CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

# GUIA PARA A SELEÇÃO DE SOLUÇÕES DE AUTENTICAÇÃO MULTIFATOR

Dezembro 2024

# ÍNDICE

# Siglas e Acrónimos

| | |
|---|---|
| ADFS | *Active Directory Federation Services* - Serviços de Federação do *Active Directory* |
| APIs | *Applications Programming Interface* - Interface de Programação de Aplicações |
| CERT.PT | Computer Emergency Response Team - Equipa de Resposta a Incidentes de Segurança Informática Nacional (Lei 46/2018) |
| CIO | *Chief Information Officer* - Responsável de Informação |
| CISO | *Chief Information Security Officer* – Responsável de Segurança de Informação |
| CNCS | Centro Nacional de Cibersegurança |
| MFA | *Multi-factor Authentication* - Autenticação Multifator |
| OTP | *One Time Password* - Palavra-passe Descartável |
| PIN | *Personal Identification Number* – Número de Identificação Pessoal |
| PRNG | *Pseudo-random Number Generator* - Gerador de números pseudoaleatórios |
| SASE | *Secure Access Service Edge* – Fronteira do Serviço de Acesso Seguro |
| SDKs | *Software Development Kits* - Kits de desenvolvimento de *software* |
| VDI | *Virtual Desktop Infrastructure* - Virtualização de área de trabalho |

# 1. Introdução

O **Guia para a Seleção de Soluções de Autenticação Multifator** é um referencial que tem como objetivo definir uma abordagem estruturada e adaptada às necessidades específicas de cada organização no processo de adoção de mecanismos de autenticação multifator.

O esquema apresentado para o processo de seleção destes mecanismos é dividido em três fases distintas:

1) Contexto Organizacional;
2) Categorização de Serviços;
3) Mapeamento de Mecanismos de Autenticação.

Esta sequência proporciona uma orientação clara e prática para a adoção eficaz de soluções de autenticação multifator, que permita equilibrar segurança com eficiência operacional, custos e usabilidade.

Este guia destina-se a:

- Pessoas com responsabilidades de gestão do sistema de segurança de informação de uma organização (CIO ou CISO);
- Pessoas com um papel de desenho, desenvolvimento, implementação ou integração de uma solução de autenticação;
- Pessoas com um papel técnico na configuração das várias ferramentas que permitem a autenticação no sistema de informação sob a sua responsabilidade;
- Equipas técnicas.

No entanto, encoraja-se a sua utilização por parte de todo o tipo de perfis que possam beneficiar deste documento.

# 2. Autenticação Multifator (MFA)

A autenticação é um processo que envolve a verificação de identidade através de um conjunto de critérios únicos, como por exemplo uma combinação de nome de utilizador e palavra-passe, tokens de autorização, cartão de identificação e/ou dados biométricos.

A autenticação poderá ser baseada em três tipos de fatores distintos:

- **Fator de Conhecimento:** algo que se sabe, como por exemplo palavras-passe e PINs.
- **Fator de Posse:** algo que se possui, como por exemplo *hardware tokens*, cartão inteligente e cartão de memória.
- **Fator Inerente:** algo que a pessoa é e pode ser identificável através do recurso a dados biométricos, como por exemplo leitura facial, impressão digital e dinâmica de escrita.

A autenticação multifator implica combinar dois ou mais fatores de autenticação no acesso a uma conta, considerando que isso poderá mitigar, de forma significativa, o risco de comprometimento de sistemas e adicionar um nível de segurança às suas contas. É esta combinação de mecanismos que se designa por autenticação multifator. Este método é projetado para mitigar várias vulnerabilidades associadas à autenticação tradicional baseada apenas num único fator, geralmente a palavra-passe.

De seguida, apresentam-se exemplos de ataques passíveis de serem mitigados através da utilização de autenticação multifator:

**Comprometimento de contas privilegiada**s: Contas privilegiadas, como as de administradores de sistemas, possuem acesso a dados sensíveis e controlam permissões relevantes, tornando-as alvos prioritários para agentes de ameaça. Em caso de comprometimento, o impacto pode ser substancial, incluindo a manipulação de sistemas, exfiltração de dados e interrupção de operações.

**Ataques de *Phishing***: Os ataques de *phishing* são amplamente utilizados para capturar as credenciais de um utilizador. No entanto, se a conta do utilizador estiver protegida com autenticação multifator, o nível de complexidade exigida ao agente de ameaça para comprometer a mesma será mais elevado, uma vez que esse agente precisará de comprometer um segundo fator de autenticação, como por exemplo um PIN enviado para um dispositivo diferente, para conseguir atingir o objetivo pretendido. O *phishing* continua a ser o tipo de incidente mais registado pelo CERT.PT em 2022, de acordo com o Relatório de Riscos e Conflitos 2023 do Observatório de Cibersegurança do CNCS.

**Ataques de Força Bruta *(Bruteforce Attacks)***: Através de um ataque de força bruta, um agente de ameaça poderá descobrir o nome de utilizador e a palavra-passe correspondente de uma conta, recorrendo a um processo de tentativa-erro automatizado. No entanto, caso a conta esteja protegida com um outro fator de autenticação, a probabilidade de acesso ao recurso será menor.

***Keyloggers***: Um *keylogger* é um tipo de programa de monitorização ou *spyware*. Este programa grava as teclas pressionadas pelo utilizador e regista nomes de utilizador, palavras-passe, respostas a perguntas de segurança, dados bancários e de cartões de crédito, sites visitados, entre outros. No entanto, caso o utilizador adote um segundo ou terceiro fator de autenticação, a palavra-passe não será suficiente para o agente de ameaça aceder ao sistema. Por exemplo, se a autenticação multifator estiver

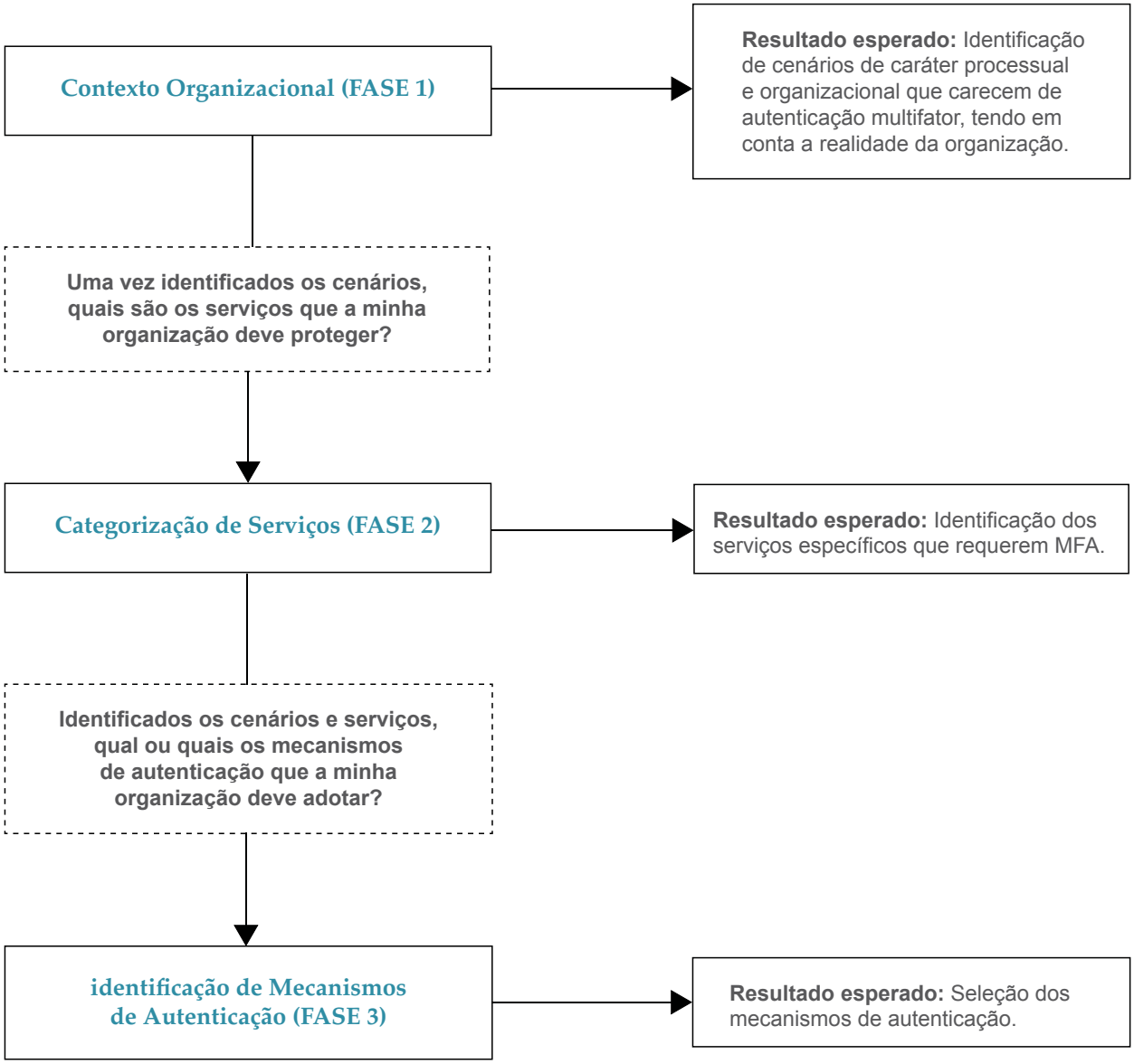
configurada através de uma aplicação de autenticação no dispositivo móvel, o utilizador autorizado só conseguirá iniciar sessão se aceitar o pedido de autenticação no dispositivo móvel. Sem acesso a este dispositivo, os agentes de ameaça não conseguem comprometer o sistema, mesmo com um *keylogger* instalado.

***Infostealers***: Os *infostealers*, ou *stealers*, são um tipo de código malicioso (*malware*) desenvolvido para sub-repticiamente recolher dados sensíveis de um sistema. Os *infostealers* recolhem dados extremamente delicados tais como palavras-passe, *cookies*, detalhes bancários, carteiras de criptomoedas, e-mails e outros documentos. Este código malicioso representa um desafio elevado, pois permite contornar algumas das boas práticas clássicas na proteção de dados. No entanto, mesmo que o *infostealer* consiga obter credenciais de acesso, um segundo fator de autenticação, por exemplo, um Chave de Segurança FIDO, poderá impedir que o agente de ameaça utilize as credenciais recolhidas para comprometer uma conta.

Em suma, todas as ameaças que dependam do comprometimento de uma palavra-passe para se concretizarem são mitigadas pela necessidade de o agente de ameaça ter de aceder a pelo menos mais um fator para poder comprometer a conta em causa.

# 3. Processo de Adoção de Autenticação Multifator

Este esquema para o processo de implementação de MFA divide-se em três fases sequenciais, permitindo que a organização selecione os diferentes mecanismos, de acordo com o seu contexto organizacional, serviços, custos associados e experiência para o utilizador.



## 3.1 Contexto Organizacional (FASE 1)

A organização deve determinar as condições externas e internas que são relevantes para a tomada de decisão na seleção de mecanismos de autenticação para os sistemas internos da organização em diferentes contextos. As recomendações deste Guia devem ser analisadas em relação ao contexto em que ocorre a autenticação, devendo para tal ser realizada uma análise dos riscos no que respeita à implementação de soluções de autenticação (consulte aqui o Guia para Gestão de Riscos, publicado pelo Centro Nacional de Cibersegurança). Para esta ponderação poderão ser tomados em consideração aspetos como a criticidade da solução que requer autenticação, o grau de exposição ao risco do(s) recurso(s) a proteger (e.g. se está publicado na internet ou apenas disponível internamente), o número de utilizadores associados, outras medidas de segurança suplementares, etc. Dever-se-á ter sempre em consideração que diferentes contextos enfrentam diferentes ameaças e, portanto, não têm as mesmas necessidades de segurança.

Assim, apresentamos uma lista de potenciais contextos onde, tendo em conta a natureza da organização, poderá fazer sentido aplicar soluções MFA. Note-se que esta não é uma lista exaustiva.

| | |
|---|---|
| **Políticas de Autenticação** | A organização deverá implementar soluções de autenticação que estejam em conformidade com as suas políticas gerais e políticas granulares que poderão existir a vários níveis: por utilizador, aplicação, grupo, departamento, função, dispositivo, entre outros.<br><br>As políticas de autenticação gerais possibilitam a definição de um perímetro global de segurança para toda organização. As políticas granulares permitem à organização configurar políticas de proteção específicas nomeadamente para aplicações sensíveis, utilizadores de maior risco, etc. |
| **Usabilidade e Acessibilidade** | A solução de autenticação deverá ser fácil de utilizar por todos os utilizadores autorizados, com o mínimo de perturbação no seu trabalho diário. Isto inclui utilizadores internos, como funcionários (no escritório e remotos), e utilizadores externos, como fornecedores, *freelancers*, clientes, cidadão, etc.<br><br>A escolha do mecanismo de autenticação deverá ser adequada ao contexto e acaute- lar possíveis constrangimentos por parte dos utilizadores ou dispositivos necessários. A organização deve adotar mecanismos acessíveis a pessoas com deficiência, e deve considerar possíveis limitações (rede, dispositivo, entre outros) que impeçam ou limitem a autenticação do utilizador. |
| **Autenticação de Terceiros** | Caso a cadeia de fornecimento seja parte integrante do ecossistema da organização, esta deve ser considerada na política de autenticação. |
| **Mecanismos de Autorização/ Reconfirmação Multifator para Operações de Alto Risco** | No momento de autenticação, o utilizador confirma a sua identidade digital para aceder aos recursos disponibilizados pelo sistema. Posteriormente a estar autenticado, devem ser acionados mecanismos de autorização/ reconfirmação multifator para executar operações de alto risco como alterar uma palavra-passe, transferir dinheiro, enviar documentos sensíveis, entre outros. |

| | |
|---|---|
| **Acesso através de um dispositivo que não é habitual** | Em caso de início de sessão num serviço com recurso a um dispositivo que o utilizador não tenha utilizado anteriormente, a solução de autenticação deve solicitar um fator de autenticação adicional. A solução deverá registar os dispositivos utilizados anteriormente. |
| **Acesso através de uma localização que não é habitual** | Caso a ligação a um serviço seja proveniente de uma localização diferente do habitual, a solução de autenticação deve solicitar ao utilizador que utilize um fator de autenticação adicional. Importa considerar que a utilização de localização como caraterística única de contexto poderá ter impacto direto na usabilidade e, consequentemente, uma possível má utilização do sistema. Idealmente, a localização deverá ser caracterizada por múltiplos parâmetros que reduzam a possibilidade de falsos positivos ou deverá ser cruzada com outras possíveis características, nomeadamente comportamentais. |
| **Infraestrutura baseada na *Cloud*** | Caso a infraestrutura da organização contemple soluções *Cloud*, a solução de autenticação a adotar deverá ser integrável com o(s) serviço(s) de *Cloud* utilizados. |
| **Integração com aplicações em sistemas legados** | Caso a organização possua aplicações obsoletas ou desatualizadas, a solução de autenticação multifator a adotar deve considerar as seguintes características para garantir a sua operacionalidade com as aplicações existentes:<br>• APIs para o registo da solução;<br>• *Software Development Kits* (SDKs);<br>• Linha de comandos para registar a solução MFA e processar notificações *push*;<br>• Ambiente *Sandbox* para testar com segurança a solução MFA num ambiente que não seja o de produção. |
| **Acessos privilegiados** | A solução de autenticação multifator deverá ser utilizada para controlo de acessos privilegiados, tanto no âmbito de administração de sistemas como na execução de processos críticos da organização. O anteriormente referido deverá ser particularmente levado em consideração no caso de serviços de maior criticidade e exposição como, por exemplo, “Acesso a consolas de gestão dos serviços mais críticos de suporte à infraestrutura” e “Acesso remoto a servidores”. |
| **Cadeia de valor do fornecimento das soluções de autenticação** | Particularmente em acessos críticos, é crucial validar a cadeia de valor que fornece as soluções de autenticação, quer seja este de software ou de *hardware*.<br>A validação deverá ter em conta o processo de desenvolvimento de componentes críticos (cripto-processadores, PRNG, algoritmia, *software*, entre outros), das suas especificações/configurações (parametrizações de cifra, entre outros) e da sua capacidade de ser auditados/validados e mantidos. |
| **Infraestrutura Híbrida** | No caso de uma infraestrutura híbrida, baseada em soluções *cloud* e *on-premises*, a solução deverá considerar os dois âmbitos, podendo até funcionar como mecanismo de controlo entre ambos. |
| **Sustentabilidade Ambiental** | A organização deverá implementar soluções de autenticação que sejam compatíveis com as suas Políticas de Sustentabilidade Ambiental. Por exemplo, a organização poderá optar pela utilização de soluções *hardware* com certificações ambientais (ISO 14000, que estabelece diretrizes quanto à gestão ambiental nas organizações; ISO 5001, relativa à gestão da eficiência energética, entre outros). |

## Recomendações gerais no âmbito do contexto organizacional

- Planear e prever uma possível variedade de necessidades de acesso (por exemplo, ao posto de trabalho, ligações remotas, acessos privilegiados, entre outros);
- Configurar políticas contextuais sempre que possível;
- Considerar os normativos e requisitos legais inerentes ao contexto em que a organização aplica as soluções multifator;
- O tratamento e o processamento de dados pessoais deverão reger-se pelos princípios e imperativos legais definidos no Regulamento Geral sobre a Proteção de Dados – Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 – e na Lei n.º 58/2019 de 8 de agosto;
- Planear e prever a necessidade de implementação de mecanismos de autenticação multifator para acesso remoto.

| NOTA | Em termos de implementação de soluções de autenticação, é especialmente crítico a aplicação do princípio do "menor privilégio possível durante o menor tempo possível". |
|---|---|

## 3.2 Categorização de Serviços (FASE 2)

Selecionados os contextos organizacionais que requerem MFA, a organização deve agora identificar, através da tabela que se segue, e considerando a arquitetura da sua infraestrutura, o tipo de serviços na sua organização que requerem a implementação de soluções de autenticação.
Note que esta não é uma lista exaustiva.

| | |
|---|---|
| **Serviços de suporte à infraestrutura: Acesso a serviços exclusivamente internos** | • Diretório de utilizadores<br>• Partilha de ficheiros<br>• E-mail<br>• Impressão<br>• Restabelecimento de Palavra-Passe ou desbloqueio de conta em *self-service* com recurso a uma AD FS (*Active Directory Federation Services*)<br>• ... |
| **Serviços de suporte à infraestrutura: Acesso a serviços expostos ao exterior** | • E-mail<br>• Webmail<br>• VPN<br>• Soluções SASE<br>• Soluções VDI<br>• ... |
| **Outros serviços (internos)** | • Gestão Documental<br>• *Customer Relationship Management* (CRM)<br>• *Enterprise Resource Planning* (ERP)<br>• Gestão de Assiduidade<br>• Gestão de Recursos Humanos<br>• Ferramentas de *Identity and access management* (IAM)<br>• ... |
| **Acesso a consolas de gestão dos serviços mais críticos de suporte à infraestrutura** | • *Firewall*<br>• Sistema Hypervisor<br>• Filtragem de *e-mail*<br>• Solução PAM (Gestão acessos privilegiados)<br>• ... |
| **Outros serviços (externos)** | • *Amazon Cloud Services*<br>• *Google Cloud Services*<br>• *Microsoft 365*<br>• *Microsoft Azure*.<br>• ... |

| | |
|---|---|
| **Acesso a postos de trabalho e outros dispositivos corporativos** | • *Desktops*<br>• *Laptops*<br>• Dispositivos móveis<br>• ... |
| **Acesso remoto a servidores** | • *Secure Shell Access* (SSH)<br>• *Remote Desktop Protocol* (RDP)<br>• ... |
| **Integração de aplicações em *cloud*** | • Integração com o Sistema de Gestão de Recursos Humanos (HRMS)<br>• Serviços de integração de diretório (*Active Directory e Lightweight Directory Access Protocol*)<br>• Compatibilidade com outros controlos de gestão de identidade como gestores de *passwords* e segurança de *endpoints*<br>• Restabelecimento de Palavra-passe ou desbloqueio de conta em *self-service*<br>• ... |

## Recomendações a considerar no processo de seleção de serviços

- Verificar cuidadosamente os requisitos de conformidade dos mecanismos de MFA com os serviços em questão;

- Definir a priorização de serviços que requerem a aplicação de mecanismos de MFA;

- Considerar a implementação faseada do MFA. Por exemplo, numa primeira fase a organização poderá começar por implementar o MFA em utilizadores com privilégios de administração e operação de sistemas. Na segunda fase deste processo, poderá ser abrangido o executivo e, numa terceira etapa, os restantes utilizadores internos e utilizadores convidados externamente;

- Considerar a disponibilização de mecanismos de acesso redundantes, mas com idêntico nível de segurança, para conceder acesso ao(s) serviço(s) por utilizadores que se tenham esquecido, ou não estejam na posse (em situação de esquecimento ou furto) do mecanismo de autenticação inicialmente solicitado.

## 3.3 Identificação de Mecanismos de Autenticação (FASE 3)

Uma vez identificados os cenários e os serviços que a organização pretende proteger através da combinação de dois ou mais mecanismos de autenticação, a organização deverá proceder à seleção da solução a implementar.

### 3.3.1 Tabela Resumo

A seguinte tabela, dividida pelos três tipos de fatores de autenticação (fator de conhecimento, de posse e de inerência) visa apoiar essa seleção, identificando o nível de proteção, a usabilidade e o custo. Note que esta não é uma lista exaustiva. São descritos mecanismos e não soluções tecnológicas, sendo que deverá ser adotada uma solução que integre dois ou mais dos mecanismos descritos.

| Tipo de Fator | Mecanismos | Nível de Proteção | Usabilidade | Custo |
|---|---|---|---|---|
| **Fator de Conhecimento: algo que o Utilizador sabe** | Número de Identificação pessoal PIN (*Personal Identification Number*) | Baixo | Elevado | Baixo - Nenhum |
| | Palavra-Passe | Baixo - Médio | Médio | Baixo - Nenhum |
| | Palavras-Passe cognitivas KBA (*Knowledge-Based Authentication*) | Baixo | Médio | Médio |
| **Fator de Posse: algo que o Utilizador tem** | *Token* de *Hardware* RSA e OATH (RSA/OATH *Hardware Token*) | Elevado | Baixo | Elevado |
| | Cartão de Memória | Baixo | Médio | Baixo |
| | Cartão Inteligente (*Smart Card*) | Médio | Médio | Médio |
| | Segurança FIDO (FIDO *Security Key*) | Muito Elevado | Médio | Elevado |
| | Palavra-Passe Descartável (*One Time* Palavra-Passe - OTP) | Médio - Elevado | Médio - Elevado | Baixo - Médio |
| | Notificações *Push* (*Push Notifications*) | Médio | Elevado | Médio |
| | Código Qr (Qr *Code*) | Médio | Médio | Baixo |
| **Fator Inerente: algo que o Utilizador é** | Autenticação Biométrica | Muito Elevado | Elevado | Alto*<br>*na situação de não ser fornecido pelo dispositivo habitual do utilizador |
| | Autenticador FIDO (FIDO *Authenticator*) | Muito Elevado | Muito Elevado | Baixo |

**Segue-se a descrição detalhada de cada mecanismo:**

## 3.3.2 Fator de Conhecimento: algo que o Utilizador sabe


### 1. MECANISMO: NÚMERO DE IDENTIFICAÇÃO PESSOAL PIN (PERSONAL IDENTIFICATION NUMBER)

| Nível de Proteção | Usabilidade | Custo |
|---|---|---|
| Baixo | Elevado | Baixo - Nenhum |

#### Definição

Mecanismo que requer uma sequência de números (tipicamente 4 a 6 dígitos) usada para autenticar uma identidade ou para verificar a autorização de acesso.

#### Prós

- Fácil de Memorizar.
- Fácil de Implementar e com baixo custo.
- Usado normalmente como um fator adicional de autenticação.

## Contras

- O código PIN, devido à baixa complexidade a que é inerente, pode ser mais facilmente comprometido por ataques de força bruta, não devendo, por isso, ser o único mecanismo de autenticação para aceder a um sistema ou recurso.
- Vulneráveis a ataques de *phishing* e de força bruta.
- Mecanismo dependente das práticas e da maturidade dos utilizadores.

**Exemplos de más práticas:**

- A reutilização em múltiplos serviços ou soluções, a reutilização de PINs antigos e a alteração com pouca ou nenhuma frequência podem ser fatores de comprometimento das soluções, pois basta que o PIN de uma delas seja comprometido, para que o agente de ameaça tenha acesso às restantes soluções;
- Partilha do PIN com outros indivíduos;
- PIN escritos em formato físico ou digital (quando não se encontram cifradas) em locais acessíveis a outros indivíduos.

## Observações/Recomendações

Os códigos PIN devem ser alterados periodicamente.

Se o PIN for o único mecanismo de autenticação usado para aceder a um sistema, deve estar associado um limite reduzido de tentativas falhadas (por exemplo, três) que conduza ao bloqueio do sistema até à introdução de um segundo mecanismo de autenticação, ou a um bloqueio temporário.

É desaconselhável usar um código PIN como fator único para proteger um *website*.

Não devem ser armazenados códigos PIN centralmente.

## Exemplos de aplicação (Não exaustivo)

- Fator de autenticação em ATMs após introdução do cartão bancário;
- Dispositivos móveis para desbloqueio do cartão SIM e do dispositivo;
- Sistemas de vigilância (alarmes).


## 2. MECANISMO: PALAVRA-PASSE

| Nível de Proteção | Usabilidade | Custo |
|---|---|---|
| **Baixo - Médio** | **Médio** | **Baixo - Nenhum** |

### Definição

Mecanismo que requer uma sequência de caracteres (letras, números e outros símbolos) usada para autenticar uma identidade ou para verificar a autorização de acesso.

### Prós

- Palavras-passe longas e complexas são significativamente mais seguras contra ataques de força bruta e de dicionário do que um PIN.
- Baixo custo de implementação uma vez que a maioria dos sistemas as usam por defeito.

### Contras

- Vulnerável a ataques de *phishing.*
- Difícil de memorizar quando são longas complexas e quando têm de ser periodicamente alteradas.
- As bases de dados de credenciais tornam-se mais vulneráveis a ataques de SQL *Injection* quando não são cifradas com chave privada e guardadas centralmente e separadamente do sistema de autenticação.
- Mecanismo dependente das práticas e da maturidade dos utilizadores.

**Exemplos de más práticas:**

- As palavras-passe de baixa complexidade podem ser comprometidas por ataques de força bruta e de dicionário;

- A reutilização em múltiplos serviços ou soluções, a reutilização de palavras-passe antigas e a alteração com pouca ou nenhuma frequência podem ser fatores de comprometimento dessas soluções, uma vez que, caso uma das credenciais seja comprometida, o agente de ameaça poderá obter acesso às restantes soluções;

- Partilha de palavras-passe com outros indivíduos;

- Palavras-passe escritas em formato físico ou digital (quando não se encontram cifradas) em locais acessíveis a outros indivíduos.

## Observações/Recomendações*

A organização deverá definir uma política de palavra-passe, considerando:

- O uso de palavras-passe com um **mínimo de 12 carateres**, bem como uma combinação de carateres especiais, letras maiúsculas, minúsculas e números;
- A alteração da palavras-passe sempre que haja suspeita que a mesma tenha sido comprometida;
- A não aceitação de palavras-passe usadas anteriormente.

* Recomendações presentes no website do CNCS.

A organização pode incluir também na sua política a alteração da palavras-passe com uma determinada regularidade, definindo um espaço temporal entre novas palavras-passe, sob a pena de o utilizador ficar sem acesso, até definição de uma nova palavra-passe.
O uso de um *software* gestor de palavras-passe pode ser considerado pela organização de forma a auxiliar os utilizadores. Esta aplicação deve ser protegida por uma autenticação forte.

As bases de dados que contêm as credenciais (lista de utilizadores e palavras-passe) devem ser cifradas com chave privada e guardadas centralmente e separadamente do sistema de autenticação utilizado na organização.

É aconselhável que a organização promova ataques simulados de *phishing* de forma a analisar o comportamento dos seus utilizadores e a promover a formação dos mesmos.

## Exemplos de aplicação (Não exaustivo)

- Primeiro fator de autenticação na maioria dos sistemas computacionais, para o acesso a contas de utilizadores, contas de *e-mail*, contas aplicacionais, redes, *websites*.

## 3. MECANISMO: PALAVRAS-PASSE COGNITIVAS KBA (KNOWLEDGE-BASED AUTHENTICATION)

| Nível de Proteção | Usabilidade | Custo |
|---|---|---|
| Baixo | Médio | Médio |

### Definição

Mecanismo de autenticação baseada no conhecimento, que requer que o utilizador responda a uma série de perguntas para verificar a sua identidade.

### Prós

- As questões são fornecidas no mesmo dispositivo, sendo ele um *smartphone* ou um computador, não é necessário um dispositivo adicional para a autenticação;
- Usados normalmente como um fator adicional de autenticação.

### Contras

- Algumas das perguntas utilizadas baseiam-se em informações que os agentes de ameaça podem encontrar em redes sociais, através de outras fontes públicas, e também informação proveniente de *leaks* (exfiltração de informação);
- É comum o utilizador falhar no questionário, mesmo tendo sido o próprio a fornecer as respostas previamente;
- Pode envolver algum investimento ou contratualização da aplicação que irá proporcionar este mecanismo.

## Observações/Recomendações

O armazenamento desta informação deverá ser devidamente acautelado. Nesse sentido, os repositórios que contêm estes dados devem ser cifrados com chave privada e armazenados centralmente e separadamente do sistema de autenticação utilizado. Deve ainda evitar-se a utilização deste fator como primeiro fator de autenticação.

Existem dois mecanismos de palavras-passe cognitivas (KBA):

- **KBA Estático** - também conhecido por "segredos partilhados (*shared secrets*)" e "perguntas de segredos partilhados (*shared secret questions*)", é um dos mecanismos mais utilizados, onde as perguntas estáticas do KBA são escolhidas pelo utilizador quando este se regista no sistema. Desta forma, tanto as perguntas como as respostas fornecidas são armazenadas para serem usadas quando a verificação de identidade for necessária. Exemplo: "Qual é o nome do seu primeiro animal de estimação?";

- **KBA Dinâmico** - também é conhecido como "perguntas fora da carteira (*out-of-wallet questions*)", consiste em perguntas lançadas ao utilizador sem que o mesmo as tenha definido previamente. As perguntas normalmente são mais específicas e podem recorrer à seleção da resposta em escolha múltipla. Exemplo: "Selecione os últimos dígitos do seu número de segurança social." As respostas a estas perguntas podem ser recolhidas de múltiplas fontes, sendo que os respetivos dados devem ser armazenados numa base de dados da organização, devidamente protegida.

## Exemplos de aplicação (Não exaustivo)

- Recuperação de palavras-passe.

## 3.3.3 Fator de Posse: algo que o Utilizador tem

### 1. MECANISMO: *TOKEN* DE *HARDWARE* RSA E OATH (RSA/OATH *HARDWARE TOKEN*)

| Nível de Proteção | Usabilidade | Custo |
|---|---|---|
| Elevado | Baixo | Elevado |

#### Definição

Dispositivo físico de reduzidas dimensões que o utilizador possui, com capacidade de gerar um código PIN (normalmente de 6 dígitos) que deve ser introduzido pelo utilizador no processo de autenticação, concedendo-lhe acesso aos sistemas e recursos.

#### Prós

- Mecanismo difícil de comprometer remotamente;
- Muitos sistemas que recorrem a *hardware token* não necessitam de acesso à internet para funcionar, o que os torna mais fáceis de isolar, minimizando a superfície de ataque;
- A probabilidade de um agente malicioso comprometer um *hardware token* é reduzida face a outras ameaças;
- Fácil de transportar.

### Contras

- Investimento elevado nos *tokens* e no sistema que os suporta;
- Custos de manutenção;
- Vulnerável ao roubo, perda e esquecimento do dispositivo;
- Um *hardware token* apropriado por um agente malicioso, pode causar um impacto significativo em sistemas críticos da organização, uma vez que o utilizador legítimo normalmente possui privilégios elevados.

### Observações/Recomendações

Este dispositivo, sob a forma de um cartão inteligente (*smartcard*), *key fob*, ou *pen usb*, possui um algoritmo que gera um conjunto de PINs a cada 30 ou 60 segundos. O Servidor de autenticação possui uma cópia desse algoritmo permitindo-o estar coordenado com o dispositivo. Desta forma, ao inserir o número presente no dispositivo, o utilizador comprova que está na posse do mesmo.

Não é expectável que clientes e colaboradores em geral transportem *hardware tokens*, devendo este mecanismo ser utilizado por um número restrito de membros da organização que efetivamente necessitam de aceder a recursos ou sistemas específicos com elevado nível de acesso.

### Exemplos de aplicação (Não exaustivo)

- Fator adicional para acesso a redes, aplicações ou locais de alta segurança, possivelmente sem acesso à *internet*.

## 2. MECANISMO: CARTÃO DE MEMÓRIA

| Nível de Proteção | Usabilidade | Custo |
|---|---|---|
| Baixo | Médio | Baixo |

### Definição

Dispositivo que contém informação, mas que não a processa. Pode conter um RFID ou uma banda magnética e é usado para identificar e autenticar o acesso de um utilizador num recurso ou serviço.

### Prós

- Fácil de transportar;
- Custo reduzido.

### Contras

- Vulnerável ao roubo, furto, perda, partilha e esquecimento;
- Cartões vulneráveis a clonagem.

### Exemplos de aplicação (Não exaustivo)

- Cartões de Identificação de colaboradores;
- Cartões de pagamento.

## 3. MECANISMO: CARTÃO INTELIGENTE (SMART CARD)

| Nível de Proteção | Usabilidade | Custo |
|---|---|---|
| **Médio** | **Médio** | **Médio** |

### Definição

Dispositivo em formato de cartão com memória interna, circuitos e microprocessador integrados, que contém informação encriptada, e que normalmente é decifrada a partir de um PIN. A informação decifrada é usada posteriormente para autenticação.

### Prós

- Pode ser automaticamente inutilizado;
- Fácil de transportar.

### Contras

- Vulnerável ao roubo, furto, perda, partilha e esquecimento;
- Vulnerável a ataques físicos que procuram manipular os circuitos do cartão para extrair informação;
- Investimento significativo em cartões e leitores;
- Vulnerável à interceção da comunicação entre o cartão e o servidor.

## Observações/Recomendações

Os cartões inteligentes guardam uma quantidade de informação superior aos cartões de memória.

Recomenda-se que, assim que o cartão deixe de ter uso, que o mesmo seja destruído e que o contacto magnético “dourado” seja danificado, para que o cartão possa ficar eficazmente inutilizado.

Em situações de roubo, furto ou fraude a perda do cartão deve ser comunicada imediatamente à organização para que o mesmo seja cancelado automaticamente.

## Exemplos de aplicação (Não exaustivo)

- Cartões de cidadão;
- Cartões bancários com “*chip*” externo;
- Cartões SIM.

## 4. MECANISMO: CHAVE DE SEGURANÇA FIDO (FIDO *SECURITY KEY*)

| Nível de Proteção | Usabilidade | Custo |
|---|---|---|
| **Muito Elevado** | **Médio** | **Elevado** |

### Definição

Dispositivo físico de dimensões reduzidas que o utilizador possui, e que lhe concede acesso exclusivo a serviços a partir de uma autenticação criptográfica assimétrica, mais concretamente a partir de criptografia de chave pública (par de chaves pública/privada único).

### Prós

- Mecanismo não requer o uso de palavras-passe, KBA, e SMS OTP para o acesso a serviços *online* (*websites*), sendo por isso um fator mitigador de ataques de *phishing* na organização;
- Autenticação forte;
- Mecanismo suportado por diversos *browsers*.

### Contras

- Dependendo da dimensão da organização o Investimento pode ser mais elevado (compra dos dispositivos);
- Vulnerável a roubo, furto, perda ou esquecimento do dispositivo.

## Observações/Recomendações

Estes dispositivos, também conhecidos por "*Hard FIDO Authentication Tokens*", apresentam-se sob a forma de *pen-usb* ou *key fob*, e comunicam com computadores e dispositivos móveis via USB, NFC (*Near Field Communication*) ou BLE (*Bluetooth Low Energy*).

Este tipo de autenticação requer que o utilizador registe cada domínio do *website* em que deseja autenticar-se no seu autenticador FIDO. No momento do registo, com o dispositivo conectado o autenticador gera um par de chaves pública/privada exclusivamente para esse domínio, envia a chave pública para esse *site*, e a chave privada é retida pelo dispositivo (a chave privada nunca sai do dispositivo).

Posteriormente, sempre que o utilizador pretenda aceder ao serviço *online*, o serviço *online* irá desafiar o autenticador, e a partir da inserção do dispositivo que contém a chave pública, a autenticação acontecerá devido à correspondência entre a chave pública e privada.

Caso o utilizador aceda a um serviço *online* falso, assim que se tentar autenticar no respetivo domínio, a autenticação falhará, uma vez que o domínio não possui a chave pública necessária à autenticação.

As chaves são acedidas pelos navegadores de *internet* (*browsers*) e a autenticação com o *website* é assegurada pelo protocolo TLS (*Transport Layer Security*).

De forma a diminuir o investimento inicial, aconselha-se a que as organizações que desejam adotar este mecanismo selecionem para o efeito um grupo de utilizadores com a necessidade de aceder a serviços de maior criticidade para a organização.

Este mecanismo permite também a autenticação em dispositivos do utilizador mesmo *offline,* desde que os mesmos já se encontrem registados por um método de criação de chave pública *online*.

Este mecanismo é normalmente acompanhado por um segundo fator de autenticação da categoria "algo que é" (reconhecimento facial ou leitura de impressão digital) "ou algo que sabe" (PIN).

## Exemplos de aplicação (Não exaustivo)

- Primeiro fator de autenticação para acesso a computadores corporativos e serviços *online* (bancários, *e-mail*, redes sociais, compras, entre outros).


## 5. MECANISMO: PALAVRA-PASSE DESCARTÁVEL (*ONE TIME PASSWORD* - OTP)

| Nível de Proteção | Usabilidade | Custo |
|---|---|---|
| **Médio - Elevado** | **Médio - Elevado** | **Baixo - Médio** |

### Definição

A palavra-passe descartável, também conhecida por "palavra-passe de uso único" trata-se de um conjunto de carateres numérico ou alfanumérico gerado automaticamente e válido para uma utilização num curto espaço de tempo. Pode ser fornecida por SMS, *e-mail*, *soft token* (aplicação para *smartphone*), e chamada de voz ao utilizador, devendo o mesmo inseri-la no sistema de modo a garantir uma única autenticação, comprovando assim que está na posse do dispositivo que contem a palavra-passe.

### Prós

- OTP por voz é um mecanismo altamente disponível, uma vez que só requer a utilização de um dispositivo que permita efetuar chamadas de voz (telefone fixo, telemóvel ou *smartphone*);
- OTP por *soft token* pode ser facilmente desativado na situação de perda do *smartphone*;
- Mecanismo requer menos investimento comparativamente a *hardware tokens.*

### Contras

- O OTP via *e-mail* é um método tão seguro quão seguras forem as credenciais utilizadas para aceder ao mesmo;
- A comunicação de OTPs por chamada de voz ou sms é vulnerável à troca do cartão SIM do dispositivo móvel (SIM *Swapping*);
- A comunicação de OTPs via SMS ou chamada de voz pode implicar custos de comunicação acrescidos.

### Observações/Recomendações

A organização deverá considerar a quantidade de utilizadores, o nível de criticidade dos serviços e recursos protegidos por OTP, e os recursos fornecidos aos utilizadores, como por exemplo:

- Se os utilizadores não usam *smartphone* corporativo, mas sim um telefone fixo ou um telemóvel, o OTP deve ser comunicado por SMS ou chamada;
- Se os utilizadores têm exclusivamente acesso ao *e-mail*, e não a outros dispositivos corporativos, o OTP deve ser comunicado por *e-mail*;
- Se os utilizadores usam *smartphone* ou computador corporativo, pode-se optar por instalar um *software* / aplicação que fornece uma série de OTPs.

Os OTPs não devem ser enviados para números telefónicos, aplicações de dispositivos móveis, ou *e-mails*, que estejam fora do domínio ou que não pertençam à organização.

**Exemplo de ataque de *phising*:** Os ataques de *phising* para comprometimento de OTPs são ocasionalmente espoletados por *phishing proxies*, que permitem que os agentes de ameaças encaminhem os utilizadores para *websites* falsos com domínios e aparência idêntica aos *websites* legítimos, onde os agentes de ameaças podem inspecionar, alterar e solicitar informações em tempo real, levando a que os utilizadores forneçam o seu OTP por estarem convencidos de que se trata de um *website* legítimo.

### Exemplos de aplicação (Não exaustivo)

- Os OTPs comunicados por *e-mail* são úteis para a reposição de palavras-passe.
- Os OTPs comunicados por *soft token* são tipicamente utilizados como um segundo fator de autenticação em redes corporativas e serviços *online*.
- Os OTPs comunicados via SMS são úteis para validar os números de telemóvel dos utilizadores.
- Os OTPs comunicados por voz são úteis para validar transações financeiras ou relacionadas com a criação de contas.

## 6. MECANISMO: NOTIFICAÇÕES *PUSH* (*PUSH NOTIFICATIONS*)

| Nível de Proteção | Usabilidade | Custo |
|---|---|---|
| **Médio** | **Elevado** | **Médio** |

### Definição

Mecanismo assente num serviço de autenticação que notifica o utilizador de uma tentativa de acesso a um serviço *online*, e solicita o acesso a partir de uma aplicação instalada no seu *smartphone*. O acesso é garantido assim que o utilizador valida com "um clique" o acesso, na sua aplicação.

### Prós

- Em termos de usabilidade, este mecanismo permite uma autenticação fácil e relativamente rápida sem necessidade de introdução de palavras-passe.
- Mecanismo disponível para *smartphones*, dispositivos utilizados com maior frequência e, desse modo, menos vulneráveis a perda ou esquecimento por parte dos utilizadores, comparativamente a *hardware tokens* ou outros dispositivos físicos de autenticação.

### Contras

- Vulnerável a ataques de Engenharia Social.

## Observações/Recomendações

Estes mecanismos são normalmente utilizados como segundo fator de autenticação, contudo, em situações em que os agentes de ameaças já ultrapassaram o primeiro fator (por comprometimento das credenciais de acesso) a organização deve sensibilizar os seus colaboradores para impedir ataques como:

- ***MFA Fatigue***, em que os utilizadores recebem inúmeras notificações de tentativas de acesso, com o objetivo de fazer o utilizador aprovar o acesso por conveniência, sem verificar a sua origem.

- **Engenharia Social,** em que o agente de ameaça comunica com o utilizador de forma a convencê-lo a validar o acesso no seu *smartphone*.

## Exemplos de aplicação (Não exaustivo)

- Segundo fator de autenticação quando é iniciada uma sessão de um serviço *online* num dispositivo desconhecido.

## 7. MECANISMO: CÓDIGO QR (QR *CODE*)

| Nível de Proteção | Usabilidade | Custo |
|---|---|---|
| **Médio** | **Médio** | **Baixo** |

### Definição

O código QR é um mecanismo em formato de código de barras bidimensional que permite a leitura de diversas informações, inclusive URLs, através de um *scan*.

### Prós

- Mecanismo não requer o uso de palavras-passe e PINs para o acesso a serviços *online* (*websites*), sendo por isso um fator mitigador de ataques de *phishing* na organização.
- Em termos de usabilidade, o facto de o utilizador não ter de voltar a fazer o processo normal de autenticação para o serviço, permite que o mesmo faça uma autenticação rápida e fácil.

### Contras

- A perda, furto ou roubo do dispositivo que concede a autenticação, que faz a leitura do código QR, pode provocar acessos indevidos se o agente de ameaça conseguir desbloquear o dispositivo;
- Mecanismo dependente de um *smartphone* já registado que terá de estar na posse do utilizador. Deste modo, na situação de esquecimento, furto, roubo ou perda do dispositivo, o mecanismo de autenticação noutros dispositivos não poderá ser concretizado;
- A leitura de um código QR não legítimo pode causar danos na aplicação.

## Observações/Recomendações

Os códigos QR são imagens digitalizáveis que podem ser utilizadas para armazenar e recuperar dados. A técnica de autenticação através de códigos QR é utilizada essencialmente para serviços *online* a partir do uso de uma aplicação para *smartphone* já autenticada, para posteriormente autenticar o serviço num novo dispositivo sem a necessidade de seguir o mesmo processo de autenticação.

Recomenda-se que os utilizadores tenham adotado mecanismos de desbloqueio adequados dos seus dispositivos (*smartphones*).

As organizações devem optar por soluções que permitam a eliminação da conta do *smartphone* em caso de perda, furto ou roubo do mesmo.

## Exemplos de aplicação (Não exaustivo)

- Serviços *online* que permitam o uso de vários dispositivos em simultâneo.

## 3.3.4 Fator Inerente: algo que o Utilizador é

### 1. MECANISMO: AUTENTICAÇÃO BIOMÉTRICA

| Nível de Proteção | Usabilidade | Custo |
|---|---|---|
| **Muito Elevado** | **Elevado** | **Alto*** |

*na situação de não ser fornecido pelo dispositivo habitual do utilizador

#### Definição

Mecanismo de autenticação que mede e compara padrões provenientes de caraterísticas biológicas únicas de indivíduos, com o objetivo de validar que o utilizador é legítimo.

Os mecanismos de autenticação biométrica podem ser baseados em caraterísticas físicas ou comportamentais. Um exemplo de característica comportamental é a dinâmica de escrita.

São exemplos de características físicas:

- A impressão digital;
- O reconhecimento da íris;
- O reconhecimento facial;
- A digitalização da retina;
- A geometria da mão;
- O reconhecimento de voz.

### Prós

- As caraterísticas de um determinado indivíduo são únicas e requerem um elevado esforço por parte do agente de ameaça para falsificar e replicar.
- Mecanismos como impressão digital e reconhecimento facial estão incorporados na maioria dos *smartphones* e computadores portáteis recentes, não havendo por isso a necessidade dos utilizadores transportarem consigo outro dispositivo (*token*).
- A autenticação só é validada após ser realizada uma leitura precisa dos padrões, tornando estes mecanismos fiáveis do ponto de vista da segurança.

### Contras

- Alguns mecanismos são dependentes de dispositivos que estão na posse do utilizador, portanto na situação de esquecimento, furto, roubo ou perda do dispositivo, o mecanismo de autenticação não poderá ser concretizado.
- Alguns mecanismos são vulneráveis a modificações no corpo do utilizador.
- Alguns dos mecanismos envolvem investimentos em *hardware* para leitura ou captação de imagem.

### Observações/Recomendações

Os dados biométricos dos utilizadores são normalmente guardados de forma cifrada no próprio dispositivo.

A organização deve ter em conta que será necessário o tratamento adicional de dados pessoais especiais (biométricos) que poderão necessitar de cuidados adicionais no seu tratamento e autorização.

Quando estes mecanismos de autenticação são utilizados juntamente com outros mecanismos tradicionais (como utilização de credenciais de acesso tipo nome de utilizador/palavra-passe), o processo de autenticação torna-se mais seguro.

A maioria dos mecanismos não são invasivos, com exceção da digitalização da retina que dispara um feixe de luz para o olho do utilizador.

Observações sobre cada um dos mecanismos:

- **Impressão digital** - Identificação única que combina uma série de cumes e vales (linhas e espaços) presentes nos dedos das mãos dos indivíduos. O padrão da impressão digital pode ser afetado pela abrasão, o crescimento e as lesões nos dedos.

- **Reconhecimento da íris** - Identificação única capturada à distância a partir de infravermelhos. A íris tem a vantagem de ser muito estável, pois é formada no nascimento e mantêm-se inalterada durante a vida do indivíduo. Envolve o investimento em *hardware*.

- **Reconhecimento Facial** - Identificação única, tipicamente com recurso a Inteligência Artificial para identificar uma face humana numa imagem, ler os principais pontos chaves da imagem extraída e finalmente compará-la com outras faces numa base de dados. É usualmente encontrada em *smartphones* e computadores portáteis, com recurso à câmara frontal e a uma combinação de projetores de luz e sensores para capturar diversas imagens de forma a validar a pessoa.

- **Digitalização da Retina** - Identificação única que analisa a complexa rede de vasos sanguíneos que alimentam a retina. Envolve o investimento num *hardware* que dispara um feixe de luz para o olho. O padrão da retina pode ser afetado por doenças como o glaucoma, a diabetes, e doenças generativas.

- **Geometria da Mão** - Identificação única com recurso a um digitalizador que mede cerca de 90 caraterísticas especificas em menos de 1 segundo, como o comprimento, a largura e a profundidade da geometria dos dedos. Envolve o investimento em *hardware*.

- **Reconhecimento de Voz** - Identificação única que analisa as características únicas da fala de um utilizador. O reconhecimento pode ser afetado pelo ambiente envolvente (barulho e ruído), e é um mecanismo vulnerável a ataques de *voice spoofing* ou "*deepfakes*".

- **Dinâmica de Escrita** - Identificação única com recurso a um *software* que mede o ritmo de escrita no teclado, tendo em conta o tempo de permanência (tempo em que uma determinada chave é mantida) e o tempo de voo (tempo para se mover entre as teclas).

### Exemplos de aplicação (Não exaustivo)

- Controlos de acesso físico;

- Autenticação por Aplicações Móveis para serviços *online*;

- Sistemas de gestão de identidade;

- Fator adicional para acesso a redes, aplicações e locais de alta segurança.

## 2. MECANISMO: AUTENTICADOR FIDO (FIDO AUTHENTICATOR)

| Nível de Proteção | Usabilidade | Custo |
|---|---|---|
| **Muito Elevado** | **Muito Elevado** | **Baixo** |

### Definição

Mecanismo que concede acesso a serviços a partir de uma autenticação criptográfica assimétrica, mais concretamente a partir de criptografia de chave pública (par de chaves pública/privada único), usando autenticadores biométricos existentes nos dispositivos móveis (*smartphones* e computadores portáteis) dos utilizadores.

### Prós

- Mecanismo suportado por diversos fabricantes de *smartphones*, computadores e respetivos sistemas operativos;
- Necessidade de investimento reduzida;
- Aumento contínuo dos *websites* e serviços *online* que suportam autenticação FIDO;
- Mecanismo não vulnerável a ataques de engenharia social para o roubo de credenciais;
- Não depende de outros dispositivos;
- Autenticação fácil e rápida sem comprometer o utilizador do ponto de vista de segurança.

### Contras

- Mecanismo dependente de dispositivos que estão na posse do utilizador, portanto na situação de esquecimento, roubo ou perda do dispositivo o mecanismo de autenticação não poderá ser concretizado.

## Observações/Recomendações

Mecanismo de autenticação semelhante ao identificado na categoria “algo que o utilizador tem”, mas que difere no dispositivo usado, que ao contrário de ser uma chave de segurança física como uma pen usb ou chaveiro (*key-fob*), é o dispositivo móvel utilizado habitualmente pelo utilizador, com leitor de impressão digital ou capacidade de reconhecimento facial incorporados.

Relativamente a requisitos, o dispositivo móvel deverá ter um sistema operativo que permita a instalação de um autenticador FIDO que será usado para aceder a serviços *online* a partir do *browser* e, por sua vez, esses serviços *online* deverão ser compatíveis com o autenticador FIDO, o que permitirá cumprir com o padrão WebAuthn.

No momento do registo no serviço *online* é solicitado ao utilizador que escolha um autenticador FIDO disponível, e que seja compatível com a política de aceitação do serviço *online*. De seguida, o utilizador desbloqueia o autenticador FIDO, usando um método de desbloqueio definido previamente no dispositivo (por impressão digital, reconhecimento facial), que por sua vez cria um novo par de chaves pública/privada único.

A chave privada e respetivos dados biométricos são guardados e retidos localmente no dispositivo. A chave pública é enviada para o serviço *online* e associada à conta do utilizador.

No processo de autenticação, após conclusão do processo de registo, o serviço *online* solicita que o utilizador efetue a autenticação utilizando um dispositivo anteriormente registado, e o utilizador, por sua vez, desbloqueia o autenticador FIDO com recurso ao mecanismo definido aquando do registo. Uma vez que o dispositivo usa a conta solicitada pelo serviço *online*, o mesmo seleciona a chave privada para assinar o desafio e envia-o de volta para o serviço *online*. O serviço *online* verifica o desafio com a chave pública e concede desta forma acesso ao utilizador.

## Exemplos de aplicação (Não exaustivo)

- Mecanismo reconhecido e cada vez mais disponível em múltiplos sistemas operativos e serviços *online*.

## 3.4 Recomendações a considerar na fase de implementação

- Garantir a implementação de mecanismos de monitorização e auditoria das soluções de autenticação, nos sistemas e infraestrutura;
- Implementar procedimentos para a substituição segura de dispositivos de autenticação;
- Comunicar aos colaboradores eventuais alterações às políticas de utilização de mecanismos de autenticação;
- Formar periodicamente os utilizadores das soluções sobre o funcionamento das mesmas, e os meios através dos quais podem reportar anomalias ou solicitar apoio;
- Considerar a implementação de mecanismos que possam desabilitar contas de utilizadores que possam ter sido comprometidas;
- Considerar a implementação de canais de comunicação ou mecanismos que possam habilitar o utilizador a recuperar o acesso a serviços;
- Garantir que a solução de autenticação selecionada armazena, de forma segura, os registos das ações realizadas pelos utilizadores envolvidos (entradas/*login*, e saídas/*logout* e operações realizadas de acordo com o conjunto de políticas estabelecidas pela organização).

| NOTA | Devem ser comunicados os pedidos de autenticação autorizados e não autorizados aos sistemas de auditoria e monitorização da organização. Isto permite que o sistema de monitorização assinale atividades irregulares. |
|---|---|

## 3.5 Início de Sessão Único (SSO - *Single Sign-On*)

As organizações podem ainda considerar a adequação do sistema de **Início de Sessão Único (SSO - Single *Sign-On*).** O SSO é uma funcionalidade que permite ao utilizador iniciar sessão apenas uma vez e aceder a sistemas e aplicações diferentes e independentes. Consequentemente, este método de autenticação evita que os utilizadores introduzam credenciais para cada serviço. O SSO permite-lhes iniciar sessão uma vez através de um sistema de autenticação central conhecido como Fornecedor de Identidade (IdP). O MFA pode ser combinado com o SSO para proporcionar segurança e conveniência ao utilizador, uma vez que o primeiro acrescenta uma ou mais camadas de verificação, dificultando o acesso não autorizado, enquanto o SSO aumenta o nível de usabilidade.

# 4. Considerações Finais

A autenticação multifator é uma solução que permite às organizações reduzir o risco de concretização de alguns ataques. No entanto, esta solução deverá operar, em simultâneo, com as políticas e medidas de cibersegurança da organização, formando uma barreira comum de sistemas de segurança. O CNCS apresenta, através do Quadro Nacional de Referência para a Cibersegurança (QNRCS), um conjunto de controlos que podem ser implementados, e que apoiam as organizações a construir uma estratégia de segurança contextual e focada em pessoas, processos e tecnologia.

# 5. Parceiros

No âmbito de elaboração deste guia, o Centro Nacional de Cibersegurança (CNCS) contou com contributos de diversas entidades, nomeadamente:

- Agência para a Modernização Administrativa (AMA);
- Centro de Gestão da Rede Informática do Governo (CEGER);
- Ministério dos Negócios Estrangeiros (MNE);
- Segurança Social;
- Secretaria-Geral da Presidência do Conselho de Ministros (SGPCM);
- Serviços Partilhados do Ministério da Saúde (SPMS).

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Centro Nacional de Cibersegurança
Rua da Junqueira, 69 | 1300-342 Lisboa
cncs@cncs.gov.pt | (+351) 210 497 400