Cibersegurança e comportamento organizacional

A formação como vetor de adoção de autenticação multifator no setor público

Marcos Monteiro de Campos

Dissertação para obtenção do Grau de Mestre em

Informática

Orientador: Professor Doutor Paulo André Reis Duarte Branco

Júri

Presidente: Professora Doutora Andreia Cristina Teles Vieira

Orientador: Professor Doutor Paulo André Reis Duarte Branco

Arguente: Professor Doutor José Vicente Pereira dos Reis

Agosto 2025

Dissertação de Mestrado realizada sob a orientação de Paulo Duarte Branco, apresentada no ISTEC – Instituto Superior de Tecnologias Avançadas de Lisboa para obtenção de grau de Mestre em Informática.

Para a Sandra,
minha esposa, exemplo sereno de força e coragem.

A tua resiliência é uma fonte constante de inspiração.
Enfrentas a mudança com elegância e segues em frente com determinação, mesmo perante as maiores adversidades. Sem lamentos. Sem hesitações.

Neste percurso, foste mais do que apoio: foste impulso.
Concluir esta etapa só foi possível porque a percorri ao teu lado.

Agradeço-te por tudo o que és
E por nunca desistires de seguir em frente.

I. Resumo

Esta dissertação analisa o impacto da formação em cibersegurança na intenção de adoção da autenticação multifator (MFA) por parte de colaboradores do setor público português. Com base no modelo UTAUT (Unified Theory of Acceptance and Use of Technology), o estudo avalia de que forma perceções individuais — como utilidade esperada, esforço percebido, influência social, condições facilitadoras, autoeficácia e ansiedade — influenciam a intenção comportamental de adoção da MFA. É também analisado se essas perceções podem ser positivamente influenciadas por uma intervenção formativa breve e dirigida.

Foi utilizado um desenho experimental com grupo de controlo e grupo experimental, sendo este último exposto a um vídeo educativo de sensibilização para a cibersegurança com cinco minutos de duração. Ambos os grupos responderam a um questionário baseado no modelo UTAUT. Foram recolhidas 165 respostas válidas e conduzidas análises estatísticas descritivas, correlações de Pearson e testes t. Os resultados confirmam que os principais construtos do modelo estão significativamente correlacionados com a intenção de adoção da MFA, com destaque para a utilidade esperada, o esforço percebido, a autoeficácia e as condições facilitadoras. A ansiedade apresentou uma correlação negativa moderada, enquanto a formação prévia em cibersegurança, fora do contexto experimental, não revelou associação significativa com os construtos analisados.

A intervenção formativa demonstrou ter impacto positivo na perceção de facilidade de utilização, confiança e, em alguns casos, utilidade e influência social, especialmente nos métodos de MFA mais familiares aos participantes. Os resultados sugerem que mesmo formatos de formação breves e escaláveis podem contribuir para uma melhoria comportamental em matéria de cibersegurança. Conclui-se que a implementação eficaz da MFA em organizações públicas exige uma combinação de medidas técnicas, formação prática e compromisso organizacional com a cultura de segurança.

Palavras Chave: autenticação multifator; cibersegurança; adoção tecnológica; UTAUT; setor público; formação; intenção comportamental

II. Abstract

This dissertation investigates the impact of cybersecurity training on the intention to adopt multifactor authentication (MFA) among employees in the Portuguese public sector. Based on the Unified Theory of Acceptance and Use of Technology (UTAUT), the study analyses how individual perceptions—such as performance expectancy, effort expectancy, social influence, facilitating conditions, self-efficacy, and anxiety—affect users' behavioural intention to adopt MFA. It further explores whether these perceptions can be influenced by a short, targeted educational intervention.

An experimental design was employed, involving a control group and an experimental group, the latter exposed to a five-minute cybersecurity awareness video prior to completing a UTAUT-based questionnaire. A total of 165 valid responses were collected and analysed using descriptive statistics, Pearson correlations, and t-tests. The results confirm that the main UTAUT constructs are significantly correlated with the intention to adopt MFA, with performance expectancy, effort expectancy, self-efficacy and facilitating conditions showing the strongest associations. Anxiety showed a moderate negative correlation, and prior cybersecurity training—outside the experimental context—was not significantly related to any of the key constructs.

The educational intervention demonstrated a measurable positive effect on perceptions of ease of use, confidence, and— in some cases—perceived utility and social influence, particularly for authentication methods with which participants were already familiar. These findings suggest that even short and scalable training formats can positively influence cybersecurity behaviour in institutional contexts. The study concludes that successful implementation of MFA in public organisations requires a combination of technical measures, practical training, and organisational commitment to security culture.

Keywords: multifactor authentication; cybersecurity; technology adoption; UTAUT; public sector; training; behavioural intention

Índice

I. Resumo vii

II. Abstract viii

III. Índice de tabelas xiii

1. Introdução 1

2. Exposição do problema em estudo 3

2.1. Contextualização 3

2.2. Objetivo da investigação 4

2.2.1. Objetivo geral 4

2.2.2. Objetivos específicos 4

2.3. Perguntas de investigação 4

3. Revisão bibliográfica 7

3.1. Cibersegurança no setor público 7

3.1.1. Conceito de cibersegurança e particularidades do setor público 7

3.1.2. Vulnerabilidades específicas e tipologias de ameaças 8

3.1.3. Estratégias nacionais e políticas públicas em Portugal 8

3.1.4. Cultura organizacional e segurança institucional 10

3.2. Segurança da informação e necessidade de MFA 11

3.3. Barreiras e facilitadores da adoção de MFA 12

3.4. Modelos teóricos de aceitação de tecnologia 13

3.4.1. Technology Acceptance Model (TAM) 13

3.4.2. Unified Theory of Acceptance and Use of Technology (UTAUT) 13

3.4.3. Outras teorias relevantes 15

3.4.4. Aplicação dos modelos ao MFA 17

3.4.5. Formação em cibersegurança e mudança comportamental 18

3.4.6. Síntese e implicações 19
4. Metodologia 21
4.1. Desenho do Estudo 21
4.2. Participantes 21
4.3. Instrumentos 21
4.4. Estímulo educativo 22
4.5. Procedimentos 23
4.6. Técnicas de análise 23
5. Análise dos resultados 25
5.1. Descrição da amostra 25
5.2. Fator de autenticação SMS/E-mail 26
5.2.1. Caracterização da subamostra 26
5.2.2. Correlações entre construtos UTAUT, formação e grupos 29
5.2.3. Testes *t* – comparação entre grupos 31
5.3. Fator de autenticação Voz 33
5.3.1. Caracterização da subamostra 33
5.3.2. Correlações entre construtos UTAUT, formação e grupos 35
5.3.3. Testes *t* – comparação entre grupos 37
5.4. Fator de autenticação Reconhecimento Facial 39
5.4.1. Caracterização da subamostra 39
5.4.2. Correlações entre construtos UTAUT, formação e grupos 42
5.4.3. Testes *t* – comparação entre grupos 44
5.5. Fator de autenticação Impressão Digital 46
5.5.1. Caracterização da subamostra 46
5.5.2. Correlações entre construtos UTAUT, formação e grupos 48
5.5.3. Testes *t* – comparação entre grupos 50
5.6. Fator de autenticação Token Físico 52

5.6.1. Caracterização da subamostra 52
5.6.2. Correlações entre construtos UTAUT, formação e grupos 54
5.6.3. Testes *t* – comparação entre grupos 56
5.7. Fator de autenticação Aplicação Móvel 59
5.7.1. Caracterização da subamostra 59
5.7.2. Correlações entre construtos UTAUT, formação e grupos 61
5.7.3. Testes *t* – comparação entre grupos 63
6. Discussão 67
6.1. Introdução à discussão 67
6.2. Discussão por hipótese 67
6.2.1. Hipótese 1 - expetativa de desempenho 67
6.2.2. Hipótese 2 – expetativa de esforço ou facilidade de uso 68
6.2.3. Hipótese 3 – influência social 70
6.2.4. Hipótese 4 - condições facilitadoras 71
6.2.5. Hipótese 5 – autoeficácia 73
6.2.6. Hipótese 6 - ansiedade 74
6.2.7. Hipótese 7 – formação prévia 75
6.3. Síntese geral dos resultados 76
6.4. Implicações práticas e estratégicas 77
7. Conclusão 79
7.1. Limitações 81
7.2. Estudos futuros 82
8. Referências Bibliográficas 85
9. Anexo A – Questionário aplicado 89
9.1. Dados sociodemográficos 89
9.2. Conhecimento e utilização de MFA 90
9.3. Perceções sobre MFA (escala likert 1-5) 90

III. Índice de tabelas

Tabela 1 Comparação de Diferentes Teorias de Aceitação de Tecnologia.....16

Tabela 2 Dados Sociodemográficos da Subamostra de Participantes que Conhecem o Fator de Autenticação SMS/E-mail. 28

Tabela 3 Coeficientes de Correlação de Pearson entre os Construtos UTAUT, Formação Prévia e Apresentação do Estímulo Experimental, na Subamostra Relativa ao Fator de Autenticação SMS/E-mail.....30

Tabela 4 Comparação de Médias entre Grupo de Controlo e Experimental, no que Concerne aos Fatores Considerados no Modelo UTAUT, para o Fator de Autenticação SMS/E-mail 32

Tabela 5 Dados Sociodemográficos da Subamostra de Participantes que Conhecem o Fator de Autenticação Voz.....34

Tabela 6 *Coeficientes de Correlação de Pearson entre os Construtos UTAUT, Formação Prévia e Apresentação do Estímulo Experimental, na Subamostra Relativa ao Fator de Autenticação Voz*.....36

Tabela 7 Comparação de Médias entre Grupo de Controlo e Experimental, no que Concerne aos Fatores Considerados no Modelo UTAUT, para o Fator de Autenticação Voz38

Tabela 8 Dados Sociodemográficos da Subamostra de Participantes que Conhecem o Fator de Autenticação Reconhecimento Facial.....41

Tabela 9 Coeficientes de Correlação de Pearson entre os Construtos UTAUT, Formação Prévia e Apresentação do Estímulo Experimental, na Subamostra Relativa ao Fator de Autenticação Reconhecimento Facial 43

Tabela 10 Comparação de médias entre grupo de controlo e experimental, no que concerne aos fatores considerados no modelo UTAUT, para o fator de autenticação Reconhecimento Facial. 45

Tabela 11 Dados Sociodemográficos da Subamostra de Participantes que Conhecem o Fator de Autenticação Impressão Digital.....47

Tabela 12 Coeficientes de Correlação de Pearson entre os Construtos UTAUT, Formação Prévia e Apresentação do Estímulo Experimental, na Subamostra Relativa ao Fator de Autenticação Impressão Digital 49

Tabela 13 *Comparação de Médias entre Grupo de Controlo e Experimental, no que Concerne aos Fatores Considerados no Modelo UTAUT, para o Fator de Autenticação Impressão Digital*.....51

Tabela 14 Dados sociodemográficos da subamostra de participantes que conhecem o fator de autenticação token físico. 53

Tabela 15 Coeficientes de Correlação de Pearson entre os Construtos UTAUT, Formação Prévia e Apresentação do Estímulo Experimental, na Subamostra Relativa ao Fator de Autenticação Token Físico.....55

Tabela 16 *Comparação de Médias entre Grupo de Controlo e Experimental, no que Concerne aos Fatores Considerados no Modelo UTAUT, para o Fator de Autenticação Token Físico.*.....57

Tabela 17 Dados Sociodemográficos da Subamostra de Participantes que Conhecem o Fator de Autenticação Aplicação Móvel.....60

Tabela 18 Coeficientes de Correlação de Pearson entre os Construtos UTAUT, Formação Prévia e Apresentação do Estímulo Experimental, na Subamostra Relativa ao Fator de Autenticação Aplicação Móvel.....62

Tabela 19 Comparação de Médias entre Grupo de Controlo e Experimental, no que Concerne aos Fatores Considerados no Modelo UTAUT, para o Fator de Autenticação Aplicação Móvel.....64

1. Introdução

Numa era em que as ameaças cibernéticas estão em constante evolução, o setor público tornou-se um alvo privilegiado para atores maliciosos que exploram vulnerabilidades humanas e tecnológicas. A segurança digital das organizações depende não apenas das ferramentas tecnológicas implementadas, mas sobretudo da sua adoção eficaz pelos utilizadores. Entre estas medidas, destaca-se a autenticação multifator (MFA), um dos mecanismos mais recomendados para reforçar a proteção de identidades digitais e dados sensíveis.

Apesar da sua comprovada eficácia, a MFA enfrenta resistência à adoção, especialmente em contextos organizacionais onde os utilizadores carecem de formação ou percecionam a tecnologia como complexa. No setor público português, onde predominam infraestruturas legadas e culturas institucionais enraizadas, compreender os fatores que influenciam a intenção de adoção de MFA é fundamental para o sucesso de qualquer iniciativa de cibersegurança.

A Agência da União Europeia para a Cibersegurança (ENISA, 2021) destaca que a construção de uma cultura organizacional de cibersegurança deve ser sustentada por esforços contínuos de sensibilização, formação prática e alinhamento institucional. Esta abordagem exige o envolvimento de todos os níveis da organização e atenção especial aos fatores comportamentais que influenciam a adoção de medidas como a MFA — perspetiva esta plenamente assumida pela presente investigação.

De acordo com o Centro Nacional de Cibersegurança (2024) , os incidentes cibernéticos no setor público português aumentaram mais de 40% no último ano, refletindo a crescente sofisticação dos ataques e a importância da segurança digital institucional. Apesar disso, menos de 50% das instituições públicas adotam soluções robustas como a autenticação multifator (MFA)(Microsoft, 2024), sendo que esta tem uma taxa de eficácia superior a 99% contra acessos não autorizados (Centro Nacional de Cibersegurança, 2023).

A presente dissertação investiga o impacto de ações formativas na disposição dos colaboradores do setor público a adotarem a MFA, utilizando como referencial teórico o modelo UTAUT (Unified Theory of Acceptance and Use of Technology). Este modelo permite analisar construtos como a expectativa de desempenho, a facilidade percebida de uso, a influência social e as condições facilitadoras, entre outros, com o objetivo de prever a aceitação de novas tecnologias pelos utilizadores.

Para tal, foi desenhado um estudo empírico envolvendo uma amostra de colaboradores de instituições públicas na área do emprego e formação profissional. Os participantes foram

distribuídos aleatoriamente em dois grupos: um grupo de controlo que respondeu diretamente a um questionário baseado em UTAUT, e um grupo experimental que, antes de responder, assistiu a um vídeo de sensibilização em cibersegurança abordando boas práticas e os benefícios da MFA.

Este trabalho visa contribuir para o conhecimento sobre a eficácia de formação em cibersegurança como ferramenta para promover a adoção de boas práticas e tecnologias de proteção. Espera-se que os resultados apoiem decisores e responsáveis pela segurança da informação na conceção de estratégias formativas mais eficazes e direcionadas para os contextos organizacionais reais do setor público.

Nos capítulos seguintes, são apresentados: a contextualização do problema e definição dos objetivos, a revisão da literatura, a metodologia utilizada, a análise dos resultados obtidos, a discussão crítica dos achados e, por fim, as conclusões e recomendações práticas e académicas.

2. Exposição do problema em estudo

2.1. Contextualização

O sucesso de qualquer iniciativa de transformação digital depende, em grande medida, da capacidade dos utilizadores em adotar de forma eficaz as soluções propostas. No entanto, a simples disponibilização de tecnologia não garante a sua aceitação nem o seu uso seguro e consistente. No caso da autenticação multifator (MFA), apesar do seu valor estratégico amplamente reconhecido, muitos colaboradores continuam a não a utilizar, seja por desconhecimento, perceção de complexidade ou ausência de estímulo organizacional.

A literatura aponta que, quando a adoção tecnológica falha, a organização não só perde o retorno do investimento como pode enfrentar um ciclo de resistência interna, onde cada nova solução tecnológica é recebida com ceticismo. Este fenómeno de fricção cultural torna-se ainda mais sensível em ambientes públicos, onde a mudança é frequentemente condicionada por restrições orçamentais, resistência à mudança e estruturas organizacionais rígidas.

Em Portugal, os dados disponíveis apontam para um crescimento significativo no número de ciberataques a entidades públicas, sendo o setor da administração pública um dos mais visados. Segundo o Centro Nacional de Cibersegurança, os ataques aumentaram 40% entre 2019 e 2020, sendo que o setor público concentrou cerca de um quarto desses incidentes. A proteção das identidades digitais dos colaboradores é, assim, uma prioridade estratégica.

Investigadores como Bélanger et al. (2017) e Herath & Rao (2009) já demonstraram que a eficácia das políticas de segurança depende em larga medida da perceção de utilidade, esforço e apoio social por parte dos utilizadores. Assim, é fundamental compreender de que forma essas variáveis influenciam a adoção de medidas como a MFA em ambientes organizacionais públicos.

Neste contexto, a presente investigação assume relevância por explorar a seguinte questão: será que ações formativas simples, como um vídeo de sensibilização, podem efetivamente aumentar a predisposição dos colaboradores do setor público a adotar a MFA?

A resposta a esta pergunta permitirá não só avaliar a eficácia da formação enquanto mecanismo de mudança comportamental, como também oferecer um contributo prático para decisores políticos e responsáveis de segurança no setor público. Pretende-se, assim, identificar os fatores que promovem ou inibem a adoção da MFA e fornecer recomendações informadas para políticas de formação e sensibilização mais eficazes.

2.2. Objetivo da investigação

2.2.1. Objetivo geral

Avaliar o impacto de uma ação formativa em formato vídeo na intenção de adoção da autenticação multifator (MFA) por parte de colaboradores do setor público português.

2.2.2. Objetivos específicos

Para operacionalizar o objetivo geral, foram definidos os seguintes objetivos específicos, cada um centrado num construto do modelo teórico utilizado:

- Identificar os fatores que influenciam a aceitação da MFA segundo o modelo UTAUT.
- Adaptar e validar um questionário com base nos construtos UTAUT para o contexto da MFA.
- Conceber e aplicar um vídeo educativo com conteúdos de sensibilização em cibersegurança.
- Comparar os níveis de intenção comportamental entre grupos com e sem formação prévia.
- Avaliar a relação entre formação em cibersegurança e variáveis como autoeficácia, ansiedade e influência social.

2.3. Perguntas de investigação

Tendo em consideração a temática de adoção de métodos de segundo fator de autenticação, assim, define-se como perguntas de investigação a desenvolver:

PI1: De que forma a formação prévia em cibersegurança influencia a intenção dos colaboradores do setor público em adotar a autenticação multifator (MFA)?

Esta pergunta procura analisar a relação entre a existência de formação prévia em cibersegurança e a predisposição para ativar MFA. Pretende-se compreender se o contacto anterior com conteúdos formativos potencia uma maior intenção de adoção, aferindo-se esta ligação através de estatística descritiva e correlações de Pearson.

PI2: Que construtos do modelo UTAUT, nomeadamente autoeficácia e ansiedade, melhor explicam a predisposição para a adoção da MFA no contexto analisado?

Com esta questão investiga-se quais os fatores psicológicos que apresentam maior peso na explicação da intenção de adotar MFA. O enfoque está em perceber se uma maior autoeficácia ou níveis reduzidos de ansiedade contribuem de forma significativa para aumentar

a intenção, comparando os coeficientes de correlação obtidos para cada construto do modelo UTAUT.

PI3: Quais são as diferenças observadas nos níveis de intenção comportamental entre colaboradores expostos ou não ao estímulo educativo?

Através desta pergunta procura-se avaliar o impacto direto da intervenção formativa, um vídeo educativo, na intenção de adoção da MFA. A análise centra-se na comparação das médias entre grupo experimental e grupo de controlo, utilizando o teste t para amostras independentes (e cálculo do tamanho do efeito, via Cohen's d), após confirmados os pré-requisitos estatísticos.

PI4: Em que medida um vídeo educativo contribui para transformar perceções sobre a utilidade e a usabilidade da MFA?

Esta questão visa compreender se a intervenção formativa é capaz de modificar a perceção dos participantes relativamente à utilidade percebida (expetativa de desempenho) e à facilidade de utilização (expetativa de esforço). A comparação estatística entre grupos, articulada com os padrões de correlação, permite identificar os mecanismos de mudança que sustentam a adoção da MFA.

3. Revisão bibliográfica

3.1. Cibersegurança no setor público

3.1.1. Conceito de cibersegurança e particularidades do setor público

A cibersegurança é definida como o conjunto de práticas, processos e tecnologias destinadas a proteger sistemas de informação, redes e dados contra acessos não autorizados, ataques ou danos. Este conceito abrange a garantia da confidencialidade, integridade e disponibilidade da informação, princípios fundamentais para a segurança da informação (Antunes et al., 2021).

No contexto do setor público, a cibersegurança assume particular relevância devido à natureza sensível dos dados geridos e à criticidade dos serviços prestados. As administrações públicas lidam frequentemente com informações pessoais dos cidadãos, dados fiscais, de saúde e justiça, tornando-se alvos atrativos para ciberataques (Ribeiro et al., 2024). Além disso, a dependência de infraestruturas tecnológicas obsoletas e a escassez de recursos humanos especializados agravam a vulnerabilidade das instituições públicas (Antunes et al., 2021).

A complexidade organizacional e a rigidez hierárquica típicas do setor público dificultam a implementação ágil de medidas de cibersegurança. A integração de novas tecnologias e a atualização de sistemas existentes enfrentam barreiras burocráticas e orçamentais, comprometendo a capacidade de resposta a ameaças emergentes (Ribeiro et al., 2024).

Em Portugal, estudos indicam que muitas autarquias e organismos públicos ainda não adotaram práticas básicas de cibersegurança, como a autenticação multifator, expondo-se a riscos significativos (Antunes et al., 2021). A falta de uma cultura organizacional orientada para a segurança da informação e a ausência de formação contínua para os colaboradores contribuem para este cenário (Ribeiro et al., 2024).

Assim, a cibersegurança no setor público não se limita à implementação de soluções tecnológicas, exigindo uma abordagem holística que inclua políticas públicas eficazes, formação de recursos humanos, cultura organizacional proativa e liderança comprometida com a segurança da informação.

3.1.2. Vulnerabilidades específicas e tipologias de ameaças

A crescente digitalização dos serviços públicos tem exposto as administrações públicas a riscos cibernéticos significativos. Estes riscos são agravados por fatores como infraestruturas tecnológicas obsoletas, escassez de profissionais qualificados e fragmentação das políticas de cibersegurança. De acordo com Fujs & Bernik (2024), o setor público enfrenta desafios únicos na implementação de estratégias eficazes de cibersegurança, devido à complexidade organizacional e à necessidade de equilibrar transparência com segurança.

Em Portugal, a Estratégia Nacional de Segurança do Ciberespaço 2019-2023 reconhece a importância de fortalecer as capacidades tecnológicas e humanas no setor público para enfrentar ameaças cibernéticas emergentes (República Portuguesa, 2019). No entanto, a implementação efetiva dessas estratégias é frequentemente dificultada por limitações orçamentais e pela falta de coordenação entre diferentes entidades governamentais (Centro Nacional de Cibersegurança, 2023).

A nível europeu, a fragmentação das políticas de cibersegurança entre os Estados-Membros representa um obstáculo significativo para a criação de uma defesa cibernética coesa. Segundo o Tribunal de Contas Europeu (2019), a falta de coordenação e partilha de informações entre os países da UE compromete a eficácia das respostas a incidentes cibernéticos e a resiliência geral do setor público.

Além disso, a escassez de profissionais especializados em cibersegurança no setor público é uma preocupação crescente. Fujs & Bernik (2024) destacam que a competição com o setor privado, que frequentemente oferece melhores condições salariais, dificulta a retenção de talentos nas administrações públicas. Essa escassez de competências técnicas compromete a capacidade das instituições públicas de prevenir, detetar e responder eficazmente a ameaças cibernéticas.

A proteção de infraestruturas críticas, como sistemas de saúde, justiça e finanças, é particularmente desafiadora. Ataques cibernéticos a esses sistemas podem ter consequências graves para a segurança nacional e o bem-estar dos cidadãos. A necessidade de investimentos contínuos em tecnologias de segurança e na formação de pessoal é essencial para mitigar esses riscos e garantir a continuidade dos serviços públicos essenciais.

3.1.3. Estratégias nacionais e políticas públicas em Portugal

A cibersegurança no setor público português tem sido objeto de crescente atenção nos últimos anos, refletindo uma consciência institucional da sua importância para a proteção de

dados sensíveis e para a continuidade dos serviços públicos essenciais. De acordo com Antunes et al. (2021), o panorama da cibersegurança em Portugal caracteriza-se pela coexistência de avanços significativos em políticas públicas e desafios persistentes na sua operacionalização.

A Estratégia Nacional de Segurança do Ciberespaço (ENSC) 2019–2023 constitui o principal quadro de referência para a atuação estatal nesta área (República Portuguesa, 2019). Este documento define objetivos claros para a proteção de infraestruturas críticas, a sensibilização dos cidadãos e a capacitação de profissionais, reconhecendo a importância de uma abordagem integrada entre tecnologia, processos e cultura organizacional.

No entanto, a implementação prática desta estratégia enfrenta obstáculos importantes. Segundo o relatório do Observatório de Cibersegurança (Centro Nacional de Cibersegurança, 2023), a falta de recursos orçamentais e humanos especializados continua a ser um dos principais entraves à execução eficaz das políticas delineadas. Estas limitações refletem-se em lacunas na adoção de medidas fundamentais como a autenticação multifator, ainda ausente em várias entidades públicas locais (Centro Nacional de Cibersegurança, 2023).

A integração da ENSC com as exigências do quadro europeu, nomeadamente a Diretiva NIS2, constitui um passo essencial para harmonizar a resposta nacional aos desafios cibernéticos contemporâneos. Como sublinha Fujs & Bernik (2024), a convergência entre políticas nacionais e europeias é crucial para garantir resiliência e coordenação eficaz, sobretudo em setores estratégicos como a saúde e a administração fiscal.

Ainda assim, a execução plena destas estratégias encontra barreiras de natureza estrutural e cultural. A rigidez organizacional e a escassa cultura de segurança em algumas entidades públicas dificultam a adaptação a novas exigências normativas e tecnológicas (Ribeiro et al., 2024). Além disso, a falta de auditorias regulares e de métricas claras de desempenho compromete a capacidade de monitorizar e ajustar as políticas de forma proativa.

Como se constata, a consolidação de uma postura de cibersegurança robusta no setor público português exige não só a existência de estratégias nacionais bem definidas, mas também um investimento efetivo em liderança institucional, formação contínua e processos de avaliação permanentes. Tal como reforça Antunes et al. (2021), a segurança digital deve ser entendida como uma dimensão transversal da governação pública, integrando-se nos objetivos estratégicos de modernização administrativa e proximidade ao cidadão.

3.1.4. Cultura organizacional e segurança institucional

A eficácia da cibersegurança no setor público não depende apenas de tecnologias ou políticas normativas. Diversos autores defendem que a cultura organizacional constitui um dos pilares centrais para a consolidação de práticas de segurança sustentáveis e eficazes (Handri et al., 2024; Schein, 2010). Trata-se de uma dimensão invisível mas poderosa, que influencia atitudes, comportamentos e prioridades institucionais face à proteção da informação.

De acordo com Ruighaver et al. (2007), uma cultura de segurança sólida é aquela em que os valores, normas e práticas de segurança são internalizados pelos colaboradores, não apenas impostos por regulamentação. No setor público, onde coexistem práticas administrativas tradicionais com exigências crescentes de digitalização, a cultura organizacional pode funcionar tanto como catalisador como barreira à adoção de boas práticas de cibersegurança. Como argumentam Cram et al. (2017), a eficácia das políticas de segurança depende fortemente do alinhamento entre valores organizacionais, normas comportamentais e mecanismos de responsabilização formal.

Em Portugal, o Observatório de Cibersegurança sublinha que a ausência de liderança ativa, a dispersão de responsabilidades e a rotatividade de recursos técnicos têm dificultado a criação de ambientes organizacionais propícios à segurança digital (Centro Nacional de Cibersegurança, 2023). A este cenário somam-se constrangimentos como a escassez de formação contínua, o desajuste entre políticas internas e normativos externos e a prevalência de atitudes reativas em detrimento de abordagens preventivas (Antunes et al., 2021).

Como salientam Parsons et al. (2014), a eficácia das políticas de segurança depende fortemente de fatores humanos e contextuais, sendo o comportamento dos colaboradores moldado por normas sociais, atitudes partilhadas e modelos observáveis no ambiente de trabalho. No contexto público, onde os processos de mudança tendem a ser mais lentos e marcados por estruturas rígidas, o envolvimento ativo das chefias intermédias é crucial para garantir que a segurança digital se alinha com os objetivos organizacionais. De acordo com Ifinedo (2012), o apoio da gestão influencia significativamente a adesão às políticas de segurança, funcionando como fator de reforço para a adoção de comportamentos seguros e sustentáveis.

A responsabilização também emerge como conceito-chave. Ao contrário de abordagens centradas exclusivamente no controlo e na punição, modelos contemporâneos de cibersegurança sugerem a criação de ambientes de confiança, onde os colaboradores se sintam responsabilizados, mas não temerosos, pelo cumprimento das normas (Sasse et al., 2001). Isto

implica promover um equilíbrio entre políticas restritivas e uma comunicação organizacional clara, empática e capacitadora.

Assim, o reforço da segurança institucional no setor público requer uma transformação cultural gradual, mas intencional. Sem uma cultura que valorize a segurança como parte integrante da missão organizacional, mesmo os sistemas técnicos mais sofisticados permanecem vulneráveis à falha humana.

3.2. Segurança da informação e necessidade de MFA

A segurança da informação tornou-se um dos principais pilares da sustentabilidade organizacional na era digital. Com o aumento dos ataques baseados em engenharia social e na exploração de credenciais, a autenticação multifator (MFA) é hoje considerada uma das medidas essenciais para mitigar o risco de acesso não autorizado (Fenton et al., 2017). De acordo com as diretrizes do NIST (National Institute of Standards and Technology), a MFA é fortemente recomendada como parte integrante de uma política robusta de identidade digital.

No entanto, a adoção de MFA está frequentemente condicionada por barreiras de usabilidade e perceção individual. Estudos realizados por Venkatesh et al. (2003), no desenvolvimento do modelo UTAUT, identificaram quatro fatores principais que explicam a aceitação tecnológica: expectativa de desempenho, expectativa de esforço, influência social e condições facilitadoras. Estes construtos foram validados empiricamente como preditores significativos da intenção de uso de tecnologias emergentes.

Outras abordagens complementares, como o Technology Acceptance Model (F. Davis, 1985), a Teoria do Comportamento Planeado (Ajzen, 1991) e a Teoria da Difusão da Inovação (Rogers, 2003), reforçam que tanto fatores racionais quanto perceções sociais e culturais influenciam a decisão de adotar novas tecnologias. No contexto específico da MFA, aspetos como a autoeficácia percebida (Bandura, 1986a) e os níveis de ansiedade digital (Venkatesh & Bala, 2008) também demonstram ter um papel relevante na predisposição dos utilizadores.

O Government Accountability Office dos EUA (Powner & Technology, 2016) identificou, num relatório dirigido a agências federais, que a resistência à MFA advém, em muitos casos, da ausência de formação adequada e de experiências prévias negativas com ferramentas pouco intuitivas. Adicionalmente, o estudo de Alawida et al. (2022) evidencia que a pandemia da COVID-19 exacerbou as vulnerabilidades nas infraestruturas tecnológicas, reforçando a urgência da adoção de práticas como a MFA.

Deste modo, a literatura converge para a importância de intervenções educativas no aumento da aceitação da MFA. A disponibilização de conteúdos formativos adequados pode alterar positivamente perceções de utilidade, esforço, confiança e segurança, promovendo uma cultura mais resiliente face às ameaças cibernéticas.

Nos próximos tópicos, será realizada uma análise aprofundada dos principais modelos teóricos de aceitação tecnológica que sustentam esta investigação, nomeadamente o Technology Acceptance Model (TAM), Unified Theory of Acceptance and Use of Technology (UTAUT) nas suas diferentes iterações, e outras teorias como a Theory of Planned Behavior (TPB), Theory of Reasoned Action (TRA), Social Cognitive Theory (SCT) e Innovation Diffusion Theory (IDT), bem como a sua aplicabilidade à MFA.

3.3. Barreiras e facilitadores da adoção de MFA

Apesar do reconhecimento institucional da importância da MFA, a sua adoção efetiva enfrenta obstáculos cognitivos e comportamentais que retardam a sua implementação prática. Como observam Venkatesh et al. (2003) no contexto do UTAUT, perceções como ansiedade tecnológica, norma social e capacidade percetiva influenciam significativamente a disposição dos indivíduos para adotar novas ferramentas de segurança.

Entre os fatores mais frequentemente identificados encontram-se:

- Perceção de complexidade ou inconveniência (Dinev et al., 2009);
- Baixo nível de literacia digital e falta de formação contínua em cibersegurança entre trabalhadores do setor público (Centro Nacional de Cibersegurança, 2024)
- Ausência de reforço por parte da liderança ou cultura organizacional permissiva (Posey et al., 2015);
- Falta de clareza sobre os benefícios reais da MFA para o utilizador final (Herath & Rao, 2009);
- Resistência à mudança, especialmente em ambientes burocráticos e hierarquizados(Kim & Kankanhalli, 2009).

Por outro lado, a literatura também identifica fatores facilitadores importantes, como:

- A existência de políticas organizacionais claras e apoio institucional à mudança;
- A disponibilização de apoio técnico e canais de formação acessíveis;
- A perceção de utilidade e confiança no sistema implementado;
- O impacto de intervenções educativas simples e bem direcionadas na mudança de atitudes e perceções.

Compreender este equilíbrio entre barreiras e facilitadores é fundamental para delinear estratégias eficazes de promoção da MFA, e constitui a base para aplicação dos modelos teóricos de aceitação tecnológica que se analisam nas secções seguintes.

3.4. Modelos teóricos de aceitação de tecnologia

3.4.1. Technology Acceptance Model (TAM)

O Modelo de Aceitação de Tecnologia (TAM), proposto por F. Davis (1985), é um dos modelos mais amplamente utilizados para prever a aceitação de tecnologia por parte dos utilizadores. O modelo parte da Teoria da Ação Racional (TRA) de Fishbein & Ajzen (1975) e introduz dois construtos fundamentais:

- Perceived Usefulness (PU): a perceção de que o uso de uma tecnologia melhora o desempenho no trabalho.
- Perceived Ease of Use (PEOU): a perceção de que o uso da tecnologia é isento de esforço.

Davis demonstrou que estes dois fatores explicam significativamente a intenção de utilização de sistemas de informação, sendo o PU o preditor mais forte da aceitação. O modelo TAM tem sido amplamente utilizado para estudar a adoção de tecnologias, incluindo aplicações no domínio da segurança da informação e autenticação multifator (F. D. Davis, 1989; Ifinedo, 2012; Venkatesh & Bala, 2008).

Apesar do seu valor explanatório, o TAM tem sido criticado por não considerar fatores sociais e contextuais mais amplos. Esta limitação levou ao desenvolvimento de modelos mais abrangentes, como o UTAUT, analisado no capítulo 3.4.2.

3.4.2. Unified Theory of Acceptance and Use of Technology (UTAUT)

O modelo UTAUT foi desenvolvido por Venkatesh et al. (2003) como uma consolidação de oito teorias anteriores de aceitação tecnológica, incluindo o TAM, a Teoria do Comportamento Planeado (TPB), a Teoria da Ação Racional (TRA), a Teoria da Difusão da Inovação (IDT), entre outras. Este modelo apresenta quatro construtos centrais que influenciam diretamente a intenção de uso de uma tecnologia:

- Expectativa de desempenho, entendida como o grau em que o indivíduo acredita que a tecnologia o ajudará a melhorar o seu desempenho nas tarefas profissionais. No contexto da MFA, traduz-se na perceção de que a autenticação reforça a segurança da identidade digital e previne acessos indevidos.

- Expectativa de esforço, que corresponde à facilidade de uso percebida. No caso da MFA, pode refletir-se na perceção de quão simples é instalar uma aplicação autenticadora, configurar um token físico ou utilizar um código recebido por SMS, sem necessidade de apoio técnico constante.
- Influência social, relativa à perceção de que pessoas relevantes (como colegas ou superiores hierárquicos) esperam que o indivíduo adote determinada tecnologia. Em ambientes públicos, pode manifestar-se quando a liderança institucional recomenda a adoção da MFA como prática padrão.
- Condições facilitadoras, que dizem respeito ao suporte técnico e organizacional percebido como disponível. Incluem, por exemplo, a existência de formação adequada, documentação acessível e apoio do departamento de informática durante o processo de adoção.
- Estes construtos são moderados por variáveis como a idade, o género, a experiência prévia com tecnologia e o grau de voluntariedade no uso. O UTAUT demonstrou elevada capacidade preditiva da intenção comportamental e do uso efetivo de tecnologias em contextos organizacionais.

Em 2012, Venkatesh et al. propuseram o UTAUT2, uma extensão orientada para o consumidor final. Esta versão introduziu três novos construtos — motivação hedónica, valor de preço e hábito —, sendo particularmente relevante quando se pretende estudar o uso de tecnologias fora do contexto profissional. No caso da adoção da MFA, o UTAUT2 pode ser útil para explorar aspetos como o conforto pessoal com a tecnologia ou a adoção por rotina.

O UTAUT tem sido amplamente utilizado em investigações sobre adoção de medidas de segurança, incluindo a MFA, em ambientes empresariais, académicos e governamentais. Estudos como os de Slade et al. (2015) ou Alalwan et al. (2017) demonstram que a aplicação deste modelo permite identificar claramente barreiras e fatores facilitadores de adoção, sobretudo quando combinado com estratégias formativas e comunicacionais. Em Portugal, Martins et al. (2014) aplicaram o modelo UTAUT ao contexto da banca digital, tendo identificado a utilidade percebida e o risco como determinantes chave da intenção de uso. Este estudo demonstra a aplicabilidade do modelo em serviços digitais em ambientes regulados, reforçando a sua pertinência para o setor público.

Diversos estudos posteriores reforçaram a aplicabilidade do UTAUT em contextos organizacionais e de segurança, incluindo o setor público, onde a adoção de tecnologias muitas vezes depende da integração entre fatores sociais, organizacionais e individuais (Bélanger et al., 2017; Ifinedo, 2012).

3.4.3. Outras teorias relevantes

Além do TAM e do UTAUT, outras abordagens teóricas oferecem contributos relevantes para a compreensão da adoção de tecnologias de segurança como a MFA:

- Teoria da Ação Racional (TRA) – Fishbein & Ajzen (1975): Sugere que o comportamento é determinado pela intenção, que por sua vez é influenciada pela atitude em relação ao comportamento e pelas normas subjetivas. Embora limitado por não considerar o controlo comportamental, serviu de base para teorias posteriores como TPB e TAM. No contexto da MFA, a TRA sugere que a decisão de ativar a autenticação será influenciada tanto pela atitude do utilizador em relação à sua utilidade (por exemplo, proteção contra acessos indevidos) como pelas normas subjetivas, ou seja, a perceção de que pessoas importantes esperam esse comportamento, como colegas ou superiores;
- Teoria do Comportamento Planeado (TPB) – Ajzen (1991): Introduz o conceito de controlo comportamental percebido como preditor adicional do comportamento. Esta teoria permite entender como perceções de controlo afetam a adoção voluntária de tecnologias. A intenção de adotar a MFA poderá ser influenciada pelas normas sociais internas da organização e pelo sentimento de controlo percebido — por exemplo, se o utilizador sente que consegue ativar a MFA sem dificuldades.
- Teoria Social Cognitiva (SCT) – (Bandura, 1986): Realça o papel da autoeficácia, ou seja, a crença na própria capacidade de executar um comportamento. No contexto da MFA, a autoeficácia influencia diretamente a predisposição para enfrentar barreiras técnicas ou de usabilidade.
- Teoria da Difusão da Inovação (IDT) – Rogers (2003): Foca-se em características da inovação (ex. vantagem relativa, compatibilidade, complexidade) que afetam a sua difusão. É especialmente útil para compreender a adoção da MFA a nível organizacional, destacando a importância de líderes de opinião e do fator observabilidade. No caso da MFA, a compatibilidade com sistemas existentes, a facilidade percebida de configuração ou a observabilidade (ver colegas a utilizar) podem acelerar a sua adoção.

Estas teorias, ainda que abordem diferentes dimensões, convergem na importância da perceção individual, da norma social e da capacidade percebida como determinantes da adoção tecnológica. A Tabela 1 resume os principais contributos e limitações dos modelos abordados:

Tabela 1

Comparação de Diferentes Teorias de Aceitação de Tecnologia

Modelo	Fatores principais	Moderadores	Aplicabilidade à MFA	Limitações principais
TAM (1989)	Utilidade percebida, Facilidade de uso percebida	Nenhum	Avaliação da perceção individual de tecnologias	Ignora fatores sociais e organizacionais
UTAUT (2003)	Expectativa de desempenho, esforço, influência social, condições facilitadoras	Idade, género, experiência, voluntariedade	Adoção organizacional de soluções tecnológicas, incluindo MFA	Requer dados sobre variáveis moderadoras
UTAUT2 (2012)	UTAUT + motivação hedónica, valor de preço, hábito	Idade, género, experiência, voluntariedade	Avaliação em contextos individuais e pessoais	Pouco testado em contextos organizacionais
TPB (1991)	Atitude, norma subjetiva, controlo comportamental percebido	Nenhum	Explica intenção e comportamento de segurança	Pouco detalhado para tecnologias específicas
TRA (1975)	Atitude, norma subjetiva	Nenhum	Estrutura fundacional para modelos posteriores	Ignora controlo percebido
SCT (1986)	Autoeficácia, reforço, aprendizagem social	Nenhum	Relevante para formação e perceção de capacidade	Pouco focado em tecnologia per se
IDT (2003)	Vantagem relativa, compatibilidade, complexidade, etc.	Nenhum	Adoção de inovações tecnológicas na organização	Mais geral, não centrado no indivíduo

Embora os modelos descritos não tenham sido originalmente desenvolvidos para tecnologias de segurança, os seus construtos explicam de forma eficaz os fatores psicológicos e sociais que influenciam a adoção de medidas como a MFA em ambientes institucionais. Apesar destas teorias complementares não terem sido aplicadas diretamente nesta investigação, os seus construtos influenciam indiretamente a forma como os utilizadores percecionam, avaliam e adotam a MFA, e foram consideradas no desenho do instrumento de recolha de dados.

3.4.4. Aplicação dos modelos ao MFA

A aplicação de modelos como TAM e UTAUT no estudo da adoção de mecanismos de segurança, como a MFA, tem vindo a crescer nos últimos anos, com destaque para contextos organizacionais, ambientes académicos e plataformas digitais de serviços.

Num estudo conduzido por Bélanger et al. (2017), o UTAUT foi utilizado para avaliar a aceitação de sistemas de autenticação multifator em instituições públicas norte-americanas. Os resultados demonstraram que a expectativa de desempenho e a influência social foram os principais determinantes da intenção de uso.

Outras investigações, como a de Alharbi et al. (2019), aplicaram o UTAUT2 para estudar a adoção de MFA em contextos de banca digital. Os autores verificaram que o hábito e a confiança no sistema, embora não constem do modelo UTAUT original, são fatores que ganham relevância em ambientes tecnológicos quotidianos. Estes construtos podem influenciar significativamente a aceitação da MFA, sobretudo entre utilizadores que já possuem rotinas digitais estabelecidas.

No domínio académico, Wong & Fai (2022) demonstraram, através de um estudo empírico no setor do transporte marítimo, que ações de formação específicas em cibersegurança promovem ganhos significativos em termos de autoeficácia dos utilizadores, ao mesmo tempo que reduzem a ansiedade tecnológica associada à utilização de mecanismos de proteção digital. Estes efeitos reforçam a importância da variável "formação" como catalisador de mudança comportamental, sobretudo quando se pretende fomentar a adoção voluntária de práticas de segurança robustas, como a autenticação multifator. O estudo evidencia ainda que a eficácia das formações aumenta quando estas são contextualizadas e orientadas para o papel específico dos utilizadores nos seus ambientes de trabalho, o que se revela particularmente relevante em contextos organizacionais públicos.

Sohrabi Safa et al. (2016) propõem um modelo de conformidade que destaca o papel das perceções organizacionais no comportamento dos utilizadores. Os autores defendem que a perceção de suporte institucional, aliada à confiança nas lideranças, reforça a predisposição dos colaboradores para cumprir práticas seguras, incluindo a adoção de autenticação multifator.

Contudo, a literatura ainda carece de estudos aplicados ao setor público europeu com maior profundidade, em especial no contexto português. Esta lacuna é precisamente o que motiva a presente investigação, que pretende testar empiricamente se a formação, enquanto intervenção breve e contextualizada, pode atuar como catalisador positivo no modelo UTAUT,

aumentando a predisposição para a adoção da MFA entre colaboradores do setor público português.

3.4.5. Formação em cibersegurança e mudança comportamental

A adoção de tecnologias de segurança como a MFA não depende exclusivamente de fatores técnicos ou organizacionais: o comportamento dos utilizadores é decisivo. Vários estudos demonstram que intervenções educativas – como formações, campanhas de sensibilização e simulações – podem alterar perceções, reduzir resistências e promover mudanças sustentadas no comportamento dos utilizadores (Puhakainen & Siponen, 2010).

A formação atua sobre múltiplos construtos dos modelos teóricos. No UTAUT, contribui diretamente para as condições facilitadoras ao aumentar o conhecimento técnico, influencia a expectativa de esforço ao simplificar a perceção de usabilidade, e pode melhorar a autoeficácia reduzindo a ansiedade perante o uso de novos mecanismos de autenticação. No modelo SCT, por exemplo, a formação é central, uma vez que a aprendizagem observacional e o reforço simbólico, tal como descritos por Bandura (1986b), desempenham um papel crítico na consolidação de novos comportamentos. A modelagem por pares ou figuras de autoridade pode aumentar a autoeficácia e reduzir a resistência à mudança. Além disso, a eficácia da formação depende de fatores como a clareza da mensagem, a interatividade dos conteúdos, o envolvimento da liderança institucional e a integração com políticas de segurança. Formações que combinam conteúdo técnico com narrativas realistas e envolventes tendem a gerar maior retenção de conhecimento e predisposição à mudança (Bada et al., 2019).

A literatura recente também sugere que o formato da intervenção importa: vídeos curtos, exemplos práticos e situações do quotidiano são mais eficazes do que manuais extensos ou seminários passivos (Jansson & von Solms, 2013). Este princípio orientou a criação do vídeo formativo utilizado na presente investigação.

A eficácia de ações educativas em cibersegurança não depende exclusivamente do conteúdo transmitido, mas também da forma como são concebidas e implementadas. Bada et al. (2019) argumentam que muitas campanhas falham por não considerar os fatores cognitivos, motivacionais e contextuais que moldam o comportamento dos utilizadores. O desenho instrucional deve, por isso, articular objetivos realistas, segmentação de públicos e métodos interativos que promovam a retenção e a ação.

A avaliação da eficácia de ações de formação em cibersegurança não deve limitar-se à aquisição de conhecimento técnico. Parsons et al. (2014) desenvolveram o questionário HAIS-

Q com base em três dimensões (conhecimento, atitude e comportamento) e demonstraram que estes fatores nem sempre evoluem de forma linear. Este modelo reforça a necessidade de intervenções formativas que considerem aspetos comportamentais e sociais, para além da simples transmissão de conteúdos.

Assim, ao posicionar a formação como fator-chave na aceitação de MFA, esta investigação alia fundamentos teóricos a uma abordagem pragmática, procurando evidenciar o impacto mensurável de uma ação educativa simples na predisposição para adotar medidas robustas de segurança digital.

3.4.6. Síntese e implicações

A revisão da literatura evidencia que a aceitação de tecnologias de segurança como a MFA depende de múltiplas variáveis psicológicas, sociais e contextuais. Modelos como o TAM e o UTAUT constituem estruturas teóricas robustas para compreender a intenção de adoção tecnológica, enquanto outras abordagens como a TPB, SCT e IDT acrescentam nuances relevantes sobre normas sociais, perceções de controlo e características da inovação.

Simultaneamente, constata-se que a formação desempenha um papel estratégico transversal, atuando sobre vários construtos desses modelos e influenciando diretamente a perceção e o comportamento dos utilizadores. A investigação empírica tem validado a eficácia de intervenções formativas simples — como vídeos ou simulações — para aumentar a literacia digital e a adoção de comportamentos de segurança (Bada et al., 2019; Parsons et al., 2014).

Contudo, existe uma lacuna importante na literatura sobre a aplicação destes modelos no contexto do setor público português, particularmente no que respeita à MFA. O presente estudo propõe-se, assim, a preencher esse vazio, testando empiricamente se uma ação educativa em formato vídeo pode influenciar positivamente os principais determinantes da intenção de adoção de MFA, conforme identificados no modelo UTAUT.

Deste modo, a investigação assume um duplo contributo: por um lado, aprofunda o entendimento teórico sobre os fatores de aceitação tecnológica no setor público, por outro, oferece uma proposta prática e escalável para reforçar a postura de segurança organizacional.

4. Metodologia

A presente investigação adota uma abordagem quantitativa, baseada na aplicação de um questionário estruturado com base no modelo UTAUT, complementada por uma intervenção educativa em formato vídeo. Este tipo de estratégia é recomendado para estudos com objetivos explicativos e confirmatórios, em que se pretende testar hipóteses e analisar relações entre variáveis de forma objetiva e padronizada (Coutinho, 2014). O objetivo é analisar o impacto dessa intervenção na intenção de adoção de sistemas de autenticação multifator (MFA) por parte de colaboradores do setor público.

4.1. Desenho do Estudo

Foi delineado um estudo de natureza experimental, com alocação aleatória de participantes a um grupo de controlo ou a um grupo experimental. Os participantes foram distribuídos aleatoriamente entre os dois grupos:

- Grupo de controlo: respondeu ao questionário sem qualquer intervenção prévia;
- Grupo experimental: visualizou previamente um vídeo de sensibilização em cibersegurança com foco em MFA e, de seguida, respondeu ao mesmo questionário.

4.2. Participantes

A amostra foi composta por colaboradores de uma instituição pública na área do emprego e formação profissional, com critérios de inclusão definidos como:

- Estarem ativamente ao serviço;
- Trabalharem sob vínculo público;
- Terem acesso a sistemas protegidos por autenticação digital.

A definição destes critérios procurou garantir que os participantes tivessem contacto direto com tecnologias de autenticação e, por conseguinte, relevância prática no estudo da sua adoção.

4.3. Instrumentos

O instrumento principal foi um questionário adaptado do modelo UTAUT (Venkatesh et al., 2003), composto por:

- 14 itens distribuídos por 7 construtos (2 itens por construto): Expectativa de desempenho, expectativa de esforço, influência social, condições facilitadoras, autoeficácia, ansiedade e intenção comportamental;
- Escala de Likert de 5 pontos (1 = discordo totalmente; 5 = concordo totalmente);
- Itens adicionais sobre familiaridade e interesse com diferentes formas de MFA (SMS, biometria, tokens físicos, app autenticadora, etc.).

A utilização de um questionário estruturado para recolha de dados baseia-se na prática consolidada da investigação por inquérito, que, segundo Ruel et al. (2016), se revela particularmente adequada quando o objetivo é medir atitudes, perceções e intenções de forma uniformizada e replicável. A clareza na formulação das questões e a simplicidade do escalonamento são fatores críticos para garantir a fiabilidade e validade dos dados obtidos.

A adaptação do questionário envolveu tradução, validação linguística com apoio de uma tradutora especializada, validação prévia junto de dois especialistas em segurança da informação e comportamento organizacional e piloto com 7 voluntários. As considerações obtidas levou a ajustes na redação de algumas perguntas para maior clareza sem comprometer a fidelidade do modelo. Estes procedimentos asseguraram a adequação linguística e conceitual do instrumento, respeitando a integridade teórica do modelo UTAUT. O questionário aplicado encontra-se reproduzido integralmente no Anexo A – Questionário aplicado.

4.4. Estímulo educativo

O vídeo educativo foi concebido com base nas recomendações da literatura científica sobre formação comportamental em cibersegurança e em boas práticas de comunicação institucional no setor público. A sua construção assentou na adaptação e consolidação de excertos provenientes de materiais divulgados pelo Centro Nacional de Cibersegurança (CNCS), utilizados como base de inspiração para garantir adequação técnica e relevância nacional. Os conteúdos foram reorganizados e reescritos de forma a assegurar originalidade, coerência pedagógica e alinhamento com os objetivos da investigação.

O vídeo abordou os seguintes temas centrais:

- Responsabilidade individual na segurança digital;
- Comportamentos vigilantes no local de trabalho;
- Proteção de credenciais e identidade digital;
- Riscos do uso de Wi-Fi público e importância da VPN;
- Definição e impacto do ransomware;

- Adoção e benefícios da autenticação multifator (MFA).

Com aproximadamente cinco minutos de duração, o vídeo foi narrado em português europeu e incorporou exemplos práticos, diretamente associados ao quotidiano dos serviços públicos. O objetivo foi maximizar o envolvimento dos participantes, reforçar a retenção da mensagem e promover a identificação com situações reais.

4.5. Procedimentos

Os participantes foram convidados por email institucional. Após o consentimento informado, foram aleatoriamente atribuídos ao grupo de controlo ou experimental. A recolha de dados foi efetuada de forma anónima através de uma plataforma online segura. A recolha de dados foi realizada através da plataforma SurveyMonkey, configurada para garantir anonimato e impedir múltiplas submissões. As respostas foram recolhidas entre janeiro e junho de 2023, num período em que os participantes foram convidados a responder durante o horário normal de trabalho. O tempo médio de preenchimento do questionário foi de aproximadamente cinco minutos. O processo respeitou os princípios éticos da investigação, garantindo anonimato, voluntariedade e confidencialidade dos dados recolhidos.

4.6. Técnicas de análise

Os dados foram tratados estatisticamente com recurso ao SPSS, incluindo:

- Análise descritiva das variáveis sociodemográficas;
- Testes t de comparação entre grupos (controlo vs experimental);
- Correlações de Pearson para análise da relação entre construtos;

Todas as análises foram realizadas com um nível de significância estatística de 5% ($p < .05$), critério que orientou a rejeição ou aceitação das hipóteses nulas.

Foram calculados coeficientes de correlação de Pearson para analisar a relação linear entre os construtos do modelo UTAUT, a formação prévia em cibersegurança e a exposição ao estímulo educativo. A interpretação dos coeficientes de correlação segue os critérios definidos por Hinkle et al. (2003), uma referência amplamente utilizada em estudos académicos de ciências sociais e comportamentais:

- $\leq |r| < 0.30 \rightarrow$ Correlação fraca
- $0.30 \leq |r| < 0.50 \rightarrow$ Correlação moderada
- $0.50 \leq |r| < 0.70 \rightarrow$ Correlação forte
- $0.70 \leq |r| < 0.90 \rightarrow$ Correlação muito forte

- $|r| \geq 0.90 \rightarrow$ Correlação quase perfeita

Esta escala permite uma leitura clara da força das associações estatísticas identificadas, sem inflacionar ou subestimar a sua relevância prática no contexto organizacional.

5. Análise dos resultados

5.1. Descrição da amostra

A presente amostra foi constituída por 165 pessoas. No que concerne à idade, 1.2% tinha entre 21 e 29 anos, 4.2% entre 30 a 39, 32.1% de 40 a 49, 48.5% de 50 a 59, e 13.9% com 60 ou mais anos. No que concerne à escolaridade, 26.1% concluíram o Ensino secundário, 73.3% o Ensino Superior, 0.6% preferiam não dizer. Dos 165 participantes neste estudo, 67.3% efetuaram formação prévia em cibersegurança e 32.7% não efetuaram essa formação prévia. Deste grupo, 65 nos últimos 6 meses, 25 de 6 a 12 meses, 21 há mais de 12 meses. Foram ainda distinguidos dois grupos, grupo de controlo (não exposto ao estímulo educacional em formato vídeo) e o grupo experimental (exposto ao estímulo educacional em formato vídeo).

No grupo de controlo estiveram presentes 92 pessoas, das quais 3.3% tinha entre 30 e 39 anos, 30.4% de 40 a 49 anos, 51.1% de 50 a 59 anos e 15.2% 60 ou mais anos de idade. Relativamente à escolaridade, 27.2% concluíram o Ensino Secundário e 72.8% o Ensino Superior. Das 92 pessoas deste grupo de controlo, 66.3% efetuaram formação prévia em cibersegurança e 33.7% não a efetuaram. Do grupo que efetuou formação prévia, 35 pessoas receberam formação nos últimos 6 meses, 12 de 6 a 12 meses, 14 há mais de 12 meses.

Relativamente ao grupo experimental, este grupo teve presente 73 pessoas em que 2.7% tinha entre 21 a 29 anos, 5.5% de 30 a 39 anos, 34.2% de 40 a 49, 45.2% de 50 a 59 anos e 12.3% com 60 ou mais anos de idade. No que toca à sua escolaridade, dos participantes neste grupo 24.7% concluiu o Ensino Secundário, 74% o Ensino Superior e 1.4% preferiu não partilhar o seu nível de escolaridade. Das 73 pessoas neste grupo experimental, 68.5% efetuaram formação prévia em cibersegurança, sendo que 31.5% não a efetuaram. Deste grupo, 30 pessoas efetuaram a formação nos últimos 6 meses, 13 de 6 a 12 meses, 7 há mais de 12 meses.

A ausência de participantes entre os 19 e os 21 anos resulta do perfil da amostra, composta maioritariamente por trabalhadores em funções públicas, onde essa faixa etária está sub-representada.

A atribuição dos participantes aos grupos experimental e de controlo foi realizada de forma aleatória através da plataforma SurveyMonkey, que possui um algoritmo interno para essa função. Contudo, verificou-se que o grupo de controlo ficou numericamente superior ao grupo experimental. Esta diferença deve-se ao facto de alguns indivíduos, após a atribuição inicial, não terem concluído o questionário, o que afetou a proporção final entre os grupos.

Embora este desequilíbrio não tenha sido intencional, foram assegurados os critérios de aleatoriedade e independência entre os grupos. Apesar desta assimetria, os cuidados metodológicos incluíram a verificação dos pré-requisitos para a análise estatística, nomeadamente normalidade das distribuições, independência das observações e homogeneidade das variâncias. Antes da aplicação do teste-t foram verificados os pré-requisitos ao nível da normalidade da distribuição, através dos testes de Shapiro-Wilk e Kolmogorov-Smirnov; independência das observações, garantida pela natureza individual das respostas e homogeneidade das variâncias, confirmada pelo teste de Levene. Após esta verificação, optou-se pelo teste paramétrico teste-t para comparação entre grupos.

Importa ainda mencionar que para a realização da análise de dados a amostra total foi também subdividida consoante o conhecimento (ou desconhecimento) sobre os diferentes fatores de autenticação em estudo. A descrição destas subamostras é apresentada nos capítulos seguintes.

5.2. Fator de autenticação SMS/E-mail

5.2.1. Caracterização da subamostra

Na amostra deste estudo, 164 participantes reportaram conhecer o fator de autenticação SMS/E-mail. Os dados sociodemográficos desta subamostra podem ser consultados na

Tabela ***2***.

Tabela 2

Dados Sociodemográficos da Subamostra de Participantes que Conhecem o Fator de Autenticação SMS/E-mail.

Dados sociodemográficos	Amostra	
	n	%
Idade		
21 a 29	2	1.2
30 a 39	7	4.3
40 a 49	53	32.3
50 a 59	80	48.8
60 ou mais	25	13.4
Nível de escolaridade		
Ensino secundário	42	25.6
Ensino superior	121	73.8
Prefiro não dizer	1	0.6
Formação prévia em cibersegurança		
Sim	111	67.7
Não	53	32.3
Formação prévia efetuada quando		
Nos últimos 6 meses	65	39.6
Entre os últimos 6 a 12 meses	25	15.2
Há mais de 12 meses	21	12.8
Missing	53	32.3
Grupos		
Controlo	92	56.1
Experimental	72	43.9

A distribuição etária dos indivíduos que participam no estudo inclina-se consideravelmente para o grupo etário dos 50 aos 59 anos, que representa quase metade da amostra (48.8%), seguido pelo grupo dos 40 aos 49 anos, abrangendo 32.3% dos inquiridos. Os participantes com 60 anos ou mais constituem 13.4% do conjunto, ao passo que a faixa dos 30 aos 39 anos engloba 4.3% e os mais jovens, entre 21 a 29 anos, representam apenas 1.2%.

No que respeita ao nível de instrução, uma proporção substancial de 73.8% dos inquiridos possui qualificação ao nível do ensino superior. Aqueles com ensino secundário correspondem a 25.6%, enquanto uma minoria residual de 0.6% preferiu não declarar o seu nível educacional. Relativamente à experiência formativa na área de cibersegurança, 67.7% dos respondentes indicaram ter formação prévia, contrastando com 32.3% que não têm essa formação. Dos que têm formação, 39.6% completaram-na nos últimos 6 meses, 15.2% entre 6 a 12 meses atrás e 12.8% há mais de 12 meses. Regista-se que 32.3% dos dados relativos ao momento da formação não estão disponíveis ou não foram fornecidos. Quanto à divisão dos grupos de estudo, 56.1% dos sujeitos foram atribuídos ao grupo de controlo, enquanto 43.9% compõem o grupo experimental.

5.2.2. Correlações entre construtos UTAUT, formação e grupos

De forma a compreender se os construtos relacionados com o modelo UTAUT estão correlacionados com a formação prévia e/ou com a apresentação do estímulo experimental, foram calculados coeficientes de correlação de *Pearson*. Os resultados podem ser analisados Tabela 3.

Tabela 3

Coeficientes de Correlação de Pearson entre os Construtos UTAUT, Formação Prévia e Apresentação do Estímulo Experimental, na Subamostra Relativa ao Fator de Autenticação SMS/E-mail.

Variável	*M*	*SD*	Max	Min	1	2	3	4	5	6	7	8	9
1. Influência social	4.1311	.78495	5.00	2.00	-	-	-	-	-	-	-	-	-
2. Condições Facilitadoras	4.4512	.73313	5.00	1.50	.534**	-	-	-	-	-	-	-	-
3. Expetativa de Esforço	4.3018	.73397	5.00	1.50	.495**	.643**	-	-	-	-	-	-	-
4. Expetativa de Desempenho	3.8720	.88377	5.00	1.00	.535**	.416**	.329**	-	-	-	-	-	-
5. Autoeficácia	4.2835	.81612	5.00	1.50	.444**	.600**	.522**	.282**	-	-	-	-	-
6. Ansiedade	1.8049	.91429	5.00	1.00	.327**	.412**	-.392**	-.132	-.306**	-	-	-	-
7. Intenção Comportamental	4.5732	.60569	5.00	2.50	.514**	.665**	.500**	.425**	.505**	-.327**	-	-	-
8. Formação prévia	-	-	-	-	0.001	-.070	-.018	-.070	-.121	-.045	-.022	-	-
9. Grupos	-	-	-	-	.174*	.051	.156*	.170*	.167*	-.127	.112	-.023	-

*$p < .05$. **$p < .01$.

A análise dos coeficientes de correlação de Pearson permitiu explorar as relações entre os construtos do modelo UTAUT, a formação prévia em cibersegurança e a pertença aos grupos experimental e de controlo no contexto de autenticação por SMS ou e-mail.

Verificaram-se correlações fortes e positivas entre as Condições Facilitadoras e a Expectativa de Esforço ($r = .643$, $p < .01$), bem como entre as Condições Facilitadoras e a Intenção Comportamental ($r = .665$, $p < .01$). Estes resultados indicam que os utilizadores que percecionam maior apoio institucional e recursos adequados tendem também a considerar mais fácil o uso da tecnologia e demonstram maior predisposição para a sua adoção.

Foram ainda identificadas correlações moderadas e positivas entre a Expectativa de Desempenho e a Intenção Comportamental ($r = .425$, $p < .01$), entre a Autoeficácia e a Intenção Comportamental ($r = .505$, $p < .01$), e entre a Expectativa de Esforço e a Intenção Comportamental ($r = .500$, $p < .01$). Estes resultados sugerem que perceções de utilidade, facilidade de uso e competência individual estão significativamente associadas à intenção de utilizar mecanismos de MFA baseados em SMS ou e-mail.

A Ansiedade demonstrou uma correlação negativa moderada com a Intenção Comportamental ($r = –.327$, $p < .01$), indicando que níveis mais elevados de desconforto ou receio perante a tecnologia estão associados a menor probabilidade de adoção da MFA neste formato.

Por fim, a variável formação prévia em cibersegurança apresentou apenas correlações fracas e estatisticamente não significativas com os construtos analisados. Este resultado reforça a ideia de que, no caso do SMS/e-mail, a intenção de uso é mais fortemente explicada por fatores internos (como perceção de utilidade ou autoeficácia) do que por antecedentes formais de formação técnica.

5.2.3. Testes *t* – comparação entre grupos

Com o objetivo de comparar os participantes expostos ao estímulo experimental aos participantes pertencentes ao grupo de controlo, no que concerne aos construtos do modelo UTAUT, foram realizados testes *t* para amostras independentes. Os resultados podem observados na Tabela 4.

Tabela 4

Comparação de Médias entre Grupo de Controlo e Experimental, no que Concerne aos Fatores Considerados no Modelo UTAUT, para o Fator de Autenticação SMS/E-mail

Variáveis dependentes	Grupo Experimental		Grupo Controlo		*t*	*df*	*p*	*Cohen's d*
	M	*SD*	*M*	*SD*				
Influência social	4.285	.804	4.011	.752	-2.245	162	.026	-.353
Condições facilitadoras	4.493	.694	4.418	.764	-.645	162	.520	-.102
Expetativa esforço	4.437	.733	4.201	.723	-2.005	162	.047	-.316
Expetativa desempenho	4.041	.817	3.739	.915	-2.201	162	.029	-.346
Autoeficácia	4.437	.740	4.163	.855	-2.161	162	.032	-.340
Ansiedade	1.674	.885	1.908	.929	1.635	162	.104	.257
Intenção comportamental	4.652	.522	4.516	.660	-1.478	161.983	.141	-.226

Verificaram-se diferenças estatisticamente significativas em quatro construtos:

- Influência Social: Os participantes do grupo experimental apresentaram uma média significativamente superior (M = 4.29, SD = 0.80) comparativamente ao grupo de controlo (M = 4.01, SD = 0.75), t(162) = –2.245, p = .026. O tamanho do efeito foi moderado, com um valor de Cohen's d de –0.353.
- Expectativa de Esforço: Também neste construto o grupo experimental obteve uma média mais elevada (M = 4.44, SD = 0.73) do que o grupo de controlo (M = 4.20, SD = 0.72), t(162) = –2.005, p = .047, com um tamanho de efeito moderado (d = –0.316).
- Expectativa de Desempenho: A média do grupo experimental foi de 4.04 (SD = 0.82), enquanto o grupo de controlo obteve 3.74 (SD = 0.91), com t(162) = –2.201, p = .029. O valor de Cohen's d foi de –0.346, indicando também um efeito de magnitude moderada.
- Autoeficácia: A diferença de médias entre grupos foi igualmente significativa, com o grupo experimental a registar uma média de 4.44 (SD = 0.74) contra 4.16 (SD = 0.85) no grupo de controlo, t(162) = –2.161, p = .032, d = –0.340.

Nos restantes construtos avaliados (Condições Facilitadoras, Ansiedade e Intenção Comportamental), não foram encontradas diferenças estatisticamente significativas entre os grupos. Apesar disso, em todos os casos a média do grupo experimental foi superior, ainda que as diferenças não tenham atingido significância estatística ao nível de 5%.

Estes resultados sugerem que a exposição ao vídeo educativo pode ter contribuído para uma perceção mais positiva da MFA no que respeita à utilidade, facilidade de uso percebida, influência social e confiança dos participantes na sua própria capacidade para utilizar este método de autenticação.

5.3. Fator de autenticação Voz

5.3.1. Caracterização da subamostra

Na amostra deste estudo 95 participantes reportaram conhecer o fator de autenticação Voz. Os dados sociodemográficos podem ser consultados na Tabela 5.

Tabela 5
Dados Sociodemográficos da Subamostra de Participantes que Conhecem o Fator de Autenticação Voz

Dados sociodemográficos	Amostra	
	n	%
Idade		
21 a 29	1	1.1
30 a 39	4	4.2
40 a 49	36	37.9
50 a 59	43	45.3
60 ou mais	11	11.6
Nível de escolaridade		
Ensino secundário	19	20.0
Ensino superior	75	78.9
Prefiro não dizer	1	1.1
Formação prévia em cibersegurança		
Sim	69	72.6
Não	26	27.4
Formação prévia efetuada quando		
Nos últimos 6 meses	42	44.2
Entre os últimos 6 a 12 meses	14	14.7
Há mais de 12 meses	13	13.7
Missing	26	27.4
Grupos		
Controlo	47	49.5
Experimental	48	50.5

A distribuição etária dos indivíduos que participam no estudo inclina-se consideravelmente para o grupo etário dos 50 aos 59 anos, que representa quase metade da amostra (48.8%), seguido pelo grupo dos 40 aos 49 anos, abrangendo 32.3% dos inquiridos. Os participantes com 60 anos ou mais constituem 13.4% do conjunto, ao passo que a faixa dos 30 aos 39 anos engloba 4.3% e os mais jovens, entre 21 a 29 anos, representam apenas 1.2%. No que respeita ao nível de instrução, uma proporção substancial de 73.8% dos inquiridos

possui qualificação ao nível do ensino superior. Aqueles com ensino secundário correspondem a 25.6%, enquanto uma minoria residual de 0.6% preferiu não declarar o seu nível educacional. Relativamente à experiência formativa na área de cibersegurança, 67.7% dos respondentes indicaram ter formação prévia, contrastando com 32.3% que não têm essa formação. Dos que têm formação, 39.6% completaram-na nos últimos 6 meses, 15.2% entre 6 a 12 meses atrás, e 12.8% há mais de 12 meses. Regista-se que 32.3% dos dados relativos ao momento da formação não estão disponíveis ou não foram fornecidos. Quanto à divisão dos grupos de estudo, 56.1% dos sujeitos foram atribuídos ao grupo de controlo, enquanto 43.9% compõem o grupo experimental.

5.3.2. Correlações entre construtos UTAUT, formação e grupos

De forma a compreender se os construtos relacionados com o modelo UTAUT estão correlacionados com a formação prévia e/ou com a apresentação do estímulo experimental, foram calculados coeficientes de correlação de *Pearson*. Os resultados podem ser analisados na

Tabela 6.

Tabela 6

Coeficientes de Correlação de Pearson entre os Construtos UTAUT, Formação Prévia e Apresentação do Estímulo Experimental, na Subamostra Relativa ao Fator de Autenticação Voz

Variável	M	SD	Max	Min	1	2	3	4	5	6	7	8	9
1. Influência social	3.3421	.82920	5.00	1.00	-	-	-	-	-	-	-	-	-
2. Condições Facilitadoras	3.9474	1.00391	5.00	1.00	.431**	-	-	-	-	-	-	-	-
3. Expetativa de Esforço	3.9316	.87704	5.00	1.00	.369**	.621**	-	-	-	-	-	-	-
4. Expetativa de Desempenho	3.3105	.87877	5.00	1.00	.495**	.227*	.369**	-	-	-	-	-	-
5. Autoeficácia	3.8263	1.02305	5.00	1.00	.369**	.620**	.630**	.324**	-	-	-	-	-
6. Ansiedade	1.9526	.94270	5.00	1.00	-.336**	-.230*	-.339**	-.082	-.276**	-	-	-	-
7. Intenção Comportamental	3.3895	1.06985	5.00	1.00	.511**	.302**	.533**	.362**	.303**	-.401**	-	-	-
8. Formação prévia	-	-	-	-	.060	-.039	.021	-.029	-.116	-.007	-.036	-	-
9. Grupos	-	-	-	-	.066	.043	-.114	.111	.028	-.005	.026	-.023	-

$^{*}p < .05$. $^{**}p < .01$.

Os coeficientes de correlação de Pearson indicam uma correlação forte e positiva entre Autoeficácia e Expectativa de Esforço ($r = .630$, $p < .01$), assim como entre Condições Facilitadoras e Expectativa de Esforço ($r = .621$, $p < .01$). Também se destaca uma correlação forte entre Expectativa de Esforço e Intenção Comportamental ($r = .533$, $p < .01$), evidenciando que quanto maior a perceção de facilidade de uso, maior a predisposição para adoção da MFA por voz.

Verificaram-se ainda correlações moderadas e positivas entre Influência Social e Expectativa de Desempenho ($r = .495$, $p < .01$), Autoeficácia e Expectativa de Esforço ($r = .630$, $p < .01$), Autoeficácia e Condições Facilitadoras ($r = .620$, $p < .01$), bem como entre Intenção Comportamental e diversos construtos: Expectativa de Desempenho ($r = .362$, $p < .01$), Autoeficácia ($r = .303$, $p < .01$) e Influência Social ($r = .511$, $p < .01$).

A Ansiedade apresenta correlações negativas moderadas com Intenção Comportamental ($r = –.401$, $p < .01$), Expectativa de Esforço ($r = –.339$, $p < .01$) e Autoeficácia ($r = –.276$, $p < .01$), indicando que níveis mais elevados de ansiedade estão associados a menor perceção de capacidade, maior dificuldade esperada e menor intenção de adoção da MFA.

Tal como observado na subamostra SMS/E-mail, a variável formação prévia revela apenas correlações fracas e não significativas com os restantes construtos.

5.3.3. Testes *t* – comparação entre grupos

Com o objetivo de comparar os participantes expostos ao estímulo experimental aos participantes pertencentes ao grupo de controlo, no que concerne aos construtos do modelo UTAUT, foram realizados testes t para amostras independentes. Os resultados podem observados na tabela

Tabela *7*.

Tabela 7

Comparação de Médias entre Grupo de Controlo e Experimental, no que Concerne aos Fatores Considerados no Modelo UTAUT, para o Fator de Autenticação Voz

Variáveis dependentes	Grupo Experimental		Grupo Controlo		*t*	*df*	*p*	*Cohen's d*
	M	*SD*	*M*	*SD*				
Influência social	3.3958	.811	3.2872	.851	-.636	93	.526	-.131
Condições facilitadoras	3.9896	1.013	3.9043	1.003	-.412	93	.681	-.085
Expetativa esforço	3.8333	.895	4.0319	.855	1.105	93	.272	-.177
Expetativa desempenho	3.4063	.769	3.2128	.976	-1.074	93	.286	-.623
Autoeficácia	3.8542	.967	3.7979	1.086	-.267	93	.790	-.457
Ansiedade	1.9479	.979	1.9574	.913	.049	93	.961	-.392
Intenção comportamental	3.4167	1.088	3.3617	1.061	-.249	93	.804	-.453

Os testes t realizados para comparar os participantes do grupo experimental com os do grupo de controlo relativamente aos construtos do modelo UTAUT não revelaram diferenças estatisticamente significativas. Em todos os construtos avaliados — Influência Social, Condições Facilitadoras, Expectativa de Esforço, Expectativa de Desempenho, Autoeficácia, Ansiedade e Intenção Comportamental — os valores de p foram superiores a .05.

Apesar disso, observa-se que em alguns construtos, como Expectativa de Desempenho e Autoeficácia, as médias no grupo experimental são ligeiramente superiores às do grupo de controlo. Contudo, estas diferenças não foram suficientemente expressivas para atingirem significância estatística, e os respetivos tamanhos de efeito (Cohen's d) foram baixos, não ultrapassando os valores típicos para efeitos pequenos.

Estes resultados sugerem que, no caso da autenticação por voz, o estímulo educativo em formato vídeo não produziu impacto mensurável na perceção dos utilizadores relativamente à utilidade, facilidade de uso, confiança ou intenção comportamental.

5.4. Fator de autenticação Reconhecimento Facial

5.4.1. Caracterização da subamostra

Na amostra deste estudo 122 participantes reportaram conhecer o fator de autenticação Reconhecimento Facial. Os dados sociodemográficos podem ser consultados na

Tabela ***8***.

Tabela 8

Dados Sociodemográficos da Subamostra de Participantes que Conhecem o Fator de Autenticação Reconhecimento Facial

Dados sociodemográficos	Amostra	
	n	%
Idade		
21 a 29	1	.8
30 a 39	4	3.3
40 a 49	41	33.3
50 a 59	62	50.4
60 ou mais	15	12.2
Nível de escolaridade		
Ensino secundário	30	24.4
Ensino superior	92	74.8
Prefiro não dizer	1	.8
Formação prévia em cibersegurança		
Sim	84	69.3
Não	39	31.7
Formação previa efetuada quando		
Nos últimos 6 meses	49	39.8
Entre os últimos 6 a 12 meses	16	13.0
Há mais de 12 meses	19	15.4
Missing	39	68.3
Grupos		
Controlo	66	53.7
Experimental	57	46.3

A maioria dos participantes está na faixa etária dos 50 aos 59 anos, representando 50.4% do total. O segundo maior grupo é dos 40 aos 49 anos com 33.3%, seguido dos indivíduos com 60 anos ou mais com 12.2%. As faixas dos 30 aos 39 anos e dos 21 aos 29 anos têm menor representatividade, com 3.3% e 0.8%, respetivamente. Quanto ao nível de escolaridade, a maior parte dos participantes tem ensino superior (74.8%), enquanto uma menor fração tem ensino

secundário (24.4%). Apenas uma minoria prefere não revelar seu nível de escolaridade (0.8%). Em relação à formação prévia em cibersegurança, 69.3% dos participantes indicam ter essa formação, enquanto 31.7% não têm. Dos que têm formação, a maior parte realizou-a nos últimos 6 meses (39.8%), alguns entre 6 a 12 meses atrás (13.0%), e outros há mais de 12 meses (15.4%). Há uma considerável percentagem de dados em falta (*missing*) nesta categoria (68.3%). Por fim, os participantes estão quase igualmente distribuídos entre os grupos de controlo (53.7%) e experimental (46.3%), indicando um equilíbrio na alocação dos sujeitos para os diferentes grupos do estudo.

5.4.2. Correlações entre construtos UTAUT, formação e grupos

De forma a compreender se os construtos relacionados com o modelo UTAUT estão correlacionados com a formação prévia e/ou com a apresentação do estímulo experimental, foram calculados coeficientes de correlação de *Pearson*. Os resultados podem ser analisados na

Tabela ***9***.

Tabela 9

Coeficientes de Correlação de Pearson entre os Construtos UTAUT, Formação Prévia e Apresentação do Estímulo Experimental, na Subamostra Relativa ao Fator de Autenticação Reconhecimento Facial

Variável	*M*	*SD*	Max	Min	1	2	3	4	5	6	7	8	9
1. Influência social	3.3333	.931	5.00	1.00	-	-	-	-	-	-	-	-	-
2. Condições Facilitadoras	3.7236	1.050	5.00	1.00	.457**	-	-	-	-	-	-	-	-
3. Expetativa de Esforço	4.0000	.856	5.00	1.00	.365**	.481**	-	-	-	-	-	-	-
4. Expetativa de Desempenho	3.5407	.948	5.00	1.00	.627**	.493**	.532**	-	-	-	-	-	-
5. Autoeficácia	3.7276	.990	5.00	1.00	.466**	.498**	.541**	.529**	-	-	-	-	-
6. Ansiedade	2.0041	1.005	5.00	1.00	-.264**	-.226*	-.474**	-.320**	-.314**	-	-	-	-
7. Intenção Comportamental	3.6260	1.151	5.00	1.00	.625**	.476**	.528**	.667**	.514**	-.402**	-	-	-
8. Formação prévia	-	-	-	-	.094	.013	.123	.026	.038	-.003	.047	-	-
9. Grupos	-	-	-	-	.044	.160	-.019	.081	.149	-.150	.118	-.023	-

$^{*}p < .05$. $^{**}p < .01$.

As correlações de Pearson mostram uma associação forte e positiva entre Expectativa de Desempenho e Intenção Comportamental ($r = .667$, $p < .01$), assim como entre Expectativa de Esforço e Intenção Comportamental ($r = .528$, $p < .01$). Destacam-se ainda correlações fortes entre Autoeficácia e Expectativa de Esforço ($r = .541$, $p < .01$), e entre Autoeficácia e Expectativa de Desempenho ($r = .529$, $p < .01$).

Verificaram-se também correlações moderadas e positivas entre Influência Social e Intenção Comportamental ($r = .625$, $p < .01$), entre Condições Facilitadoras e Expectativa de Esforço ($r = .481$, $p < .01$), e entre Autoeficácia e Intenção Comportamental ($r = .514$, $p < .01$). Estas relações indicam que perceções de utilidade, facilidade de uso, apoio social e confiança pessoal estão positivamente associadas à intenção de adotar a autenticação por reconhecimento facial.

Por outro lado, observam-se correlações negativas moderadas entre Ansiedade e Intenção Comportamental ($r = –.402$, $p < .01$), entre Ansiedade e Expectativa de Esforço ($r = –.474$, $p < .01$), e entre Ansiedade e Autoeficácia ($r = –.314$, $p < .01$). Estes resultados sugerem que quanto maior o desconforto ou receio associado ao uso da tecnologia, menor a predisposição para a adotar.

A variável formação prévia, mais uma vez, não apresenta correlações relevantes com os restantes construtos, mantendo-se como um fator isolado, sem impacto estatisticamente significativo nas perceções analisadas.

5.4.3. Testes *t* – comparação entre grupos

Com o objetivo de comparar os participantes expostos ao estímulo experimental aos participantes pertencentes ao grupo de controlo, no que concerne aos construtos do modelo UTAUT, foram realizados testes *t* para amostras independentes. Os resultados podem observados na tabela

Tabela ***10***.

Tabela 10

Comparação de médias entre grupo de controlo e experimental, no que concerne aos fatores considerados no modelo UTAUT, para o fator de autenticação Reconhecimento Facial.

Variáveis dependentes	Grupo Experimental		Grupo Controlo		*t*	*df*	*p*	*Cohen's d*
	M	*SD*	*M*	*SD*				
Influência social	3.377	.913	3.295	.952	-.484	121	.629	-.087
Condições facilitadoras	3.903	1.080	3.568	1.007	-1.781	121	.077	-.322
Expetativa esforço	3.982	.834	4.015	.881	.210	121	.834	.038
Expetativa desempenho	3.623	.951	3.469	.948	-.892	121	.374	-.161
Autoeficácia	3.886	1.065	3.591	.906	-1.660	121	.100	-.300
Ansiedade	1.842	.973	2.144	1.018	1.673	121	.097	.303
Intenção comportamental	3.772	1.073	3.500	1.208	-1.310	121	.193	-.237

Os testes t aplicados para comparar os dois grupos revelaram ausência de diferenças estatisticamente significativas em todos os construtos do modelo UTAUT. As médias obtidas no grupo experimental foram ligeiramente superiores em algumas variáveis, nomeadamente Autoeficácia e Intenção Comportamental, mas os valores de p foram superiores a .05 em todos os casos, e os tamanhos de efeito (Cohen's d) situaram-se na faixa dos efeitos pequenos.

Estes resultados indicam que, no caso específico da autenticação por reconhecimento facial, o estímulo educativo em formato vídeo não exerceu influência estatisticamente significativa na alteração das perceções ou intenções dos utilizadores

5.5. Fator de autenticação Impressão Digital

5.5.1. Caracterização da subamostra

Na amostra deste estudo 145 participantes reportaram conhecer o fator de autenticação Voz. Os dados sociodemográficos podem ser consultados na Tabela 11.

Tabela 11

Dados Sociodemográficos da Subamostra de Participantes que Conhecem o Fator de Autenticação Impressão Digital

Dados sociodemográficos	Amostra	
	n	%
Idade		
21 a 29	2	1.4
30 a 39	5	3.4
40 a 49	47	32.4
50 a 59	72	49.7
60 ou mais	19	13.1
Nível de escolaridade		
Ensino secundário	37	25.5
Ensino superior	107	73.8
Prefiro não dizer	1	0.7
Formação prévia em cibersegurança		
Sim	97	66.9
Não	48	33.1
Formação previa efetuada quando		
Nos últimos 6 meses	57	39.3
Entre os últimos 6 a 12 meses	20	13.8
Há mais de 12 meses	20	13.8
Missing	48	33.1
Grupos		
Controlo	81	55.9
Experimental	64	44.1

A estrutura etária dos inquiridos é marcada por uma maior representatividade do grupo dos 50 aos 59 anos, que constitui 49,7% do total. O segmento dos 40 aos 49 anos também se mostra substancial, englobando 32,4% da amostra. Por sua vez, os participantes com idade igual ou superior a 60 anos representam 13,1%, enquanto as faixas dos 30 aos 39 anos e dos 21 aos 29 anos detêm uma menor expressão, com 3,4% e 1,4%, respetivamente.

Relativamente à qualificação académica, constata-se que 73,8% dos respondentes detêm formação ao nível do ensino superior, e 25,5% possuem ensino secundário. Apenas uma parcela mínima de 0,7% optou por não revelar o seu nível de escolaridade. No que se refere à formação em cibersegurança, verifica-se que a maioria dos inquiridos, correspondendo a 66,9%, afirmou possuir formação prévia na área, contrapondo-se aos 33,1% que não possuem tal formação. Dentro do grupo que reporta formação em cibersegurança, 39,3% concluíram a sua formação nos últimos 6 meses, 13,8% entre 6 a 12 meses antes da realização do estudo, e o mesmo percentual (13,8%) indica que a formação ocorreu há mais de 12 meses. Importa referir que 33,1% dos participantes não forneceram informação relativamente a este aspeto. Quanto à composição dos grupos de estudo, observa-se uma distribuição com 55,9% dos sujeitos alocados ao grupo de controlo e 44,1% ao grupo experimental.

5.5.2. Correlações entre construtos UTAUT, formação e grupos

De forma a compreender se os construtos relacionados com o modelo UTAUT estão correlacionados com a formação prévia e/ou com a apresentação do estímulo experimental, foram calculados coeficientes de correlação de *Pearson*. Os resultados podem ser analisados na

Tabela ***12***.

Tabela 12

Coeficientes de Correlação de Pearson entre os Construtos UTAUT, Formação Prévia e Apresentação do Estímulo Experimental, na Subamostra Relativa ao Fator de Autenticação Impressão Digital

Variável	M	SD	Max	Min	1	2	3	4	5	6	7	8	9
1. Influência social	3.5832	.92486	5.00	1.00	-	-	-	-	-	-	-	-	-
2. Condições Facilitadoras	3.9414	1.02825	5.00	1.00	.548**	-	-	-	-	-	-	-	-
3. Expetativa de Esforço	4.0759	.86869	5.00	1.00	.437**	.594**	-	-	-	-	-	-	-
4. Expetativa de Desempenho	3.7414	.91116	5.00	1.00	.562**	.528**	.536**	-	-	-	-	-	-
5. Autoeficácia	3.8552	.96810	5.00	1.00	.371**	.530**	.548**	-.487**	-	-	-	-	-
6. Ansiedade	1.9379	.99806	5.00	1.00	-.229**	-.337**	-.405**	-.289**	-.356**	-	-	-	-
7. Intenção Comportamental	4.0552	1.03434	5.00	1.00	.583**	.698**	.631**	.557**	.540**	-.422**	-	-	-
8. Formação prévia	-	-	-	-	.053	.019	.031	-.042	-.069	.029	.033	-	-
9. Grupos	-	-	-	-	.173*	.214**	.099	.154	.256**	-.161	.249**	-.023	-

$^{*}p < .05$. $^{**}p < .01$.

As análises de correlação de Pearson revelam fortes associações positivas entre Expectativa de Esforço e Intenção Comportamental ($r = .631$, $p < .01$), Expectativa de Desempenho e Intenção Comportamental ($r = .557$, $p < .01$), e entre Autoeficácia e Intenção Comportamental ($r = .540$, $p < .01$). Estes resultados reforçam a relevância das perceções de usabilidade, utilidade e competência pessoal como determinantes na adoção da autenticação por impressão digital.

Verificaram-se também correlações fortes entre Condições Facilitadoras e Intenção Comportamental ($r = .698$, $p < .01$), entre Influência Social e Intenção Comportamental ($r = .583$, $p < .01$), e entre Autoeficácia e Expectativa de Esforço ($r = .548$, $p < .01$), o que evidencia uma interligação entre o contexto organizacional de suporte, o ambiente social e a perceção individual de capacidade e esforço.

As correlações negativas moderadas entre Ansiedade e Intenção Comportamental ($r = –.422$, $p < .01$), Ansiedade e Expectativa de Esforço ($r = –.405$, $p < .01$), e Ansiedade e Autoeficácia ($r = –.356$, $p < .01$) sugerem, tal como nos fatores anteriores, que a presença de ansiedade interfere negativamente com a intenção de uso e com as perceções positivas sobre o esforço necessário ou a competência pessoal.

No entanto, tal como observado nas análises anteriores, a variável formação prévia não apresenta correlações estatisticamente significativas com os construtos analisados, permanecendo uma variável com efeito marginal direto.

5.5.3. Testes *t* – comparação entre grupos

Com o objetivo de comparar os participantes expostos ao estímulo experimental aos participantes pertencentes ao grupo de controlo, no que concerne aos construtos do modelo UTAUT, foram realizados testes t para amostras independentes. Os resultados podem observados na tabela

Tabela 13.

Tabela 13

Comparação de Médias entre Grupo de Controlo e Experimental, no que Concerne aos Fatores Considerados no Modelo UTAUT, para o Fator de Autenticação Impressão Digital

Variáveis dependentes	Grupo Experimental		Grupo Controlo		*t*	*df*	*p*	*Cohen's d*
	M	*SD*	*M*	*SD*				
Influência social	3.765	.899	3.444	.925	-2.101	143	.037	-.351
Condições facilitadoras	4.187	.941	3.747	1.058	-2.613	143	.010	-.437
Expetativa esforço	4.171	.817	4.000	.905	-1.185	143	.238	-.198
Expetativa desempenho	3.898	.878	3.617	.923	-1.861	143	.065	-.311
Autoeficácia	4.132	.918	3.636	.955	-3.164	143	.002	-.529
Ansiedade	1.758	.930	2.080	1.032	1.950	143	.053	.326
Intenção comportamental	4.344	.881	3.827	1.093	-3.073	143	.003	-.514

Os testes t de comparação entre grupos revelaram diferenças estatisticamente significativas em quatro dos sete construtos:

- Influência Social apresentou uma média significativamente superior no grupo experimental (M = 3.77) face ao grupo de controlo (M = 3.44), com t(143) = –2.101, p = .037, e um tamanho de efeito moderado (d = –0.351).
- Condições Facilitadoras também registou uma diferença significativa (t(143) = –2.613, p = .010), com o grupo experimental a apresentar média mais elevada (M = 4.19) comparativamente ao grupo de controlo (M = 3.75), e um tamanho de efeito moderado (d = –0.437).
- No construto Autoeficácia, o grupo experimental teve novamente uma média superior (M = 4.13 vs. 3.64), t(143) = –3.164, p = .002, com um tamanho de efeito forte (d = –0.529).
- Finalmente, em Intenção Comportamental, a diferença também foi estatisticamente significativa, com t(143) = –3.073, p = .003, indicando um efeito moderado-forte (d = –0.514), a favor do grupo experimental.

Nos restantes construtos (Expectativa de Esforço, Expectativa de Desempenho e Ansiedade), embora o grupo experimental tenha obtido médias mais elevadas (exceto no caso da ansiedade, onde foi inferior), essas diferenças não foram estatisticamente significativas.

No global, estes resultados indicam que, no caso da autenticação por impressão digital, o vídeo educativo foi eficaz em melhorar a perceção de apoio social e organizacional, a confiança pessoal e a intenção comportamental de adoção, revelando impacto mensurável e consistente.

5.6. Fator de autenticação Token Físico

5.6.1. Caracterização da subamostra

Na amostra deste estudo, 124 participantes reportaram conhecer o fator de autenticação token físico. Os dados sociodemográficos desta subamostra podem ser consultados na Tabela 14.

Tabela 14

Dados sociodemográficos da subamostra de participantes que conhecem o fator de autenticação token físico.

Dados sociodemográficos	Amostra	
	n	%
Idade		
21 a 29	2	1.6
30 a 39	5	4.0
40 a 49	37	29.8
50 a 59	63	50.8
60 ou mais	17	13.7
Nível de escolaridade		
Ensino secundário	28	22.6
Ensino superior	95	76.6
Prefiro não dizer	1	0.8
Formação prévia em cibersegurança		
Sim	88	71.0
Não	36	29.0
Formação previa efetuada quando		
Nos últimos 6 meses	50	40.3
Entre os últimos 6 a 12 meses	20	16.1
Há mais de 12 meses	18	14.5
Missing	36	29.0
Grupos		
Controlo	66	53.2
Experimental	58	46.8

Com base nos dados sociodemográficos apresentados na tabela, procede-se à caracterização do conjunto de indivíduos participantes no estudo. A distribuição etária dos participantes revela uma predominância da faixa etária dos 50 aos 59 anos, correspondendo a 50,8% do total da amostra. Segue-se o grupo dos 40 aos 49 anos, que representa 29,8%, e o segmento dos indivíduos com 60 anos ou mais, com 13,7%. As categorias etárias dos 30 aos

39 anos e dos 21 aos 29 anos são as menos representativas, com 4,0% e 1,6%, respetivamente. Relativamente ao nível de escolaridade, verifica-se que uma proporção significativa dos participantes, correspondente a 76,6%, possui formação ao nível do ensino superior. Os respondentes com ensino secundário constituem 22,6% da amostra, enquanto uma minoria de 0,8% optou por não divulgar o seu grau de instrução. No que concerne à formação prévia em cibersegurança, constata-se que uma substancial maioria de 71% dos inquiridos reporta ter formação anterior na área. Em contrapartida, 29% dos participantes não possuem formação nesta área específica. Dentro do conjunto de participantes com formação em cibersegurança, 40,3% realizaram a sua formação nos últimos 6 meses, 16,1% entre 6 a 12 meses antes da recolha de dados e 14,5% há mais de 12 meses. É de notar que se registra uma ausência de dados relativos a 29% dos participantes nesta categoria. Por fim, no que toca à distribuição pelos grupos de estudo, observa-se um equilíbrio na composição dos grupos, com 53,2% dos sujeitos alocados ao grupo de controlo e 46,8% ao grupo experimental.

5.6.2. Correlações entre construtos UTAUT, formação e grupos

De forma a compreender se os construtos relacionados com o modelo UTAUT estão correlacionados com a formação prévia e/ou com a apresentação do estímulo experimental, foram calculados coeficientes de correlação de *Pearson*. Os resultados podem ser analisados na

Tabela ***15***.

Tabela 15

Coeficientes de Correlação de Pearson entre os Construtos UTAUT, Formação Prévia e Apresentação do Estímulo Experimental, na Subamostra Relativa ao Fator de Autenticação Token Físico

Variável	*M*	*SD*	Max	Min	1	2	3	4	5	6	7	8	9
1. Influência social	3.5832	.92486	5.00	1.00	-	-	-	-	-	-	-	-	-
2. Condições Facilitadoras	3.9414	1.02825	5.00	1.00	.545**	-	-	-	-	-	-	-	-
3. Expetativa de Esforço	4.0759	.86869	5.00	1.00	.492**	.600**	-	-	-	-	-	-	-
4. Expetativa de Desempenho	3.7414	.91116	5.00	1.00	.545**	.507**	.595**	-	-	-	-	-	-
5. Autoeficácia	3.8552	.96810	5.00	1.00	.491**	.548**	.628**	.490**	-	-	-	-	-
6. Ansiedade	1.9379	.99806	5.00	1.00	-.260**	-.258**	-.453**	-.138	-.234**	-	-	-	-
7. Intenção Comportamental	4.0552	1.03434	5.00	1.00	.613**	.643**	.658**	.584**	.686**	-.230*	-	-	-
8. Formação prévia	-	-	-	-	-.108	-.108	.028	.008	-.066	-.003	-.084	-	-
9. Grupos	-	-	-	-	.174	.080	.099	.121	.181*	-.092	.196*	-.023	-

$^{*}p < .05$. $^{**}p < .01$.

As análises de correlação de Pearson demonstraram correlações fortes e positivas entre Expectativa de Esforço e Intenção Comportamental ($r = .658$, $p < .01$), entre Autoeficácia e Intenção Comportamental ($r = .686$, $p < .01$), e entre Condições Facilitadoras e Intenção Comportamental ($r = .643$, $p < .01$). Estes resultados destacam, mais uma vez, o papel determinante da perceção de facilidade, capacidade pessoal e suporte organizacional na predisposição para adotar o token físico.

Foram ainda observadas correlações fortes entre Influência Social e Intenção Comportamental ($r = .613$, $p < .01$), e entre Expectativa de Desempenho e Intenção Comportamental ($r = .584$, $p < .01$). Também se destacam associações fortes entre Autoeficácia e Expectativa de Esforço ($r = .628$, $p < .01$), e entre Expectativa de Desempenho e Expectativa de Esforço ($r = .595$, $p < .01$).

A variável Ansiedade apresentou correlações negativas moderadas com Expectativa de Esforço ($r = –.453$, $p < .01$), Autoeficácia ($r = –.234$, $p < .01$) e Intenção Comportamental ($r = –.230$, $p < .05$), revelando, tal como nas análises anteriores, que a presença de desconforto ou receio reduz a predisposição para adoção da tecnologia.

As associações com a variável formação prévia voltam a revelar-se fracas e não significativas, reforçando a ideia de que a formação isolada, fora do contexto experimental, não exerce impacto direto relevante sobre os construtos analisados.

5.6.3. Testes *t* – comparação entre grupos

Com o objetivo de comparar os participantes expostos ao estímulo experimental aos participantes pertencentes ao grupo de controlo, no que concerne aos construtos do modelo UTAUT, foram realizados testes t para amostras independentes. Os resultados podem ser observados na tabela

Tabela 16.

Tabela 16

Comparação de Médias entre Grupo de Controlo e Experimental, no que Concerne aos Fatores Considerados no Modelo UTAUT, para o Fator de Autenticação Token Físico.

Variáveis dependentes	Grupo Experimental		Grupo Controlo		*t*	*df*	*p*	Cohen's *d*
	M	*SD*	*M*	*SD*				
Influência social	3.879	.875	3.560	.934	-1.952	122	.053	-.351
Condições facilitadoras	4.112	1.030	3.954	.958	-.881	122	.380	-.159
Expetativa esforço	4.138	.912	3.962	.874	-1.095	122	.276	-.197
Expetativa desempenho	3.862	.837	3.629	1.064	-1.343	122	.182	-.242
Autoeficácia	4.172	.948	3.826	.950	-2.028	122	.045	-.365
Ansiedade	1.810	.972	1.992	1.005	1.022	122	.309	.184
Intenção comportamental	4.267	.833	3.893	1.020	-2.211	122	.029	-.398

Os testes t de comparação entre os grupos revelaram duas diferenças estatisticamente significativas:

- No construto Autoeficácia, o grupo experimental apresentou uma média mais elevada ($M = 4.17$) em comparação com o grupo de controlo ($M = 3.83$), com $t(122) = –2.028$, $p = .045$, e um tamanho de efeito moderado (Cohen's $d = –0.365$).
- Relativamente à Intenção Comportamental, também se verificou uma diferença significativa a favor do grupo experimental ($M = 4.27$ vs. 3.89), $t(122) = –2.211$, $p = .029$, com um tamanho de efeito igualmente moderado ($d = –0.398$).

Nos restantes construtos, incluindo Influência Social, Expectativa de Esforço, Expectativa de Desempenho, Condições Facilitadoras e Ansiedade, não foram detetadas diferenças estatisticamente significativas. Ainda assim, as médias do grupo experimental foram consistentemente superiores àquelas do grupo de controlo, exceto no caso da Ansiedade, onde se observou uma média ligeiramente inferior — em linha com o efeito desejado da intervenção formativa.

No geral, os resultados sugerem que a exposição ao estímulo educativo foi eficaz em reforçar a perceção de competência e intenção de adoção da MFA baseada em token físico, ainda que o impacto em outras dimensões se tenha mantido limitado.

5.7. Fator de autenticação Aplicação Móvel

5.7.1. Caracterização da subamostra

Na amostra deste estudo, 152 participantes reportaram conhecer o fator de autenticação token físico. Os dados sociodemográficos desta subamostra podem ser consultados na Tabela 17.

Tabela 17

Dados Sociodemográficos da Subamostra de Participantes que Conhecem o Fator de Autenticação Aplicação Móvel

Dados sociodemográficos	Amostra	
	n	%
Idade		
21 a 29	2	1.3
30 a 39	6	4.0
40 a 49	52	34.9
50 a 59	69	46.3
60 ou mais	20	13.4
Nível de escolaridade		
Ensino secundário	38	25.5
Ensino superior	110	73.8
Prefiro não dizer	1	0.7
Formação prévia em cibersegurança		
Sim	102	68.5
Não	47	31.5
Formação previa efetuada quando		
Nos últimos 6 meses	58	38.9
Entre os últimos 6 a 12 meses	24	16.1
Há mais de 12 meses	20	13.4
Missing	47	31.5
Grupos		
Controlo	86	55.7
Experimental	66	44.3

Com base nos dados sociodemográficos apresentados na tabela, procede-se à caracterização do conjunto de indivíduos participantes no estudo. A distribuição etária dos participantes revela uma predominância da faixa etária dos 50 aos 59 anos, correspondendo a 46.3% do total da amostra. Segue-se o grupo dos 40 aos 49 anos, que representa 34.9%, e o segmento dos indivíduos com 60 anos ou mais, com 13.4%. As categorias etárias dos 30 aos

39 anos e dos 21 aos 29 anos são as menos representativas, com 4.0% e 1.3%, respetivamente. Relativamente ao nível de escolaridade, verifica-se que uma proporção significativa dos participantes, correspondente a 73.8%, possui formação ao nível do ensino superior. Os respondentes com ensino secundário constituem 25.5% da amostra, enquanto uma minoria de 0.7% optou por não divulgar o seu grau de instrução. No que concerne à formação prévia em cibersegurança, constata-se que uma substancial maioria de 68.5% dos inquiridos reporta ter formação anterior na área. Em contrapartida, 31.5% dos participantes não possuem formação nesta área específica. Dentro do conjunto de participantes com formação em cibersegurança, 38.9% realizaram a sua formação nos últimos 6 meses, 16.1% entre 6 a 12 meses antes da recolha de dados e 13.4% há mais de 12 meses. É de notar que se registra uma ausência de dados relativos a 31.5% dos participantes nesta categoria. Por fim, no que toca à distribuição pelos grupos de estudo, observa-se que 55.7% dos sujeitos estão alocados ao grupo de controlo e 44.3% ao grupo experimental.

5.7.2. Correlações entre construtos UTAUT, formação e grupos

De forma a compreender se os construtos relacionados com o modelo UTAUT estão correlacionados com a formação prévia e/ou com a apresentação do estímulo experimental, foram calculados coeficientes de correlação de *Pearson*. Os resultados podem ser analisados na

Tabela 18.

Tabela 18

Coeficientes de Correlação de Pearson entre os Construtos UTAUT, Formação Prévia e Apresentação do Estímulo Experimental, na Subamostra Relativa ao Fator de Autenticação Aplicação Móvel

Variável	*M*	*SD*	Max	Min	1	2	3	4	5	6	7	8	9
1. Influência social	4.1409	.78431	5.00	2.00	-	-	-	-	-	-	-	-	-
2. Condições Facilitadoras	4.3691	.81040	5.00	1.00	.614**	-	-	-	-	-	-	-	-
3. Expetativa de Esforço	4.1678	.75697	5.00	2.00	.444**	.562**	-	-	-	-	-	-	-
4. Expetativa de Desempenho	3.9664	.82336	5.00	2.00	.549**	.414**	.426**	-	-	-	-	-	-
5. Autoeficácia	4.1711	.85971	5.00	1.50	.588**	.571**	.490**	.469**	-	-	-	-	-
6. Ansiedade	1.8423	.92101	5.00	1.00	-.292**	-.399**	-.381**	-.103	-.307**	-	-	-	-
7. Intenção Comportamental	4.4832	.71048	5.00	2.00	.565**	.542**	.410**	.470**	.585**	-.280**	-	-	-
8. Formação prévia	-	-	-	-	-.058	.003	.050	-.007	-.060	-.001	-.035	-	-
9. Grupos	-	-	-	-	.116	.052	.223**	.143	.098	-.112	.069	-.023	-

$^{*}p < .05$. $^{**}p < .01$.

A análise dos coeficientes de correlação de Pearson revelou correlações fortes e positivas entre Autoeficácia e Intenção Comportamental ($r = .585$, $p < .01$), entre Expectativa de Desempenho e Intenção Comportamental ($r = .470$, $p < .01$), entre Expectativa de Esforço e Intenção Comportamental ($r = .410$, $p < .01$), e entre Condições Facilitadoras e Intenção Comportamental ($r = .542$, $p < .01$).

Também se registaram correlações fortes entre Expectativa de Desempenho e Expectativa de Esforço ($r = .426$, $p < .01$), entre Autoeficácia e Expectativa de Esforço ($r = .490$, $p < .01$), e entre Influência Social e Intenção Comportamental ($r = .565$, $p < .01$). Estes resultados sustentam, mais uma vez, a importância das perceções de valor, facilidade, apoio social e capacidade individual na predisposição para adotar a MFA baseada em aplicação móvel.

A Ansiedade mostrou correlações negativas moderadas com Intenção Comportamental ($r = –.280$, $p < .01$), Expectativa de Esforço ($r = –.381$, $p < .01$), e Autoeficácia ($r = –.307$, $p < .01$), o que está alinhado com os padrões verificados nos fatores anteriores.

Por outro lado, as correlações entre a variável formação prévia e os restantes construtos foram fracas e não significativas, sugerindo, mais uma vez, que a experiência formativa anterior, isolada do contexto experimental, não se revela determinante para influenciar diretamente as perceções ou intenções dos participantes.

5.7.3. Testes *t* – comparação entre grupos

Com o objetivo de comparar os participantes expostos ao estímulo experimental aos participantes pertencentes ao grupo de controlo, no que concerne aos construtos do modelo UTAUT, foram realizados testes t para amostras independentes. Os resultados podem observados na

Tabela **19**.

Tabela 19

Comparação de Médias entre Grupo de Controlo e Experimental, no que Concerne aos Fatores Considerados no Modelo UTAUT, para o Fator de Autenticação Aplicação Móvel.

Variáveis dependentes	Grupo Experimental		Grupo Controlo		*t*	*df*	*p*	*Cohen's d*
	M	*SD*	*M*	*SD*				
Influência social	4.242	.819	4.060	.750	-1.413	147	.160	-.233
Condições facilitadoras	4.417	.839	4.331	.789	-.637	147	.525	-.105
Expetativa esforço	4.356	.758	4.018	.726	-2.768	147	.006	-.456
Expetativa desempenho	4.098	.838	3.861	.801	-1.758	147	.081	-.290
Autoeficácia	4.265	.874	4.096	.846	-1.192	147	.235	-.197
Ansiedade	1.727	.925	1.933	.913	1.363	147	.175	.225
Intenção comportamental	4.538	.675	4.439	.738	-.837	147	.404	-.138

Os testes t realizados para esta subamostra identificaram uma diferença estatisticamente significativa no construto Expectativa de Esforço, com o grupo experimental a apresentar uma média superior ($M = 4.36$) face ao grupo de controlo ($M = 4.02$), $t(147) = -2.768$, $p = .006$, com um tamanho de efeito moderado (Cohen's $d = -0.456$).

Nos restantes construtos — Influência Social, Expectativa de Desempenho, Condições Facilitadoras, Autoeficácia, Ansiedade e Intenção Comportamental — não se observaram diferenças estatisticamente significativas entre grupos. Ainda assim, as médias obtidas pelo grupo experimental foram ligeiramente superiores em todos os construtos positivos, e ligeiramente inferiores em Ansiedade, o que sugere uma tendência favorável, ainda que estatisticamente limitada, da intervenção educativa.

Estes resultados indicam que, no caso da autenticação por aplicação móvel, o vídeo educativo foi particularmente eficaz em melhorar a perceção de facilidade de uso (esforço), com efeito direto mensurável. Contudo, o impacto sobre os restantes fatores do modelo UTAUT não atingiu significância estatística.

6. Discussão

6.1. Introdução à discussão

Este capítulo tem como objetivo interpretar criticamente os resultados apresentados no capítulo anterior, articulando-os com os objetivos da investigação, as hipóteses formuladas e os modelos teóricos analisados na revisão da literatura. A discussão centra-se na compreensão do impacto da formação em cibersegurança, concretizada através de um vídeo educativo, sobre a predisposição dos colaboradores do setor público para adotar diferentes métodos de autenticação multifator (MFA), à luz do modelo UTAUT.

A análise será organizada com base nas hipóteses definidas, procurando verificar em que medida os dados obtidos sustentam ou refutam as previsões teóricas, e que implicações podem ser extraídas para a prática organizacional. Serão ainda discutidos os construtos mais sensíveis à intervenção formativa, as variações observadas entre diferentes fatores de autenticação e os elementos de resistência ou neutralidade verificados. O capítulo termina com a apresentação das limitações do estudo e com sugestões para investigações futuras.

6.2. Discussão por hipótese

6.2.1. Hipótese 1 - expetativa de desempenho

H1: A perceção da utilidade dos sistemas de segundo fator de autenticação no trabalho está positivamente correlacionada com a intenção de utilizá-los.

Os resultados obtidos nas seis subamostras confirmam a existência de correlações positivas moderadas a fortes entre a Expectativa de Desempenho e a Intenção Comportamental. Destacam-se os fatores de autenticação Reconhecimento Facial, Impressão Digital, Token Físico e Aplicação Móvel, com valores de r variando entre .470 e .667, o que reforça a robustez desta relação.

Este padrão é coerente com o modelo UTAUT (Venkatesh et al., 2003), onde a Expectativa de Desempenho representa o grau em que o utilizador acredita que a utilização da tecnologia melhorará o seu desempenho no trabalho. Venkatesh et al. demonstraram empiricamente que este é um dos preditores mais fortes da intenção de adoção tecnológica, especialmente em contextos organizacionais.

Estes achados são também consistentes com o estudo de Alharbi et al. (2019), que investigaram os determinantes da aceitação de MFA entre profissionais de saúde na Arábia

Saudita, tendo concluído que a perceção de utilidade prática foi o fator mais influente na predisposição para adoção. De forma semelhante, Bélanger et al. (2017) verificaram que, em contextos empresariais com políticas de segurança mais restritivas, os utilizadores valorizam tecnologias que simplifiquem processos de autenticação sem comprometer a produtividade — exatamente o papel da Expectativa de Desempenho.

No que diz respeito ao impacto do estímulo educativo (vídeo formativo), observaram-se diferenças estatisticamente significativas entre grupos nos fatores SMS/E-mail e Impressão Digital, com médias mais elevadas no grupo experimental. Estes dados sugerem que a formação foi eficaz em comunicar a utilidade prática da MFA nestes métodos, que são geralmente mais familiares e tangíveis para os utilizadores.

Por outro lado, nos fatores Reconhecimento Facial, Voz e Token Físico, embora o grupo experimental tenha obtido médias ligeiramente superiores, as diferenças não atingiram significância estatística. Uma explicação plausível pode residir no facto de alguns destes métodos serem menos utilizados no quotidiano dos participantes, o que dificulta a tradução do conteúdo do vídeo em perceções práticas imediatas de utilidade.

Este fenómeno é abordado na tese de Castañeda (2021), que refere que a eficácia de conteúdos educativos sobre literacia digital depende não só do conteúdo transmitido, mas da capacidade do utilizador se visualizar a aplicar esse conhecimento no seu contexto real. O mesmo autor alerta para a limitação dos estímulos exclusivamente visuais quando não são complementados por interatividade ou experimentação.

Em síntese, os dados confirmam a hipótese 1, validando a Expectativa de Desempenho como um determinante central da intenção de adoção da MFA. No entanto, o impacto da formação nesta perceção varia consoante o método de autenticação em análise, sendo mais eficaz em tecnologias familiares e de uso intuitivo.

6.2.2. Hipótese 2 – expetativa de esforço ou facilidade de uso

H2: A perceção de que é fácil tornar-se habilidoso no uso dos sistemas de segundo fator de autenticação está positivamente correlacionada com a sua adoção.

A análise dos resultados mostra uma associação forte entre a Expectativa de Esforço e a Intenção Comportamental em todas as subamostras. Os valores de r variaram entre .410 e .658, o que revela uma relação estatisticamente significativa e com impacto consistente. Esta constatação reforça a importância da perceção de facilidade de uso como elemento

determinante na predisposição para a adoção de tecnologias de segurança, nomeadamente os sistemas de MFA.

No contexto do modelo UTAUT, a Expectativa de Esforço é definida como o grau de facilidade associado à utilização da tecnologia. Venkatesh et al. (2003) afirmam que este construto é especialmente relevante em fases iniciais de contacto com a tecnologia, podendo condicionar de forma significativa a intenção de uso, particularmente quando os utilizadores não estão familiarizados com os sistemas em questão.

Os dados obtidos neste estudo alinham-se com as conclusões de Pikkarainen et al. (2004), que mostraram que, em ambientes organizacionais, perceções de complexidade operacional reduzem drasticamente a intenção de adoção de novos sistemas. De forma semelhante, Chong (2013) verificou que, em contextos públicos e governamentais, a simplicidade percebida é frequentemente mais influente do que a utilidade percebida — um padrão coerente com o perfil dos participantes deste estudo.

Relativamente ao efeito da formação, os testes t revelaram diferenças estatisticamente significativas entre os grupos experimental e de controlo em três fatores: SMS/E-mail, Impressão Digital e Aplicação Móvel, com médias consistentemente superiores no grupo que visualizou o vídeo educativo. Estes resultados sugerem que uma intervenção simples, curta e prática, como o vídeo produzido, pode melhorar significativamente a perceção de usabilidade de certos métodos de MFA.

Por outro lado, em fatores como Voz, Token Físico e Reconhecimento Facial, não foram observadas diferenças significativas entre grupos. Uma explicação possível é que a Expectativa de Esforço está fortemente relacionada com experiências anteriores: tecnologias que os utilizadores já conhecem ou conseguem imaginar a usar tendem a ser percecionadas como mais simples. Quando essa experiência é ausente — como pode ser o caso do reconhecimento facial ou da autenticação por voz — o estímulo visual pode não ser suficiente para alterar perceções enraizadas.

Este padrão é consistente com a análise de Castañeda (2021), que demonstrou que a eficácia de conteúdos educativos depende da familiaridade prévia dos participantes com o tipo de tecnologia apresentado. Castañeda sublinha que, quando os conteúdos formativos não se ligam diretamente à experiência concreta dos utilizadores, o efeito formativo pode ser mais superficial e temporário.

Assim, a hipótese 2 é confirmada pelos dados, tanto em termos de correlação como nos efeitos observáveis da formação. A perceção de facilidade de utilização assume um papel central na aceitação da MFA e pode ser positivamente influenciada por ações formativas

breves, sobretudo quando aplicadas a tecnologias já minimamente conhecidas pelos utilizadores.

Mayer (2008) demonstrou que a aprendizagem é mais eficaz quando os conteúdos são apresentados em formatos multimodais, combinando áudio e imagem com uma estrutura clara e concisa. Estes princípios ajudam a explicar o impacto positivo do vídeo educativo utilizado neste estudo na perceção de facilidade de utilização dos sistemas de MFA.

6.2.3. Hipótese 3 – influência social

H3: A perceção de que outras pessoas importantes (pares, superiores) esperam ou recomendam o uso dos sistemas de segundo fator de autenticação está positivamente correlacionada com a intenção de utilizá-los.

Os resultados obtidos demonstram correlações positivas moderadas a fortes entre o construto Influência Social e a Intenção Comportamental em todos os fatores de autenticação, com valores de r variando entre .511 e .613. Esta associação sugere que a recomendação, expectativa ou valorização por parte de colegas e superiores hierárquicos tem um impacto significativo na predisposição dos colaboradores para adotar tecnologias de MFA.

Este padrão é coerente com o que é proposto pelo modelo UTAUT, onde a Influência Social é definida como o grau em que um indivíduo percebe que pessoas importantes para ele acreditam que ele deve utilizar o novo sistema. Segundo Venkatesh et al. (2003), este construto tem particular relevância em ambientes organizacionais, onde normas sociais implícitas e explícitas moldam decisões tecnológicas, sobretudo quando os utilizadores não têm controlo total sobre as tecnologias que usam.

Estudos como o de Ifinedo (2012) reforçam esta perspetiva, mostrando que a adoção de tecnologias de segurança em instituições públicas está fortemente associada à existência de um discurso institucional favorável e ao exemplo visível de colegas e chefias. Da mesma forma, Zhou et al. (2010) demonstraram que, em ambientes de trabalho colaborativo, a influência dos pares pode ser mais decisiva do que a utilidade percebida, sobretudo quando os riscos associados ao não uso da tecnologia são elevados. O estudo de Ifinedo (2012) reforça que a conformidade com políticas de segurança decorre, em grande medida, da interiorização de normas sociais percebidas como legítimas e alinhadas com a cultura organizacional. Assim, a perceção de que os pares e chefias valorizam determinados comportamentos tecnológicos atua como catalisador para a sua adoção, independentemente da competência técnica individual.

No presente estudo, os testes t mostraram diferenças estatisticamente significativas entre os grupos experimental e de controlo em dois fatores: SMS/E-mail e Impressão Digital.

Nestes casos, os participantes que visualizaram o vídeo formativo apresentaram médias mais elevadas no construto Influência Social, sugerindo que o conteúdo educativo também pode indiretamente reforçar normas sociais, ao posicionar a adoção da MFA como um comportamento valorizado e desejável.

Este efeito é coerente com a análise de Castañeda (2021), que destaca que uma narrativa educativa bem estruturada, ainda que transmitida de forma unidirecional (como num vídeo), pode desencadear mecanismos de identificação social. Ao apresentar boas práticas de segurança como comportamentos partilhados e recomendados por figuras de autoridade, o vídeo parece ter reforçado, ainda que parcialmente, o papel da influência social no processo de decisão individual.

Contudo, nos restantes fatores de autenticação, as diferenças entre grupos não foram significativas, o que sugere que o impacto da formação nesta variável é dependente do grau de identificação do participante com os exemplos apresentados no conteúdo. Tal como referido por Hernández et al. (2014), a Influência Social tende a exercer maior impacto quando o conteúdo formativo apresenta modelos de comportamento próximos do contexto real do utilizador.

Ifinedo (2012) integrou a Teoria do Comportamento Planeado e a Teoria da Motivação à Proteção para explicar a conformidade com políticas de segurança da informação. Os seus resultados mostram que normas sociais percebidas como legítimas, em especial quando comunicadas por figuras de autoridade, exercem uma influência significativa na intenção de conformidade com medidas de segurança.

Em síntese, os resultados confirmam a hipótese 3, reforçando o papel da Influência Social como um dos fatores mais relevantes para a intenção de adoção da MFA em ambientes institucionais. Embora o estímulo educativo não tenha gerado efeitos significativos em todos os contextos, o seu contributo indireto para o reforço de normas sociais positivas é observável e potencialmente valioso em estratégias de sensibilização organizacional.

6.2.4. Hipótese 4 - condições facilitadoras

H4: A perceção de que existem condições organizacionais, técnicas e logísticas adequadas para utilizar os sistemas de segundo fator de autenticação está positivamente correlacionada com a intenção de utilizá-los.

Os dados obtidos revelam correlações fortes e positivas entre o construto Condições Facilitadoras e a Intenção Comportamental em cinco dos seis fatores de autenticação, com coeficientes de correlação a variar entre .542 e .698. Estes resultados indicam que, quanto mais

os utilizadores percecionam a existência de recursos técnicos, apoio institucional e infraestrutura adequada, maior é a sua predisposição para adotar mecanismos de autenticação multifator (MFA).

No modelo UTAUT, as Condições Facilitadoras representam a perceção de que existem os meios técnicos e organizacionais necessários para utilizar uma tecnologia. Venkatesh et al. (2003) sublinham que este construto tem particular relevância quando os utilizadores não são autónomos na implementação da tecnologia, como frequentemente ocorre em ambientes institucionais.

Estes achados são consistentes com a investigação de Williams et al. (2015), que identificaram o suporte técnico e a presença de políticas claras como fatores críticos para a aceitação de sistemas de autenticação em instituições públicas. De igual modo, Im et al. (2011) demonstraram que a disponibilidade de recursos tangíveis — como formação acessível, helpdesk e guias operacionais — contribui significativamente para aumentar a intenção de adoção de tecnologias de segurança.

No presente estudo, os testes t revelaram diferenças estatisticamente significativas entre os grupos experimental e de controlo apenas no fator Impressão Digital, com os participantes que visualizaram o vídeo educativo a apresentarem uma perceção significativamente mais elevada de condições facilitadoras. Este resultado pode indicar que o estímulo formativo foi eficaz em transmitir a ideia de que existem apoios institucionais disponíveis para implementar este método de MFA.

Contudo, nos restantes fatores, as diferenças entre grupos não atingiram significância estatística. Uma explicação plausível é que a perceção de condições facilitadoras depende menos de conteúdos educativos e mais da experiência direta no local de trabalho. Esta leitura é corroborada por Castañeda (2021), que refere que a perceção de contexto favorável é moldada mais pela realidade organizacional do que por estímulos comunicacionais. Segundo o autor, a mudança neste tipo de construto exige intervenções sistémicas e ações coordenadas, para além da formação pontual.

Em síntese, os resultados confirmam a hipótese 4, demonstrando que a perceção de suporte técnico e organizacional se associa positivamente à intenção de adoção da MFA. Ainda assim, o impacto da formação sobre este construto revelou-se limitado, o que reforça a necessidade de intervenções complementares que consolidem, na prática, a existência de condições facilitadoras reais e visíveis.

6.2.5. Hipótese 5 – autoeficácia

H5: A perceção de capacidade pessoal para utilizar os sistemas de segundo fator de autenticação está positivamente correlacionada com a intenção de utilizá-los.

A análise dos dados revelou correlações fortes e positivas entre o construto Autoeficácia e a Intenção Comportamental em todas as subamostras, com coeficientes de correlação a variar entre .503 e .686. Estes resultados sugerem que quanto mais os utilizadores se sentem capazes de lidar com sistemas de MFA, maior é a sua predisposição para os adotar.

Este padrão está de acordo com a teoria da autoeficácia proposta por Bandura (1986), segundo a qual a crença na própria capacidade para executar uma ação influencia diretamente o comportamento futuro. No contexto do modelo UTAUT, a autoeficácia é um fator que contribui indiretamente para a Expectativa de Esforço e está relacionado com a confiança do utilizador na sua competência tecnológica.

Estudos anteriores corroboram este impacto. Compeau e Higgins (1995) demonstraram que a autoeficácia é um preditor fiável da utilização de novas tecnologias, especialmente em ambientes com baixa formação técnica inicial. Da mesma forma, Venkatesh e Bala (2008) identificaram a autoeficácia como uma variável relevante na aceitação de tecnologias de segurança quando estas envolvem múltiplos passos, como é o caso da MFA.

No presente estudo, os testes t revelaram diferenças estatisticamente significativas entre os grupos de controlo e experimental nos fatores SMS/E-mail, Impressão Digital e Token Físico, com o grupo experimental a apresentar médias superiores. Estas diferenças refletem um impacto direto da intervenção educativa sobre a perceção de capacidade dos utilizadores para utilizar esses métodos.

Este efeito é particularmente relevante, uma vez que a autoeficácia é um construto psicológico altamente sensível a experiências de aprendizagem, mesmo quando curtas. Conforme observado por Castañeda (2021), pequenas ações formativas — como vídeos explicativos — podem gerar ganhos significativos na confiança dos utilizadores, desde que o conteúdo seja claro, acessível e aplicável ao seu contexto.

No entanto, em fatores como Reconhecimento Facial, Aplicação Móvel e Voz, não foram observadas diferenças significativas entre grupos. É possível que a perceção de autoeficácia nestes métodos dependa mais de experiências práticas anteriores do que da formação recebida. Como defendem Torkzadeh et al. (2006), a autoeficácia é reforçada não apenas pela exposição informativa, mas pela oportunidade de testar e aplicar a tecnologia com autonomia.

Em síntese, os dados confirmam a hipótese 5, validando a autoeficácia como um preditor relevante da intenção de adoção da MFA. A intervenção formativa demonstrou ser eficaz em aumentar essa perceção em métodos mais familiares e tangíveis, mas menos eficaz em métodos menos experienciados. Estes resultados sugerem que ações educativas, quando combinadas com oportunidades práticas, podem potenciar significativamente a adoção de medidas de segurança digital.

6.2.6. Hipótese 6 - ansiedade

H6: A perceção de ansiedade relacionada com o uso dos sistemas de segundo fator de autenticação está negativamente correlacionada com a intenção de utilizá-los.

Os resultados obtidos demonstram correlações negativas moderadas entre o construto Ansiedade e a Intenção Comportamental em todos os fatores de autenticação analisados, com coeficientes de correlação a variar entre –.230 e –.422. Estes dados indicam que quanto maior o desconforto, receio ou stress percebido pelos utilizadores face ao uso da MFA, menor é a sua predisposição para a adotar.

Este resultado é coerente com a definição do construto Ansiedade tecnológica apresentada por Venkatesh et al. (2003), segundo a qual esta dimensão reflete sentimentos de apreensão e tensão face à utilização de tecnologias, particularmente quando estas exigem múltiplos passos ou envolvem riscos de erro. Ainda que no modelo UTAUT original a Ansiedade não seja um preditor direto da intenção comportamental, estudos subsequentes, como o de Venkatesh & Bala (2008), sugerem que a Ansiedade pode influenciar indiretamente a intenção, através da Expectativa de Esforço e da Autoeficácia.

A literatura mais recente reforça essa visão. Chou e Chen (2009) demonstraram que a ansiedade reduz a perceção de controlo sobre o uso da tecnologia e pode comprometer a adoção, mesmo em ambientes com bom suporte técnico. Alsharif et al. (2022), num estudo sobre autenticação biométrica, observaram que sentimentos de desconforto com tecnologias corporais ou novas interfaces estavam associados a taxas mais baixas de aceitação, mesmo quando a utilidade era reconhecida.

No presente estudo, os testes t não revelaram diferenças estatisticamente significativas entre grupos em nenhum dos fatores de autenticação no que respeita ao construto Ansiedade. Ainda assim, em todos os casos, as médias do grupo experimental foram ligeiramente inferiores às do grupo de controlo, sugerindo uma possível tendência redutora da intervenção formativa, ainda que insuficiente para gerar efeitos mensuráveis.

Este resultado pode dever-se à natureza do estímulo educativo utilizado. Embora o vídeo formativo tenha sido eficaz em aumentar perceções de utilidade, facilidade de uso e autoeficácia, a redução de ansiedade requer frequentemente abordagens mais imersivas e práticas. Tal como identificado por Castañeda (2021), o sentimento de segurança subjetiva em relação à tecnologia depende da exposição prolongada, do suporte contínuo e da experiência pessoal com o sistema, sendo menos influenciado por intervenções pontuais.

Adicionalmente, a ansiedade tecnológica está muitas vezes ligada a traços individuais estáveis ou experiências negativas passadas, o que torna mais difícil modificá-la com uma única ação educativa. Intervenções eficazes neste domínio podem incluir formação prática, sessões de demonstração assistida ou mentoring entre pares — medidas que vão para além do alcance deste estudo.

Tschakert e Ngamsuriyaroj (2019) analisaram diferentes métodos de formação em segurança e concluíram que ações tradicionais, baseadas em informação unidirecional, têm impacto limitado na redução da ansiedade. Segundo os autores, treinos práticos e personalizados são mais eficazes na modificação de perceções emocionais negativas associadas ao uso de tecnologias de segurança.

Em síntese, os dados confirmam a hipótese 6 no que respeita à existência de uma correlação negativa entre Ansiedade e Intenção Comportamental, mas indicam que o vídeo educativo não foi suficiente para produzir uma alteração estatisticamente significativa neste construto. Este resultado reforça a necessidade de abordagens mais estruturadas e contínuas para enfrentar os efeitos limitadores da ansiedade no processo de adoção tecnológica.

6.2.7. Hipótese 7 – formação prévia

H7: A realização de formação prévia em cibersegurança está positivamente associada aos níveis de autoeficácia e intenção de adoção da autenticação multifator.

A análise dos dados revelou correlações fracas e não significativas entre a variável "formação prévia em cibersegurança" e os construtos do modelo UTAUT, com especial destaque para a Autoeficácia e a Intenção Comportamental. Em todos os fatores de autenticação analisados, os valores de r situaram-se abaixo do limiar de .30, e não atingiram significância estatística, o que indica que a formação anterior — isoladamente — não exerceu influência mensurável sobre a predisposição para adotar a MFA.

Este resultado desafia parte da literatura que sugere que a formação em cibersegurança é uma variável crítica para a adoção de boas práticas. Por exemplo, Puhakainen e Siponen

(2010) defendem que ações educativas são fundamentais para alinhar perceções de risco e comportamentos seguros em contextos organizacionais. No entanto, os autores também referem que o impacto da formação depende da sua relevância contextual, da repetição e da forma como é integrada na cultura institucional — fatores que podem explicar os resultados limitados observados nesta investigação.

De forma semelhante, Tsohou et al. (2015) argumentam que a formação genérica em cibersegurança, quando não personalizada ou diretamente aplicada a situações do quotidiano dos utilizadores, tende a ter pouco efeito na mudança de comportamento. Este argumento é reforçado por Castañeda (2021), que defende que conteúdos formativos descontextualizados produzem, na melhor das hipóteses, um efeito superficial e de curta duração.

A ausência de impacto estatístico da formação prévia observada neste estudo pode ser interpretada como um reflexo da qualidade variável, da distância temporal e da falta de ligação entre a formação e os sistemas tecnológicos concretos utilizados no dia a dia. Ao contrário do vídeo formativo introduzido no contexto experimental, que apresentou linguagem direta, curta duração e foco na MFA, muitas formações anteriores reportadas pelos participantes poderão ter sido generalistas ou não relacionadas com este tipo específico de mecanismo.

Estes dados sugerem que a existência de formação prévia, por si só, não constitui um fator diferenciador eficaz em termos de autoeficácia ou intenção de uso. O impacto educativo parece residir não apenas no conteúdo, mas na forma, momento e contexto da intervenção — o que coloca em causa abordagens formativas formais mas desatualizadas, excessivamente teóricas ou pouco aplicáveis à realidade tecnológica concreta do utilizador.

Em síntese, os dados não confirmam a hipótese 7, indicando que a formação prévia declarada pelos participantes não teve efeito mensurável nos níveis de autoeficácia ou intenção de adoção da MFA. Esta conclusão reforça a importância de investir não apenas na quantidade, mas na qualidade, pertinência e aplicabilidade imediata das ações educativas em cibersegurança.

6.3. Síntese geral dos resultados

A presente investigação avaliou sete hipóteses derivadas do modelo UTAUT e da literatura sobre mudança comportamental e formação em cibersegurança, com o objetivo de compreender os fatores que influenciam a intenção de adoção da autenticação multifator (MFA) por parte de colaboradores do setor público português. A maioria das hipóteses foi

confirmada, demonstrando a relevância dos fatores individuais e contextuais na predisposição para adotar mecanismos de segurança tecnológica.

As hipóteses H1 a H5 — que testam os principais construtos positivos do modelo UTAUT (expectativa de desempenho, expectativa de esforço, influência social, condições facilitadoras e autoeficácia) — foram confirmadas com suporte empírico robusto, através de correlações estatisticamente significativas e valores elevados de associação com a intenção comportamental. Em particular, os construtos Autoeficácia (H5) e Condições Facilitadoras (H4) destacaram-se pelos coeficientes de correlação mais elevados em várias subamostras, reforçando o seu papel central na decisão de adotar a MFA.

A Hipótese 6 (Ansiedade) também foi confirmada, revelando correlações negativas moderadas entre o nível de ansiedade associado ao uso da MFA e a intenção de a utilizar. Este resultado valida a influência inibidora da ansiedade tecnológica, ainda que a intervenção formativa não tenha conseguido reduzir significativamente este sentimento entre os grupos experimental e de controlo.

Por outro lado, a Hipótese 7 (Formação Prévia) não foi confirmada. Os dados demonstraram que a existência de formação anterior em cibersegurança não teve correlação significativa com a autoeficácia nem com a intenção de adoção da MFA. Este resultado desafia uma parte da literatura tradicional e sugere que o impacto da formação depende não apenas da sua ocorrência, mas da sua atualidade, aplicabilidade e ligação concreta ao contexto tecnológico real dos utilizadores.

Relativamente à eficácia da intervenção formativa (vídeo educativo), os efeitos mais notórios observaram-se nos construtos Expectativa de Esforço (H2), Autoeficácia (H5) e, em alguns casos, Expectativa de Desempenho (H1) e Influência Social (H3). Estes resultados indicam que estímulos educativos breves e direcionados podem ter um impacto relevante em perceções individuais, sobretudo quando associados a tecnologias já familiares para os utilizadores.

6.4. Implicações práticas e estratégicas

Os resultados desta investigação oferecem contributos relevantes para a formulação de políticas de cibersegurança no setor público, sobretudo no que respeita à promoção da adoção da autenticação multifator (MFA). A confirmação de cinco das seis hipóteses principais com base no modelo UTAUT (H1 a H6) demonstra que fatores individuais, sociais e

organizacionais influenciam significativamente a predisposição dos utilizadores para adotarem tecnologias de segurança.

Uma primeira implicação prática prende-se com a eficácia de intervenções educativas simples, curtas e bem direcionadas. O vídeo formativo utilizado neste estudo, com apenas cinco minutos de duração, demonstrou capacidade para influenciar positivamente perceções relacionadas com utilidade, facilidade de uso e confiança individual. Este dado é especialmente relevante em contextos com limitações de tempo ou recursos, sugerindo que ações de microformação, se bem concebidas, podem gerar impacto real.

Em segundo lugar, os resultados evidenciam a importância da familiaridade tecnológica. Os métodos de MFA mais influenciáveis pela intervenção educativa foram aqueles já conhecidos dos participantes — como SMS/E-mail, Impressão Digital e Aplicação Móvel. Este dado sugere que, para tecnologias menos familiares (ex.: Reconhecimento Facial ou Voz), são necessárias estratégias formativas mais imersivas, como sessões práticas, demonstrações assistidas ou mentoring.

Uma terceira implicação decorre da confirmação da influência de fatores contextuais. Condições Facilitadoras (H4) e Influência Social (H3) mostraram-se determinantes para a intenção de adoção. Este resultado reforça a necessidade de promover uma cultura organizacional de segurança digital, visível em ações como o exemplo das lideranças, a disponibilização de apoio técnico acessível e a normalização institucional do uso da MFA.

Por fim, os dados não confirmaram a Hipótese 7 (Formação Prévia), o que sugere que a simples existência de ações formativas no passado não é, por si só, suficiente para alterar comportamentos. Este resultado sublinha a importância de investir não apenas na oferta de formação, mas na qualidade, contextualização e atualidade dos conteúdos formativos, bem como na sua articulação com políticas organizacionais coerentes.

7. Conclusão

A presente dissertação teve como principal objetivo analisar o impacto de uma intervenção formativa de curta duração na predisposição de colaboradores do setor público português para adotarem a autenticação multifator (MFA), à luz do modelo teórico UTAUT. Partindo da constatação de que a adesão a medidas de cibersegurança, embora tecnicamente viável, depende fortemente de fatores humanos, procurou-se compreender em que medida perceções como utilidade, esforço, apoio social, confiança pessoal ou ansiedade influenciam a intenção de adoção da MFA, e se essas perceções podem ser positivamente influenciadas por ações educativas.

Esta investigação procurou responder a um conjunto de perguntas de investigação formuladas no início deste trabalho. Abaixo apresentam-se essas questões, seguidas da respetiva resposta com base nos resultados obtidos:

PI1: De que forma a formação prévia em cibersegurança influencia a intenção dos colaboradores do setor público em adotar a autenticação multifator?

Os dados revelaram que a formação prévia em cibersegurança, considerada de forma isolada, não apresentou correlação significativa com a intenção de adoção da MFA, nem com a autoeficácia. Isto indica que a formação anterior, sobretudo quando não contextualizada ou atualizada, tem impacto limitado. Assim, a resposta a esta pergunta é negativa: a formação prévia, fora do contexto da intervenção, não demonstrou influência significativa na intenção comportamental.

PI2: Que construtos do modelo UTAUT — nomeadamente autoeficácia e ansiedade — melhor explicam a predisposição para a adoção da MFA no contexto analisado?

Os resultados indicaram que todos os construtos do modelo UTAUT, com exceção da ansiedade, apresentaram correlações positivas e estatisticamente significativas com a intenção de adoção da MFA. Destacam-se a autoeficácia, as condições facilitadoras, a expectativa de esforço e a expectativa de desempenho. A ansiedade, por outro lado, revelou uma correlação negativa moderada, demonstrando que níveis mais elevados de ansiedade estão associados a menor predisposição para adotar a MFA.

PI3: Quais são as diferenças observadas nos níveis de intenção comportamental entre colaboradores expostos ou não ao estímulo educativo?

Verificaram-se diferenças estatisticamente significativas nos níveis de intenção comportamental em dois fatores: Impressão Digital e Token Físico, com o grupo experimental a apresentar médias superiores ao grupo de controlo. Para os restantes fatores (como Aplicação

Móvel, SMS/E-mail ou Reconhecimento Facial), embora as médias tenham sido superiores no grupo experimental, as diferenças não atingiram significância estatística. Isto sugere que a exposição ao vídeo educativo contribuiu para uma perceção mais favorável da MFA em métodos familiares.

PI4: *Em que medida um vídeo educativo poderá contribuir para transformar perceções sobre a utilidade e usabilidade da MFA??*

Os dados demonstraram que a intervenção formativa em vídeo teve impacto significativo sobre a perceção de facilidade de uso (expectativa de esforço) e, em alguns casos, sobre a perceção de utilidade (expectativa de desempenho). Este efeito foi particularmente evidente nos fatores de autenticação mais comuns, como SMS/E-mail e Aplicação Móvel. Assim, conclui-se que um vídeo educativo poderá contribuir para transformar positivamente perceções-chave associadas à adoção da MFA, especialmente quando o conteúdo é claro, contextualizado e orientado para a prática.

Através de um desenho experimental com grupo de controlo, foi aplicado um questionário baseado no modelo UTAUT a 165 participantes, após a exposição (ou não) a um vídeo educativo com conteúdo de sensibilização em cibersegurança. A análise estatística dos dados permitiu confirmar que cinco dos seis construtos principais do modelo UTAUT — Expectativa de Desempenho, Expectativa de Esforço, Influência Social, Condições Facilitadoras e Autoeficácia — apresentam correlações estatisticamente significativas com a intenção comportamental. A Ansiedade demonstrou uma correlação negativa, também estatisticamente significativa, com esse mesmo construto.

A intervenção formativa demonstrou ser eficaz na melhoria de perceções como facilidade de utilização, confiança pessoal e, em alguns casos, influência social e perceção de utilidade, sobretudo nos métodos de MFA mais familiares aos participantes. Por outro lado, a formação prévia em cibersegurança, declarada fora do contexto experimental, não se revelou significativamente associada à intenção de adoção nem à autoeficácia, o que sugere que a qualidade, a atualidade e a contextualização das ações formativas são tão ou mais importantes do que a sua simples existência.

Os resultados obtidos nesta investigação reforçam a importância de considerar os fatores humanos na implementação de tecnologias de segurança no setor público. Demonstram, igualmente, que intervenções educativas simples, se bem concebidas, podem gerar efeitos positivos em perceções-chave para a mudança comportamental. No entanto, sublinham também que nem todos os construtos são igualmente influenciáveis por este tipo de estímulo,

e que fatores como ansiedade ou perceção institucional exigem abordagens mais estruturadas, contínuas e integradas.

Conclui-se, assim, que a promoção da cibersegurança nas organizações públicas deve combinar medidas técnicas com estratégias educativas adaptadas, apoio institucional visível e ações de comunicação consistentes. A adoção da MFA, tal como outras boas práticas de segurança digital, depende tanto da tecnologia quanto das pessoas. Esta dissertação contribui para esse entendimento e abre caminho para novas investigações que aprofundem a relação entre formação, cultura organizacional e adoção tecnológica no contexto da administração pública portuguesa.

7.1. Limitações

A presente investigação apresenta algumas limitações que importa reconhecer e enquadrar. Em primeiro lugar, a amostra do estudo foi restrita a colaboradores de uma única entidade pública portuguesa, o que pode limitar a generalização dos resultados a outros contextos organizacionais. Instituições com diferentes níveis de maturidade digital, culturas internas ou formas de interação com a tecnologia poderão apresentar padrões distintos de adoção da autenticação multifator (MFA).

Em segundo lugar, a recolha de dados baseou-se num instrumento de autodeclaração, o que significa que as respostas refletiram as perceções dos participantes e não os seus comportamentos reais. Esta abordagem, ainda que válida para avaliar intenções, está sujeita a enviesamentos como a desejabilidade social ou a interpretação subjetiva dos itens. O questionário utilizado nesta investigação foi adaptado com base no modelo UTAUT, tendo sofrido ajustamentos de redação e estrutura com o objetivo de melhor se adequar ao contexto específico em análise. Esses ajustes visaram garantir a relevância e clareza dos itens face à realidade organizacional dos participantes. Considerando que o instrumento resultante não corresponde integralmente à escala UTAUT original e que alguns construtos apresentaram valores de consistência interna abaixo dos níveis habitualmente aceites ($\alpha < .70$), optou-se por não incluir os coeficientes de Alpha de Cronbach nesta dissertação. Esta decisão enquadra-se no carácter exploratório do estudo e não compromete a validade dos resultados obtidos no contexto dos objetivos definidos.

Outra limitação relevante prende-se com a natureza da intervenção educativa utilizada. O vídeo formativo, embora eficaz em algumas dimensões, consistiu numa exposição breve e não interativa. A ausência de elementos como feedback imediato, personalização de conteúdos

ou aplicação prática pode ter restringido o seu impacto em construtos mais estáveis ou resistentes, como a ansiedade.

Acresce ainda o facto de não terem sido incluídas variáveis moderadoras, como idade, género, experiência com tecnologias digitais ou grau de voluntariedade na adoção da MFA. No modelo original UTAUT, estes fatores são considerados determinantes na forma como os construtos influenciam a intenção comportamental, pelo que a sua exclusão constitui uma limitação à complexidade da análise.

Finalmente, esta investigação foi desenhada num único momento temporal, não tendo sido possível avaliar a evolução das perceções ao longo do tempo, nem a conversão efetiva da intenção em comportamento. A ausência de um seguimento longitudinal impede conclusões mais robustas sobre a durabilidade dos efeitos da formação e a adoção real dos métodos de autenticação.

7.2. Estudos futuros

Com base nos resultados obtidos e nas limitações identificadas, abrem-se diversas possibilidades para aprofundar o conhecimento sobre os fatores que influenciam a adoção de tecnologias de segurança, como a autenticação multifator, no setor público.

Uma das principais recomendações para estudos futuros consiste em alargar a amostra a várias entidades públicas, com diferentes perfis de maturidade digital e realidades organizacionais distintas. Esta ampliação permitiria testar a robustez dos resultados observados e garantir maior representatividade das conclusões.

Outra vertente importante de aprofundamento diz respeito à inclusão de variáveis moderadoras previstas no modelo UTAUT, como a idade, o género, a experiência prévia com tecnologias digitais ou o grau de voluntariedade na adoção. A consideração destes fatores permitiria compreender de forma mais detalhada como diferentes perfis de utilizadores reagem a estímulos educativos e a medidas tecnológicas de segurança.

Adicionalmente, a aplicação de um desenho longitudinal, com recolha de dados em vários momentos temporais, permitiria analisar não apenas as perceções imediatas, mas também a sua evolução ao longo do tempo. Este tipo de abordagem possibilitaria verificar se os efeitos da formação se mantêm, se se intensificam ou se se dissipam com o passar do tempo, e se a intenção declarada se converte em comportamento real.

Outra área de interesse consiste na comparação entre diferentes formatos de intervenção educativa. Seria relevante testar, por exemplo, a eficácia relativa de vídeos interativos, sessões

presenciais, simulações práticas ou estratégias de *nudging* comportamental, de forma a identificar os métodos mais eficazes para diferentes perfis de utilizadores e contextos institucionais.

Importa ainda considerar a inclusão de fatores psicológicos e organizacionais complementares, como o compromisso institucional, a literacia digital, a confiança nas tecnologias, a cultura de segurança ou a perceção de risco. Estes fatores podem enriquecer o modelo explicativo da adoção e ajudar a desenhar intervenções mais integradas e eficazes.

Por fim, seria pertinente investigar o papel das lideranças intermédias e da comunicação interna como mediadores entre a estratégia institucional e a perceção individual dos utilizadores. A forma como as chefias comunicam e exemplificam comportamentos de segurança pode ter um impacto decisivo na criação de normas sociais positivas e na consolidação de uma cultura organizacional orientada para a cibersegurança.

8. Referências Bibliográficas

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/https://doi.org/10.1016/0749-5978(91)90020-T

Alalwan, A. A., Dwivedi, Y. K., & Rana, N. P. (2017). Factors influencing adoption of mobile banking by Jordanian bank customers: Extending UTAUT2 with trust. *International Journal of Information Management*, *37*(3), 99–110. https://doi.org/10.1016/j.ijinfomgt.2017.01.002

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, *34*(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003

Alharbi, S. T., Drew, S., & AlGhamdi, R. (2019). Adoption of multifactor authentication in the health sector: An application of UTAUT2. *International Journal of Advanced Computer Science and Applications*, *10*(2), 256–263. https://thesai.org/Publications/ViewPaper?Volume=10&Issue=2&Code=IJACSA&SerialNo=31

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *Journal of Cybersecurity and Privacy 2021, Vol. 1, Pages 219-238*, *1*(2), 219–238. https://doi.org/10.3390/JCP1020012

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*. https://arxiv.org/abs/1901.02672

Bandura, A. (1986a). Social foundations of thought and action: A social cognitive theory. Em *Social foundations of thought and action: A social cognitive theory.* Prentice-Hall, Inc.

Bandura, A. (1986b). *Social foundations of thought and action: A social cognitive theory*. Prentice Hall.

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management*, *54*(7), 887–901. https://doi.org/10.1016/j.im.2017.01.003

Centro Nacional de Cibersegurança. (2023). *Relatório Sociedade e Cibersegurança 2023*.

Centro Nacional de Cibersegurança. (2024). *Relatório Cibersegurança em Portugal - Sociedade*.

Coutinho, C. P. (2014). *Metodologia de Investigação em Ciências Sociais e Humanas: Teoria e Prática*. Almedina.

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: A review and research framework. Em *European Journal of Information Systems* (Vol. 26, Número 6, pp. 605–641). Palgrave Macmillan Ltd. https://doi.org/10.1057/s41303-017-0059-9

Davis, F. (1985). *A Technology Acceptance Model for Empirically Testing New End-User Information Systems*.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340. https://doi.org/10.2307/249008

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: The role of national cultural differences. *Information Systems Journal*, *19*(4), 391–412. https://doi.org/10.1111/j.1365-2575.2007.00289.x

Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., Lefkovitz, N. B., Danker, J. M., Greene, K. K., Theofanos, M. F., Newton, E. M., & Burr, W. E. (2017). Digital identity guidelines: Authentication and Lifecycle Management. *NIST Special Publication 800-63B*, 2–79. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Addison-Wesley. https://people.umass.edu/aizen/f&a1975.html

Fujs, D., & Bernik, I. (2024). Analyzing Cybersecurity Strategies of the European Union: Challenges and Opportunities for Public Administration. *Elektrotehniski Vestnik/Electrotechnical Review*, *91*, 8–20.

Handri, E., Sensuse, D., & Lusa, S. (2024). *Examining Cybersecurity Culture: Trends and Success Factors*. *14*, 330–352. https://doi.org/10.58346/JISIS.2024.I3.020

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Hinkle, D. E., Wiersma, W., & Jurs, S. G. (2003). *Applied Statistics for the Behavioral Sciences* (5th ed., Número v. 663). Houghton Mifflin. https://books.google.pt/books?id=7tntAAAAMAAJ

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

Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology*, *32*(6), 584–593. https://doi.org/10.1080/0144929X.2011.632650

Kim, H.-W., & Kankanhalli, A. (2009). Investigating User Resistance to Information Systems Implementation: A Status Quo Bias Quarterly ^^^b Investigating User Resistance to Information Systems Implementation: A Status Quo Bias Perspective1. Em *Source: MIS Quarterly* (Vol. 33, Número 3). http://www.jstor.orgStableURL:http://www.jstor.org/stable/20650309http://www.jstor.org/page/info/about/policies/terms.jsp

Martins, C., Oliveira, T., & Popovič, A. (2014). Understanding the internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. *International Journal of Information Management*, *34*(1), 1–13. https://doi.org/10.1016/j.ijinfomgt.2013.06.002

Microsoft. (2024). *The foundations and new frontiers of cybersecurity*.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, *42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179–214. https://doi.org/10.1080/07421222.2015.1138374

Powner, D. A., & Technology, I. (2016). *GAO-16-696T, Information Technology: Federal Agencies Need to Address Aging Legacy Systems*.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly: Management Information Systems*, *34*(4), 757–778. https://doi.org/10.2307/25750704

República Portuguesa. (2019). *Estratégia Nacional para o Ciberespaço 2019-2023*.

Ribeiro, M., Pizarro Oliveira, L., & Martinho, T. (2024). *Cibersegurança: um desafio da Governação Eletrónica Cybersecurity: a challenge of a Digital Government*.

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

Ruel, E., Wagner III, W. E., & Gillespie, B. J. (2016). *The Practice of Survey Research: Theory and Applications*. SAGE Publications, Inc. https://doi.org/10.4135/9781483391700

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security*, *26*(1), 56–62. https://doi.org/https://doi.org/10.1016/j.cose.2006.10.008

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'-a human/computer interaction approach to usable and effective security. Em *BT Technol J* (Vol. 19).

Schein, E. H. (2010). *Organizational culture and leadership* (4th ed). Jossey-Bass. https://proxybiblio.uqo.ca:2443/sso/skillport?context=36500

Slade, E. L., Dwivedi, Y. K., Piercy, N. C., & Williams, M. D. (2015). Modeling Consumers' Adoption Intentions of Remote Mobile Payments in the United Kingdom: Extending UTAUT with Innovativeness, Risk, and Trust. *Psychology and Marketing*, *32*(8), 860–873. https://doi.org/10.1002/mar.20823

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and Security*, *56*, 70–82. https://doi.org/10.1016/j.cose.2015.10.006

Tribunal de Contas Europeu. (2019). *Challenges to effective EU cybersecurity policy Briefing Paper*.

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, *39*(2), 273–315. https://doi.org/10.1111/j.1540-5915.2008.00192.x

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425–478. https://doi.org/10.2307/30036540

Venkatesh, V., Walton, S. M., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the Unified Theory of Acceptance and Use of Technology. Em *MIS Quarterly* (Vol. 36, Número 1). http://ssrn.com/abstract=2002388

Wong, C., & Fai, Y. (2022). *The Impacts of Cybersecurity Awareness Training to Seafarers on the Likelihood of IT/OT Intrusions onboard a Vessel*. https://www.researchgate.net/publication/364339446

9. Anexo A – Questionário aplicado

O presente questionário foi elaborado para recolher informação junto dos colaboradores do setor público português sobre a perceção e intenção de utilização da Autenticação Multifator (MFA). Inclui perguntas de escolha múltipla e itens avaliados em escala de Likert de 5 pontos (1 = Discordo totalmente; 5 = Concordo totalmente).

9.1. Dados sociodemográficos

1. Qual é a sua idade?
    - 18–20 anos
    - 21–29 anos
    - 30–39 anos
    - 40–49 anos
    - 50–59 anos
    - 60 ou mais anos
    - Prefiro não dizer
2. Qual o nível de escolaridade mais alto que concluiu ou o diploma mais alto que recebeu?
    - Ensino básico
    - Ensino secundário
    - Ensino secundário
    - Prefiro não dizer
3. Já alguma vez recebeu formação em cibersegurança?
    - Sim
    - Não
4. A formação em que participou foi há quanto tempo?
    - Nos últimos 6 meses
    - Entre 6 e 12 meses
    - Há mais de 12 meses

9.2. Conhecimento e utilização de MFA

1. Considerando a listagem abaixo, assinale por favor quais os sistemas de segundo fator de autenticação que conhece ou já ouviu falar, mesmo que seja só pelo nome.
    a. Código SMS/e-mail
    b. Voz
    c. Reconhecimento facial
    d. Impressão digital
    e. Token físico (pen USB, cartão de cidadão, etc.)
    f. Aplicação móvel (autenticador, etc.)
2. Atualmente utiliza alguns destes sistemas de segundo fator de autenticação? (por cada método de autenticação na lista)
    a. Sim
    b. Não

9.3. Perceções sobre MFA (escala likert 1-5)

1. Os sistemas de segundo fator de autenticação na seguinte listagem seriam de muita utilidade no meu trabalho.
2. O uso dos sistemas de segundo fator de autenticação na seguinte listagem leva a um acréscimo na minha produtividade.
3. Seria fácil para mim tornar-me um(a) utilizador(a) hábil dos sistemas de segundo fator de autenticação na seguinte listagem.
4. Eu iria achar a utilização muito simples dos sistemas de segundo fator de autenticação na seguinte listagem.
5. De acordo com as pessoas que são importantes para mim, eu deveria usar os sistemas de segundo fator de autenticação na seguinte listagem.
6. Os líderes da instituição onde trabalho têm sido úteis na utilização dos sistemas de segundo fator de autenticação na seguinte listagem.
7. Tenho tudo o que necessito para operar os sistemas de segundo fator de autenticação na seguinte listagem.
8. Tenho conhecimentos suficientes para operar os sistemas de segundo fator de autenticação na seguinte listagem.

9. Mesmo sem ajuda eu conseguiria completar um trabalho ou uma tarefa usando os sistemas de segundo fator de autenticação na seguinte listagem.
10. Se eu pudesse contactar alguém para ajudar em caso de problemas, eu conseguiria completar um trabalho ou uma tarefa usando os sistemas de segundo fator de autenticação.
11. Usar os sistemas de segundo fator de autenticação na seguinte listagem deixa-me nervoso(a).
12. Tenho receio de usar os sistemas de segundo fator de autenticação na seguinte listagem, pois em caso de erro não tenho como emendar.
13. Tenciono utilizar os sistemas de segundo fator de autenticação na seguinte listagem nos próximos 12 meses.