean et al., 2021; Mitchell., 2019). Essas habilidades permitirão que os agentes da AGI possuam inteligência muito além da capacidade humana e podem levar ao desenvolvimento de questões complexas como a saúde humana e o aquecimento global do planeta (Salmon et al., 2021). A superinteligência artificial envolve agentes que funcionarão com um nível de inteligência superior ao capaz do ser humano. Para o autor Cabrera-Sanchéz et al., (2021) a ASI consiste na forma mais precisa da IA, pois será capaz de fazer descobertas pioneiras em campos gerais, científicos, académicos, criativos e sociais, levando potencialmente a redundância de seres humanos.

De acordo com Veiga e Pires (2023), a agência europeia para a segurança e saúde no trabalho (2015, citado por Veiga e Pires,2023) refere a existência de dois tipos de inteligência artificial: fraca e forte. A IA fraca refere-se à tecnologia que soluciona problemas num campo de aplicação limitado, enquanto a IA forte refere-se a um equipamento hipotético que exibe um comportamento semelhante ao ser humano, mas pensa de forma incessante e incansável.

A “IA fraca” ou “IA estreita”, consiste na capacidade de os sistemas de computação utilizarem algoritmos ajustados para casos muito específicos, permitindo executar tarefas operacionais críticas nas organizações. Este tipo de sistemas é programado para realizar apenas uma tarefa definida, não possuindo capacidade de desenvolver inteligência própria (Iansiti & Lakhani, 2020, como citado em Violante e Andrade, 2022). Um exemplo deste tipo de IA são os assistentes virtuais como a Cortana da Microsoft, que procura respostas numa base de dados previamente estruturada, segundo padrões definidos ou integrando funcionalidades de linguagem natural, como Q&A no Excel ou no Power BI.

Por outro lado, a “IA forte” refere-se a sistemas capazes de desempenhar qualquer atividade lógica, incluindo processos de tomada de decisão, aprendizagem e resolução de problemas em diferentes domínios, de forma semelhante aos humanos. Este tipo de IA pressupõe a possibilidade de desenvolver formas próprias de inteligência, aproximando-se de conceitos como o Teste de Turing (IBM cloud education, 2020; Sabouret, 2020, como citado em Violante e Andrade, 2022). No entanto, segundo Quaresma e Silva (2021, como citado em Violante e Andrade, 2022), apesar de simular processos cognitivos humanos, a IA forte continua a ser considerada pela comunidade científica como uma possibilidade ainda hipotética.

Os conceitos de *machine learnin*g e *deep learning* são frequentemente confundidos e, por vezes, utilizados como sinónimos do termo inteligência artificial (IA). Contudo, importa distingui-los e compreender de que forma se relacionam com o conceito de IA.

O *machine learning* constitui um subcampo da IA que permite aos sistemas computacionais analisar grandes volumes de dados e identificar padrões ou construir modelos preditivos. Desta forma, quando é introduzida nova informação, o sistema consegue prever o resultado com base nos padrões previamente aprendidos (Brown, 2021, como citado em Violante e Andrade, 2022). Assim, quanto maior for o volume de dados utilizados no treino, maior será a precisão dos modelos gerados.

No âmbito do *machine learning*, os dados podem ser processados segundo dois tipos principais de aprendizagem: supervisionada e não supervisionada. A aprendizagem supervisionada corresponde a modelos preditivos desenvolvidos a partir de dados rotulados, cujo objetivo é identificar uma função capaz de prever um rotulo ou valor para novos exemplos, com base nos respetivos atributos de entrada (Gama et al., 2017, como citado em Violante e Andrade, 2022).

Por sua vez, a percentagem não supervisionada abrange métodos como o agrupamento, que consiste na associação de dados segundo níveis de semelhança, a sumarização, que visa simplificar e interpretar conjuntos extensos de dados, e a associação, cujo objetivo é identificar padrões de ligação entre variáveis.

O *deep learning* representa um subcampo avançado do *machine learning*, inspirado na estrutura e funcionamento do cérebro humano, em particular nas redes neurais artificiais. Estas redes são compostas por múltiplas camadas de nódulos interligados, responsáveis por identificar correlações ou padrões ocultos entre variáveis, procurando simular processos cognitivos humanos (Kissinger et al., 2021, como citado em Violante e Andrade, 2022). Quanto mais profunda for a rede neural, isto é, quanto maior o número de camadas, maior será a sua capacidade de reconhecer estruturas complexas em grandes volumes de dados.

2.1.2. Aplicações de IA na Segurança de informação

Nos últimos anos, investigadores na área da cibersegurança começaram a explorar abordagens baseadas em Inteligência Artificial (IA) para melhorar a segurança digital. Tecnologias de IA, como a aprendizagem automática, podem ser utilizadas na cibersegurança para desenvolver modelos inteligentes destinados à classificação de malware, deteção de intrusões e análise de ameaças (Li, 2018). Os algoritmos de aprendizagem automática são treinados com vastas quantidades de dados, incluindo informações históricas sobre ameaças e dados da rede e dos dispositivos terminais, para identificar padrões que seriam difíceis de reconhecer por humanos (Moisset, 2023).

Existe, no entanto, a preocupação de que os métodos de aprendizagem automática possam ser facilmente manipulados através da introdução de dados enganosos, um fenómeno conhecido como ataques adversariais. Ao monitorizar e analisar padrões de forma contínua, os algoritmos de IA podem detetar desvios que possam indicar potenciais ameaças, como acessos não autorizados ou atividades anómalas de utilizadores (Masum, 2023). Da mesma forma, os cibercriminosos também estão a utilizar IA para lançar ciberataques cada vez mais sofisticados, enquanto ocultam os seus rastos (Zeadally et al., 2020).

2.1.3. Desafios e ameaças em segurança de informação relacionados à IA

Segundo as autoras do artigo (Somova, Gocheva, Kasakliev, 2024), os riscos de segurança e vulnerabilidade manifestam-se em diferentes *softwares* e aplicações, incluindo tecnologias baseadas em engenharia social, a utilização de *chatbots* de inteligência artificial, questões de segurança da informação política e a disrupção de infraestruturas de informação.

1) Tecnologias baseadas em engenharia social. A engenharia social (ES) é considerada um dos problemas mais comuns que a segurança da informação enfrenta atualmente, uma vez que os ataques podem ser detetados, mas não impedidos (Salahdine, 2019). A ES é uma técnica de manipulação que explora o erro humano para obter informações privadas, aceder a sistemas protegidos, disseminar *malware* ou realizar outras atividades perigosas. Os ataques de ES apresentam diversas formas baseadas em tecnologia, como *phishing*, *vishing, baiting* e *pretexting*, podendo ser potenciados pelo uso de inteligência artificial (IA).
2) Utilização de *chatbots* de inteligência artificial. Uma das principais aplicações da Inteligência Artificial (IA) é o desenvolvimento de *bots*, que são programas informáticos concebidos para atuar como agentes autónomos em nome de um utilizador ou de outro programa, simulando atividades humanas (Ukov, 2022). Nesse contexto, os *chatbots* correspondem a programas informáticos especificamente projetados para reproduzir interações humanas, seja por meio de texto ou voz, utilizando técnicas de IA, processamento de linguagem natural e aprendizagem automática (Adamopoulou, 2020).
3) Questões de segurança da informação política. O impacto da Inteligência Artificial (IA) na política será profundo e pode até gerar uma revolução política (Gallego, 2022). A IA tem o potencial de ser utilizada para criar vídeos, gravações de áudio e conteúdos escritos altamente persuasivos, como *deep fakes*, que podem disseminar informações imprecisas, fabricar notícias falsas e manipular o sentimento público (Thompson, 2023). Alguns investigadores especulam que a facilidade com que uma grande quantidade de textos pode ser gerada para apoiar uma tese política, mesmo que infundada ou tendenciosa, pode multiplicar a manipulação da opinião pública (Farina, 2023). Porém, o uso da IA na política também apresenta aspetos positivos. Os sistemas de IA têm o potencial de

aumentar a legitimidade política, ao identificar questões sociais prementes, prever os possíveis resultados de políticas e avaliar a eficácia das mesmas (Starke, 2020). Outro estudo sugere que, embora seja difícil prever se o desenvolvimento das tecnologias baseadas em IA mudará radicalmente o paradigma político existente, tal desenvolvimento pode capacitar formas mais difusas de participação política para além das eleições (Savaget et al., 2019).

4) Disrupção da infraestrutura de informação. A infraestrutura de informação de uma organização pode ser alvo de ameaças tanto internas quanto externas, as quais podem ser exacerbadas pela aplicação de tecnologias de Inteligência Artificial. Tais ameaças podem resultar na interrupção ou paralisação das operações empresariais, ou ainda no surgimento de anomalias que possam culminar em desastres de segurança, afetando até Infraestruturas Críticas de Informação (ICI) como telecomunicações, transporte aéreo, setor financeiro, rede elétrica, entre outros serviços essenciais para o funcionamento da economia e das atividades cotidianas (Wilson, 2014).

2.2. Perceção de Segurança

2.2.1. Teorias da perceção de segurança

Os autores Liang e Xue (2010) definem a o conceito de perceção de ameaça como o grau em que o individuo perceciona um ataque malicioso de IT como perigoso ou prejudicial. Os utilizadores de tecnologias de informação desenvolvem perceção de ameaça, monitorizando o ambiente de computação e detetando potenciais perigos. Segundo a psicologia da saúde e na análise de risco, os autores sugerem que a perceção de ameaça é formada pela suscetibilidade percebida e pela gravidade percebida.

Liang e Xue (2009, 2010), como referido por Klein (2014), definem a suscetibilidade percebida como a probabilidade subjetiva de um indivíduo ser afetado negativamente por um *malware*. Por outro lado, a gravidade percebida corresponde ao grau em que um indivíduo percebe que os efeitos adversos causados pelo *malware* serão graves. De acordo com Klein (2014), os autores defendem ainda que estudos sobre comportamentos de proteção na área da saúde fornecem bases teóricas aplicáveis à segurança da informação, uma vez que a perceção de ameaça combinada com a probabilidade e gravidade motiva a adoção de comportamentos de proteção.

Muitas teorias têm sido utilizadas por muitos pesquisadores na busca de soluções para desafios que afetam a segurança do sistema de informação (Zoto, Kowalski, Lopez-Rojas, & Kianpour, 2018; Charitoudi & Blyth, 2013; Shahri & Mohanna, 2016; Han, Dai, Tianlin Han, & Dai, 2015; Lubua & Pretorius, 2019). A compreensão das diversas teorias de segurança de SI e as suas contribuições ajudam a compreender a literatura de segurança de SI e a identificar os fatores que afetam a segurança de SI da organização. As teorias de segurança de SI mais utilizadas são a teoria da sociotécnica, a teoria cognitiva distribuída e a teoria geral da discussão.

Teoria técnica social

Esta teoria considera o fator humano como o ponto-chave na deteção e prevenção da segurança da informação, embora atualmente a segurança da informação seja percebida principalmente como uma questão teórica (Zoto, Kowalski, Lopez-Rojas, & Kianpour, 2018; Charitoudi & Blyth, 2013). A teoria técnica social é eficaz na modelagem da segurança do sistema e do seu ambiente, examinando a cultura, o problema de usabilidade, o controle interno de segurança e os requisitos de segurança (Zoto, Kowalski,

Lopez-Rojas, & Kianpour, 2018; Charitoudi & Blyth, 2013). Assim, a teoria técnica social pode ser utilizada para analisar como as pessoas/ seres humanos podem ser fatores que contribuem para a segurança dos Sistemas de Informação com base na sua perceção e abordagem para a segurança da organização.

Teoria cognitiva distribuída

Esta teoria consiste no processo autoefeciente, consignado como uma pessoa poder usar as habilidades e não no tipo de habilidades que uma pessoa possui, portanto, pode ser usada na segurança do sistema de informação como autoeficiencia de segurança (Shahri & Mohana, 2016). As teorias cognitivas distribuídas propõem a colaboração entre indivíduos para atingir um objetivo comum, portanto, a segurança do sistema de informação deve estar em consonância com a cognição humana, a medida que a informação e distribuída mais em um ambiente virtual (Han, Dai, Tianlin Han, & Dai, 2015).

Teoria Geral da discussão

A teoria geral da discussão foi adotada para a segurança do sistema de informação com o intuito de incutir medo, através de consequências nos indivíduos para desencorajar uma ação que ameace a segurança do sistema de informação (Hu, Xu, Dinev, & Ling, 2011). Esta teoria baseia-se na certeza e na severidade das sanções, defendendo que as punições devem ser aplicadas de acordo com a gravidade da ação ilícita cometida por um indivíduo contra a segurança da informação. Esta teoria é importante para a segurança da informação, uma vez que hackear TI tornou-se um jogo ou hobby, deste modo algo necessita ser feito, pois estas ações custam aproximadamente até 2.7 bilhões de dólares anualmente (Lubua & Pretorius, 2019; Hu, Xu, Dinev, & Ling, 2011).

2.2.2. Fatores que influenciam a perceção de segurança

Segundo diversos autores (Furnell et al., 2008; Merkow & Breithaupt, 2014; Whitman & Mattord, 2017), como referido por Jesus Jorge (2021), a definição de segurança da informação, tradicionalmente assente nos princípios de confidencialidade, integridade e disponibilidade, tem sido progressivamente alargada, integrando ocorrências como danos acidentais ou intencionais, destruição, roubo, modificação não autorizada ou uso indevido, de forma a refletir a crescente complexidade e interconectividade dos ambientes organizacionais.

Cherdantseva e Hilton (2013), também citados por Jesus Jorge (2021), esclarecem que a confidencialidade diz respeito à proteção dos dados contra acessos não autorizados, a integridade corresponde à capacidade de prevenir ou reverter alterações indevidas, e a disponibilidade refere-se ao acesso à informação por utilizadores autorizados em tempo útil.

Whitman e Mattord (2017), igualmente referidos por Jesus Jorge (2021), destacam que o valor da informação depende das características que possui. Podendo aumentar ou diminuir consoante estas se alterem, e enfatizam a importância da sua disponibilização atempada para manter utilidade e pertinência. Para além disso, os mesmos autores identificam outras características relevantes, tais como autenticidade, exatidão, utilidade e posse.

Por sua vez, Merkow e Breithaupt (2014), como referido por Jesus Jorge (2021), estabelecem doze princípios para garantir o sucesso na segurança da informação, salientando que nada é totalmente seguro, que a complexidade é um obstáculo à segurança e que esta deve assentar numa abordagem de prevenção, deteção e correção.

Princípios
1. Não existe segurança absoluta.
2. Os três objetivos de segurança são a confidencialidade, a integridade e a disponibilidade.
3. A defesa em profundidade como estratégia.

4. Quando deixadas sozinhas, as pessoas tendem a tomar as piores decisões de segurança.
5. A segurança informática depende de dois tipos de requisitos: funcionais e de garantia.
6. A segurança através da obscuridade não é uma resposta.
7. Segurança= Gestão de riscos.
8. Os três tipos de controlos de segurança são preventivos, detetivos e responsivos.
9. A complexidade é inimiga da segurança.
10. O medo, a incerteza e a dúvida não funcionam na venda de segurança.
11. Pessoas, processos e tecnologia são todos necessários para garantir adequadamente a segurança de um sistema ou instalação.
12. A divulgação aberta de vulnerabilidades é benéfica para a segurança.

Fonte: Adaptado de Merkow e Breithaupt (2014, p.19-30)

Para organizar sistematicamente os fatores que afetam a segurança da informação, o autor utilizou o modelo conceitual de comportamento de segurança da informação desenvolvido por Leach (2003) conforme mostrado na figura 1.

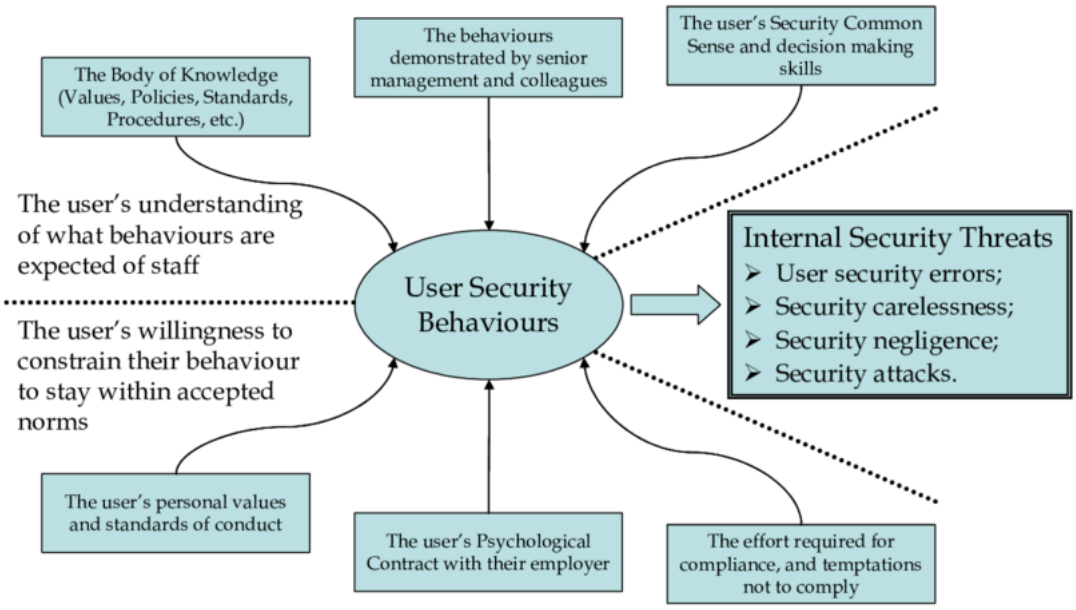


Figura 1- Factors affecting security behavior. Adapted from (Leach 2003)

O modelo de Leach (2003), Factors Affecting Security Behavior, procura compreender os fatores que influenciam o comportamento de segurança dos utilizadores dentro das organizações.

Os fatores influenciadores dividem-se em dois grupos, conforme ilustrado na figura 1. O primeiro grupo, que abrange a compreensão do utilizador sobre os comportamentos que a empresa espera dele, é distinto do segundo grupo, composto por fatores que influenciam a disposição pessoal do utilizador para restringir o seu comportamento de modo a manter-se dentro das normas aceites e aprovadas.

2.2.3 Estudos anteriores sobre os a perceção de segurança em contextos de tecnologia

A perceção de segurança da informação em contextos tecnológicos tem vindo a merecer uma crescente atenção na literatura científica, reflexo da importância cada vez maior que a proteção da informação assume no panorama digital contemporâneo. Importa salientar que esta perceção não se limita à avaliação objetiva dos sistemas de segurança existentes, mas é antes influenciada por múltiplos fatores de natureza subjetiva, como a confiança, a experiência prévia com incidentes de segurança, a literacia digital, entre outros (Li, Jung & Lee, 2021).

De acordo com diversos estudos, a perceção de segurança é compreendida como a avaliação subjetiva que os utilizadores fazem da eficácia, fiabilidade e transparência dos

mecanismos de proteção da informação. Esta perceção influencia diretamente os comportamentos dos utilizadores, nomeadamente no que diz respeito à adesão a políticas de segurança ou à adoção de práticas seguras no uso de sistemas de informação (Ifinedo, 2012).

No contexto organizacional, tem-se verificado que a perceção de segurança é significativamente moldada por fatores como o apoio da gestão, a cultura organizacional e a qualidade da comunicação interna. Ifinedo (2012) demonstrou que, quando os colaboradores percecionam um compromisso institucional com a segurança da informação, tendem a apresentar níveis mais elevados de conformidade com as políticas de segurança. De forma semelhante, Li, Jung e Lee (2021) analisaram o ambiente académico e constataram que a conformidade com as políticas de segurança depende fortemente da perceção de eficácia dos controlos implementados.

A literatura tem igualmente evidenciado a importância da confiança e da usabilidade dos sistemas como fatores centrais na construção da perceção de segurança. Vance, Siponen e Pahnila (2012) observaram que os utilizadores que confiam nos sistemas de informação e que consideram as suas interfaces intuitivas e acessíveis desenvolvem uma perceção mais favorável quanto à segurança, mesmo quando a robustez técnica desses sistemas possa ser questionável. Este achado sugere que a perceção de segurança pode divergir significativamente da realidade técnica, reforçando a necessidade de abordagens integradas que considerem tanto os aspetos técnicos como os humanos.

Em termos metodológicos, os estudos sobre a perceção de segurança da informação recorrem frequentemente a metodologias quantitativas, com destaque para a aplicação de inquéritos estruturados com escalas de *Likert* e para a utilização de Modelos de Equações Estruturais (SEM), permitindo explorar relações entre variáveis como a confiança, o risco percebido e a intenção de utilização de tecnologias seguras (Posey, Roberts & Lowry, 2010). Paralelamente, investigações qualitativas têm-se revelado úteis para compreender dimensões mais subjetivas e contextuais, nomeadamente através de entrevistas em profundidade.

Apesar do número crescente de estudos nesta área, subsistem lacunas significativas, nomeadamente no que concerne à análise da perceção de segurança em contextos culturais distintos, como é o caso de Portugal. Além disso, a rápida evolução tecnológica, em particular no domínio da inteligência artificial e dos sistemas de decisão

automatizados, coloca novos desafios à perceção de segurança, carecendo de investigações atualizadas e contextualmente situadas.

2.3. Comportamentos em Segurança de Informação

2.3.1. Comportamentos de Segurança de Informação e adoção de práticas seguras

Considerando os fortes impactos relacionados com as atividades de cibercrime, as suas causas, motivações e os seus efeitos foram amplamente estudados no passado (Anderson et al. 2013, Lagazio et al. 2014, Romanosky 2016).

Atualmente, a literatura em cibersegurança, sugere que é um tema bastante estudado e atual, em que a maioria das pesquisas esta centrada nas implicações para as organizações (Saridakis et al., 2015). Assim, contrariamente aos funcionários de uma empresa, os utilizadores domésticos não estão sujeitos a formação (Anderson et al., 2010), e frequentemente, não estão conscientes dos riscos do uso da internet, pois o mesmo não tem conhecimento preparado para a jornada online (Kritzinger et al., 2010). Alem disso, conforme afirma o autor Anderson et al., (2010), este tipo de utilizadores "representam um ponto fraco significativo para alcançar a segurança do ciberespaço na infraestrutura".

Um estudo recente da Comissão Europeia (2017) afirma que 51% da população europeia os cidadãos não se sentem bem informados sobre as ameaças cibernéticas e, o estudo também refere que 87% que o risco de se tornarem vítimas de cibercrime está aumentando. Estes valores são bastantes preocupantes, pois refletem a maioria dos indivíduos não se sente preparada para enfrentar os desafios atuais, ameaças que resultam de experiências pessoais, da experiência de outras pessoas e de notícias dos média (Tsai et al.,2016). Assim, pela falta de conhecimento em cibercrime é possível chegar-se a variável de consciencialização do cibercrime. Segundo o autor Dodge et al. (2007), a variável consciencialização é difícil de caracterizar devido a "natureza individual de cada utilizador".

Alem disso, existem diversos modelos que propuseram estudar a perceção de ameaça do individuo (Kritzinger et al., 2010; Poepjes et al.,2012), assim é importante analisar a influencia na intenção comportamental do utilizador e o comportamento protetor. As abordagens atuais incluem a Teoria da escolha racional (RCT), a Teoria da Reactância e a Teoria da Justiça, que são mais focadas no contexto organizacional. Em contrapartida, Rogers (1975, 1983) propôs a teoria da Proteção da Motivação (PMT), que se baseia na Teoria da ação Racionalizada (Fishbein et al.,1975).

Estudos têm enfatizado a importância do aspeto humano da segurança da informação. Björck (2005) afirmou que uma gestão adequada cria uma atmosfera de segurança da informação na organização e que, sem diretrizes claras, a empresa não teria sucesso em integrar adequadamente os procedimentos de segurança da informação. Albrechtsen (2008) argumentou que a qualidade da gestão afeta a conscientização, motivação e comportamento dos colaboradores, exigindo, portanto, o compromisso dos níveis de gestão com a manutenção da segurança da informação dentro da organização.

O comportamento inadequado em relação à segurança da informação pode derivar de várias qualidades do indivíduo: amargura, intenção maliciosa, falta de conhecimento, negligência, indiferença, entre outras. Alguns desses problemas podem ser resolvidos pela criação de conscientização. Funcionários que estão cientes das consequências devastadoras que as deficiências de segurança da informação podem causar tendem a ser menos indiferentes e mais conscientes das falhas de segurança no seu local de trabalho (Chen & Li, 2018). Embora os procedimentos formais de segurança da informação tenham um grande efeito sobre o comportamento dos funcionários, procedimentos que não promovem a conscientização não impactam o comportamento dos funcionários. Uma das formas eficazes de combater a negligência e a descuido é gerar conscientização entre os usuários. Estabelecer uma conscientização sobre as ameaças de segurança ajudará os funcionários a entender a gravidade das ameaças e a melhorar sua conformidade com os procedimentos de segurança (Gundu & Flowerday, 2013).

2.3.2. Fatores que influenciam os comportamentos de segurança

Nos dias de hoje, em que quase todas as atividades dependem de alguma forma de tecnologia, a segurança digital tornou-se um tema incontornável. Quando se fala em comportamentos de segurança digital, refere-se ao modo como os utilizadores agem no sentido de proteger os seus dados e equipamentos face a ameaças digitais. A verdade é que esses comportamentos não surgem por acaso: são moldados por diversos fatores, desde o conhecimento individual até ao ambiente organizacional em que a pessoa está inserida.

1. Fatores Individuais

Um dos aspetos que mais influencia a forma como alguém se comporta online é o seu nível de conhecimento. Vários estudos têm mostrado que quanto maior a literacia digital de um indivíduo, maior a probabilidade de este adotar práticas seguras (Ng, Kankanhalli, & Xu, 2009). Além disso, pessoas que percecionam maior risco face a ameaças digitais tendem a ser mais cautelosas.

Também não se pode ignorar o papel das caraterísticas psicológicas. Por exemplo, quem sente que tem controlo sobre o que acontece no ambiente digital (locus de controlo interno) geralmente toma mais iniciativa na proteção dos seus dados (Ifinedo, 2012). Outro ponto importante é a perceção de eficácia: se a pessoa acredita que determinada ação realmente protege os seus dados, é mais provável que a adote (Herath & Rao, 2009).

2. Fatores Organizacionais

Dentro das organizações, aquilo que se faz (ou não se faz) relativamente à segurança digital influência diretamente o comportamento dos colaboradores. Uma cultura organizacional forte neste domínio, com formação adequada e regras claras, tende a gerar mais adesão às boas práticas (Parsons et al., 2010). Por vezes, basta uma comunicação clara ou o exemplo da chefia para alterar comportamentos.

Além disso, o reconhecimento e valorização das boas práticas também têm impacto. Tal como em outras áreas da gestão, se os colaboradores forem recompensados por seguir as regras, há mais motivação para o fazer (Bulgurcu, Cavusoglu, & Benbasat, 2010).

3. Fatores Tecnológicos

A tecnologia em si pode facilitar ou dificultar comportamentos seguros. Quando os sistemas são fáceis de usar, mais intuitivos e pouco intrusivos, é natural que os utilizadores estejam mais dispostos a adotá-los. Pelo contrário, sistemas complicados ou que "atrapalham" o trabalho diário tendem a ser contornados (Vance, Siponen, & Pahnila, 2012).

Por isso, não basta exigir medidas de segurança – é fundamental que estas estejam desenhadas a pensar no utilizador, para que se tornem parte natural do dia a dia.

4. Fatores Socioculturais

Por fim, há também aspetos sociais e culturais que influenciam os comportamentos. Muitas vezes, as pessoas seguem o exemplo dos seus colegas. Se estiverem num ambiente onde todos se preocupam com a segurança, é provável que façam o mesmo. Mas se a cultura for de desleixo ou desvalorização da segurança, esse comportamento também se espalha (Workman, Bommer, & Straub, 2008).

Por outro lado, o país e a cultura, onde a pessoa vive também têm influência. Por exemplo, em sociedades mais sensíveis à privacidade, os utilizadores tendem a adotar mais medidas de proteção (Dinev, Goo, Hu, & Nam, 2009).

2.3.3. Estudos anteriores sobre os comportamentos de segurança em contextos de tecnologia

Vários estudos relevantes centram-se no indivíduo para identificar os fatores que motivam o comportamento de segurança, em associação com as intenções e atitudes dos utilizadores. Através de uma revisão da literatura, Lebek et al. (2014) concluíram que os construtos da Teoria da Ação Racional (TRA) e da Teoria do Comportamento Planeado (TPB) — nomeadamente atitude, normas subjetivas e controlo comportamental percebido (que inclui autoeficácia e controlabilidade) — são bons preditores da intenção de conformidade com a Política de Segurança da Informação (ISP). Além disso, identificaram que o compromisso organizacional, a perceção da eficácia das ações do colaborador e a consciencialização tecnológica também podem influenciar a intenção de conformidade dos utilizadores.

Os autores argumentam que o comportamento real não pode ser avaliado com precisão, uma vez que as intenções nem sempre se traduzem no comportamento esperado, sendo necessário o desenvolvimento de novos métodos para medir o comportamento efetivo (Lebek et al., 2014; Crossler et al., 2013). No mesmo sentido, Zhang et al. (2009) demonstram que o controlo comportamental percebido e a atitude têm um impacto significativo na intenção de conformidade com as ISPs. Além disso, verificaram que a perceção dos mecanismos de proteção da segurança (um conceito semelhante à eficácia da resposta) tem um impacto negativo na intenção de conformidade. Isso sugere que, se os colaboradores considerarem que existem fortes mecanismos técnicos de proteção para salvaguardar os ativos organizacionais, a sua intenção de cumprimento poderá diminuir (Zhang et al., 2009).

Sommestad et al. (2014) analisam o papel do indivíduo na conformidade com as políticas de segurança, identificando que as crenças (controlo comportamental percebido, avaliação da ameaça, norma descritiva e eficácia da resposta) e os valores (congruência de valores percebida, legitimidade percebida e consciencialização sobre segurança da informação) desempenham um papel crucial no cumprimento das normas de segurança. Além disso, os autores sugerem que as recompensas e punições não são bons preditores de conformidade.

Por sua vez, Son (2011) concluiu que a congruência de valores percebida e a legitimidade percebida influenciam significativamente o comportamento dos colaboradores, produzindo melhores resultados do que fatores baseados na motivação

extrínseca, como a severidade e a certeza percebidas da punição. Ifinedo (2012), apoiando-se na Teoria da Motivação para a Proteção e na Teoria do Comportamento Planeado, demonstrou que a vulnerabilidade percebida, a eficácia da resposta, a autoeficácia, a atitude face à conformidade com as políticas de segurança da informação (ISP) e as normas subjetivas influenciam a intenção de cumprir essas políticas. O estudo destaca, ainda, que os colaboradores são influenciados pelos seus colegas, superiores e outros membros do ambiente organizacional no que respeita à conformidade com as normas de segurança.

De forma semelhante, Siponen et al. (2006) demonstraram que a visibilidade entendida como o grau de acesso dos indivíduos a materiais relacionados com a segurança, tanto dentro como fora da organização e as crenças normativas influenciam a avaliação da ameaça, a qual tem impacto na intenção dos indivíduos de cumprir as políticas de segurança da informação. Num estudo posterior, Siponen et al. (2014) analisaram separadamente os dois componentes da avaliação da ameaça, concluindo que tanto a vulnerabilidade percebida quanto a severidade percebida afetam significativamente a intenção de conformidade. Além disso, identificaram que a autoeficácia, a atitude e as crenças normativas influenciam a intenção de cumprimento, sendo esta um forte preditor da conformidade real.

Capítulo 3 – Metodologia

O presente estudo, seguiu uma abordagem metodológica quantitativa, dado que a recolha dos dados se realizou por intermedio de um questionário disponibilizado via google Forms.

A investigação tem natureza teórica, na qual se pretendem aprofundar conceitos relacionados com a inteligência artificial, perceção de segurança e comportamento.

A pesquisa seguiu uma cariz descritiva, uma vez que o estudo visa compreender a perceção de segurança da informação no contexto da utilização de tecnologias de inteligência artificial em Portugal.

Para a realização desta investigação, optou-se por uma pesquisa por *survey*. A pesquisa por *survey* permite recolher informação padronizada de um número significativo de participantes, possibilitando uma análise estatística representativa da amostra.

Assim, foi elaborado um questionário com base na revisão de literatura sobre a segurança da informação e Inteligência Artificial (IA). Este questionário foi composto por perguntas fechadas e escalas de tipo Likert, que têm como principal objetivo mensurar o grau de concordância dos participantes relativamente a diferentes afirmações sobre a segurança, confiança e a utilização de IA.

O questionário foi disponibilizado online, via google Forms, garantindo o anonimato e a confidencialidade das respostas.

3.1. Desenho de investigação

De acordo com Pardal e Correia (1995), a metodologia corresponde ao conjunto estruturado de orientações que guia a investigação. Segue um sistema de normas que permite selecionar e articular as técnicas adequadas, possibilitando assim o desenvolvimento coerente do processo de verificação empírica.

A investigação foi concebida com o objetivo de cumprir os objetivos propostos do estudo, começando pela definição da metodologia de investigação e, em seguida, pelo planeamento da sua execução.

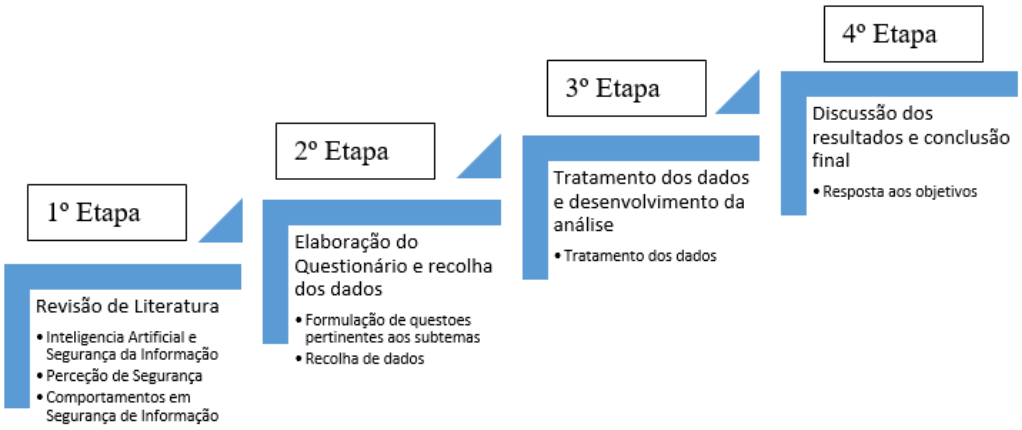


Figura 2 - Metodologia do Estudo. Fonte: elaborado pelo autor

A primeira etapa deste estudo consistiu na pesquisa de artigos científicos relacionados com os temas e subtemas em análise, nomeadamente Inteligência artificial, Segurança de informação, perceção de segurança e comportamentos em segurança de informação, recorrendo a plataformas como o B-on, Google Académico, ScienceDirect e o Scopus para acesso aos artigos científicos.

Na segunda etapa, procedeu-se à elaboração do questionário e à recolha dos dados. O questionário foi estruturado em dois blocos: o primeiro tem como objetivo recolher informações sobre o perfil sociodemográfico dos participantes, incluindo género, a idade e o nível de qualificação; o segundo procurou identificar os fatores que influenciam a perceção de segurança e de inteligência artificial em Portugal.

A terceira etapa incidiu sobre o tratamento e análise dos dados. Para estudar as relações entre as variáveis, escolheu-se o modelo UTAUT2, dado que este se revela adequado para explicar a aceitação e utilização de uma tecnologia por parte do consumidor (Arenas-Gaitán et al., 2015)

Na quarta e última etapa, realizou-se a análise dos resultados obtidos, com o objetivo de interpretá-los e discuti-los, permitindo concluir o estudo e verificar o alcance dos objetivos definidos.

O objetivo desta investigação centra-se na obtenção de novos dados empíricos, que possibilitem testar deduções derivadas da teoria e contribuam para o enriquecimento da

literatura na área da segurança da informação, com interesse académico e potencial relevância prática na perceção da utilização desta tecnologia (Hill & Hill, 1998).

3.2. Objetivos de investigação

A definição de um objetivo geral para uma dissertação exige, antes de mais, a identificação clara de uma questão ou problema dentro da área de estudo. Tal como é apresentado por Quivy e Campenhoudt (1998), a construção de uma pergunta de partida deve privilegiar a compreensão e não o julgamento, orientando-se para o conhecimento em vez da demonstração. Os autores defendem que essa pergunta deve admitir múltiplas respostas possíveis, evitando pressupor uma conclusão prévia. Além disso, sublinham que a pergunta de investigação deve incidir sobre fenómenos existentes ou já verificados, procurando compreender o contexto, as limitações e as oportunidades que este apresenta, em vez de tentar antecipar ou prever acontecimentos futuros. Esta perspetiva foi igualmente mencionada por Fonseca (2013), ao destacar a importância de formular questões de investigação que permitam captar e interpretar de forma rigorosa a realidade em análise.

Conforme referido anteriormente, o principal objetivo que se pretende atingir com o presente estudo é compreender como é que a perceção de segurança da informação em relação a automação é importante para a população portuguesa. Face ao exposto, surgiram os seguintes objetivos específicos:

1. Identificar as expectativas, opiniões sobre a automação;
2. Determinar em que medida é que a segurança na automação é uma preocupação e como influencia as atitudes em relação a automação;
3. Conhecer a perceção dos comportamentos e sentimentos relativamente a automação;
4. Perceber em que medida a perceção de segurança se reflete nos comportamentos e sentimentos face a automação.

3.3. Desenho de Hipóteses

O modelo de investigação proposto para este estudo foi adaptado do modelo UTAUT2. Foram acrescentados dois construtos ao modelo que dizem respeito à aceitação da automação e à utilização da automação. A figura 5 retrata o modelo adaptado do UTAUT2 que foi implementado no presente estudo.

O modelo UTAUT (*Unified Theory of Acceptance and Use of Technology*) surgiu como uma evolução do modelo de TAM, propondo um conjunto de quatro fatores fundamentais para explicar tanto a intenção de utilização de uma tecnologia como o comportamento real de uso. Estes fatores incluem a expectativa de desempenho, a expectativa de esforço, a influência social e as condições facilitadoras. O modelo integra ainda quatro variáveis moderadoras: a idade, o género, experiência do indivíduo e a voluntariedade do uso. A figura 3 ilustra a estrutura deste modelo.

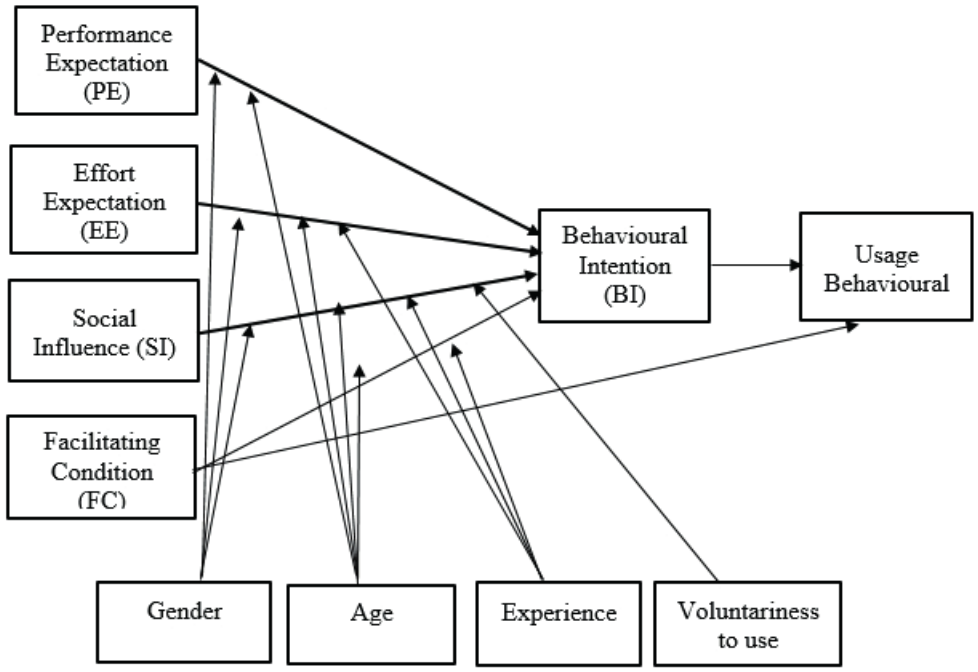


Figura 3 -Teoria Unificada de Aceitação e Uso de Tecnologia (UTAUT) (Venkatesh et al., 2003)

Posteriormente, Venkatesh et al. (2012) publicaram o modelo UTAUT2, que se encontra representado na Figura 4. Este modelo é uma extensão do UTAUT. Todavia, este modelo foca-se no contexto de uso de um sistema por parte do consumidor, em

contexto não organizacional, e que inclui três novos construtos: motivação hedónica, valor do preço e hábito (Venkatesh et al., 2012).

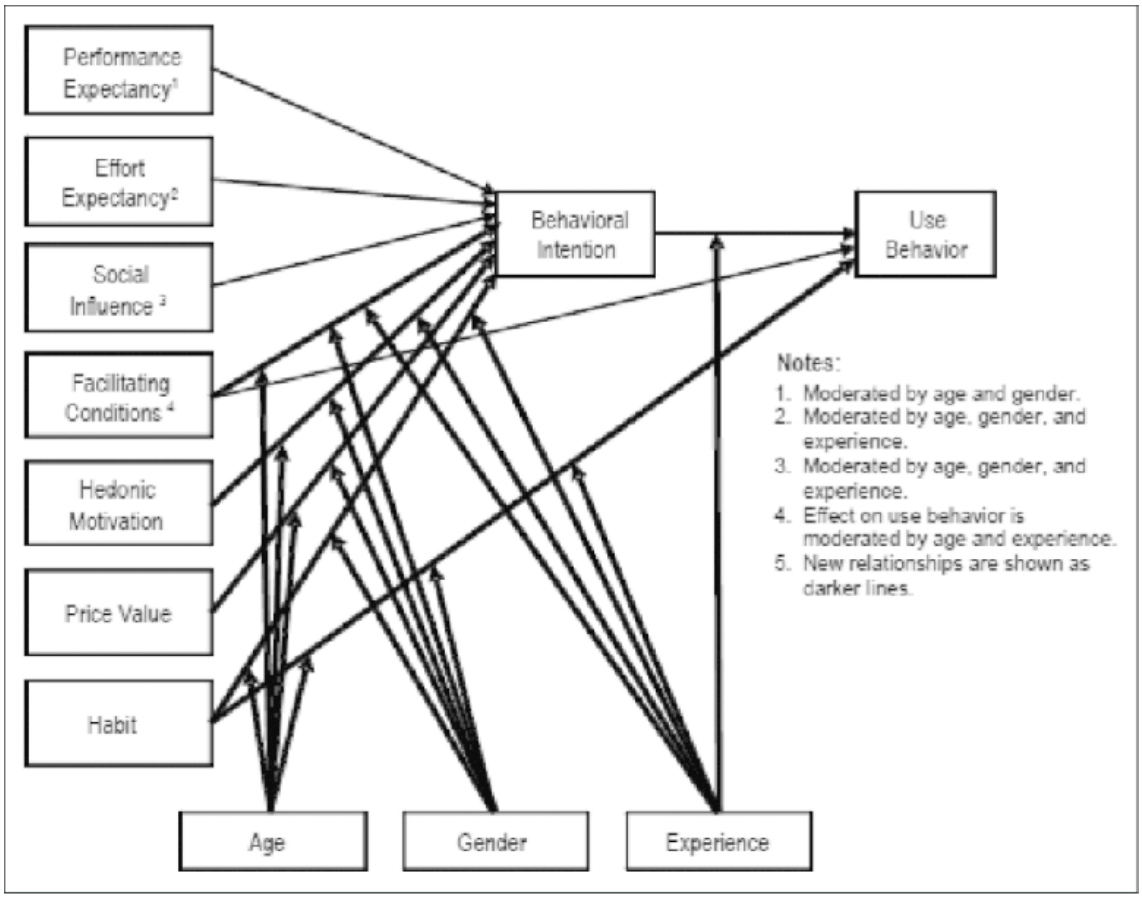


Figura 4 - Teoria Unificada de Aceitação e Uso de Tecnologia 2 (UTAUT2) (Venkatesh et al., 2012)

A escolha do modelo UTAUT2 como base teórica deste estudo justifica-se pela sua capacidade de oferecer uma estrutura abrangente e validada para analisar os fatores que influenciam a aceitação e utilização de tecnologias por parte dos indivíduos. O modelo original UTAUT foi desenvolvido para contextos organizacionais; porém, a sua versão mais recente, o UTAUT2, engloba variáveis adicionais, tais como a motivação hedónica, hábito e valor do preço, que permitem uma compreensão mais completa do comportamento do utilizador em diferentes cenários (Venkatesh, Thong, & Xu, 2012).

Ainda assim, para o contexto deste estudo, propõe-se uma adaptação do modelo, considerando como construto a perceção de segurança, e as características demográficas, procurando compreender a sua influência quer na adoção, quer no uso efetivo destas ferramentas (cf. Figura 5).

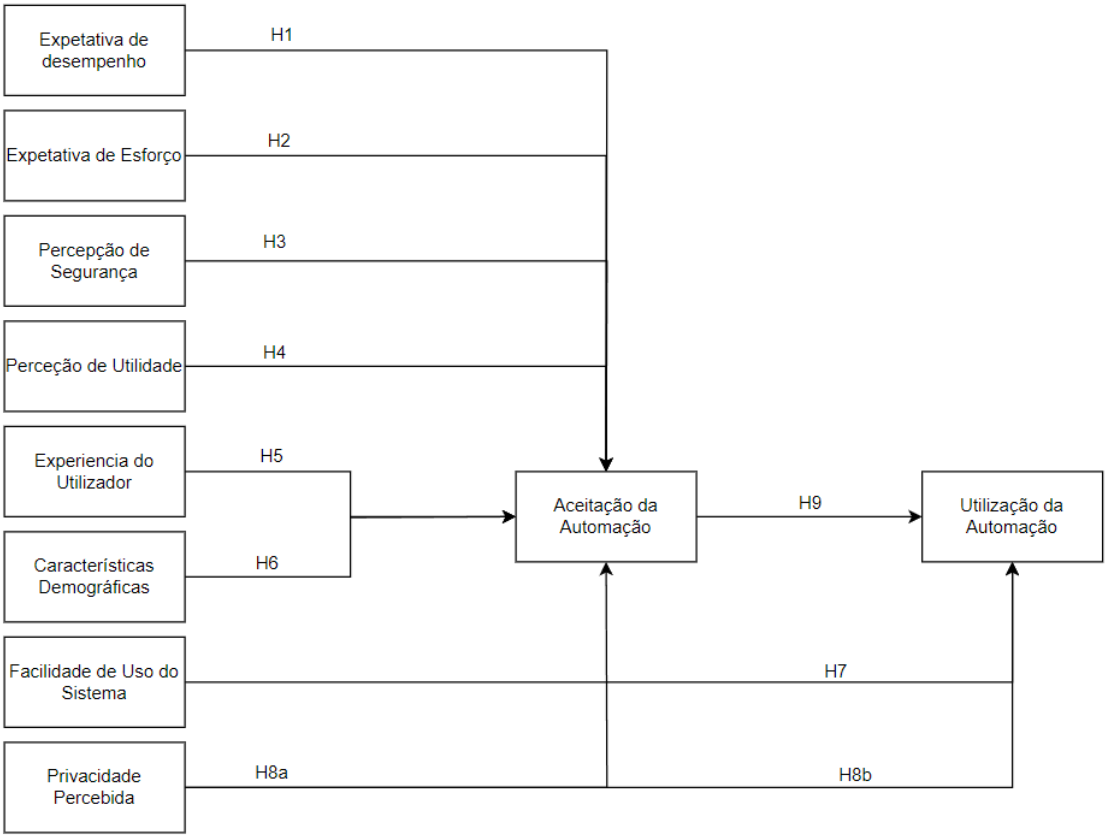


Figura 5 - Modelo de investigação proposto adaptado do modelo UTAUT2

O desenho do questionário que foi aplicado para recolha dos dados sobre o estudo foi feito com base neste modelo adaptado, apresentado na Figura 5. De seguida, apresentam-se os construtos relativamente à pertinência e contextualização do tema em estudo, sendo também apresentadas as hipóteses exploradas.

Expectativa de desempenho

A expectativa de desempenho corresponde ao grau em que o uso de uma tecnologia é percebido como benéfico para o utilizador na realização de determinadas tarefas, sendo este conceito equivalente ao de Utilidade Percebida no Modelo de Aceitação de Tecnologia (TAM) (Venkatesh et al. 2003; Venkatesh et al., 2012).

Perante estes argumentos, foi formulada a seguinte hipótese:

H1: *Quanto maior for a expetativa de desempenho maior será a aceitação da automação*

Expectativa de esforço

Por sua vez, a expetativa de esforço refere-se à perceção do utilizador relativamente à facilidade ou dificuldade de utilização de uma tecnologia, estando este conceito associado à Perceção de Facilidade de Utilização no modelo TAM (Venkatesh et al. 2003; Venkatesh et al., 2012).

Perante estes argumentos, foi formulada a seguinte hipótese:

H2: *Quanto maior for a expetativa de esforço menor será a aceitação da automação.*

Perceção de segurança

A perceção de segurança refere-se ao sentimento individual e compreensão de vários riscos objetivos existentes fora e enfatiza a influência da experiência de julgamento intuitivo individual (Zhang, M., et al, 2017) e sentimento subjetivo na cognição para analisar, controlar e gerenciar os riscos (Zhang, M., et al, 2017). A perceção de segurança é determinada pela interceção de vários fatores pessoais, sociais e institucionais (M.A. Harclerode, et al, 2016).

Na literatura de Sistemas de Informação, esta perceção funciona como uma crença contextual que reduz o risco percebido e reforça a confiança, dos mecanismos centrais para a intenção e o comportamento de uso de tecnologias (Pavlou, 2003; Kim, Ferrin, & Rao, 2008; Featherman & Pavlou, 2003; Venkatesh, Morris, Davis, & Davis, 2003). Há evidência consistente de que maior perceção de segurança está associada a maior aceitação e adoção de sistemas, ao diminuir incertezas sobre perdas financeiras, fraudes

ou divulgação indevida de informação (Salisbury, Pearson, Pearson, & Miller, 2001; Bélanger, Hiller, & Smith, 2002).

H3: *Quanto maior a perceção de segurança maior será a aceitação da automação.*

Perceção de utilidade

A perceção de utilidade é uma das variáveis mais estudadas quando se trata da adoção de tecnologia (Jeyaraj et al., 2006). Para Davis (1989), a perceção de utilidade é definida como o grau em que uma pessoa acredita que o uso de um determinado sistema aumentaria o seu desempenho em suas atividades.

Perante estes argumentos, foi formulada a seguinte hipótese:

H4: *Quanto menor for a perceção de utilidade menor será a aceitação da automação.*

Experiência do utilizador

O autor Norman introduziu o conceito de Experiência do utilizador pela primeira vez em 1995 a respeito de uma pesquisa e aplicação da interface humana (Norman et al., 1995). Na sua génese, o conceito de experiência do utilizador é entendido como a experiência entre o ser humano e o sistema, também a respeito de vários aspetos que ultrapassam a "interface humana" ou a "usabilidade". A norma ISO 9241-210 incentiva a práticas de design centrado no ser humano que enfatizam a clareza, controlo e feedback útil. Uma Experiência de utilizador bem construída tende a potenciar tanto a perceção de segurança como a perceção de utilidade, criando condições favoráveis a aceitação e ao uso sustentado (ISO, 2019; Lee & See, 2004).

H5: *Quanto maior for a experiência do utilizador maior será a aceitação da automação.*

Características demográficas

No presente estudo, as características demográficas referem-se a atributos sociodemográficos observáveis dos participantes que tipicamente se incluem em investigações de sistemas de informação e comportamento organizacional - tais como a idade, género, escolaridade, antiguidade, função. Ao mesmo tempo, sendo variáveis exogéneas e de natureza objetiva, estas características são frequentemente usadas como moderadores ou variáveis de controlo em modelos de aceitação e uso da tecnologia, devido ao seu potencial para condicionar crenças, motivações e comportamentos de adoção (Venkatesh, Morris, Davis, & Davis, 2003; Venkatesh, Thong, & Xu, 2012). Especialmente, a idade tem sido consistentemente apontada como um fator diferenciador na adoção/uso de tecnologia, com evidencia de que utilizadores mais jovens tendem a apresentar maior propensão para aceitar novas tecnologias, por outro lado utilizadores mais velhos revelam, em média, barreiras acrescidas associadas a experiência prévia, custos de transição e diferenças de competências digitais (Morris & Venkatesh, 2000; Czaja et al., 2006; Rogers, 2003).

Deste modo, para efeitos deste estudo, trata-se "características demográficas" como um vetor de atributos em que a diminuição de certos valores (em particular, idade e antiguidade) é teoricamente expetável que aumente a aceitação da automação, mantendo-se as restantes características como controlos e potenciais moderadores contextuais (Venkatesh et al., 2003; Venkatesh et al., 2012).

H6: *Quanto menor forem as características demográficas maior será a aceitação da automação*

Facilidade de uso do sistema

A facilidade de Uso tem sido destacada como um fator determinante na aceitação tecnológica, tal como apresentado por Venkatesh e Davis, (2000, conforme citado em Matias, 2020). Além disso, a definição clássica deste construto, associada ao grau de esforço percebido pelo utilizador, segue a formulação de Davis et al., (1989, conforme citado em Matias, 2020).

A facilidade de uso tem como um dos seus efeitos a melhorar a atitude relativamente à adoção, independentemente da utilidade do produto (Davis et al., 1989). Assim sendo, é possível dizer que a facilidade de uso influencia a intenção de uso dos consumidores.

Perante estes argumentos, foi formulada a seguinte hipótese:

H7: *Quanto menor for a facilidade de uso do sistema menor será a aceitação da automação*

Privacidade percebida

De acordo com Pires (2022), Mcleod (2009, citado por Pires, 2022), define a privacidade percebida como a crença do utilizador de que a informação submetida online permanece confidencial. As questões relacionadas com a privacidade e a perceção dos utilizadores têm sido estudadas em diferentes contextos e tecnologias.

De acordo com Eckert, Dal Bó, Milan e Eberle (2017), Van Slyke et al. (2006, citado por Eckert et al., 2017) concluíram que a preocupação com a privacidade da informação afeta a perceção de risco e, consequentemente, a segurança dos consumidores. Udo (2001, citado por Eckert et al., 2017) sugere que a privacidade percebida no ambiente online aumenta a perceção de segurança. Miyazaki e Fernandes (2001, citado por Eckert et al., 2017) também defendem que, quando a proteção da privacidade dos consumidores é considerada, observa-se uma maior perceção de segurança.

Perante estes argumentos, foi formulada a seguinte hipótese:

H8a: *Quanto menor for a Privacidade Percebida menor será a Aceitação da automação*

Utilização da automação

No presente estudo, define-se a utilização da automação como o grau em que as tarefas organizacionais são executadas por sistemas tecnológicos com mínima intervenção humana, abrangendo funções de aquisição de informação, analise, decisão e execução, e variando em níveis de autonomia desde apoio à decisão até execução automática (Parasuraman, Sheridan, & Wickens, 2000; Endsley & Kaber, 1999). Esta visão é coerente com a literatura sobre interação humano-automação e com o uso corrente de soluções digitais como RPA e IA aplicadas a processos administrativos e de apoio (Willcocks & Lacity, 2016; Davenport & Ronanki, 2018).

O conceito de privacidade percebida é entendido como a perceção do individuo de que os seus dados pessoais são adequadamente protegidos, controlados e utilizados de forma transparente pelo sistema, sendo o contraponto das preocupações com privacidade nos modelos de *privacy calculus* e no construto IUIPC (Malhotra, Kim, & Agarwal, 2004; Dinev & Hart, 2006). A evidencia acumulada em Sistemas de informação mostra que níveis mais elevados de privacidade tendem a reforçar a adoção e o uso de tecnologias, quer de forma direta, quer indiretamente através da confiança (Smith, Dinev, & Xu, 2011; Bélanger & Crossler, 2011). Simultaneamente, os modelos de aceitação tecnológica (TAM/UTAUT) sugerem que crenças contextuais como privacidade e segurança funcionam como facilitadores das crenças centrais (utilidade e facilidade de uso), aumentando a intenção e o comportamento de uso efetivo (Davis, 1989; Venkatesh, Morris, Davis, & Davis, 2003).

H8b: *Quanto maior for a privacidade percebida maior será a utilização da automação*

Aceitação da automação

De acordo com os autores Parasuraman e Riley (1997) a automação foi definida como uma tecnologia que executa uma função que antes era desempenhada por humanos. Assim ao executar total ou parcialmente as funções anteriormente desempenhadas por humanos, a automação torna-se um complemento para as pessoas no cumprimento das metas das tarefas. Porém, a automação raramente substitui o ser humano: a automação não substitui simplesmente a pessoa e executa as tarefas que antes eram executadas por ela.

De acordo com Muir (1994), a aceitação da automação por parte do utilizador depende muito de diversos fatores, um dos quais é a confiança de que a tecnologia funcionara

como esperado (Lee e See, 2004; Muir, 1987, 1994; Wickens e Dixon, 2007). Uma automação menos fiável resultara na desconfiança do utilizador na automação, preferindo, por isso, níveis mais baixos ou mesmo nenhuma automação. Riley (1994) defende que a aceitação da automação é influenciada por fatores para além da tecnologia e inclui fatores do local de trabalho, como a satisfação no trabalho.

Perante estes argumentos, foi formulada a seguinte hipótese:

H9: *Quanto maior for a aceitação da automação maior será a utilização da automação*

3.4. Definição do tamanho da amostra

A amostra consiste numa parcela da população total sobre a qual se realiza o estudo. Para que os resultados possam ser generalizados à população, a amostra deve ser representativa desta (Fortin, 1999). O universo da investigação corresponde à população portuguesa, que em 2024 era composta por 10 749 635 indivíduos, segundo dados do INE (2024). O tamanho ideal da amostra foi determinado com base no método de Krejcie e Morgan (1970), aplicando-se a fórmula proposta por estes proposta:

$$S = \frac{X^2 \times N \times P \times (1-P)}{d^2 \times (N-1) + X^2 \times P \times (1-P)}$$

Os parâmetros utilizados foram os seguintes: número de amostra (S = 10749635); Nível de confiança para α igual a 0,05 (X= 3,841); Margem de erro de 5% (d= 0,05).

$$S = \frac{3.841 \times 10\,749\,635 \times 0.5 \times (1-0.5)}{0.05^2 \times (10\,749\,635-1) + 3.841 \times 0.5 \times (1-0.5)} \approx 384.6$$

Conclui-se que para este estudo a amostra devera ser formada por 385 indivíduos (n= 385).

O questionário foi aplicado durante o dia 26 de junho de 2024 até ao dia 29 de janeiro de 2025. Numa fase inicial, este foi partilhado individualmente, com os contactos mais diretos do autor do estudo, através do WhatsApp e do Linkedin. Posteriormente, foram realizadas publicações periódicas nas redes sociais Facebook e Instagram. Deste forma, foi possível obter um total de 370 respostas, das quais apenas 251 foram totalmente preenchidas. Assim, apenas estas 251 respostas forma consideradas válidas para efeitos de análise.

3.5. Desenho dos instrumentos de recolha de dados

O presente estudo recorreu a um questionário estruturado como principal instrumento de recolha de dados. Este foi desenvolvido pelo autor, tendo por base os objetivos da investigação e a revisão de literatura existente sobre a perceção de segurança e a utilização da Inteligência Artificial (IA). O questionário foi criado na plataforma Google Forms, permitindo a sua distribuição digital e facilitando a participação por parte dos inquiridos.

O instrumento foi composto por um total de 32 questões, organizadas em duas secções principais. A primeira secção visava recolher dados sociodemográficos dos participantes, como idade, género, habilitações literárias. Já a segunda secção focava-se no nível de familiaridade com tecnologias de Inteligência Artificial, bem como na perceção de segurança associada à sua utilização em diferentes contextos, como a segurança pública, a vigilância ou os serviços digitais.

Todas as perguntas apresentadas foram de resposta fechada, maioritariamente baseadas em escalas de Likert de 5 pontos (1 – Discordo totalmente; 5 – Concordo totalmente), com o objetivo de medir o grau de concordância dos participantes com determinadas afirmações relacionadas com a IA. Não foram incluídas questões de resposta aberta.

3.6. Recolha de dados

A recolha de dados foi realizada entre os dias 26 de junho de 2024 e 29 de janeiro de 2025, recorrendo a um questionário online disponibilizado através da plataforma Google Forms. A partilha do questionário decorreu em duas fases distintas: numa fase inicial, foi enviado diretamente a contactos pessoais do autor, utilizando aplicações como o WhatsApp e o LinkedIn; numa segunda fase, a divulgação passou a ser feita de forma mais alargada, através de publicações regulares nas redes sociais Facebook e Instagram, com o objetivo de alcançar um maior número de participantes.

O processo de amostragem adotado foi de natureza não probabilística, por conveniência, uma vez que a participação no estudo dependeu da acessibilidade aos potenciais respondentes e da sua disponibilidade para colaborar. Como critérios de inclusão, considerou-se apenas a necessidade de os participantes serem residentes em Portugal e terem idade igual ou superior a 18 anos.

No total, foram obtidas 370 respostas ao questionário, das quais 251 se encontravam completas e foram, por isso, consideradas válidas para efeitos de análise. Estas respostas formam a base da investigação empírica apresentada no capítulo seguinte.

Capítulo 4 – Análise e discussão dos resultados

Os resultados apresentados nesta secção do trabalho visam dar resposta à questão de partida e aos objetivos definidos para a investigação científica. Para tal, procedeu-se à interpretação dos dados recolhidos através do questionário, recorrendo a métodos estatísticos apropriados.

4.1. Fase Quantitativa

4.1.1 Perfil e dimensão da amostra

A amostra considerada neste estudo é composta por 251 participantes. Numa primeira etapa, realizou-se uma análise das variáveis sociodemográficas que caracterizam a amostra, nomeadamente o género, a idade e o nível de escolaridade concluído. Posteriormente, procedeu-se a uma análise quantitativa das respostas, permitindo extrair dados relevantes para a formulação de conclusões. Das 251 respostas recolhidas, 137 participantes (54,6%) são do sexo masculino e 106 (42,2%) do sexo feminino, enquanto um pequeno grupo de 8 indivíduos (3,2%) optou por não declarar o seu género. Assim, a amostra apresenta uma distribuição relativamente equilibrada entre os géneros, com uma ligeira predominância do sexo masculino.

2- Indique o seu género:

		Frequência	Porcentagem	Porcentagem válida	Porcentagem acumulativa
Válido	Feminino	106	42,2	42,2	42,2
	Masculino	137	54,6	54,6	96,8
	Prefiro não dizer	8	3,2	3,2	100,0
	Total	251	100,0	100,0	

Tabela 1 - Caracterização da amostra (género)

Fonte: Elaborado pelo autor

Relativamente a variável “idade” observou-se uma predominância de indivíduos mais jovens na amostra. A faixa etária dos 18-24 é a mais representada, com 90 respondentes (35,9%), seguida muito de perto pela faixa dos 25-34 anos, com 89 participantes (35,5%). Em conjunto, estas duas faixas etárias perfazem 71,3 % da amostra, o que evidencia uma clara concentração de adultos jovens no estudo. As restantes faixas etárias surgem com representações mais reduzidas: 35-44 anos com 31 participantes

(12,4%), 45-54 anos com 19 (7,6%), 55-64 anos com 13 participantes (5,2%) e 65 anos ou mais com apenas 9 participantes (3,6%). Esta distribuição etária poderá refletir o perfil dos utilizadores da plataforma onde o inquérito foi divulgado, sendo um fator relevante a considerar na análise das perceções tendo em consideração a tecnologia e a inteligência artificial.

1- Indique a sua idade:

		Frequência	Porcentagem	Porcentagem válida	Porcentagem acumulativa
Válido	18-24 anos	90	35,9	35,9	35,9
	25-34 anos	89	35,5	35,5	71,3
	35-44 anos	31	12,4	12,4	83,7
	45-54 anos	19	7,6	7,6	91,2
	55-64 anos	13	5,2	5,2	96,4
	65 anos ou mais	9	3,6	3,6	100,0
	Total	251	100,0	100,0	

Tabela 2 - Caracterização da amostra (idade)

Fonte: Elaborado pelo Autor

No que respeita ao grau de escolaridade, a amostra caracteriza-se por um elevado número de inquiridos declarou possuir o ensino secundário (36,7%). Em seguida, temos a licenciatura (27,9%), o ensino básico (15,9%), o mestrado (10,8%), a pós-graduação (5,6%) e o doutoramento (3,2%). A percentagem acumulada revela que 83,7% dos participantes possuem, no máximo, formação ao nível da licenciatura, o que indica uma predominância de níveis médios de escolaridade na amostra, com reduzida representação de graus académicos avançados. Este fator poderá influenciar a forma como determinados temas — nomeadamente os relacionados com tecnologia e inteligência artificial — são compreendidos ou percecionados.

3- Indique a sua escolaridade:

		Frequência	Porcentagem	Porcentagem válida	Porcentagem acumulativa
Válido	Doutoramento	8	3,2	3,2	3,2
	Ensino Básico	40	15,9	15,9	19,1
	Ensino Secundário	92	36,7	36,7	55,8
	Licenciatura	70	27,9	27,9	83,7
	Mestrado	27	10,8	10,8	94,4
	Pós-Graduação	14	5,6	5,6	100,0
	Total	251	100,0	100,0	

Tabela 3 - Caracterização da amostra (escolaridade)

Fonte: Elaborado pelo Autor

4.1.2 Análise exploratória dos dados

Antes de avançar para análises estatísticas mais complexas, procedeu-se a uma análise exploratória dos dados com o intuito de compreender melhor o comportamento das variáveis em estudo, identificar padrões nas respostas e garantir a qualidade da informação recolhida.

Esta análise incidiu sobre um conjunto de afirmações relacionadas com a perceção dos participantes face à automação e aos sistemas baseados em inteligência artificial, nomeadamente no que respeita à utilidade, desempenho, esforço, segurança, privacidade, facilidade de uso e aceitação da tecnologia. Para cada item, foram calculadas medidas de tendência central (média, mediana e moda) e de dispersão (desvio padrão), considerando um total de 251 respostas válidas.

De forma geral, os resultados indicam uma perceção tendencialmente positiva em relação à automação. As afirmações com médias mais elevadas refletem uma atitude favorável face à experiência com estes sistemas e ao seu impacto no desempenho profissional. Por exemplo, os participantes concordaram com expressões como *"A automação pode aumentar a qualidade do meu trabalho"* (M = 3,41; DP = 1,210) e *"Quanto mais uso os sistemas automatizados, mais confiante fico na sua eficácia"* (M = 3,40; DP = 1,150). Estes resultados sugerem que, para uma parte significativa da amostra, a experiência prática com a automação é valorizada e considerada eficaz.

Paralelamente, observou-se uma valorização da utilidade e do impacto da automação nas atividades do dia a dia, com respostas como *"A automação proporciona uma utilidade significativa nas minhas atividades diárias"* (M = 3,18; DP = 1,170) e *"A*

utilização de sistemas automatizados pode ajudar a alcançar os objetivos de desempenho mais rapidamente" (M = 3,15; DP = 1,261).

No entanto, nem todos os resultados foram uniformemente positivos. Identificaram-se algumas reservas por parte dos participantes relativamente à proteção dos seus dados e à privacidade. Itens como *"Eu confio que os sistemas automatizados protegem adequadamente os meus dados privados"* (M = 2,91; DP = 1,110) e *"O uso frequente da automação aumenta as minhas preocupações com a privacidade"* (M = 3,12; DP = 1,232) revelam uma maior dispersão nas respostas e indicam que este é um tema sensível para uma parte da amostra.

Também a experiência global com os sistemas automatizados foi avaliada de forma moderadamente positiva. Afirmações como *"A minha experiência geral com os sistemas automatizados tem sido positiva"* (M = 3,20; DP = 1,127) e *"A automação torna as interações com os sistemas mais agradáveis e satisfatórias"* (M = 3,08; DP = 1,103) sugerem que, embora haja margem para melhorias, a aceitação e usabilidade são, em geral, bem avaliadas.

Esta análise inicial permite concluir que, apesar das preocupações demonstradas em relação à privacidade e segurança dos dados, os participantes reconhecem de forma clara os benefícios da automação em termos de utilidade, desempenho e eficiência. Estes resultados sustentam a pertinência de aprofundar a análise, através de métodos estatísticos multivariados, como a análise fatorial, que permitirá identificar as dimensões subjacentes às variáveis observadas.

4.1.3 Análise das correlações de Pearson

A análise das correlações de Pearson mostra que todas as variáveis em estudo — Privacidade, Aceitação, Segurança, Esforço e Desempenho — se relacionam positivamente entre si, com significância estatística elevada ($p < ,001$ em todas as associações). Os coeficientes variam entre ,578 (relação entre Privacidade e Aceitação) e ,724 (relação entre Segurança e Esforço e Desempenho), magnitudes que, de acordo com referenciais usuais, se enquadram no patamar "forte". Em particular, observam-se correlações de ,608 entre Privacidade e Segurança, ,683 entre Privacidade e Esforço e Desempenho, ,648 entre Aceitação e Segurança e ,693 entre Aceitação e Esforço e Desempenho, destacando-se a associação mais elevada entre Segurança e Esforço e Desempenho ($r = ,724$). Em termos substantivos, estes resultados indicam que perceções mais favoráveis de privacidade e segurança estão associadas a maior aceitação e a níveis superiores de esforço e desempenho, sugerindo que estas dimensões tendem a variar no mesmo sentido no contexto analisado.

Correlações

		Privacidade	Aceitação	segurança	Esforço_e_Desempenho
Privacidade	Correlação de Pearson	1	,578**	,608**	,683**
	Sig. (2 extremidades)		<,001	<,001	<,001
	N	251	251	251	251
Aceitação	Correlação de Pearson	,578**	1	,648**	,693**
	Sig. (2 extremidades)	<,001		<,001	<,001
	N	251	251	251	251
segurança	Correlação de Pearson	,608**	,648**	1	,724**
	Sig. (2 extremidades)	<,001	<,001		<,001
	N	251	251	251	251
Esforço_e_Desempenho	Correlação de Pearson	,683**	,693**	,724**	1
	Sig. (2 extremidades)	<,001	<,001	<,001	
	N	251	251	251	251

**. A correlação é significativa no nível 0,01 (2 extremidades).

Tabela 4 - Análise de correlação de Pearson

Fonte: Elaborado pelo autor

4.1.4 Teste das Hipóteses

Este subcapítulo tem como objetivo descrever o processo de construção das variáveis, os procedimentos estatísticos utilizados no SPSS e os resultados obtidos na verificação das hipóteses H1-H9.

Foram utilizados testes de correlação (Pearson ou Spearman) e um teste não paramétrico para comparação por grupos (Mann-Whitney) quando aplicável.

Através desta análise calculou-se todas as escalas no intervalo de 1 a 5 com médias dos itens. Por intermedio da função MEAN, que calcula a média com os itens respondidos. Manteve-se os nomes originais das variáveis do questionário. Sendo que, apenas foram criadas variáveis novas para as escalas e recodificações.

Para a variável Expectativa de Desempenho, H1, calculou-se a média das respostas às perguntas 4 a 8. Para a variável Esforço Percebido, H2, realizou-se dois passos. Primeiro criou-se uma média de Q9 a Q11, designada EXP_ESFORCO_POS, onde valores altos significam facilidade. Depois inverteu-se a direção para obter esforço direto com a expressão 6 menos EXP_ESFORCO_POS, gerando ESFORCO_PERCEBIDO, onde valores altos significam mais esforço. Para a Perceção de Segurança, H3, calculou-se a média de Q12 a Q14. Para a Utilidade Percebida, H4, foi utilizada a média de Q15 a Q17. Para a Experiência do Utilizador, H5, utilizou-se a média de Q18 a Q20. Para a Facilidade de Uso, H7, utilizou-se a média de Q21 a Q23.

Para a Privacidade A, H8a, alinhou-se o sentido dos itens. Inverteu-se Q24 e Q25 com a expressão 6 menos item. A questão Q26 manteve-se Q26 no sem alteração. O Cálculo da variável PRIVACIDADE_A realizou-se com a média de Q24R, Q25R e Q26. Foi realiza a confirmação dos dados através da inversão com tabelas cruzadas, Q24 com Q24R e Q25 com Q25R. Os pares apareceram nos mapeamentos esperados 1 com 5, 2 com 4, 3 com 3, 4 com 2, 5 com 1. Para a Privacidade B, H8b, inverteu-se Q27, Q28 e Q29 com a mesma regra 6 menos item. Foi feito o cálculo PRIVACIDADE_B como média de Q27R, Q28R e Q29R. Para a Aceitação, criou-se a média de Q30 a Q32. Para a Utilização, usou-se a Q31 como medida principal. Calculou-se também uma medida alternativa com a média de Q31 e Q32, apenas para robustez.

No que concerne as variáveis demográficas, estas foram transformadas em escalas numéricas sem alterar as escalas originais. Para a "idade", criou-se a variável "AGEORD" com a ordem 1 para 18–24 anos até 6 para 65 anos ou mais. Para a "escolaridade", criou-se a variável "EDUCNUM" com a ordem 1 para Básico até 6 para Doutoramento. Para o

género, criou-se a variável GENNUM com 1 para Masculino, 2 para Feminino, 9 para Prefiro não dizer. O código 9 não entrou no teste de género.

	Resultado
H1 - Quanto maior for a Expetativa de desempenho maior será a Aceitação da automação	Confirmada
H2 - Quanto maior for a Expetativa de esforço menor será a Aceitação da automação	Confirmada
H3 - Quanto maior for a Perceção de Segurança maior será a Aceitação da automação	Confirmada
H4 - Quanto menor for a Perceção de Utilidade menor será a Aceitação da automação	Confirmada
H5 - Quanto maior for a Experiência do Utilizador maior será a Aceitação da automação	Confirmada
H6 - Quanto menor forem as Características Demográficas maior será a Aceitação da automação	Não Confirmada
H7 - Quanto menor for a Facilidade de Uso do Sistema menor será a Aceitação da automação	Confirmada
H8a - Quanto menor for a Privacidade Percebida menor será a Aceitação da automação	Não Confirmada
H8b - Quanto maior for a Privacidade percebida maior será a Utilização da automação	Não Confirmada
H9 - Quanto maior for a Aceitação da Automação maior será a Utilização da automação	Confirmada

Tabela 5 – Resultados das hipóteses da investigação

4.2. Discussão dos resultados

O objetivo principal deste estudo foi avaliar a influência da perceção de segurança da informação nos comportamentos e sentimentos face a automação. Os resultados obtidos respondem de forma direta a questão de partida. A segurança percebida associa-se fortemente a utilização. Assim, pode-se concluir que valores elevados na variável "segurança percebida", podem indicar uma maior aceitação por parte da população em relação a adoção desta tecnologia, o que colabora para uma maior utilização.

A análise demográfica apresentou evidencias mistas. A variável Idade associou-se negativamente à aceitação, $\rho = -.144$, $p = .023$. Em relação ao Género, esta variável apresentou uma pequena diferença, mas significativa, $U \approx 6189$, $p \approx .046$, com valores superiores no grupo feminino. Em relação a escolaridade, esta variável surge com associação positiva, $\rho = .205$, $p = .001$, direção contraria à previsão inicial. Estes resultados sugerem que os efeitos demográficos existem, mas são modestos e específicos.

A dimensão de privacidade não confirmou as previsões. Sendo que, a Privacidade percebida apresenta correlação negativa com a aceitação, $r = -.329$, $p < .001$. A privacidade percebida apresenta também correlação negativa com a utilização, $r = -.421$, $p < .001$. Assim sendo, pode-se concluir que a variável pode despertar por parte da população preocupação em vez de confiança e controlo.

Contudo, os objetivos de investigação definidos ficaram cumpridos pelo estudo. Em que o objetivo principal é atendido, em que pode-se confirmar através dos resultados que a segurança percebida influência atitudes e relaciona-se com comportamentos de uso através da aceitação. O 1º objetivo da investigação, foi atendido, na qual as expetativas e opiniões foram mapeadas pelos efeitos de expetativa de desempenho, utilidade, facilidade, esforço e experiência, todos com valores significativos. Em relação ao 2º objetivo, este também foi atendido, na medida em que a segurança na automação surge como tema com impacto mensurável nas atitudes. O 3º objetivo, também é atendido, em que a relação entre a aceitação e utilização quantifica a ligação entre sentimentos e comportamentos. O 4º objetivo também foi atendido, a segurança percebida relaciona-se com a aceitação e, por essa via, com a utilização.

Capítulo 5 – Conclusões e recomendações

5.1. Principais conclusões

O presente capítulo tem como objetivo apresentar as principais conclusões decorrentes da investigação realizada, procurando responder à questão de investigação e aos objetivos definidos no início deste estudo. Apos a recolha, tratamento e analise dos dados, torna-se possível identificar os principais resultados obtidos, tal como a forma como estes se relacionam com as hipóteses formuladas e com a literatura previamente revista.

Neste sentido, esta investigação tem como foco avaliar a influencia da perceção de segurança da informação nos comportamentos e sentimentos face a automação.

Tendo por base a revisão de literatura decidiu-se que o modelo a adotar seria o UTAUT2, e nesse sentido, foi adaptado ao contexto do estudo e, tendo sido possível elaborar um questionário que foi depois implementado. Foram adicionados dois constructos ao modelo UTAUT2 original, sendo que foram enão explorados os seguintes 9 construtos: a expetativa de desempenho, a perceção de segurança; a perceção de utilidade, a experiência do utilizador, as características demográficas, a facilidade de uso do sistema, a privacidade percebida, a aceitação da automação, e a utilização da automação.

Este estudo tinha como objetivo responder a quatro objetivos específicos. Após análise dos dados considera-se que o objetivo principal deste estudo foi alcançado, sendo possível confirmar, através dos resultados obtidos, que a perceção de segurança exerce influencia nas atitudes e esta associada aos comportamentos de utilização através da aceitação.

Relativamente ao primeiro objetivo da investigação, foi verificado, que as expetativas e opiniões foram refletidas nos efeitos da expetativa de desempenho, utilidade, facilidade, esforço e experiência, todos com valores significativos.

Em relação ao segundo objetivo de investigação, este também foi verificado, na medida em que a segurança na automação surge como tema com impacto mensurável nas atitudes.

No que diz respeito ao terceiro objetivo, este também foi verificado, na medida em que a relação entre a aceitação e a utilização quantifica a ligação entre sentimentos e comportamentos.

Em relação ao quarto objetivo, este também foi verificado, na medida em que a segurança percebida relaciona-se com a aceitação e, por essa via, com a utilização.

5.2. Contribuições do estudo

A contribuição deste estudo está essencialmente ligada a um melhor entendimento e conhecimento a nível académico e a nível profissional, para a indústria, da perceção do utilizador português quanto à segurança face à automação, mais especificamente sobre a influência da perceção da segurança da informação nos comportamentos e sentimentos face à automação.

5.3. Limitações do estudo e propostas de investigação futura

Tal como qualquer investigação, o presente estudo apresenta algumas limitações, relacionadas sobretudo com o método de recolha de dados e com o tamanho da amostra.

O recurso ao questionário como instrumento de recolha de dados, especialmente no caso das respostas fechadas, restringe a liberdade dos participantes para expressarem opiniões mais fundamentadas sobre o tema. Para investigações futuras, seria recomendável a utilização de metodologias qualitativas, que permitam explorar crenças subjetivas e perceções individuais, possibilitando a obtenção de informações mais detalhadas e enriquecedoras sobre os tópicos abordados.

Por outro lado, a extensão do questionário, que, devido ao elevado número de perguntas associadas a objetivos semelhantes, pode dificultar a extração e interpretação das informações recolhidas, torna o processo de análise menos direto.

Adicionalmente, o número de respostas válidas representa uma limitação do estudo. Embora tenham sido recolhidos 370 questionários, apenas 251 foram considerados válidos após a exclusão de respostas incompletas. Esta redução poderá ter comprometido a representatividade da amostra e, por consequência, o potencial de generalização dos resultados.

Por fim, revela-se pertinente, em investigações futuras, aprofundar a análise comparativa entre diferentes setores de atividade ou recorrer a metodologias longitudinais, de forma a compreender como a perceção de segurança evolui à medida

que as soluções de inteligência artificial se tornam mais disseminadas no tecido empresarial português.

Referências Bibliográficas

Adamopoulou, E., & Moussiades, L. (2020). An overview of chatbot technology. *Artificial Intelligence Applications and Innovations 2020*, Neos Marmaras, Greece.

Albrechtsen, E. (2008). *Friend or foe? Information security management of employees* (Tese de doutoramento). Norwegian University of Science and Technology, Norway.

Alturas, B. (2022). *Introdução aos Sistemas de Informação Organizacionais.* 2ª edição, Lisboa: Sílabo

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. MIS Quarterly, 34(3), p.613.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M.J.G., Levi, M., Moore, T., & Savage, S. (2013) 'Measuring the cost of cybercrime', in R. Böhme (ed.), The Economics of Information Security and Privacy, Heidelberg: Springer, pp. 265–300.

Antonov, A. A. (2011). *From artificial intelligence to human super-intelligence*. Artificial Intelligence, 2(6), 35–60.

Arenas-Gaitán, J., Peral-Peral, B., & Ramón-Jerónimo, M. A. (2015). Elderly and internet banking, an application of UTAUT2. Journal of Internet Banking and Commerce, 20

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017–1041.

Bélanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *Journal of Strategic Information Systems, 11*(3–4), 245–270.

Björck, F. (2005). *Discovering information security management* (Tese de doutoramento). Stockholm University, Sweden.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523–548.

Cabrera-Sanchez, J. P., Villarejo-Ramos, A. F., Liebana-Cabanillas, F., & Shaikh, A. A. (2021). Identifying relevant segments of AI applications adopters: Expanding the UTAUT2's variables. *Telematics and Informatics*, 58, 101529. https://doi.org/10.1016/j.tele.2020.101529

Charitoudi, K., & Blyth, A. (2013). A Socio-Technical Approach to Cyber Risk Management and Impact Assessment. Journal of Information Security, 4(1), 33-41.

Chen, H., & Li, W. (2018). Understanding commitment and apathy in information security extra-role behavior from a person-organization fit perspective. *Behaviour & Information Technology, 38*(1), 1–15. https://doi.org/10.1080/0144929X.2018.1514420

Comissão Europeia. (2017). *Europeans' attitudes towards cyber security (Special Eurobarometer No. 464a)*. Directorate-General for Communication, European Commission. https://afyonluoglu.org/PublicWebFiles/Reports/EU/Eurobarometer/CS/2017%20Sept%20EU%20Eurobarometer-Europeans%E2%80%99%20attitudes%20towards%20cyber%20security.pdf

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

Czaja, S. J., Charness, N., Fisk, A. D., Hertzog, C., Nair, S. N., Rogers, W. A., & Sharit, J. (2006). Factors predicting the use of technology: Findings from the Center for Research and Education on Aging and Technology Enhancement (CREATE). *Psychology and Aging, 21*(2), 333–352.

Davenport, T. H., & Ronanki, R. (2018). Artificial intelligence for the real world. *Harvard Business Review, 96*(1), 108–116.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behavior towards protective information technologies: The role of national cultural differences. Information Systems Journal, 19(4), 391–412.

Dodge Jr, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security*, 26(1), 73–80.

Eckert, A., Dal Bó, G., Milan, G. S., & Eberle, L. (2017). E-commerce: privacidade, segurança e qualidade das informações como preditores da confiança. *Revista Pensamento Contemporâneo em Administração, 11*(5), 49–69.

Endsley, M. R., & Kaber, D. B. (1999). Level of automation effects on performance, situation awareness and workload in a dynamic control task. *Ergonomics, 42*(3), 462–492.

European Commission (2017). Resilience, Deterrence and Defence: Building strong cybersecurity in Europe. [online] Available at: https://ec.europa.eu/digital-singlemarket/ en/news/resilience-deterrence-and-defence-building-strong-cybersecurityeurope.

Farina, M., & Lavazza, A. (2023). ChatGPT in society: Emerging issues. *Frontiers in Artificial Intelligence*, 6, 1130913.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies, 59*(4), 451–474.

Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention, and behavior. Reading, Mass.: Addison-Wesley Publishing Company.

Fonseca, A. F. (2013). *Estratégia nas redes sociais das empresas de telecomunicações móveis a atuar em Portugal: perceção dos utilizadores* (Dissertação de Mestrado, ISCTE–Instituto Universitário de Lisboa).

Fonseca, M. J. S. H. (2020). *Impacto da Indústria 4.0 na organização do tempo de trabalho: Conciliação entre a vida pessoal e profissional* (Dissertação de Mestrado). Universidade Católica Portuguesa.

Fortin, M.-F. (1999). *O processo de investigação*: Da conceção à realização. Lusociência.

Gallego, A., & Kurer, T. (2022). Automation, digitalization, and artificial intelligence in the workplace: Implications for political behavior. *Annual Review of Political Science, 25*, 463–484. https://doi.org/10.1146/annurev-polisci-051120-104535

Gessinger, J., Hammes, L., & Colling, J. INTELIGÊNCIA ARTIFICIAL ARTIFICIAL INTELLIGENCE.

Gill, K. S. (2016). Artificial super intelligence: Beyond rhetoric. *AI & Society*, 31, 137–143. https://doi.org/10.1007/s00146-016-0653-0

Governo Português. (2020). *Plano de Ação para a Transição Digital* (RCM n.º 30/2020). DGAE

Gundu, T., & Flowerday, S. V. (2013). Ignorance to awareness: Towards an information security awareness process. *SAIEE Africa Research Journal, 104*(2), 69–79. https://doi.org/10.23919/SAIEE.2013.8531923

Han, D., Dai, Y., Tianlin Han, & Dai, X. (2015). Explore Awareness of Information Security: Insights from Cognitive Neuromechanism. Computational Inteligence and NeuroCience , 1-11.

Harclerode, M. A., Lal, P., Vedwan, N., Wolde, B., & Bowers, M. C. (2016). Evaluation of the role of risk perception in stakeholder engagement to prevent lead exposure in an urban setting. *Journal of Environmental Management*, 184, 132–142.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. European Journal of Information Systems, 18(2), 106–125.

Hill, M. M., & Hill, A. (1998). *A construção de um questionário*. Sílabo.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does Deterrence Work in Reducing Information Security Policy Abuse By Employees? Communications of the ACM, 54(6), 54-90.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Instituto Nacional de Estatística (INE). (2024). *População residente: Total e por sexo*. PORDATA. https://www.pordata.pt/pt/estatisticas/populacao/populacao-residente/populacao-residente-por-sexo-e-grupo-etario

ISO (2019). *ISO 9241-210:2019 — Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems*. International Organization for Standardization.

Jesus Jorge, A. D. (2021). *Segurança e Integridade da Informação em contexto organizacional* (Dissertação de Mestrado).

Jeyaraj, A., Rottman, J., & Lacity, M. (2006). A review of the predictors, linkages, and biases in IT innovation adoption research. Journal of Information Technology, 21(1):1-23. https://doi.org/10.1057/palgrave.jit.2000056

Kagermann, H., Wahlster, W., & Helbig, J. (2013). *Recommendations for implementing the strategic initiative Industrie 4.0: Final report of the Industrie 4.0 Working Group*. acatech – National Academy of Science and Engineering. Recuperado de http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Material_fuer_Sonderseiten/Industrie_4.0/Final_report__Industrie_4.0_accessible.pdf

Kasakliev, N., Somova, E., & Gocheva, M. (2024). Artificial intelligence for good and bad in cyber and information security. *Mathematics & Informatics*, 67(1), 1–8.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems, 44*(2), 544–564.

Klein, R. H. (2014). *Ameaças, controle, esforço e descontentamento do usuário no comportamento seguro em relação à segurança da informação* (Dissertação de Mestrado). Universidade Federal do Rio Grande do Sul.

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement*, 30(3), 607–610. https://doi.org/10.1177/001316447003000308

Kritzinger, E., & Solms, S. (2010). Cyber security for home users: A new way of protection through awareness enforcement. Computers & Society, 29(8), pp. 840-847.

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cybercrime on the financial sector. Computers & Society, 45, pp. 58-74.

Leach, J. (2003). Improving User Security Behavior. *Computers & Security*. 22(8).

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, H. M. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review, 37*(12), 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085

Lee, J. D., & K. A. See. 2004. "Trust in Automation: Designing for Appropriate Reliance." *Human Factors: The Journal of the Human Factors and Ergonomics Society* 46 (1): 50–80.

Li, J. (2018). Cyber security meets artificial intelligence: A survey. *Frontiers of Information Technology & Electronic Engineering, 19*, 1462–1474. https://doi.org/10.1631/FITEE.1800573

Li, Y., Jung, J. Y., & Lee, S. Y. (2021). Perceptions of Information Systems Security Compliance: An Empirical Study in Higher Education Setting. *International Journal of Information Management, 57*, 102301. https://doi.org/10.1016/j.ijinfomgt.2020.102301

Lubua, E. W., & Pretorius, P. D. (2019). Ranking Cybercrimes based on their impact to organisations' welfare. THREAT Conference Proceedings (pp. 1-11). Johannesburg: THREAT Conference Proceedings.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355.

Masum, M. (2023). *AI cybersecurity, artificial intelligence cybersecurity*. https://doi.org/10.13140/RG.2.2.36172.80009

Matias, A. C. D. F. B. F. (2020). A influência da inteligência artificial no e-commerce: O uso dos chatbots (Dissertação de mestrado).

McCarthy, J. (2004). *What is artificial intelligence?* Stanford University, Department of Computer Science. http://jmc.stanford.edu/articles/whatisai/whatisai.pdf

McLean, S., Read, G. J., Thompson, J., Baber, C., Stanton, N. A., & Salmon, P. M. (2021). The risks associated with artificial general intelligence: A systematic review. *Journal of Experimental & Theoretical Artificial Intelligence*, 33(1), 1–17.

Mendonça, C. M. C. D., Andrade, A. M. V. D., & Neto, M. V. D. S. (2018). Uso da IoT, big data e inteligência artificial nas capacidades dinâmicas e seus microfundamentos.

Mercader Uguina, J. R. (2017). *El futuro del trabajo en la era de la digitalización y la robótica*. Tirant lo Blanch.

Mitchell, M. (2019). *Artificial intelligence: A guide for thinking humans*. Penguin Random House.

Moisset, S. (2023). *How security analysts can use AI in cybersecurity*. FreeCodeCamp. https://freecodecamp.org/news/how-to-use-artificial-intelligence-in-cybersecurity/

Morris, M. G., & Venkatesh, V. (2000). Age differences in technology adoption decisions: Implications for a changing workforce. *Personnel Psychology, 53*(2), 375–403.

Muir, B. M. (1987). "Trust between Humans and Machines, and the Design of Decision Aids." *International Journal of Man-Machine Studies* 27: 527–539. doi:10.1016/S0020-7373(87)80013-5.

Muir, B. M. (1994). "Trust in Automation: Part I. Theoretical Issues in the Study of Trust and Human Intervention in Automated Systems." *Ergonomics* 37 (11): 1905–1922. doi:10.1080/00140139408964957.

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815–825.

Norman, D., Miller, J., & Henderson, A. (1995). What You See, Some of What's in the Future, And How We Go About Doing It: HI at Apple Computer, presented at the CHI '95 Mosaic of Creativity, p. 1.

Parasuraman, R., & Riley, V. A. (1997). Humans and automation: Use, misuse, disuse, abuse. *Human Factors*, 39(2), 230–253.

Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A model for types and levels of human interaction with automation. *IEEE Transactions on Systems, Man, and Cybernetics—Part A: Systems and Humans, 30*(3), 286–297.

Pardal, L., & Correia, E. (1995). Métodos e Técnicas de Investigação Social. Porto: Areal Editores.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2010). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 33, 109–123.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*(3), 101–134.

Pires, D. M. B. (2022). *Determinantes da adoção de plataformas digitais em IES: uma aplicação da UTAUT2 a alunos do IPC*.

Poepjes, R., & Lane, M. (2012). An Information Security Awareness Capability Model (ISACM). Australian Information Security Management Conference (SECAU 2012).

Posey, C., Roberts, T. L., & Lowry, P. B. (2010). Proactive personality and resistance to social engineering: A field experiment. *Journal of Management Information Systems, 26*(4), 227–248. https://doi.org/10.2753/MIS0742-1222260409

Riley, V. A. (1994). "A Theory of Operator Reliance on Automation." In *Human Performance in Automated Systems: Recent Research and Trends*, edited by M. Mouloula and R. Parasuraman, 8–14. Hillsdale, NJ: Erlbaum.

Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press.

Rogers, R. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), pp. 93-114.

Rogers, R. (1983). Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. Social Psychophysiology, pp. 153-177.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), pp. 121–135.

Rüßmann, M., Lorenz, M., Gerbert, P., Waldner, M., Justus, J., Engel, P., & Harnisch, M. (2015). Industry 4.0: *The future of productivity and growth in manufacturing industries*. The Boston Consulting Group.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet, 11*(4). https://doi.org/10.3390/fi11040089

Salisbury, W. D., Pearson, R. A., Pearson, A. W., & Miller, D. W. (2001). Perceived security and World Wide Web purchase intention. *Industrial Management & Data Systems, 101*(4), 165–177.

Salmon, P. M., Carden, T., & Hancock, P. A. (2021). Putting the humanity into inhuman systems: How human factors and ergonomics can be used to manage the risks associated with artificial general intelligence. *Human Factors and Ergonomics in Manufacturing & Service Industries*, 31(2), 223–236. https://doi.org/10.1002/hfm.20883

Saridakis, G., Benson, V., Ezingeard, J., & Tennakoon, H. (2015). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. Technological Forecasting and Social Change, 102, pp. 320-330.

Savaget, P., Chiarini, T., & Evans, S. (2019). Empowering political participation through artificial intelligence. *Science and Public Policy, 46*(3), 369–380. https://doi.org/10.1093/scipol/scy064

Shahri, A. B., & Mohanna, S. (2016). The Impact of the Security Competency on "Self-efficacy in Information Security" for Effective Health Information Security in Iran. the Advances in Intelligent Systems and Computing, 445, 51-65.

Siponen, M., Mahmood, A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & Management, 51(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

Siponen, M., Pahnila, S., & Mahmood, A. (2006). Factors influencing protection motivation and IS security policy compliance. Innovations in Information Technology. IEEE. https://doi.org/10.1109/IIT.2006.365792

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1016.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. Information Management & Computer Security, 22(1), 42–75. https://doi.org/10.1108/IMCS-08-2012-0045

Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Information & Management, 48(7), 296–302. https://doi.org/10.1016/j.im.2011.07.002

Starke, C., & Lünich, M. (2020). Artificial intelligence for political decision-making in the European Union: Effects on citizens' perceptions of input, throughput, and output legitimacy. *Data & Policy, 2*. https://doi.org/10.1017/dap.2020.19

Thompson, S. (2023). *Artificial intelligence's impact on elections and democracy could be very real*. TechInformed. https://techinformed.com/artificial-intelligences-impact-on-elections-and-democracy-could-be-very-real/

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, 59, 138–150. https://doi.org/10.1016/j.cose.2016.02.009

Ukov, T., & Tsochev, G. (2022). Machine learning algorithm for intelligent bots in multiplayer video game: A case study. *International Journal on Information Technologies and Security, 14*(4), 67–78. http://ijits-bg.com/2022.v14.i4.07

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management, 49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Veiga, R., & Pires, C. C. (2023). *Perceção do impacto da inteligência artificial em contexto ocupacional / Impact of artificial intelligence on the workplace*.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: toward a Unified https://doi.org/10.2307/30036540 View. MIS Quarterly, 27(3), 425–478.

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly, 36*(1), 157–178.

Violante, A., & Andrade, A. (2022). O potencial da inteligência artificial na gestão. Gestão e Desenvolvimento, (30), 439–479. https://doi.org/10.34632/gestaoedesenvolvimento.2022.11627

Wickens, C. D., & Dixon, S. R. (2007). The Benefits of Imperfect Diagnostic Automation: A Synthesis of the Literature. *Theoretical Issues in Ergonomics Science* 8 (3): 201–212.

Willcocks, L. P., & Lacity, M. (2016). *Service automation: Robots and the future of work*. SB Publishing.

Wilson, C. (2014). Cyber threats to critical information infrastructure. In T. Chen, L. Jarvis, & S. Macdonald (Eds.), *Cyberterrorism* (pp. 151–168). Springer, New York. https://doi.org/10.1007/978-1-4939-0962-9_7

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior, 24(6), 2799–2816.

Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. *IEEE Access, 8*, 23817–23837. https://doi.org/10.1109/ACCESS.2020.2968045

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security, 17*(4), 330–340. https://doi.org/10.1108/09685220910993954

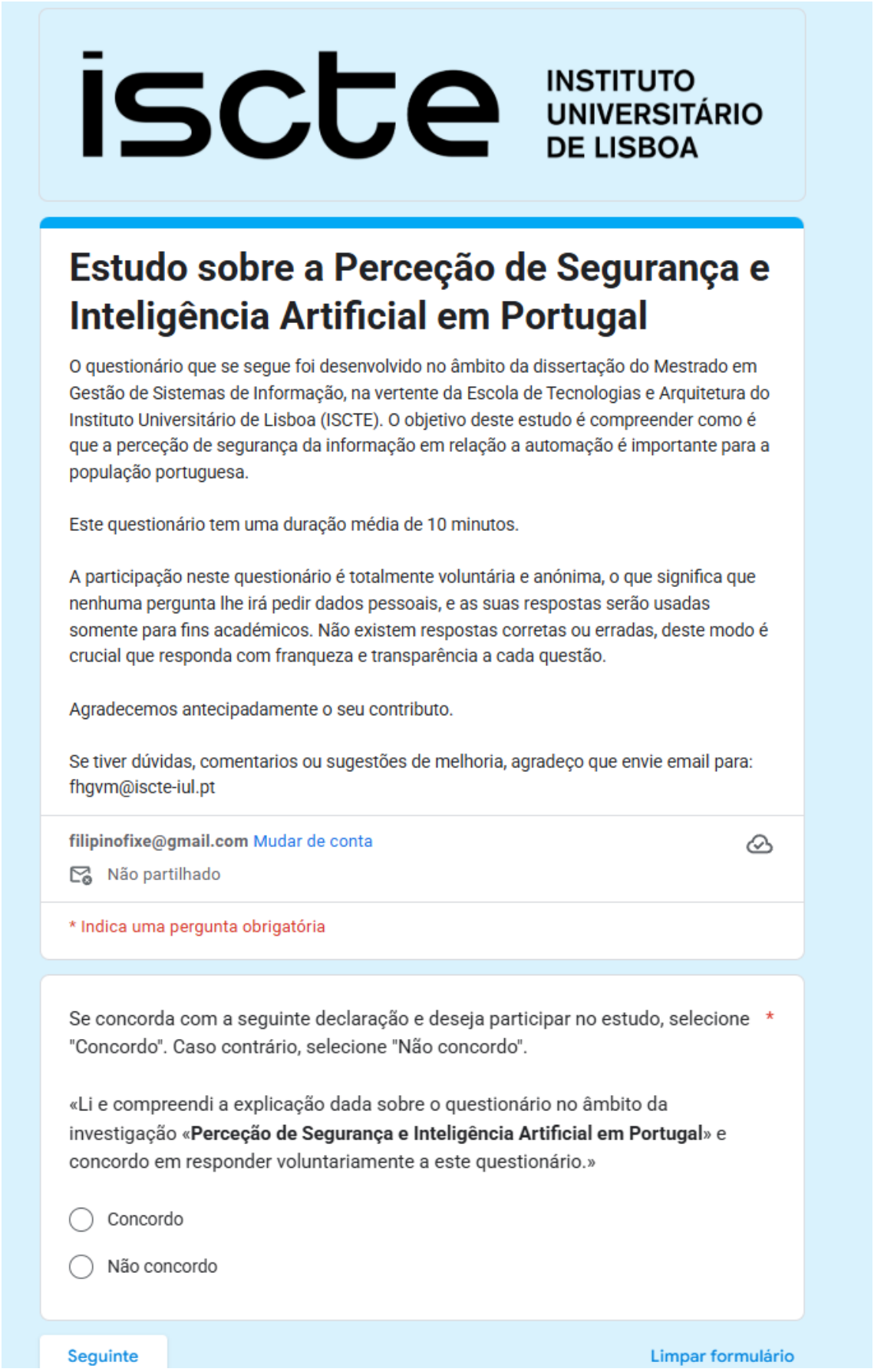
Zhang, M., Chen, J., & Zhao, D. (2017). System dynamical simulation of risk perception for enterprise decision-maker in communication of chemical incident risks. *Journal of Loss Prevention in the Process Industries*, 46, 115–125.

Zhang, M., Chen, J., Li, X., & Zhao, D. (2017). A system dynamics model for risk perception of lay people in communication regarding risk of chemical incident. *Journal of Loss Prevention in the Process Industries*, 50, 101–111.

Zoto, E., Kowalski, S., Lopez-Rojas, E. A., & Kianpour, M. (2018). Using a socio-technical systems approach to design and support systems thinking in cyber security education. 4th International Workshop on Socio-Technical Perspective in IS development (STPIS'18) (pp. 123-128). Tallinn]- Estonia: 4th International Workshop on Socio-Technical Perspective in IS development (STPIS'18).

Anexos e Apêndices

Apêndice A



INSTITUTO UNIVERSITÁRIO DE LISBOA

Estudo sobre a Perceção de Segurança e Inteligência Artificial em Portugal

O questionário que se segue foi desenvolvido no âmbito da dissertação do Mestrado em Gestão de Sistemas de Informação, na vertente da Escola de Tecnologias e Arquitetura do Instituto Universitário de Lisboa (ISCTE). O objetivo deste estudo é compreender como é que a perceção de segurança da informação em relação a automação é importante para a população portuguesa.

Este questionário tem uma duração média de 10 minutos.

A participação neste questionário é totalmente voluntária e anónima, o que significa que nenhuma pergunta lhe irá pedir dados pessoais, e as suas respostas serão usadas somente para fins académicos. Não existem respostas corretas ou erradas, deste modo é crucial que responda com franqueza e transparência a cada questão.

Agradecemos antecipadamente o seu contributo.

Se tiver dúvidas, comentarios ou sugestões de melhoria, agradeço que envie email para: fhgvm@iscte-iul.pt

filipinofixe@gmail.com Mudar de conta

Não partilhado

* Indica uma pergunta obrigatória

Se concorda com a seguinte declaração e deseja participar no estudo, selecione "Concordo". Caso contrário, selecione "Não concordo". *

«Li e compreendi a explicação dada sobre o questionário no âmbito da investigação «**Perceção de Segurança e Inteligência Artificial em Portugal**» e concordo em responder voluntariamente a este questionário.»

- ◯ Concordo
- ◯ Não concordo

Seguinte

Limpar formulário

Figura 6 - Página inicial do questionário (introdução e consentimento informado)

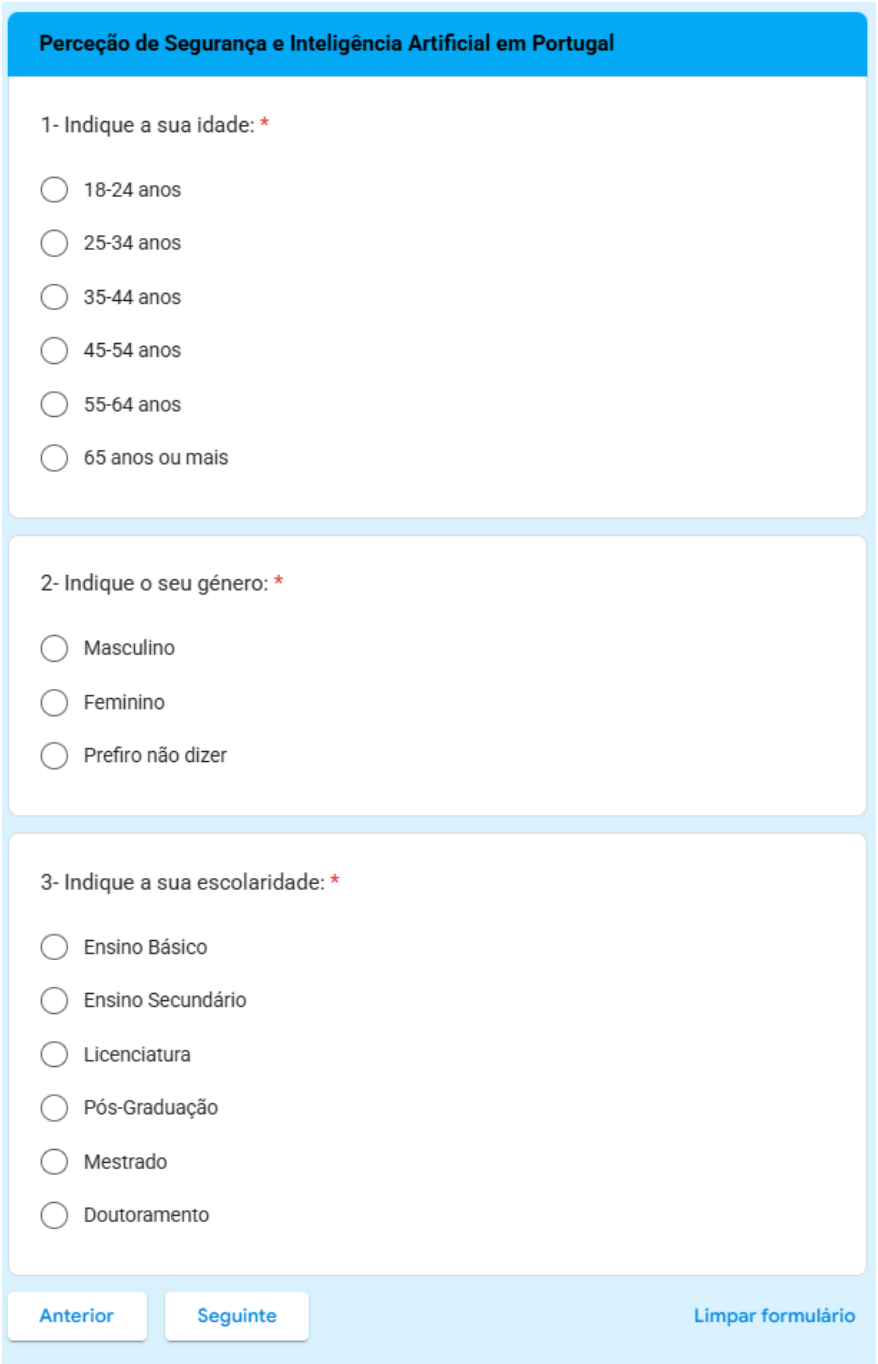


Figura 7 - Questões sobre o perfil

Perceção de Segurança e Inteligência Artificial em Portugal

4- Acredito que a automação pode melhorar significamente o meu desempenho no trabalho. *

- ◯ Discordo totalmente
- ◯ Discordo
- ◯ Nem concordo nem discordo
- ◯ Concordo
- ◯ Concordo totalmente

5- Acredito que a automação pode melhorar significamente o meu desempenho no dia-a-dia. *

- ◯ Discordo totalmente
- ◯ Discordo
- ◯ Nem concordo nem discordo
- ◯ Concordo
- ◯ Concordo totalmente

6- A utilização de sistemas automatizados pode ajudar a alcançar os objetivos de desempenho mais rapidamente. *

- ◯ Discordo totalmente
- ◯ Discordo
- ◯ Nem concordo nem discordo
- ◯ Concordo
- ◯ Concordo totalmente

Figura 8 - Questões sobre a Expectativa de Desempenho

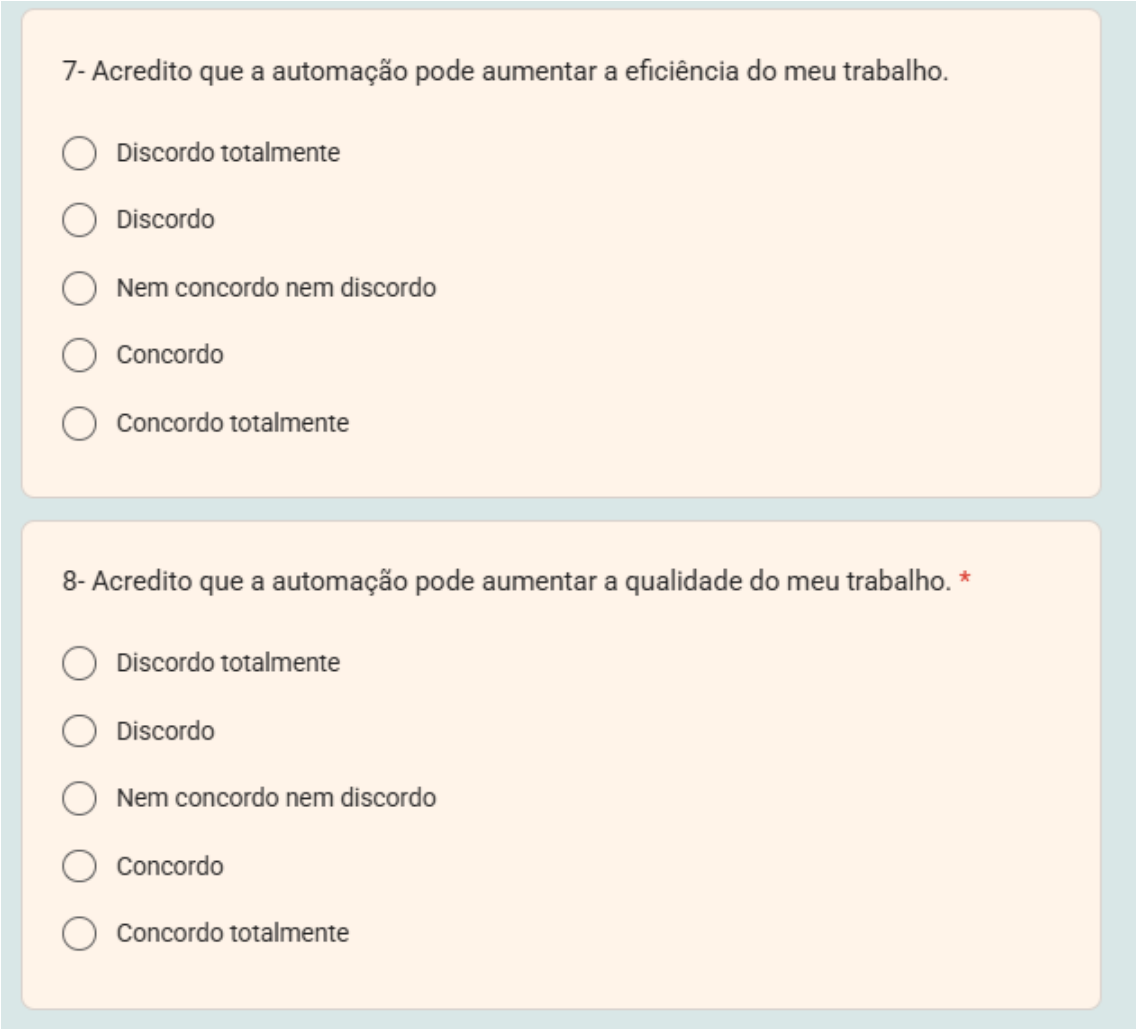


Figura 9 - Questões sobre a Expectativa de Desempenho

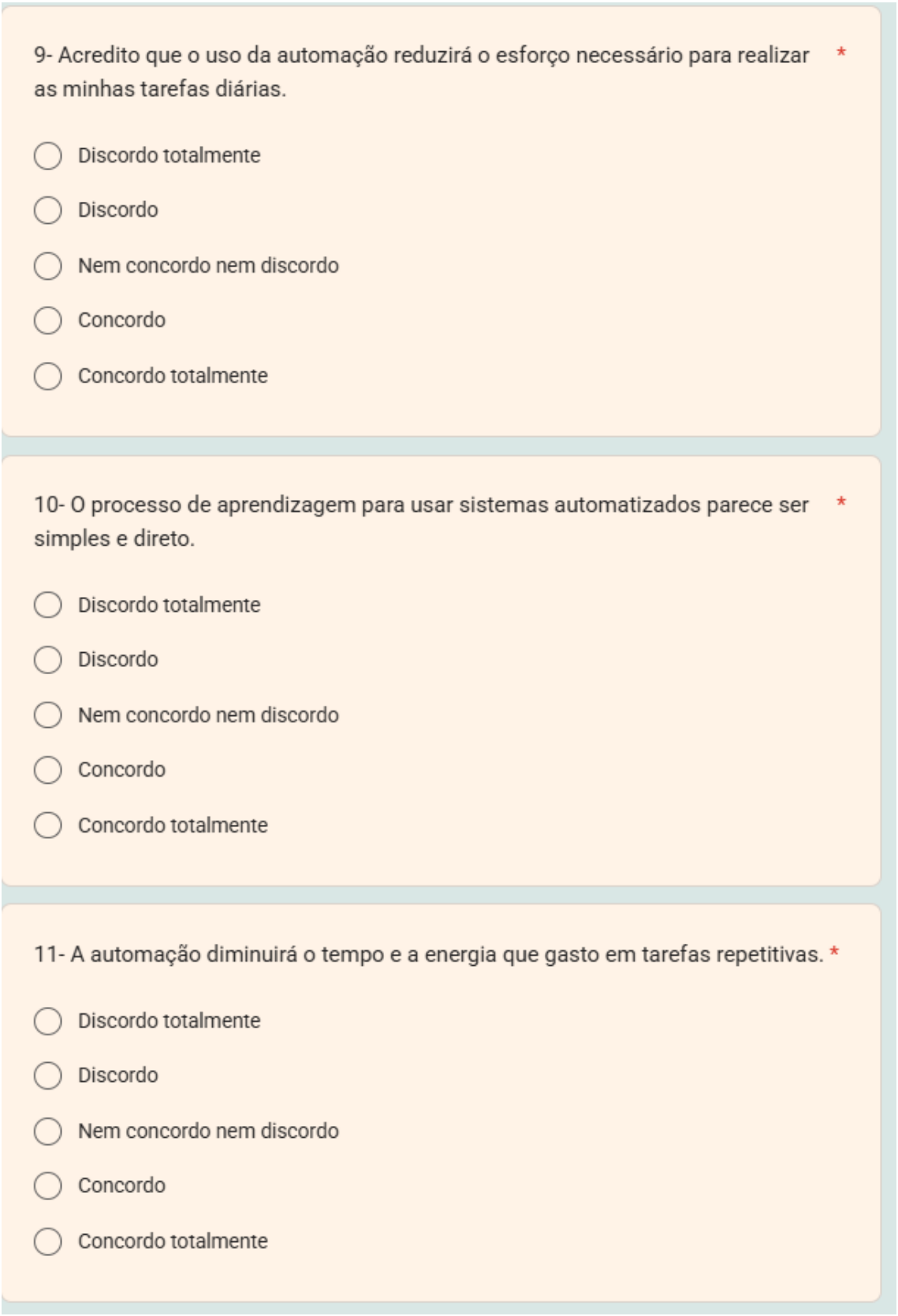


Figura 10 - Questões sobre a Expectativa de Esforço

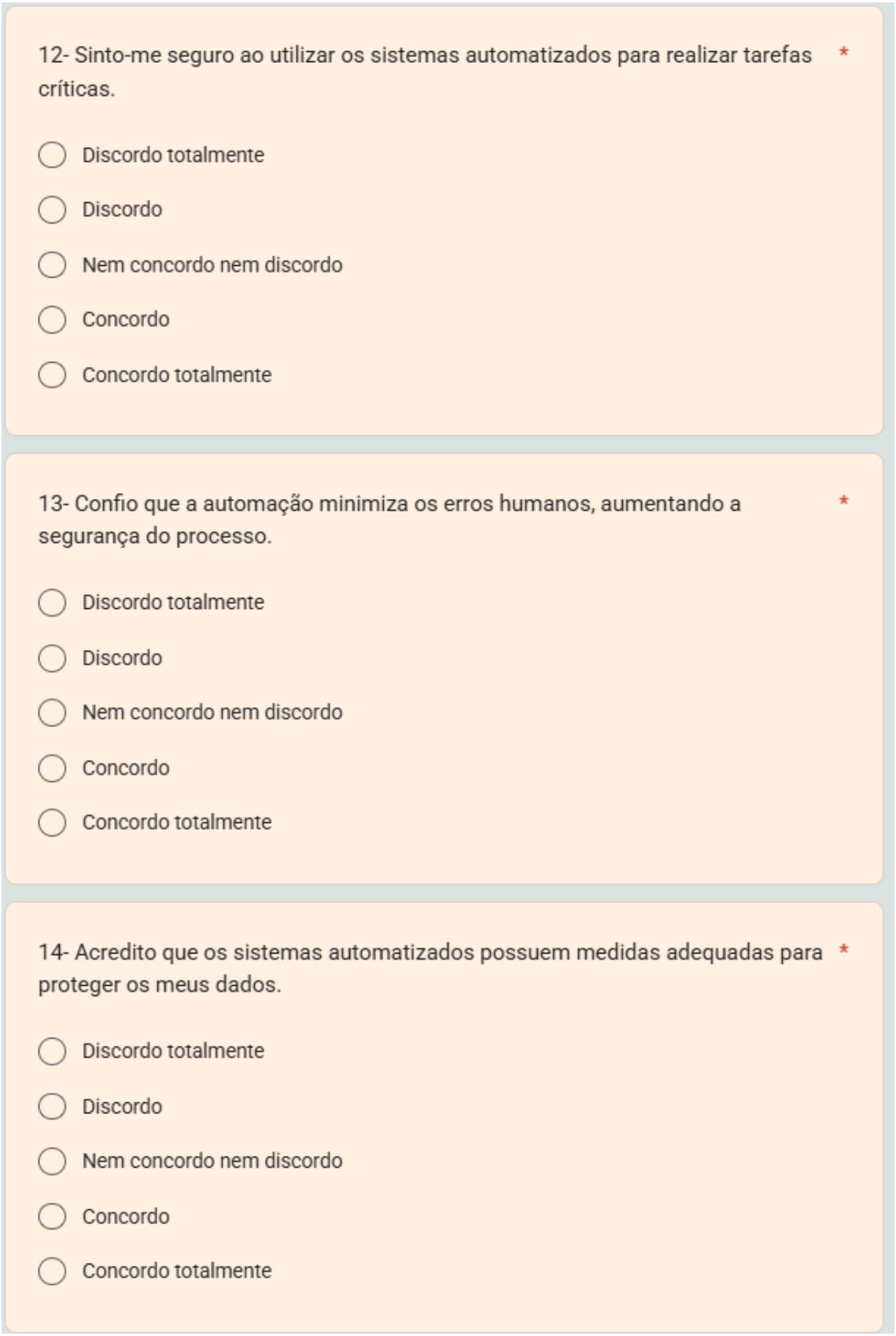


Figura 11 - Questões sobre a Perceção de Segurança

15- A automação proporciona uma utilidade significativa nas minhas atividades diárias. *

- ◯ Discordo totalmente
- ◯ Discordo
- ◯ Nem concordo nem discordo
- ◯ Concordo
- ◯ Concordo totalmente

16- Os benefícios proporcionados pela automação superam as possíveis desvantagens. *

- ◯ Discordo totalmente
- ◯ Discordo
- ◯ Nem concordo nem discordo
- ◯ Concordo
- ◯ Concordo totalmente

17- Perceciono a automação como uma ferramenta indispensável para melhorar a eficiência. *

- ◯ Discordo totalmente
- ◯ Discordo
- ◯ Nem concordo nem discordo
- ◯ Concordo
- ◯ Concordo totalmente

Figura 12 - Questões sobre a Perceção de Utilidade

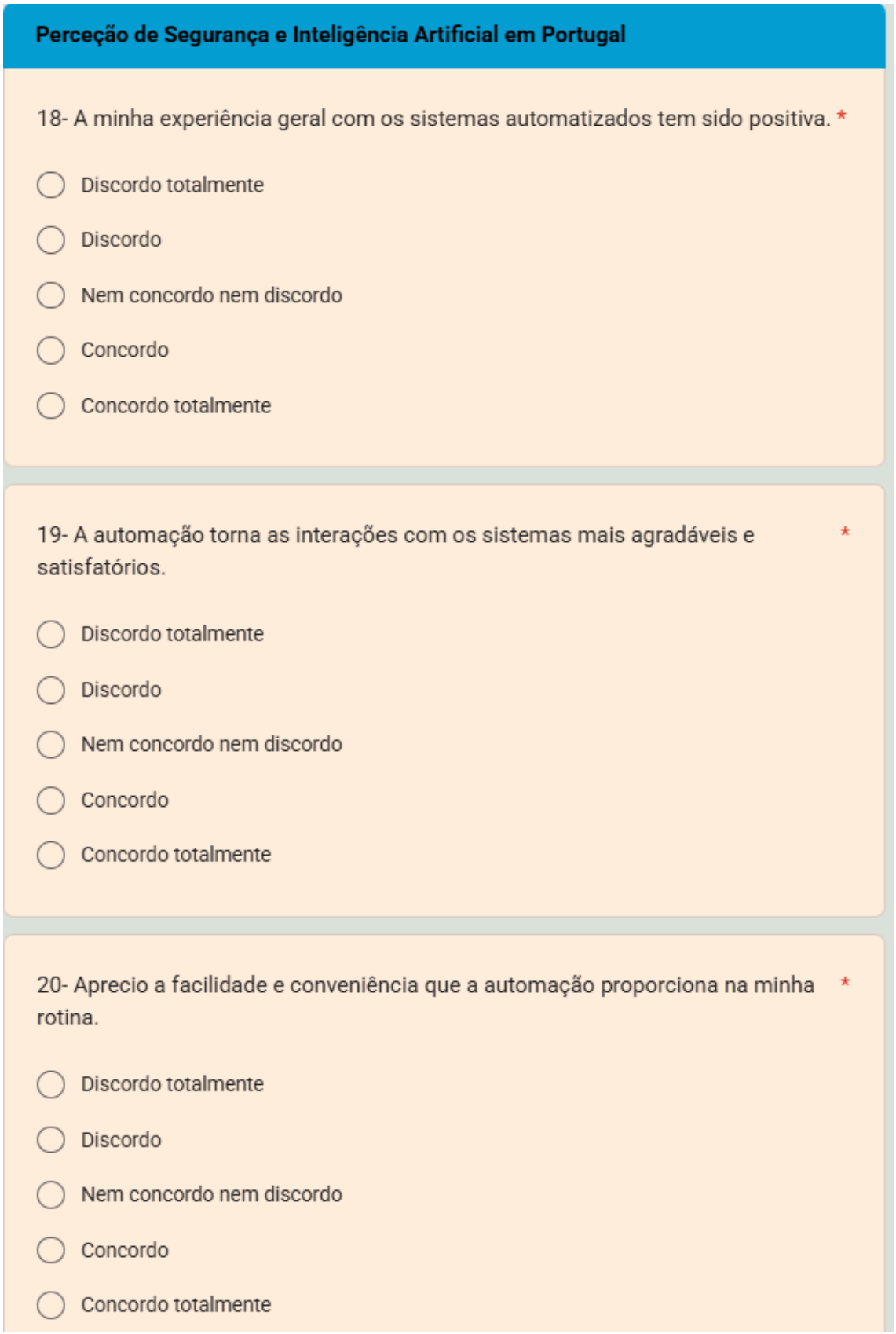


Figura 13 - Questões sobre a Experiência do Utilizador

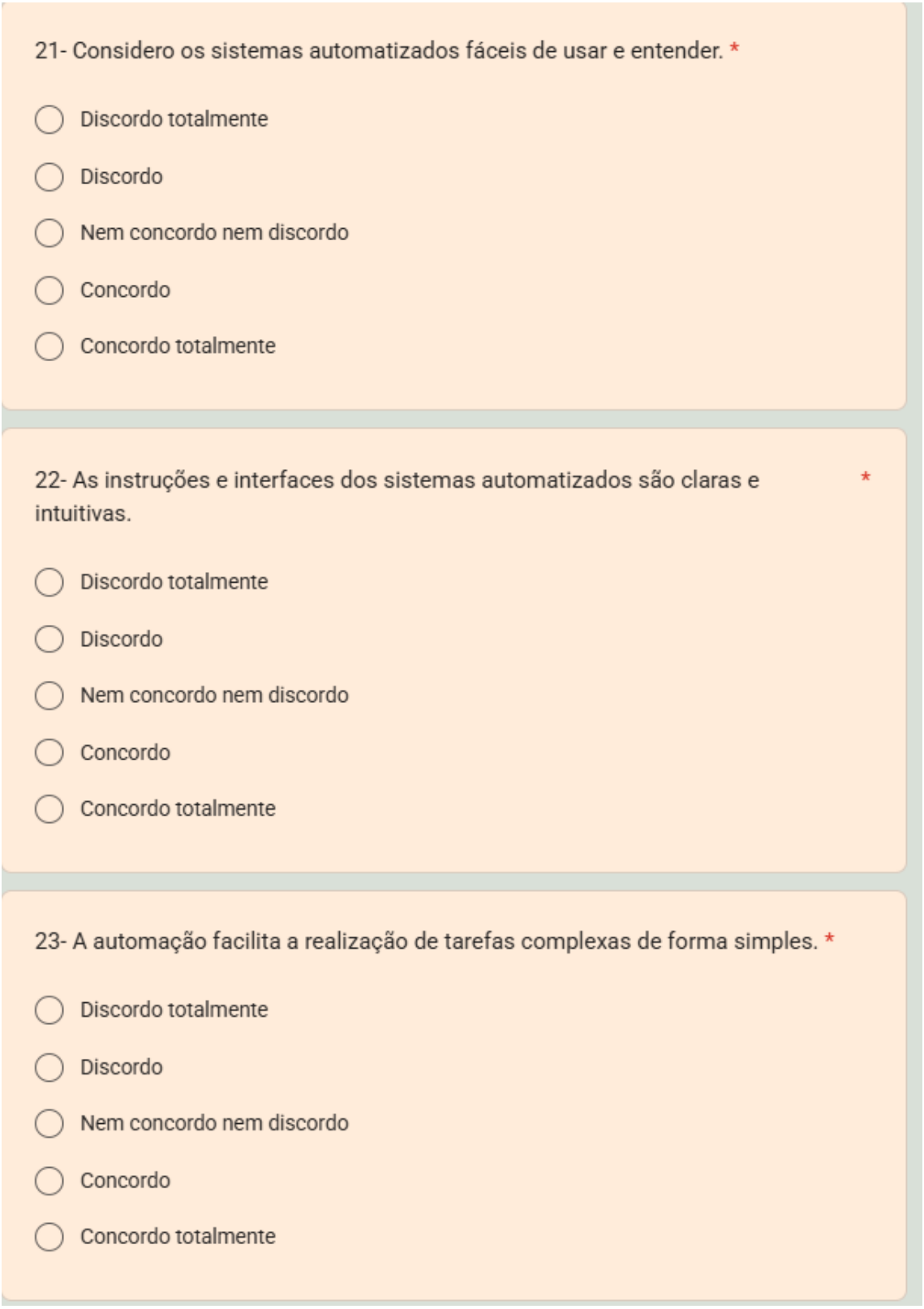


Figura 14 - Questões sobre a Facilidade de Uso

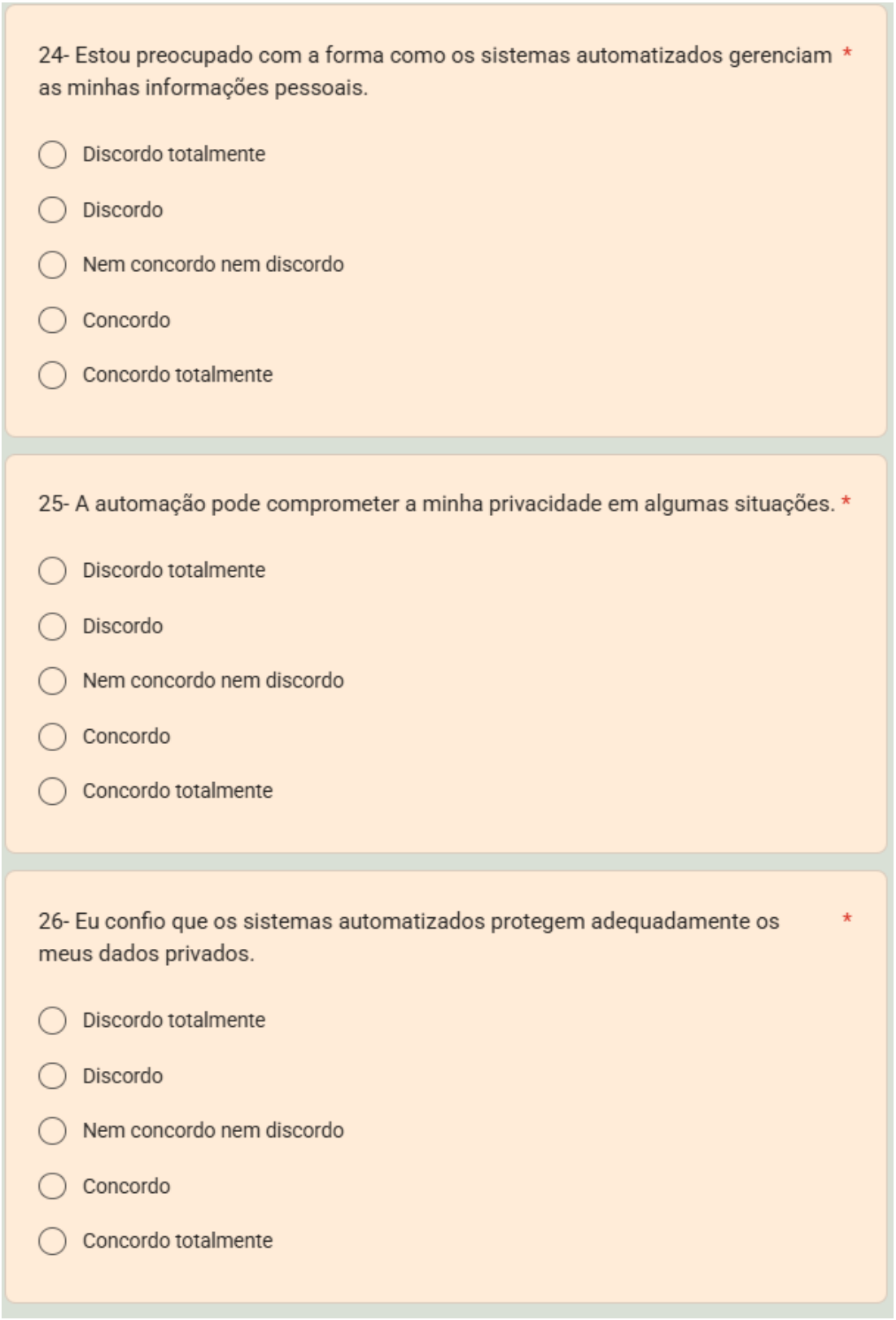


Figura 15 - Questões sobre Privacidade Percebida

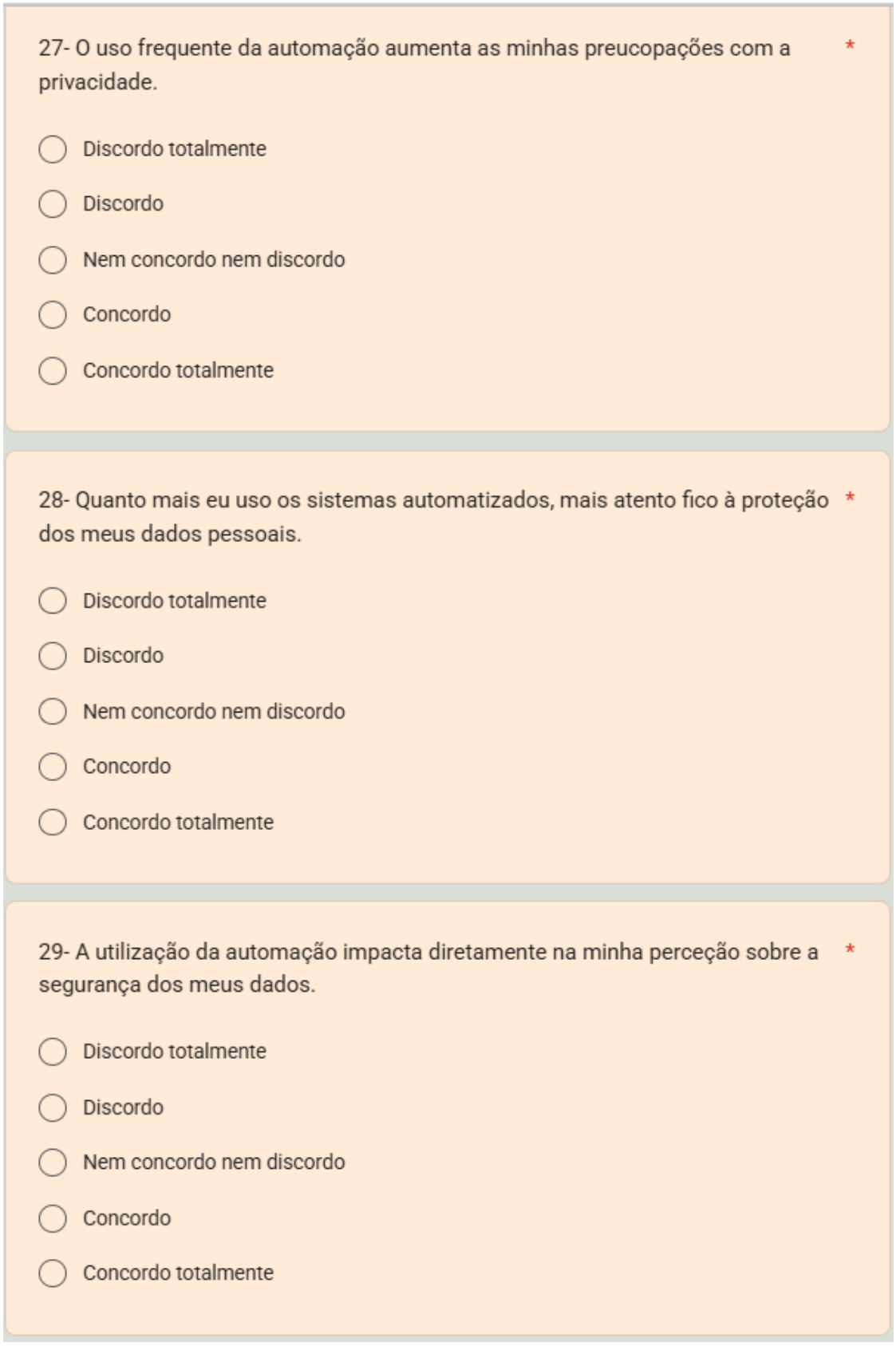


Figura 16 - Questões sobre a Privacidade Percebida

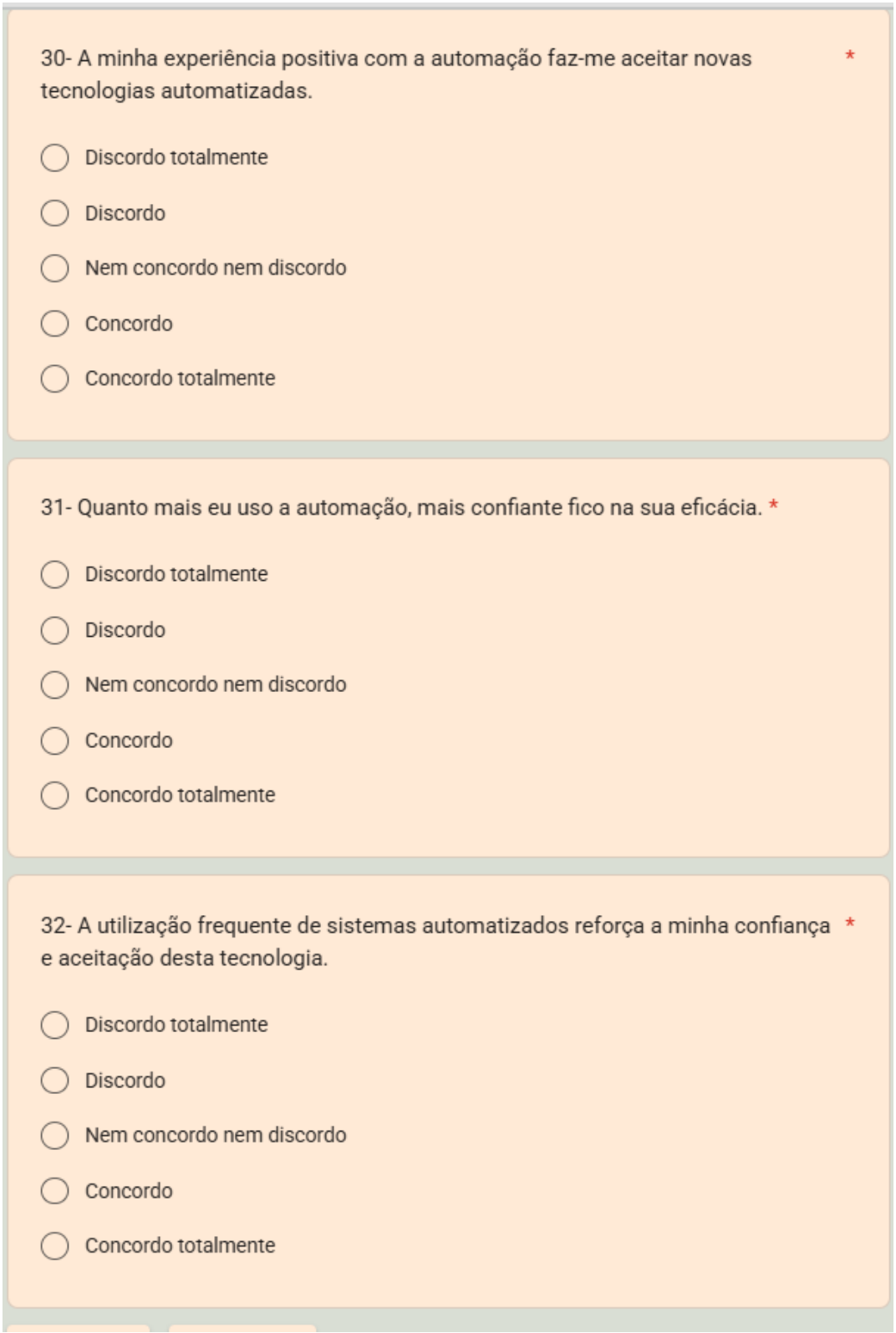


Figura 17 - Questões sobre a Aceitação da Automação

Apêndice B

Questão nº1

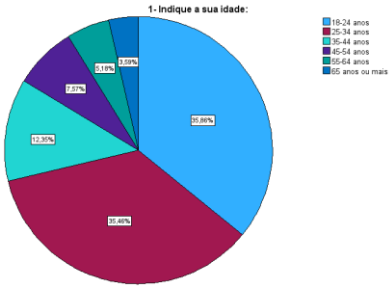


Figura 18 – Gráfico circular referente a questão nº1.

Questão nº2

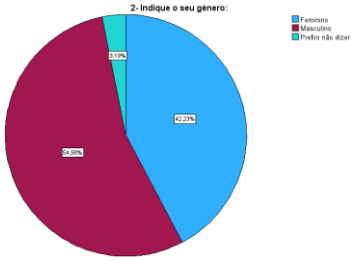


Figura 19 – Gráfico circular referente a questão nº2.

Questão nº3

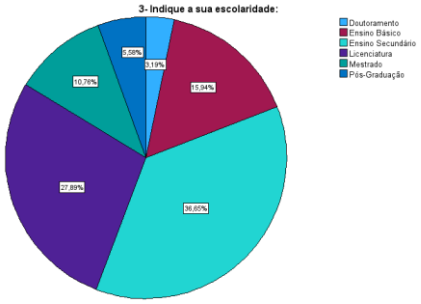


Figura 20 – Gráfico circular referente a questão nº3.

Questão nº4

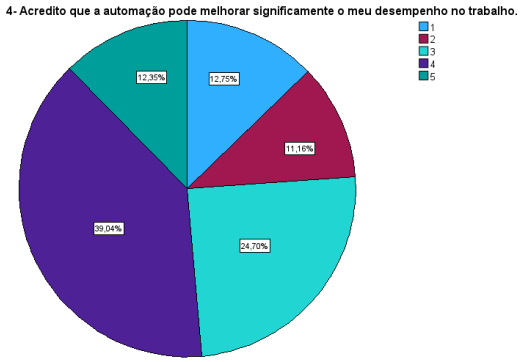


Figura 21 – Gráfico circular referente a questão nº4.

Questão nº5

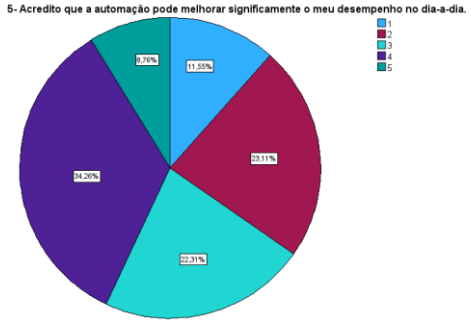


Figura 22 - Gráfico circular referente a questão nº5.

Questão nº6

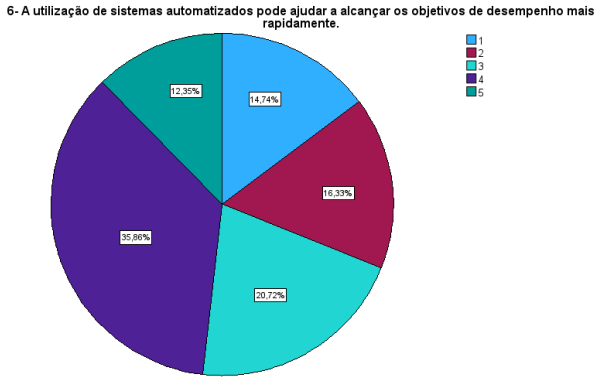


Figura 23 - Gráfico circular referente a questão nº6.

Questão nº7

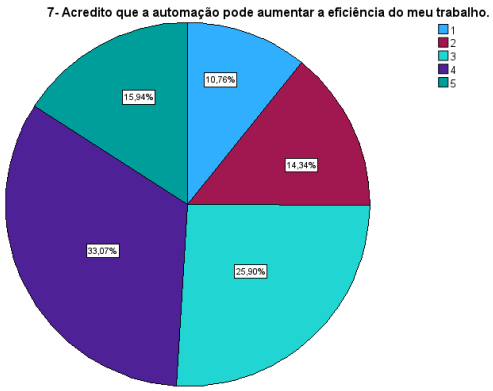


Figura 24 - Gráfico circular referente a questão nº 7.

Questão nº8

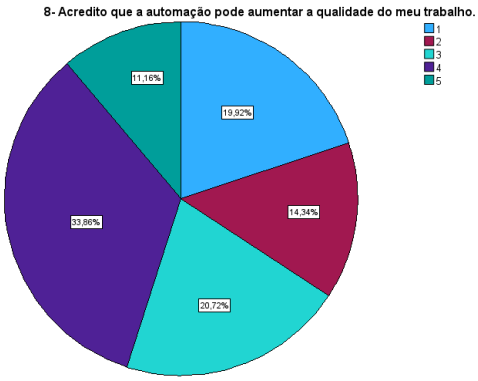


Figura 25 - Gráfico circular referente a questão nº8.

Questão nº9

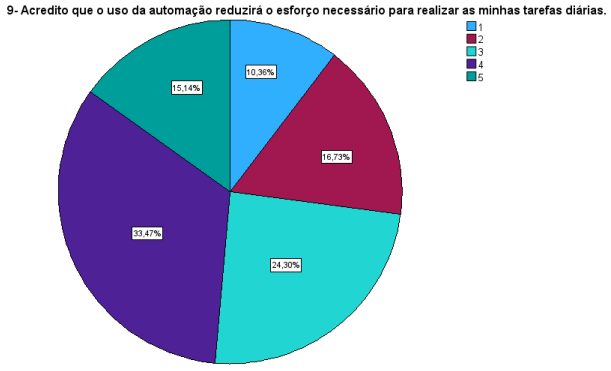


Figura 26 - Gráfico circular referente a questão nº9.

Questão nº10

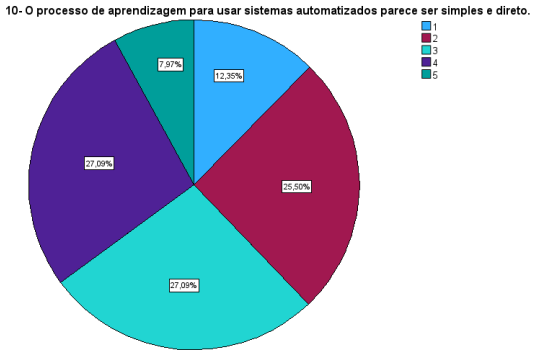


Figura 27 - Gráfico circular referente a questão nº10.

Questão nº11

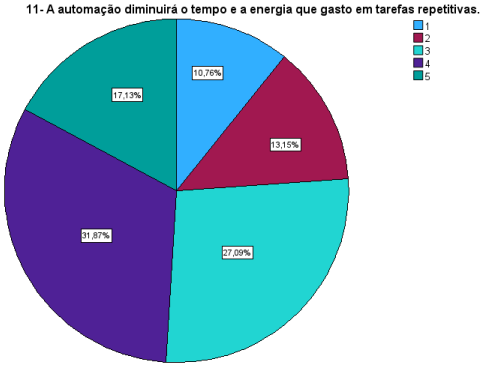


Figura 28 - Gráfico circular referente a questão nº11.

Questão nº12

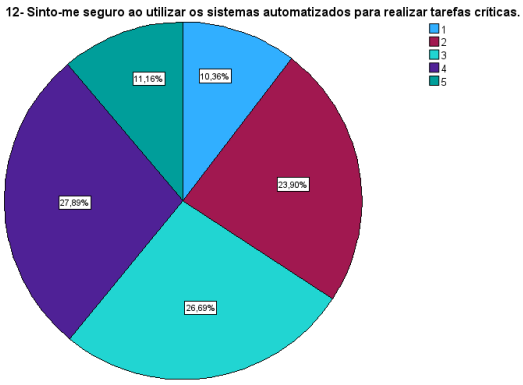


Figura 29 - Gráfico circular referente a questão nº12.

Questão nº13

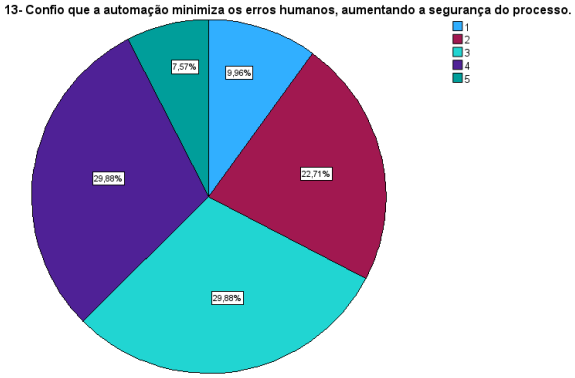


Figura 30 - Gráfico circular referente a questão nº13.

Questão nº14

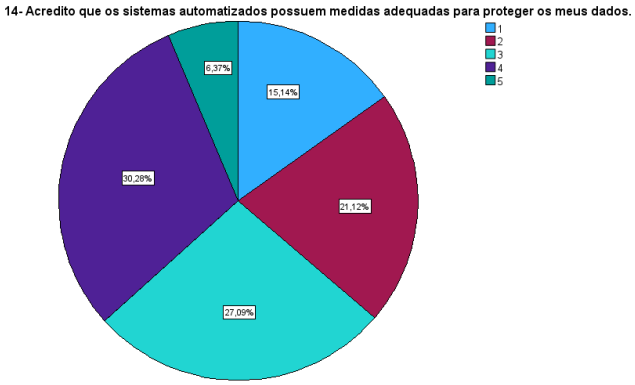


Figura 31 - Gráfico circular referente a questão nº14.

Questão nº15

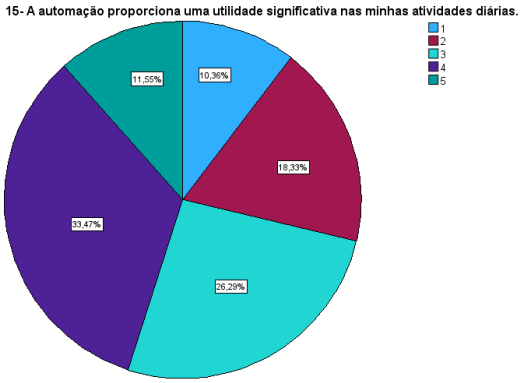


Figura 32 - Gráfico circular referente a questão nº15.

Questão nº16

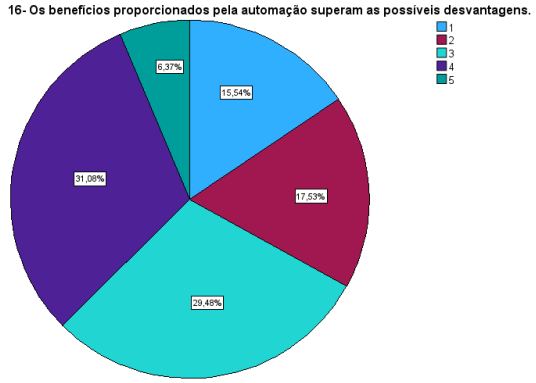


Figura 33 - Gráfico circular referente a questão nº16.

Questão nº17

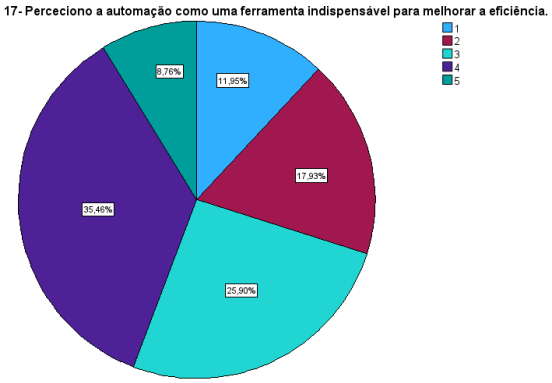


Figura 34 - Gráfico circular referente a questão nº17.

Questão nº18

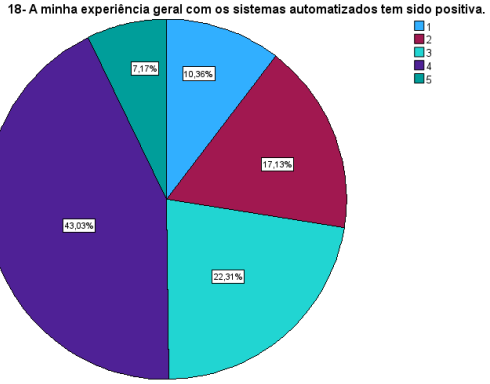


Figura 35 - Gráfico circular referente a questão nº18.

Questão nº19

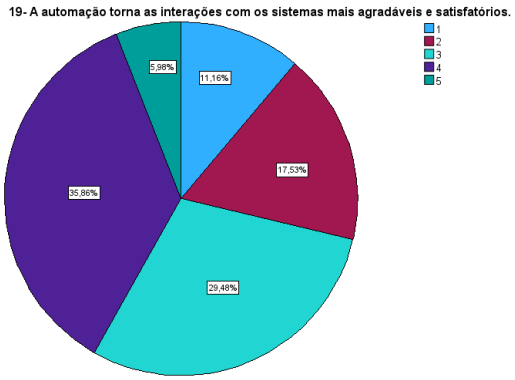


Figura 36 - Gráfico circular referente a questão nº19.

Questão nº20

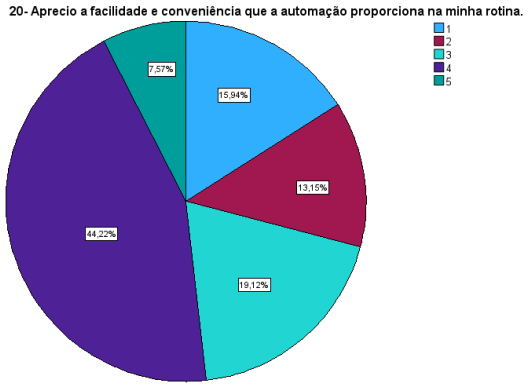


Figura 37 - Gráfico circular referente a questão nº20.

Questão nº21

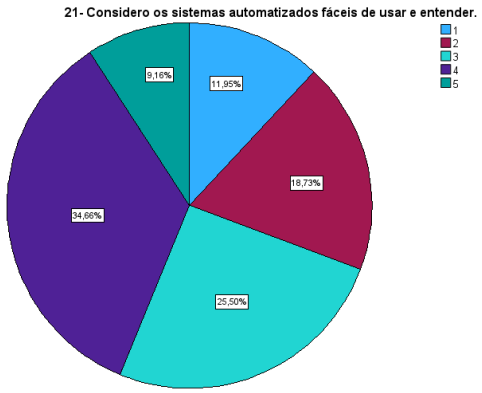


Figura 38 - Gráfico circular referente a questão nº21.

Questão nº22

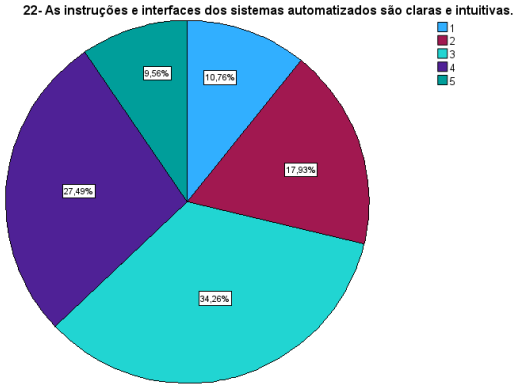


Figura 39 - Gráfico circular referente a questão nº22.

Questão nº23

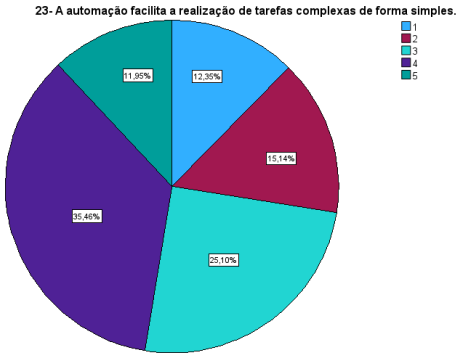


Figura 40 - Gráfico circular referente a questão nº23.

Questão nº24

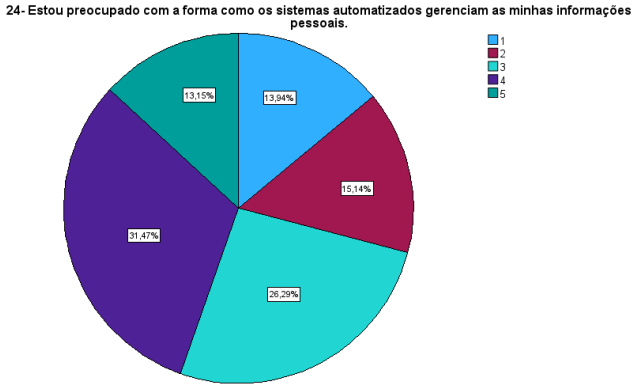


Figura 41 - Gráfico circular referente a questão nº24.

Questão nº25

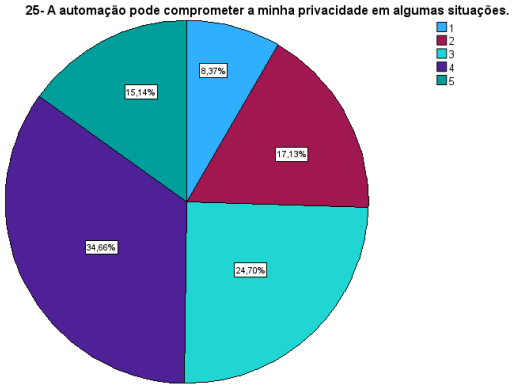


Figura 42 - Gráfico circular referente a questão nº25.

Questão nº26

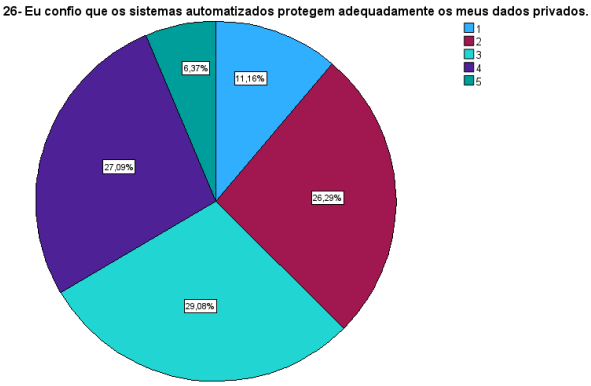


Figura 43 - Gráfico circular referente a questão nº26.

Questão nº27

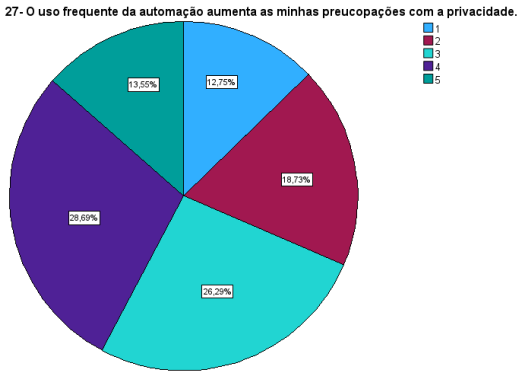


Figura 44 - Gráfico circular referente a questão nº27.

Questão nº28

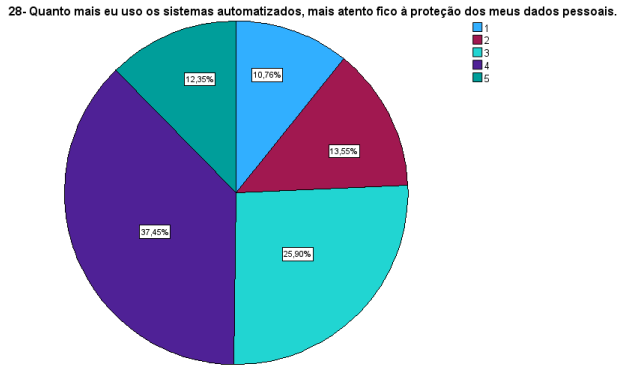


Figura 45 - Gráfico circular referente a questão nº28.

Questão nº29

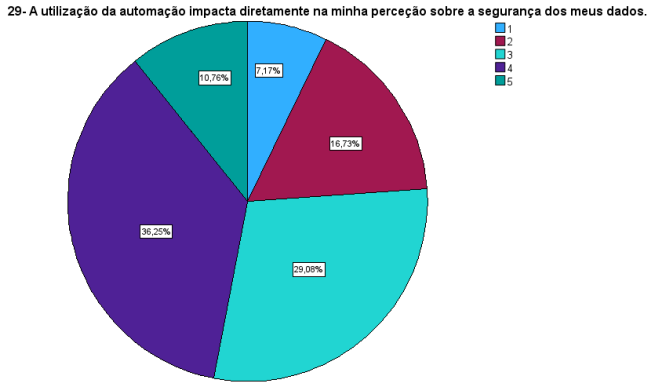


Figura 46 - Gráfico circular referente a questão nº29.

Questão nº30

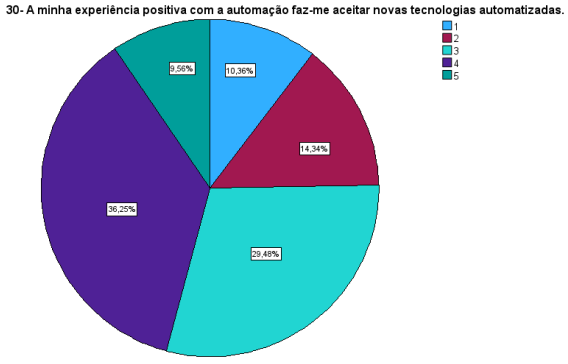


Figura 47 - Gráfico circular referente a questão nº30.

Questão nº31

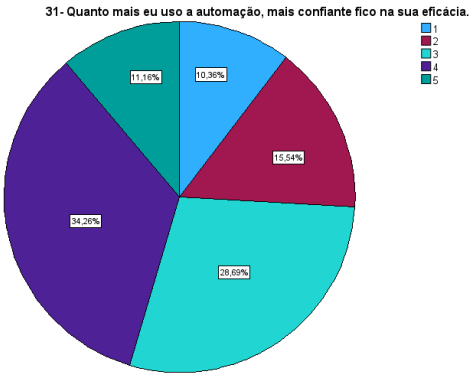


Figura 48 - Gráfico circular referente a questão nº31.

Questão nº32

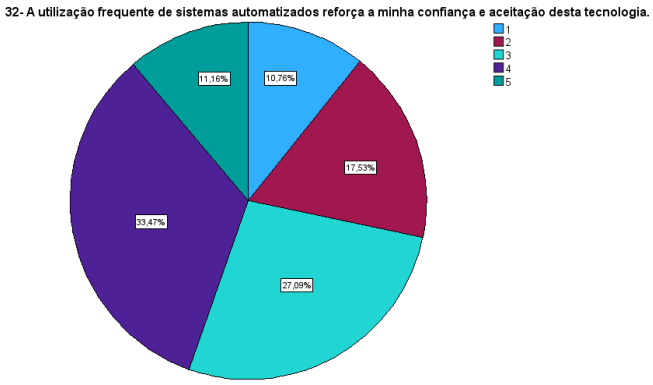


Figura 49 - Gráfico circular referente a questão nº32.