SecureAccess — Implementação e Avaliação de um Sistema de Autenticação Multifator (MFA)

1st Miguel Bento
Nº101018
ISCTE
mvboe1@iscte-iul.pt

2nd Luís Lourenço
Nº110942
ISCTE
lcmlo@iscte-iul.pt

3rd Ricardo Ourelo
Nº120141
ISCTE
rcooo2@iscte-iul.pt

4th Josué da Glória
Nº134449
ISCTE
jlgas@iscte-iul.pt

***Resumo*—Este trabalho propõe o desenvolvimento de um sistema de Autenticação Multifator (MFA) destinado a reforçar a segurança de processos de login em aplicações web. Pretende-se demonstrar, através de um protótipo funcional implementado em *Flask (Python)*, como a combinação de fatores de autenticação ("algo que o utilizador sabe" e "algo que o utilizador tem") pode mitigar ataques baseados no roubo de credenciais. Para além da vertente prática, o projeto inclui uma revisão sistemática da literatura que identifica as principais abordagens, desafios e boas práticas na adoção de MFA em sistemas de informação. Assim, o objetivo é proporcionar uma visão integrada entre a teoria e a prática, evidenciando que a MFA é uma solução eficaz, acessível e crucial para o aumento da resiliência em segurança digital.**

Palavras-chave: autenticação, multifator, login, segurança, cibersegurança

GLOSSÁRIO

Sigla	Descrição
AALs	Authenticator Assurance Levels
AI	Artificial Intelligence
BLE	Bluetooth Low Energy
CCS	Conference on Computer and Communications Security
EU	European Union
ENISA	European Union Agency for Cybersecurity
FIDO2	Fast Identity Online 2
GDPR	General Data Protection Regulation
ISO/IEC	International Organization for Standardization /
27001	International Electrotechnical Commission 27001
MFA	Multi-Factor Authentication
ML	Machine Learning
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
PIPOC	Population Intervention Comparison Outcome Context
RSL	Systematic Literature Review
SIM	Subscriber Identity Module
SMS	Short Message Service
SP	Special Publication
TOTP	Time-based One-Time Password
WebAuthn	Web Authentication API
2FA	Two-Factor Authentication

I. INTRODUÇÃO

A. Contextualização e Motivação

Nos sistemas de informação modernos, a autenticação de utilizadores constitui um dos pilares fundamentais da segurança. Apesar dos avanços em criptografia, deteção de intrusões e proteção de redes, a maioria dos incidentes de segurança continua a ocorrer devido ao uso indevido ou comprometimento de credenciais. Diversos estudos indicam que mais de 80% das violações de segurança resultam do uso de palavras-passe fracas, reutilizadas ou obtidas através de técnicas de phishing [10]. Como sublinham Tran-Truong, Nguyen e Ngo [10], "a maioria dos incidentes de segurança em sistemas de pagamento digital ainda decorre de palavras-passe fracas ou reutilizadas e ataques de engenharia social, como phishing" (p. 2).

A autenticação multifator surge como uma resposta eficaz a esta vulnerabilidade, combinando diferentes categorias de fatores — algo que o utilizador sabe (ex.: palavra-passe), algo que o utilizador tem (ex.: token ou smartphone) e algo que o utilizador é (ex.: biometria). Segundo o NIST Special Publication 800-63B [9], a utilização de múltiplos fatores de autenticação permite atingir níveis superiores de garantia (Authenticator Assurance Levels – AALs) e reduzir de forma significativa o risco de acesso não autorizado, mesmo que um dos fatores seja comprometido.

A literatura académica mais recente reforça esta perspetiva, salientando que a MFA é atualmente uma das práticas mais eficazes e escaláveis de mitigação de riscos em ambientes digitais. No entanto, a sua adoção ainda enfrenta diversos desafios relacionados com usabilidade, custos de implementação e resistência dos utilizadores [10]. Estes fatores assumem particular relevância em contextos empresariais e financeiros, onde a segurança deve ser equilibrada com a conveniência e a experiência de utilização. Assim, compreender as abordagens, benefícios e limitações associadas à MFA é fundamental para conceber sistemas de autenticação mais seguros, confiáveis e adaptáveis à realidade tecnológica atual.

B. Visão Produto

O projeto, intitulado *SecureAccess – Autenticação Multifator (MFA)*, visa demonstrar e analisar a eficácia do MFA enquanto mecanismo de reforço da segurança em sistemas de autenticação web.

A visão central consiste em articular uma revisão sistemática da literatura com o desenvolvimento de um protótipo funcional em Flask (Python), demonstrando na prática a eficácia da MFA baseada em palavra-passe e código TOTP.

Desta forma, o projeto procura demonstrar, de forma concreta, como a combinação dos dois fatores referidos anteriormente aumenta substancialmente a resiliência de um sistema face a ataques comuns como *credential stuffing*, *phishing* ou *brute-force*.

C. Objetivos

Objetivo Geral

Desenvolver, analisar e demonstrar um sistema de autenticação multifator (MFA) que evidencie as vantagens de segurança face à autenticação tradicional baseada apenas em palavra-passe.

Objetivos Específicos

- Realizar uma revisão sistemática da literatura sobre MFA, identificando os principais métodos, desafios e boas práticas descritos em publicações académicas recentes;
- Implementar um protótipo funcional de autenticação com palavra-passe + TOTP (Time-based One-Time Password) utilizando Flask;
- Avaliar e discutir a eficácia e usabilidade da solução desenvolvida, relacionando-a com as conclusões da revisão teórica;
- Comparar o desempenho e a usabilidade do sistema MFA desenvolvido com modelos de autenticação tradicionais;
- Propor melhorias futuras e medidas complementares, como a integração de chaves FIDO2/WebAuthn ou autenticação biométrica.

D. Metodologia

A metodologia do projeto divide-se em duas vertentes complementares:

- **Vertente teórica:** Aplicação do protocolo de Revisão Sistemática da Literatura (RSL) fornecido pelo docente, com definição de perguntas de pesquisa, *string* de busca, critérios de inclusão/exclusão e análise de artigos obtidos em bases académicas (Scopus, IEEE Xplore, ScienceDirect e ACM Digital Library);
- **Vertente prática:** Desenvolvimento de um protótipo em Flask que implementa MFA com TOTP, demonstrando o fluxo de autenticação em duas etapas. O código foi documentado e testado de forma a ilustrar o funcionamento do segundo fator e o impacto na segurança do *login*.

Esta abordagem combinada permite uma ligação direta entre a teoria (estado da arte) e a prática (aplicação real), oferecendo uma visão holística da eficácia e aplicabilidade da MFA.

II. Metodologia da Revisão Sistemática

A. Enquadramento e Finalidade da Revisão Sistemática

A Revisão Sistemática da Literatura (RSL) tem como finalidade identificar, analisar e sintetizar as principais contribuições científicas sobre a autenticação multifator, com foco nos métodos, desafios, benefícios e tendências de implementação.

O objetivo central é compreender o estado da arte nesta área, fornecendo uma base teórica sólida que sustenta o desenvolvimento do SecureAccess, alinhando-o com as normas internacionais de segurança digital [9].

De acordo com o protocolo adotado, a revisão seguiu um processo estruturado que incluiu a definição de perguntas, a aplicação de critérios de inclusão e exclusão e, por fim, a extração e análise dos dados relevantes.

Deste modo, esta revisão procura responder às questões de investigação definidas, mapear o conhecimento existente e identificar lacunas propondo linhas de evolução aplicáveis ao projeto SecureAccess.

B. Questões de Investigação e Orientação Metodológica

Pergunta 1: Quais são as principais técnicas e fatores utilizados em MFA (ex.: TOTP, SMS, biometria, FIDO2)?

Pergunta 2: Quais são os métodos e fatores de autenticação mais eficazes descritos na literatura científica e como podem ser aplicados em sistemas web modernos?

Pergunta 3: De que forma a implementação de um segundo fator TOTP (Time-based One-Time Password) melhora a segurança de um sistema de login tradicional baseado em palavra-passe?

C. Estratégia de Pesquisa e Fontes de Informação Científica

A estratégia de pesquisa seguiu as etapas definidas pelo protocolo de Revisão Sistemática da Literatura, com base no modelo PIPOC (Population, Intervention, Comparison, Outcome e Context).

Neste caso, a população corresponde aos utilizadores e sistemas de autenticação digital, a intervenção é a utilização da MFA, a comparação é feita face à autenticação de fator único (SFA), o resultado esperado é a melhoria da segurança e da usabilidade, e o contexto refere-se a aplicações e sistemas web.

Após a recolha, os resultados foram filtrados por título e resumo e posteriormente analisados integralmente, segundo a técnica Three-Pass Reading [6], para garantir uma avaliação rigorosa e consistente da relevância de cada estudo.

A seleção final incluiu artigos que descreviam metodologias de MFA, comparações entre abordagens, desafios de usabilidade e aplicações em contextos reais.

D. Ferramentas de Apoio e Gestão Bibliográfica

Para garantir a organização e o rastreio do processo de revisão, foram utilizadas diversas ferramentas de apoio técnico e bibliográfico.

A gestão das referências e das citações foi realizada através da plataforma Mendeley, permitindo normalizar automaticamente as referências no formato IEEE e inserir citações numéricas de forma uniforme ao longo do relatório.

Para a pesquisa e recolha dos vários artigos utilizados para a realização deste relatório foram utilizadas ferramentas académicas como o Google Scholar, Scopus e Web of Science que facilitaram o acesso completo a artigos e verificação cruzada de citações.

Estas ferramentas contribuíram de forma significativa para assegurar a transparência e a consistência metodológica da Revisão Sistemática da Literatura desenvolvida ao longo deste relatório.

III. Estado da Arte

Nos últimos anos, a MFA evoluiu para modelos mais dinâmicos e contextuais, impulsionados pelo avanço da inteligência artificial, do *machine learning* e das tecnologias móveis. Um exemplo relevante desta tendência é o trabalho de Aburbeian e Fernández-Veiga [1], que propuseram um *framework* de autenticação adaptativa para transações financeiras online, combinando MFA com algoritmos de *machine learning* para avaliar o risco de cada operação. Quando o sistema deteta comportamentos suspeitos, solicita fatores adicionais de autenticação. Este modelo reduz a fadiga do utilizador e ilustra a transição de uma MFA estática para uma abordagem baseada em risco, ajustando o nível de segurança ao contexto.

Ainda no domínio da segurança de acesso, Amft et al. [3] conduziram um estudo extensivo sobre os mecanismos de recuperação de contas em sistemas com MFA, analisando mais de 1.300 serviços online. Os autores concluíram que, apesar de a MFA fortalecer o acesso inicial, muitos sistemas falham em garantir segurança durante o processo de recuperação, permitindo contornar a autenticação reforçada através de procedimentos pouco rigorosos. Este estudo chama a atenção para a importância de conceber fluxos de recuperação que mantenham a integridade do processo de autenticação, evitando vulnerabilidades humanas e técnicas.

Outro contributo relevante surge da revisão sistemática de Podapati, Nigam e Das [7], que sintetiza o estado da arte em autenticação adaptativa e contínua em ambientes móveis. Os autores destacam o papel crescente da análise comportamental e contextual, como padrões de utilização, localização e sensores do dispositivo, na criação de sistemas de autenticação inteligentes e não intrusivos. Esta perspetiva reforça a tendência para a "autenticação invisível", em que o sistema avalia continuamente o risco sem exigir múltiplas interações explícitas do utilizador.

Por sua vez, Shukla, Varshney, Singh e Goel [8] exploraram uma abordagem *passwordless*, combinando biometria facial, proximidade física e comunicação *contactless* (NFC/BLE) para autenticação em dispositivos Android. O estudo demonstra que eliminar o fator de conhecimento (a palavra-passe) pode simplificar a experiência do utilizador e reduzir vulnerabilidades associadas à gestão de credenciais. Contudo, os autores alertam para os riscos de spoofing biométrico e para a necessidade de hardware compatível, fatores que ainda limitam a adoção generalizada deste modelo.

A. Tipos de Autenticação MFA

Dependendo da combinação de fatores de autenticação escolhidos, a MFA pode assumir diferentes formas. Por exemplo, a diretriz NIST SP 800-63B-4 [9] define três tipos principais de fatores: conhecimento (algo que o utilizador sabe), posse (algo que o utilizador tem) e inerência (algo que o utilizador é), conforme ilustrado na Figura 1.

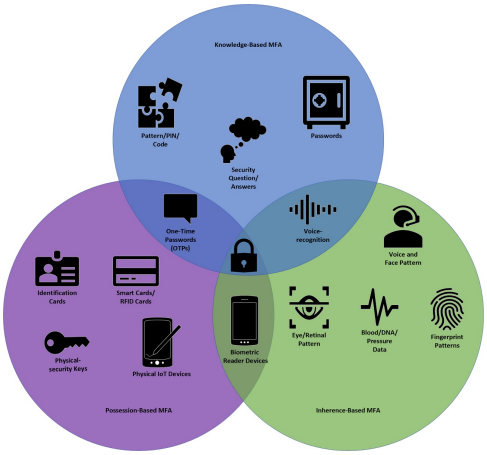

Figura 1. Diagrama Venn dos fatores em MFA.
Nota. Adaptado de *A review of multi-factor authentication in the Internet of Healthcare Things*, por T. Suleski, M. Ahmed, W. Yang e E. Wang, 2023, *Digital Health*, 9. https://journals.sagepub.com/doi/full/10.1177/20552076231177144.

A forma mais utilizada de MFA é conhecida como Autenticação de Dois Fatores (2FA), uma combinação de dois fatores diferentes. Normalmente, este modelo integra um fator de conhecimento, como uma senha ou PIN, com fatores de posse, como um código temporário enviado por SMS ou gerado por um aplicativo autenticador (TOTP) [5].

A Autenticação de Três Fatores (3FA) introduz um terceiro fator, normalmente considerado um fator inerente, como biometria (impressão digital, rosto, íris ou voz). Apesar de melhorar significativamente a segurança, este método é mais complexo em termos de tecnologia e custos de implementação [9].

A Autenticação Adaptativa (*Adaptive Authentication*), por outro lado, é mais dinâmica, pois ajusta os fatores necessários de acordo com o contexto de um utilizador. Podem existir variações como localização, endereço IP, dispositivo utilizado ou tempo de acesso, que afetam a necessidade de um fator adicional. Consideramos que este é o melhor compromisso entre segurança e o utilizador, e encontramos isso em muitos tipos de empresas para oferecer ainda mais segurança sem limitar a facilidade de uso das ferramentas [4].

Por fim, a Autenticação sem palavra-passe (*Passwordless MFA*) é um modelo emergente, substituindo a palavra-passe por combinações mais seguras de fatores, incluindo biometria e tokens criptográficos. Este tipo de dispositivo é promovido por empresas como Microsoft e Google, reduz bastante o risco

que as palavras-passe representam e oferece aos utilizadores uma experiência de utilização mais eficiente [5].

Estes vários métodos de MFA mostram toda a gama que existe quando se trata de avançar na segurança digital. A seleção de um modelo apropriado varia dependendo do contexto de aplicação, nível de segurança exigido, bem como recursos [9].

Segundo dados recolhidos pela Statista, a aplicação de MFA nas empresas evidencia uma preferência clara por soluções baseadas em aplicações autenticadoras (57,8%), seguidas por códigos SMS (39,1%) e palavras-passe temporárias (OTP) (37,4%). Métodos baseados em hardware, como chaves de segurança físicas, representam cerca de 30% da adoção, enquanto o uso de endereços de e-mail secundários é menos comum (14,7%). Estes resultados demonstram que, embora a diversidade de métodos continue a crescer, existe uma tendência clara para o uso de tecnologias móveis e aplicações autenticadoras, que equilibram segurança e conveniência de utilização [11].

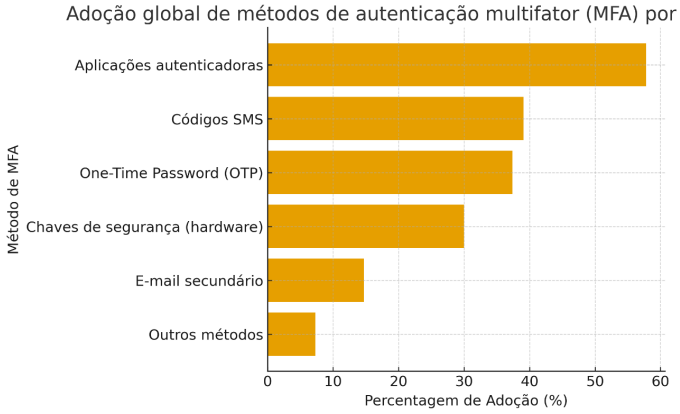

Figura 2. Adoção global de métodos de MFA
Nota. Adaptado de Statista, 2021, conforme citado em Scoop Market.us, 2025.
https://scoop.market.us/multi-factor-authentication-statistics

B. Comparação entre MFA e Autenticação de Um Único Fator

A Autenticação de Fator Único (SFA) é um método que utiliza apenas um tipo de verificação, geralmente uma palavra-passe. Esta abordagem é simples e económica, o que a torna popular em diversos contextos. No entanto, as suas falhas de segurança são amplamente conhecidas. Técnicas como *phishing*, reutilização de palavras-passe e ataques de força bruta podem ser facilmente exploradas para obter acesso não autorizado, comprometendo a segurança de forma significativa [9].

Para ilustrar a vantagem matemática da MFA face à autenticação tradicional, podemos estimar o tempo necessário para quebrar uma palavra-passe por força bruta.

Equação 1 - Tempo Médio de Quebra por Força Bruta

$$T = \frac{N^L}{2R} \tag{1}$$

onde:

- N é o número de símbolos possíveis;
- L é o comprimento da palavra-passe;
- R é o número de tentativas por segundo;
- o fator $\frac{1}{2}$ reflete o valor médio esperado antes do sucesso.

Por exemplo, para uma palavra-passe com $N = 62$ (maiúsculas, minúsculas e dígitos), $L = 10$ e um atacante capaz de testar $R = 10^9$ combinações por segundo:

$$T = \frac{62^{10}}{2 \times 10^9} \approx 4.8 \times 10^7 \text{ segundos} \approx 1.5 \text{ anos.}$$

A adição de um segundo fator TOTP torna este cenário impraticável, pois a validade do código expira em segundos, impossibilitando ataques de tentativa massiva.

A força de uma palavra-passe pode ser medida pela sua entropia, que quantifica o número médio de bits de informação ou a imprevisibilidade associada à sua composição. A fórmula é dada por:

Equação 2 – Entropia de uma palavra-passe

$$H = \log_2(N^L) \tag{2}$$

onde:

- H é a entropia total (em bits);
- N é o número de símbolos possíveis (por exemplo, 62 para letras maiúsculas, minúsculas e dígitos);
- L é o comprimento da palavra-passe.

Por exemplo, uma palavra-passe de 8 caracteres com 62 símbolos possíveis tem:

$$H = \log_2(62^8) \approx 47.6 \text{ bits}$$

correspondendo a aproximadamente 2.18×10^{14} combinações possíveis. Aumentando o comprimento, obtêm-se valores exponencialmente superiores, conforme apresentado na Tabela I abaixo.

Tabela I
ENTROPIA E TEMPO MÉDIO DE QUEBRA PARA DIFERENTES COMPRIMENTOS DE PALAVRA-PASSE

Comprimento (L)	Entropia (H)	Combinações possíveis	Tempo médio (10^9 tent./s)
8	47,6 bits	2.18×10^{14}	$\approx 1,26$ dias
12	71,4 bits	3.23×10^{21}	$\approx 51\,117$ anos
16	95,3 bits	4.77×10^{28}	$\approx 7.55 \times 10^{11}$ anos

Estes resultados demonstram que o aumento do comprimento da palavra-passe melhora exponencialmente a segurança, tornando ataques de força bruta cada vez mais inviáveis. No entanto, a autenticação baseada num só fator continua vulnerável a diversos vetores, como ataques de dicionário, reutilização de credenciais, *phishing* ou fugas de dados.

Mesmo uma palavra-passe de 16 caracteres exigiria, em média, centenas de mil milhões de anos para ser quebrada por força bruta a 10^9 tentativas por segundo, mas ataques mais sofisticados, como os de dicionário — que exploram

combinações comuns, padrões previsíveis e palavras reais — podem reduzir drasticamente o tempo necessário para comprometer uma conta. Além disso, bastaria um vazamento ou ataque de engenharia social para expor as credenciais.

A autenticação multifator traz um nível adicional de proteção ao exigir pelo menos dois tipos diferentes de verificação, que podem envolver algo que o utilizador sabe, algo que o utilizador possui ou características pessoais, conforme ilustrado na Figura 3. Esta estratégia cria camadas de defesa, tornando muito mais difícil para um invasor obter acesso ao sistema, uma vez que seria necessário comprometer múltiplos fatores independentes [9].

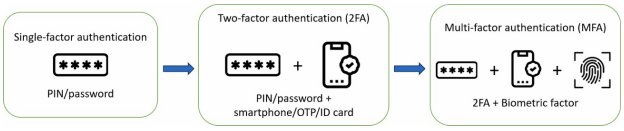

Figura 3. Tipos de autenticação. Adaptado de Tran-Truong et al. [10].

Embora a MFA exija um pouco mais de complexidade e investimento na implementação, proporciona um nível de segurança significativamente superior e é recomendada por entidades de referência como o NIST e a ENISA. Além disso, a MFA auxilia no cumprimento de exigências normativas como o GDPR, a ISO/IEC 27001 e a Diretiva PSD2, que incluem requisitos para autenticação reforçada [5].

C. TOTP

O algoritmo TOTP (*Time-based One-Time Password*) é um dos métodos mais comuns na autenticação de dois fatores. Baseia-se na geração de um código numérico temporário que muda a cada intervalo de tempo pré-definido, garantindo que o código só é válido por alguns segundos. O seu funcionamento é descrito matematicamente pela fórmula geral:

Equação 3 – Geração do código TOTP (RFC 6238)

$$\text{TOTP} = \text{Truncate}(\text{HMAC-SHA1}(K, T)) \tag{3}$$

onde:

- K é a chave secreta partilhada entre o servidor e o utilizador;
- HMAC-SHA1 é a função de autenticação por hash baseada em chave;
- T é o contador de tempo, calculado como:

$$T = \left\lfloor \frac{t - T_0}{X} \right\rfloor \tag{4}$$

sendo t o tempo atual (em segundos), T_0 o tempo inicial (*epoch*) e X o intervalo de validade (tipicamente 30 segundos).

O resultado é truncado e convertido num código numérico de seis dígitos, usado como segundo fator de autenticação. Esta abordagem é amplamente adotada em sistemas como o Google Authenticator e o Microsoft Authenticator devido à sua fiabilidade e independência de conectividade.

1) Robustez Matemática e Probabilidade de Colisão: A segurança do TOTP assenta na imprevisibilidade dos valores gerados. A probabilidade de um atacante adivinhar corretamente um código TOTP de seis dígitos é dada por:

Equação 4 – Probabilidade de acerto de um código TOTP

$$P_{TOTP} = \frac{1}{10^6} = 10^{-6} \tag{5}$$

Esta probabilidade é extremamente reduzida, e o código é temporário. Quando combinado com a autenticação por palavra-passe, resulta numa segurança composta, conforme já indicado na Equação (1). Assim, o modelo MFA baseado em TOTP aumenta a resiliência exponencial do sistema contra ataques de força bruta.

D. Vantagens da MFA

A MFA apresenta benefícios significativos, entre os quais se destaca o grande aprimoramento da segurança dos sistemas de informação. Mesmo que um fator seja comprometido, o atacante teria de contornar outro(s) fator(es) para obter acesso, reduzindo substancialmente a probabilidade de acesso não autorizado [9].

Matematicamente, a probabilidade de um atacante conseguir acesso indevido quando existem múltiplos fatores de autenticação é dada pela multiplicação das probabilidades de sucesso em cada fator individual:

Equação 5 – Probabilidade de acesso não autorizado com MFA

$$P_{MFA} = \prod_{i=1}^{n} P_i \tag{6}$$

onde:

- P_i representa a probabilidade de comprometer o i-ésimo fator de autenticação;
- n é o número total de fatores utilizados.

Por exemplo, se a probabilidade de adivinhar uma palavra-passe for $P_1 = 10^{-6}$ e a de violar um código TOTP for $P_2 = 10^{-3}$, o sistema multifator teria $P_{MFA} = 10^{-9}$. Este valor ilustra o aumento exponencial da segurança quando são usados fatores independentes.

Além disso, a MFA é reconhecida como um mecanismo essencial na proteção da identidade digital e dos dados pessoais, tanto na legislação da União Europeia (por exemplo, GDPR) quanto em normas internacionais como a ISO/IEC 27001. De acordo com Alves, Maia e Silva [2], a MFA é uma ferramenta indispensável na proteção contra ameaças de invasão e ataques de força bruta. Apesar de introduzir algum incómodo adicional aos utilizadores, os benefícios em termos de segurança são inegáveis, justificando a ampla adoção da MFA por instituições financeiras.

A validação da capacidade do sistema em utilizar mecanismos de autenticação avançados contribui ainda para a credibilidade e reputação das organizações, garantindo uma vantagem competitiva no mercado [4], [5].

E. Desafios da MFA

Embora os aspetos positivos acompanhem a adoção do MFA, eles também trazem responsabilidades técnicas e operacionais. A principal barreira é a complexidade técnica da sua execução, especialmente se o MFA for adicionado a sistemas antigos ou incorporado num programa existente, o que introduz mais modificações.

O custo extra é outro dos desafios deste mecanismo, uma vez que aplicações de MFA podem necessitar de licenças, compra de hardware ou software, e recurso humano para suporte e manutenção [9].

O MFA também pode afetar a experiência do utilizador, uma vez que etapas adicionais no processo de autenticação podem resultar em frustração ou atrasos no acesso, sobretudo se os fatores a considerar não forem devidamente integrados no fluxo de utilização [5].

A dependência tecnológica é outro obstáculo, pois a perda ou indisponibilidade do dispositivo autenticador pode impedir o acesso legítimo. Por último, embora o MFA seja muito eficaz, tende a estar sujeito a métodos de ataque mais avançados, como *SIM swapping* (troca de cartão SIM) e ataques *man-in-the-middle*, pelo que deve ser combinada com outras medidas complementares de segurança [9].

F. Síntese Crítica

A análise dos trabalhos revistos permite identificar várias tendências convergentes. Em primeiro lugar, observa-se uma clara evolução da MFA tradicional para modelos adaptativos e contextuais, nos quais o número e o tipo de fatores dependem do nível de risco identificado. Esta abordagem, discutida por Aburbeian e Fernández-Veiga [1] e Podapati et al. [7], representa um equilíbrio entre segurança e conveniência, reduzindo o esforço imposto ao utilizador sem comprometer a proteção.

Em segundo lugar, destaca-se a crescente preocupação com a usabilidade e os mecanismos de recuperação de acesso. O estudo de Amft et al. [3] mostra que a segurança global de um sistema não depende apenas da robustez técnica, mas também da coerência dos processos de suporte e gestão de falhas. Para um projeto como o *SecureAccess*, isto significa que a conceção de um sistema MFA deve incluir mecanismos de recuperação seguros e intuitivos, evitando vulnerabilidades decorrentes do comportamento humano.

Por outro lado, a tendência para autenticação sem palavra-passe (*passwordless*) representa o próximo passo evolutivo da MFA. Tal como demonstrado por Shukla et al. [8], o abandono do fator de conhecimento tradicional (palavra-passe) em favor de biometria e tokens criptográficos pode oferecer uma experiência mais fluida e reduzir significativamente o risco de *phishing*. Contudo, estas soluções ainda enfrentam desafios técnicos e económicos, nomeadamente na compatibilidade de hardware e no tratamento seguro de dados biométricos.

G. Implicações para o Projeto SecureAccess

A síntese da literatura recente sustenta a relevância do enfoque adotado neste projeto. A escolha de um modelo baseado em palavra-passe + TOTP surge como uma solução equilibrada entre viabilidade técnica, segurança e usabilidade, especialmente adequada para um protótipo académico. Esta combinação permite demonstrar, de forma prática, os benefícios concretos da MFA em contextos web, mantendo simultaneamente uma complexidade de implementação acessível.

Além disso, as conclusões dos estudos analisados orientam possíveis evoluções do sistema, como a integração de autenticação adaptativa ou de métodos biométricos complementares, ampliando o alcance e a robustez da solução. Assim, o estado da arte confirma que a MFA não é apenas uma camada adicional de proteção, mas um componente essencial de arquiteturas modernas de identidade digital, devendo ser integrada de forma coerente com políticas de segurança e experiência de utilizador.

IV. Discussão

A análise da literatura científica sobre autenticação multifator evidencia um consenso generalizado quanto à sua importância no fortalecimento da segurança digital. As fontes consultadas, nomeadamente [9], [10], [1] e [7], reforçam a ideia de que o uso de múltiplos fatores de autenticação representa um avanço fundamental na mitigação de ataques baseados em roubo de credenciais, phishing e engenharia social. No entanto, esta mesma literatura aponta que a adoção da MFA continua a enfrentar desafios significativos relacionados com custos de implementação, integração técnica e, sobretudo, usabilidade.

Com base nas conclusões obtidas na revisão sistemática da literatura, o projeto *SecureAccess* propõe-se a desenvolver um sistema de autenticação multifator aplicável a contextos web, que combine dois fatores distintos: um fator de conhecimento (palavra-passe) e um fator de posse, baseado em códigos temporários gerados por um algoritmo TOTP. A escolha desta abordagem resulta da sua elevada eficácia e simplicidade de integração, sendo atualmente uma das soluções mais utilizadas e recomendadas em ambientes empresariais e académicos [4], [5].

Pretende-se, com a futura implementação do protótipo em Flask, demonstrar de forma prática os benefícios da MFA face ao modelo tradicional de autenticação de um único fator. Espera-se que a utilização de um segundo fator reduza substancialmente a probabilidade de sucesso de ataques de força bruta ou de reutilização de credenciais, aumentando a confiança e a robustez do processo de login. Além disso, será avaliado o impacto que esta medida tem na experiência do utilizador — questão amplamente debatida por [3], que destacam a necessidade de equilibrar segurança e conveniência em sistemas MFA.

Outro objetivo importante da fase prática será testar a escalabilidade e a adaptabilidade da solução, analisando a sua viabilidade para integração com outras tecnologias, como autenticação biométrica ou chaves criptográficas FIDO2/WebAuthn. Estes mecanismos representam o próximo passo evolutivo da MFA, oferecendo níveis superiores de

segurança e reduzindo a dependência das palavras-passe, frequentemente identificadas como o elo mais fraco dos sistemas de autenticação [9].

Em síntese, esta discussão permite antecipar que o projeto *SecureAccess* poderá contribuir para demonstrar, num contexto académico e prático, como a implementação de MFA pode ser feita de forma acessível, eficaz e alinhada com as normas internacionais de segurança. A expectativa é que o projeto *SecureAccess* evidencie uma redução significativa do risco de acesso não autorizado e que os resultados da fase seguinte confirmem as vantagens apontadas pela literatura, reforçando o papel da autenticação multifator como elemento indispensável na proteção de sistemas web e na promoção de uma cultura digital mais segura.

A. *Representação Visual e Mockups do Protótipo*

Para complementar a componente teórica e demonstrar o funcionamento prático do sistema desenvolvido, foram criados *mockups* representativos das principais interfaces do protótipo *SecureAccess*.

Estes *mockups*, elaborados no Figma, ilustram o fluxo de interação do utilizador com o sistema, desde o registo até à autenticação multifator (MFA), evidenciando o equilíbrio entre segurança e usabilidade.

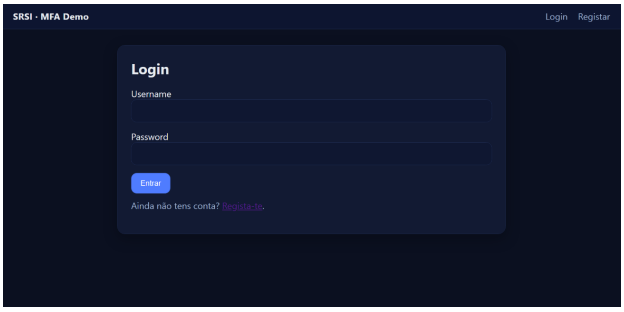

Figura 4. Ecrã inicial de login

1) Ecrã Inicial de Login: Após a autenticação primária, o sistema redireciona o utilizador para a fase de verificação do segundo fator (TOTP). Este design foi concebido com uma interface simples e intuitiva, de modo a minimizar erros de introdução e otimizar a experiência de utilização.

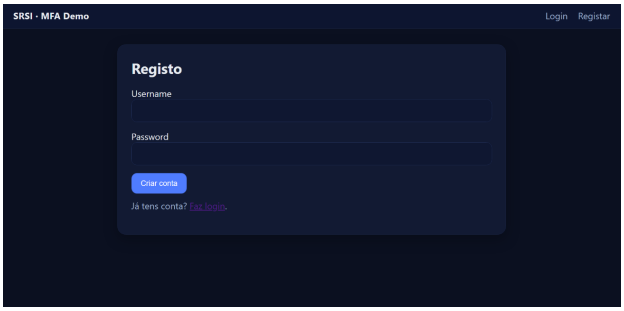

Figura 5. Ecrã de registo de utilizador

2) Ecrã de Registo: O ecrã de registo permite a criação de novos utilizadores, armazenando as credenciais na base de dados SQLite. Após o registo, o sistema solicita a ativação da MFA, em conformidade com as recomendações da norma NIST SP 800-63B [9].

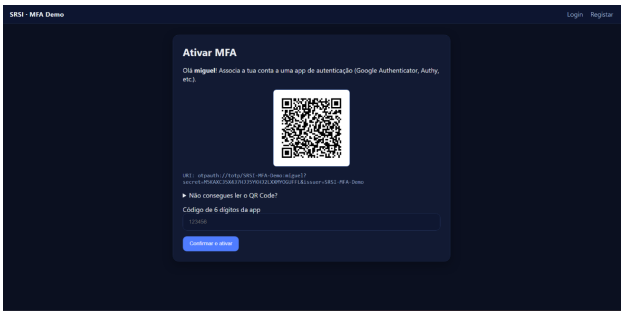

Figura 6. Ecrã de configuração do MFA (QR Code)

3) Ecrã de Configuração do MFA (QR Code): Nesta interface, é apresentado um *QR Code* que contém a chave secreta associada ao utilizador. O código deve ser lido por uma aplicação autenticadora compatível (por exemplo, Google Authenticator ou Authy). Este passo garante a geração de códigos temporários TOTP com base em intervalos de 30 segundos, conforme definido na RFC 6238.

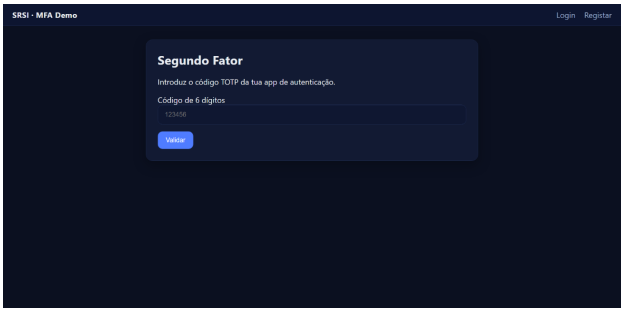

Figura 7. Ecrã de validação do código TOTP

4) Ecrã de Validação do Código TOTP: Nesta interface, o utilizador introduz o código temporário TOTP gerado pela aplicação autenticadora. O sistema verifica a validade do código e o associa ao utilizador autenticado, completando a segunda fase da autenticação.

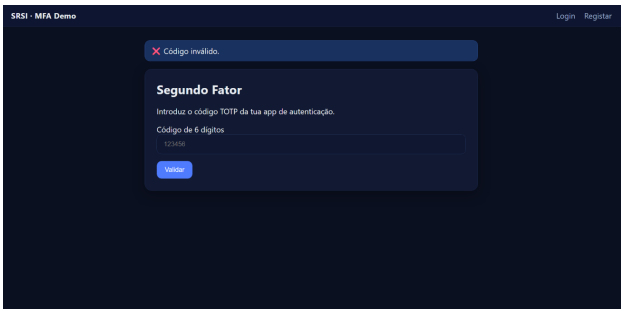

Figura 8. Ecrã de erro ou código inválido

5) Ecrã de Erro ou Código Inválido: Caso o código TOTP seja inválido ou expirado, o sistema apresenta uma mensagem

de erro clara, permitindo nova tentativa. Esta abordagem está alinhada com as boas práticas de usabilidade em segurança, evitando frustração e garantindo *feedback* imediato ao utilizador.

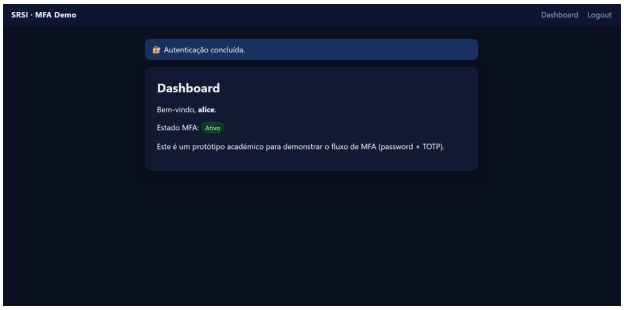

Figura 9. Ecrã de acesso concedido

6) Ecrã de Acesso Concedido: Em caso de sucesso na validação do TOTP, o utilizador é autenticado e redirecionado para o painel principal. A mensagem de sucesso e o design visual reforçam a perceção de confiança e de segurança, dois elementos fundamentais para a aceitação da MFA.

V. Conclusões

A investigação teórica desenvolvida no âmbito deste trabalho permitiu consolidar uma compreensão aprofundada sobre a importância da autenticação multifator na proteção de sistemas de informação. Através da revisão sistemática da literatura, verificou-se que a MFA é amplamente reconhecida como uma prática essencial na defesa contra ataques cibernéticos baseados em credenciais comprometidas, constituindo um pilar fundamental da segurança digital moderna [9].

Esta perspetiva é corroborada por estudos recentes [1], [7], [8] que evidenciam a evolução da MFA para modelos adaptativos e baseados em risco.

Os estudos analisados indicam que a combinação de diferentes fatores de autenticação — conhecimento, posse e inerência — oferece uma proteção significativamente mais robusta do que os sistemas baseados num único fator.

Entre as abordagens existentes, a autenticação com base em TOTP destaca-se pela sua simplicidade de implementação, compatibilidade com tecnologias existentes e eficácia comprovada na mitigação de ataques comuns, como *phishing* ou *credential stuffing* [4], [5].

A partir desta base teórica, o projeto *SecureAccess* propõe-se a desenvolver e avaliar um protótipo funcional de MFA que materialize as boas práticas identificadas na literatura. Na fase seguinte, será implementado o sistema em Flask, integrando autenticação por palavra-passe e código temporário TOTP, de modo a demonstrar de forma prática as vantagens e limitações deste modelo. Espera-se que os resultados confirmem as tendências observadas na revisão teórica, evidenciando melhorias substanciais em termos de segurança e resiliência sem comprometer de forma significativa a experiência do utilizador.

Para além da vertente técnica, o projeto procura também contribuir para a reflexão sobre a adoção sustentável de soluções de autenticação segura tanto em contextos académicos como empresariais. A MFA, quando bem concebida, não deve ser vista apenas como uma camada adicional de segurança, mas como parte integrante de uma estratégia global de gestão de identidades digitais.

Em suma, este relatório representa a primeira etapa de um trabalho mais amplo que combina investigação científica e aplicação prática. As conclusões aqui apresentadas servirão de base para a fase seguinte de desenvolvimento e avaliação experimental, onde será possível validar empiricamente os benefícios esperados e propor melhorias que possam aproximar ainda mais a MFA das necessidades reais dos utilizadores e das organizações.

VI. Trabalhos Futuros

A fase prática deste trabalho permitirá validar experimentalmente os conceitos discutidos na revisão teórica. O desenvolvimento do protótipo *SecureAccess* será realizado utilizando o *framework* Flask (Python), integrando autenticação por palavra-passe e código TOTP (*Time-based One-Time Password*).

Numa fase posterior, poderão ser exploradas as seguintes evoluções:

- Integração de métodos biométricos (impressão digital, reconhecimento facial ou voz);
- Suporte para chaves de segurança FIDO2/WebAuthn, reduzindo a dependência de palavras-passe;
- Autenticação adaptativa baseada em risco, ajustando dinamicamente os fatores exigidos conforme o contexto de login;
- Implementação de relatórios e métricas sobre tentativas de autenticação e falhas de login;
- Avaliação de desempenho e testes de usabilidade junto de utilizadores reais, para medir aceitação e conveniência.

Estas perspetivas de continuidade reforçam o potencial do projeto como base para investigação futura e aplicação prática em ambientes empresariais ou académicos.

De forma a desenvolver a componente prática do projeto, foi criado um repositório GitHub para hospedar o código-fonte, documentação e ficheiros de configuração do protótipo *SecureAccess*.

Repositório disponível em: https://github.com/ricardo-ourelo/SecureAccess

Referências

[1] A. H. M. Aburbeian and M. Fernández-Veiga, "Secure Internet Financial Transactions: A Framework Integrating Multi-Factor Authentication and Machine Learning,"*AI (Switzerland)*, vol. 5, no. 1, pp. 177–194, 2024. [Online]. Available: https://doi.org/10.3390/ai5010010

[2] V. F. Alves, M. V. da Silva, and T. de O. Maia, "O uso de autenticação multi-fator (MFA) e sua importância / The use of multi-factor authentication (MFA) and its importance,"in *Congresso de Segurança da Informação das Fatec*, 2023. [Online]. Available: https://fatecseg.fatecourinhos.edu.br/index.php/fatecseg/article/view/115/34

[3] S. Amft, S. Höltervennhoff, N. Huaman, A. Krause, L. Simko, Y. Acar, and S. Fahl, "'We've Disabled MFA for You': An Evaluation of the Security and Usability of Multi-Factor Authentication Recovery Deployments,"in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS 2023)*, pp. 3138–3152. [Online]. Available: https://doi.org/10.1145/3576915.3623180

[4] CISCO, "What is multi-factor authentication (MFA)?", 2025. [Online]. Available: https://www.cisco.com/site/us/en/learn/topics/security/what-is-multi-factor-authentication-mfa.html#tabs-35d568e0ff-item-4bd7dc8124-tab

[5] Microsoft Entra, "Microsoft Entra authentication documentation,"2025. [Online]. Available: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mfa-howitworks

[6] S. Keshav and D. R. Cheriton, "How to Read a Paper,"2007. [Online]. Available: http://ccr.sigcomm.org/online/files/p83-keshavA.pdf

[7] V. H. Podapati, D. Nigam, and S. Das, "SoK: A Systematic Review of Context- and Behavior-Aware Adaptive Authentication in Mobile Environments,"2025. [Online]. Available: http://arxiv.org/abs/2507.21101

[8] S. Shukla, G. Varshney, S. Singh, and S. Goel, "A Passwordless MFA Utilizing Biometrics, Proximity and Contactless Communication,"2024. [Online]. Available: http://arxiv.org/abs/2406.09000

[9] D. Temoshok, J. L. Fenton, Y.-Y. Choong, N. Lefkovitz, A. Regenscheid, R. Galluzzo, and J. P. Richer, *Digital Identity Guidelines: NIST Special Publication 800-63B-4*, National Institute of Standards and Technology, 2025. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-63B-4

[10] P. T. Tran-Truong, M. Q. Pham, H. X. Son, D. L. T. Nguyen, M. B. Nguyen, K. L. Tran, L. C. P. Van, K. T. Le, K. H. Vo, N. N. T. Kim, T. M. Nguyen, and A. T. Nguyen, "A systematic review of multi-factor authentication in digital payment systems: NIST standards alignment and industry implementation analysis,"*Journal of Systems Architecture*, vol. 162, 2025. [Online]. Available: https://doi.org/10.1016/j.sysarc.2025.103402

[11] Statista, "Multi-Factor Authentication (MFA) Statistics and Trends 2025,"*Scoop Market.us*, 2025. [Online]. Available: https://scoop.market.us/multi-factor-authentication-statistics