Universidade da Maia
Departamento de Ciências da Comunicação e Tecnologias da Informação

# Controlo de acessos físicos

Criação de uma solução segura de controlo de acessos físicos para a Umaia

João Pedro Couto de Sousa

Tecnologias de Informação, Comunicação e Multimédia da Universidade da Maia

Orientação

João Paredes

07/2025


# Controlo de acessos físicos

Criação de uma solução segura de controlo de acessos físicos para a UMaia

João Pedro Couto de Sousa

A033026

2024/2025

Orientação de

Eng.º João Paredes

Esta dissertação foi submetida em cumprimento parcial dos requisitos para o Mestrado em Tecnologias de Informação, Comunicação e Multimédia da Universidade da Maia

Maia, 11 de Julho, 2025

**Resumo**

O controlo de acessos em espaços técnicos sensíveis é uma componente essencial da segurança institucional. Esta dissertação apresenta o desenvolvimento de uma solução eletrónica para substituição do sistema convencional baseado em chaves físicas, aplicada ao Laboratório 10 da Universidade da Maia. A proposta pretende resolver fragilidades associadas ao uso tradicional de fechaduras mecânicas, assegurando maior fiabilidade, rastreabilidade e restrição de entrada.

A solução recorre à autenticação por cartão NFC, utilizando o cartão universitário já emitido aos utilizadores, com o intuito de simplificar o acesso e, simultaneamente, reforçar as medidas de segurança. O sistema foi concebido para ser modular e escalável, permitindo a futura integração de autenticação dupla através de código PIN, introduzido num teclado matricial.

A arquitetura do sistema contempla um *interface* com um servidor remoto responsável pela validação das credenciais, para simular o *backend*. Esta escolha permitiu maior agilidade na configuração e controlo do sistema, evitando constrangimentos impostos por dependência de *hardware* físico.

Entre as propostas para desenvolvimento futuro, destaca-se a separação lógica das funções de autenticação e ativação do mecanismo de abertura, através de dois microcontroladores distintos, bem como a adoção de protocolos de comunicação segura (como TLS), a integração de uma plataforma de gestão com interface gráfica, a introdução de uma fonte de alimentação redundante, a possibilidade de controlo simultâneo de várias portas e a inclusão de um sistema independente para registo e controlo da saída dos utilizadores.

Em suma, este trabalho contribui para o reforço da segurança física em contexto académico, promovendo a automação do controlo de acessos de forma eficaz e alinhada com as boas práticas da cibersegurança e da engenharia de sistemas embarcados.

**Expressões-chave:** Segurança, Autenticação, Sistema

**Abstract**

Access control in sensitive technical areas is an essential component of institutional security. This dissertation presents the development of an electronic solution to replace the conventional system based on physical keys, applied to Laboratory 10 at the University of Maia. The proposed system aims to address vulnerabilities associated with the traditional use of mechanical locks, ensuring greater reliability, traceability, and restricted access.

The solution employs NFC card authentication, using the university card already issued to users, with the goal of simplifying access while simultaneously enhancing security measures. The system was designed to be modular and scalable, allowing for future integration of two-factor authentication via a PIN code entered on a keypad.

The system architecture includes an interface with a remote server responsible for credential validation, simulating the backend. This approach allowed for greater flexibility in configuring and managing the system, avoiding constraints imposed by reliance on physical hardware.

Among the proposals for future development are the logical separation of authentication and door unlocking functions through the use of two distinct microcontrollers, the adoption of secure communication protocols (such as TLS), the integration of a management platform with a graphical interface, the addition of a redundant power supply, the ability to control multiple doors simultaneously, and the inclusion of an independent system for user exit logging and control.

In summary, this work contributes to strengthening physical security in an academic setting by promoting effective access control automation, aligned with best practices in cybersecurity and embedded systems engineering.

**Key-expressions:** Security, System, Autentication

# Declaração de honra

Por este meio se declara que este documento é conteúdo original, produzido pelo identificado como autor, não tendo sido previamente apresentado noutro percurso académico ou unidade curricular de qualquer instituição.

Quaisquer referências a outros trabalhos respeitam rigorosamente os regulamentos e melhores práticas de atribuição, sendo apropriadamente marcadas no texto e identificadas na secção *Referências* na página 54, sob as normas IEEE[1] de referenciação.

O autor igualmente declara não se encontrar em qualquer situação efectiva ou potencial de conflito de interesses.

[1] IEEE — *Institute of Electrical and Electronics Engineers*

# Agradecimentos

A conclusão deste trabalho representa não apenas o culminar de uma etapa académica, mas também o reflexo do apoio, dedicação e contributo de várias pessoas e instituições, às quais expresso a minha mais profunda gratidão.

Em primeiro lugar, um agradecimento muito especial ao Professor João Paredes, pela orientação incansável, pela clareza com que sempre respondeu às dúvidas e pelo tempo que dedicou ao acompanhamento deste projeto. A sua disponibilidade e exigência foram decisivas para a evolução do trabalho e para o meu crescimento académico.

À Universidade da Maia (UMAIA), agradeço pelo suporte institucional e pelos meios técnicos disponibilizados, que permitiram a implementação prática e a validação do sistema. A infraestrutura e o ambiente proporcionado foram fundamentais para o desenvolvimento desta dissertação.

À minha família, agradeço de forma sentida por todo o apoio, incentivo constante e compreensão ao longo deste percurso. O seu apoio incondicional foi essencial em todos os momentos, sobretudo nos mais exigentes.

A todos os que, direta ou indiretamente, contribuíram com sugestões, encorajamento e motivação, deixo também o meu sincero agradecimento.

# Conteúdo

# Lista de Figuras

# Lista de Tabelas

# Lista de excertos de código e terminal

# Siglas

**2FA** *Two factor authentication*

**ABAC** *Attribute-Based Access Control*

**ACK** *Acknowledgement*

**AJAX** *Asynchronous Javascript And* XML

**API** *Application Programming Interface*

**BLE** *Bluetooth Low Energy*

**CISA** *Cybersecurity Infrastructure Security Agency*

**CNCS** Centro Nacional de Ciber Segurança

**CPU** *Central Processing Unit*

**CS** *Chip Select*

**CSS** *Cascading Style Sheets*

**CSV** *Comma Separated Values*

**EAD** Ensino-Aprendizagem Digital

**EDR** *Endpoint detection and response*

**HTML** *Hypertext Markup Language*

**HTTP** *Hypertext Transfer Protocol*

**HTTPS** *Hypertext Transfer Protocol Secure*

**IA** *Artificial Intelligence*

**IBAC** *Identity-Based Access Control*

**IDE** *Integrated Development Environment*

**IEEE** *Institute of Electrical and Electronics Engineers*

**IETF** *Internet Engineering Task Force*

**INCM** Imprensa Nacional Casa da Moeda

**INESC TEC** Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência

**IoT** *Internet of Things*

**IP** *Internet Protocol*

**IPv6** *Internet Protocol version 6*

**I²C** *Inter-Integrated Circuit*

**LCD** *Liquid Crystal Display*

**MISO** *Master In Slave Out*

**MoC** *Match-On-Card*

**MOSI** *Master Out Slave in*

**NACK** *Negative Acknowledgement*

**NAT** *Network Address Translation*

**NFC** *Near-Field Communication*

**PHP** *Hypertext Preprocessor*

**PIN** *Personal Identification Number*

**POCER-SAS** Programa Operacional de Capacitação e Eficiência de Recursos dos Serviços de Ação Social

**QR** *Quick Response*

**RBAC** *Role-Based Access Control*

**RFID** *Radio-Frequency IDentification*

**RGPD** Regulamento Geral de Protecção de Dados

**SCK** *Serial Clock*

**SCL** *Serial Clock Line*

**SD** *Secure Digital*

**SDA** *Serial Data Line*

**SPI** *Serial Peripheral Interface*

**SS** *Slave Select*

**SSH** *Secure Shell*

**TFT** *Thin Film Transistor*

**TLS** *Transport Layer Security*

**UID** *Unique Identifier*

**UMAIA** *Universidade da Maia*

**UPS** *Uninterruptible Power Supply*

**URL** *Uniform Resource Locator*

**VM** *Virtual Machine*

# Capítulo 1

# Introdução

A presente dissertação aborda o processo de desenvolvimento de uma solução para controlo de acessos e identificação de presenças, explorando práticas modernas que conciliam eficiência, segurança e acessibilidade. A investigação destaca a importância de inovar processos rotineiros, promovendo melhorias no acompanhamento de presenças e simplificação logística em contextos educacionais.

## 1.1 Contexto e motivação

O Laboratório 10 da Universidade da Maia desempenha um papel essencial no ensino e investigação, sendo utilizado por alunos e docentes para atividades práticas e albergando equipamentos críticos de elevado valor, incluindo os servidores Forge, que suportam projetos e avaliações fundamentais para a universidade. Contudo, a ausência de mecanismos adequados de controlo de acessos tem gerado preocupações significativas quanto à segurança, gestão eficiente e uso adequado dos recursos.

Os problemas identificados incluem a falta de monitorização de entradas e saídas, o acesso desprotegido a equipamentos, a ausência de um sistema robusto de gestão de permissões e a dificuldade em auditar o uso do espaço. Estas fragilidades aumentam o risco de utilização indevida dos recursos e comprometem a proteção dos sistemas críticos.

## 1.2 Enquadramento

Com os avanços tecnológicos, os métodos de controlo de acessos têm evoluído significativamente para responder às necessidades de segurança em espaços críticos. Instituições de ensino e investigação, como a Universidade da Maia, enfrentam desafios específicos relacionados com a proteção de equipamentos de elevado valor, a gestão de permissões de acesso e a rastreabilidade de utilização de recursos.

Este trabalho insere-se neste contexto, propondo o desenvolvimento de uma solução tecnológica que integre sistemas avançados de controlo de acessos e gestão de permissões, com o objetivo de melhorar a segurança, simplificar a utilização do espaço e criar uma base para futuras inovações na área.

## 1.3 Objetivos

O principal objetivo deste trabalho é desenvolver um sistema de controlo de acessos para o Laboratório 10 da Universidade da Maia, de forma a aumentar a segurança dos equipamentos críticos e otimizar a gestão do espaço. Entre os objetivos específicos destacam-se:

- Implementar um sistema de controlo de acessos eficaz e monitorizar entradas e saídas;
- Reforçar a proteção dos equipamentos de rede impedindo acessos não autorizados;
- Gerir permissões de acesso partir de uma base de dados centralizada e segura;
- Promover escalabilidade, desenvolvendo uma solução tecnológica com potencial para ser expandida a outros contextos.

## 1.4 Estrutura do documento

Este relatório está estruturado de forma a garantir uma apresentação clara e lógica dos temas abordados. O documento inicia-se com *os Resumos em português e inglês* (*Abstract*), seguindo-se a *Declaração de honra*, que atesta a autenticidade do trabalho.

No Capítulo 1, *Introdução*, são apresentados o *Contexto e motivação*, o *Enquadramento* e os *Objetivos* do estudo.

O Capítulo 2, *Análise do problema*, examina as principais questões e desafios relacionados com a falta de controlo de acessos e a segurança no Laboratório 10.

O Capítulo 3, *Fundamentos Teóricos*, oferece uma análise detalhada sobre infraestruturas críticas, segurança e controlo de acessos, sustentando as bases teóricas necessárias para compreender a importância das soluções propostas.

No Capítulo 4, *Estado da Arte*, são apresentados exemplos práticos de implementação de sistemas de controlo de acessos, com foco em instituições de referência proporcionando uma visão abrangente das soluções atualmente em uso.

Cada capítulo foi estruturado para desenvolver, de forma progressiva, os temas essenciais, permitindo uma compreensão clara e fundamentada do problema e das soluções propostas.

# Capítulo 2

# Análise do problema

O Laboratório 10 da Universidade da Maia é uma área destinada ao ensino e investigação na área de redes e que contém equipamentos críticos cujas características e elevado valor tornam fundamental um controlo rigoroso sobre o acesso ao espaço e a utilização dos recursos ali presentes. Contudo, foi identificado um conjunto de problemas significativos relacionados com a falta de mecanismos de controlo de entrada e saída das pessoas que frequentam a sala, o que levanta preocupações ao nível da segurança, gestão e integridade dos equipamentos. Dado que os alunos frequentam este laboratório durante as aulas para atividades práticas relacionadas com o curso, a necessidade de um sistema que permita gerir o acesso aumenta para que as aulas sejam dadas dentro da normalidade.

Adicionalmente, é na sala técnica deste laboratório que estão alojados os servidores Forge da Universidade da Maia (um serviço de apoio ao desenvolvimento de projetos e respetiva avaliação, utilizado amplamente pela universidade), o que torna ainda mais crítica a necessidade de controlo de acessos deste laboratório.

As secções seguintes detalham os principais problemas observados.

## 2.1 Falta de controlo de acessos

Atualmente, o Laboratório 10 não possui um sistema eficaz que permita monitorizar quem entra e sai da sala, resultando numa falta de controlo sobre as pessoas que utilizam o espaço. Esta ausência de monitorização não só limita a capacidade de identificar o tempo exato que cada pessoa (aluno, docente ou pessoal de apoio) passa dentro da sala, como também impede a contabilização e análise de padrões de uso do espaço. A inexistência deste tipo de controlo pode levar a falhas de segurança e à utilização inadequada ou abusiva dos recursos.

## 2.2 Acesso desprotegido a equipamentos de grande valor

Foi também identificada uma grande facilidade de acesso aos equipamentos de rede que se encontram no laboratório. Estes equipamentos, devido ao seu custo elevado e importância para o bom funcionamento das aulas, requerem uma proteção reforçada, especialmente contra acessos não autorizados ou indevidos. A ausência de um sistema que restrinja o acesso a estes equipamentos compromete não só a segurança física dos dispositivos, mas também a integridade da rede da instituição, uma vez que qualquer falha ou manipulação pode ter consequências graves no funcionamento dos sistemas de comunicação e informática.

## 2.3 Falta de controlo de permissões de acesso

Um dos fatores que contribui para a falta de controlo de acesso é a ausência de um sistema adequado de gestão de abertura da sala. Atualmente, apesar de existir uma lista na segurança da portaria do *campus*, não existe uma base de dados que registe quem tem permissão para entrar no laboratório e quem possui as chaves de acesso do mesmo. Esta falta de controlo impede que haja uma verificação eficaz sobre quem pode entrar no laboratório.

## 2.4 Dificuldade em auditar o uso do laboratório

Sem um sistema de controlo ou monitorização que permita auditar quem utiliza o laboratório e em que condições, torna-se difícil garantir que o espaço está a ser utilizado para os fins previstos. Esta falta de registo e auditoria limita a possibilidade de corrigir práticas inadequadas e dificulta a implementação de medidas preventivas para garantir a segurança do laboratório.

# Capítulo 3

# Fundamentos Teóricos

Este capítulo aborda os conceitos fundamentais sobre segurança em infraestruturas críticas, com foco no controlo de acessos. São exploradas a definição, a importância e os desafios destas infraestruturas, bem como as tecnologias para implementar sistemas de segurança físicos e lógicos, contextualizando a sua relevância em ambientes educacionais e laboratoriais.

## 3.1 Infraestruturas críticas

Laboratórios e sistemas de rede que suportam atividades pedagógicas e de investigação exigem estratégias eficazes de proteção e controlo de acessos para garantir a continuidade e a integridade das operações dado que a sua interrupção pode ter consequências significativas. A sua proteção torna-se, portanto, uma prioridade para as instituições.

### 3.1.1 Definição de infraestruturas críticas

Infraestruturas críticas são instalações, sistemas ou ativos essenciais para o funcionamento contínuo e seguro de uma organização ou comunidade, cuja interrupção pode ter consequências significativas. Segundo a CISA[1], infraestruturas críticas são recursos físicos ou virtuais indispensáveis para a segurança, saúde e funcionamento de sistemas económicos e sociais. Escolas ou universidades, laboratórios com equipamentos de rede valiosos e vitais para a comunicação e aprendizagem enquadram-se nesta definição, devido ao seu papel crucial no suporte a atividades académicas e/ou de investigação[1].

Considera-se então:

- A presença de equipamentos de elevado valor e/ou importância operacional para a rede torna o ambiente em questão crítico;

[1]CISA – *Cybersecurity Infrastructure Security Agency*

- A interrupção, perda ou manipulação incorreta desses equipamentos pode comprometer a segurança da rede e/ou impactar diretamente o ensino e a pesquisa, bem como as operações da rede institucional.

Estes fatores fazem com que a segurança de infraestruturas críticas seja uma prioridade, exigindo uma solução de controlo que resulte de uma combinação de políticas e tecnologias adequadas.

### 3.1.2 Segurança em infraestruturas críticas

A segurança em infraestruturas críticas abrange vários pontos que têm como principal objetivo prevenir acessos não autorizados, garantir a integridade dos ativos e assegurar que todas as operações ocorram de forma segura e conforme planeado. Em laboratórios educacionais, onde há uma elevada rotatividade de utilizadores (alunos, docentes ou técnicos), a segurança assume uma relevância ainda maior, pois a exposição a possíveis riscos e ameaças aumenta.

Esses pontos tocam em diferentes tipos de segurança:

- Segurança física: previne o acesso não autorizado a espaços e equipamentos neles presentes, reduzindo a probabilidade de danos acidentais ou intencionais;
- Segurança lógica: visa proteger sistemas e redes contra acessos digitais não autorizados e ameaças relacionadas com a cibersegurança, utilizando ferramentas de configuração de rede, autenticação e controlo de permissões, nomeadamente[2]:
  - *firewall*;
  - EDR[2]
  - anti-vírus;
  - cópias de segurança;
  - *disaster recovery*;
  - ligações privadas e seguras;
  - monitorização do sistema;
- Segurança de dados: no caso de equipamentos de rede, que podem conter dados sensíveis e configurações essenciais, é crucial evitar acessos indevidos que possam comprometer a integridade e confidencialidade dos dados[3].

A implementação de mecanismos e práticas de segurança que abordem estes pontos permite reduzir significativamente os riscos e assegurar que os recursos sejam utilizados de forma segura e responsável.

[2]EDR – *Endpoint detection and response*

### 3.1.3 Importância da segurança em ambientes educacionais

Nos ambientes educacionais, a segurança de infraestruturas que influenciam o correto funcionamento das aulas assume um papel de grande relevância, visto que esses espaços são partilhados por diversos perfis de utilizadores, como estudantes e professores, o que exige atenção adicional[4]

- rotatividade de pessoas – num laboratório de ensino, o grande número de alunos e professores em constante troca de salas de aulas requer monitorização contínua de acessos e permissões, vigiando o uso indevido dos recursos;
- vulnerabilidade ao erro humano – a curiosidade natural dos alunos em explorar tecnologias pode originar acessos acidentais a equipamentos ou configurações, podendo resultar em falhas nos mesmos;
- integração da segurança com a experiência educacional – a segurança de um laboratório de redes deve equilibrar a proteção dos recursos com a acessibilidade aos mesmos, de modo a que o ambiente de laboratório continue a cumprir o seu propósito pedagógico sem comprometer a integridade dos equipamentos.

Este equilíbrio entre segurança e acessibilidade em ambientes educacionais requer uma abordagem que permita o acesso a quem dele necessita, minimizando, ao mesmo tempo, o impacto na experiência de aprendizagem para possibilitar que o espaço permaneça seguro para todos.

## 3.2 Controlo de acessos

A proteção de infraestruturas críticas exige sistemas de controlo de acesso bem estruturados que restrinjam e monitorizem quem pode entrar no espaço e quem pode aceder aos equipamentos presentes nesse local. Estes sistemas são geralmente classificados em duas categorias principais:

- controlo de acesso físico;
- controlo de acesso lógico.

Ambos são essenciais para garantir a segurança e a integridade dos equipamentos e proteger dados sensíveis que possam ser processados ou armazenados no laboratório.

### 3.2.1 Controlo de acesso físico

Segundo CNCS[3] "*Devem existir controlos de acesso físico às redes e sistemas de informação*"[5], afirmando ainda a mesma fonte que "*A organização deve proteger e gerir o acesso físico às suas infraestruturas de rede e de sistemas de informação. A organização deve aplicar este controlo aos seus colaboradores e visitantes, a zonas da organização que sejam de acesso restrito e/ou a áreas sensíveis que alojem informação confidencial, redes e/ou sistemas de informação....*". Alguns exemplos de controlo[6, 7]:

- Chaves e fechaduras convencionais – são o método mais disseminado mas possuem limitações significativas, como a dificuldade de monitorizar quem entra e sai do espaço e o risco da execução de cópias não autorizadas;
- Cartões eletrónicos *smart cards* ou RFID[4] – os cartões eletrónicos, equipados com tecnologias como RFID, são amplamente usados em ambientes com alta exigência de segurança. Estes cartões, através de um sistema preparado para isso, permitem um controlo eletrónico de acessos, criando um registo de quem entrou no espaço. Caso um cartão seja perdido, o sistema é configurado para deixar de aceitar esse cartão, mantendo a segurança do espaço sem a necessidade de mudanças físicas nas fechaduras;
- Equipamentos biométricos – tecnologias de impressão digital, reconhecimento facial e leitura da íris utilizam características únicas dos utilizadores o que pode tornar o controlo de acessos mais robusto. Este tipo de equipamentos não elimina a necessidade de utilização de objetos físicos, como chaves ou cartões, no entanto pode ser utilizado como complemento de acesso.

### 3.2.2 Controlo de acesso lógico

O controlo de acesso lógico complementa o controlo físico, sendo focado na restrição de acesso a recursos. Este tipo de controlo aplica-se a redes, servidores, bases de dados, sistemas de gestão e outros equipamentos críticos de rede[8]:

- Autenticação de utilizadores – a autenticação é o processo de confirmação da identidade do utilizador antes de permitir acesso aos recursos digitais. Isto pode ser feito através de senhas, autenticação de dois fatores 2FA[5] ou métodos biométricos (como reconhecimento facial ou impressão digital). Cada utilizador possui um conjunto de credenciais único, garantindo que apenas pessoas autorizadas possam aceder aos sistemas (isto caso as mesmas não partilhem credenciais)[9];

[3] CNCS – Centro Nacional de Ciber Segurança
[4] RFID – *Radio-Frequency IDentification*
[5] 2FA – *Two factor authentication*

- Permissões e privilégios de acesso: o controlo de acesso lógico também envolve a definição de diferentes níveis de permissões para os utilizadores – por exemplo, os alunos podem ter acesso limitado a certos equipamentos, enquanto docentes e técnicos de rede possuem privilégios elevados – o que resulta em que cada utilizador tenha acesso apenas aos recursos necessários para as suas atividades, prevenindo a manipulação indevida de equipamentos críticos;

- Auditoria e monitorização de atividades digitais: a monitorização contínua das atividades nos sistemas e dispositivos digitais é essencial para vigiar eventuais falhas existentes no sistema. As auditoria permitem registar as atividades realizadas nos equipamentos, facilitando a identificação de possíveis incidentes de segurança[10].

### 3.2.3 Exemplos de controlo de acessos

Existem várias abordagens de controlo de acessos, cada uma com características e benefícios específicos. A escolha de um sistema de controlo de acesso deve considerar as necessidades específicas do laboratório, o perfil dos utilizadores e o nível de segurança requerido. Alguns exemplos:

- IBAC, ou *Identity-Based Access Control*, (figura 3.1) é uma abordagem que concede ou nega acesso com base na identidade individual do utilizador, como o nome de utilizador e a palavra-passe[11]:
  - Vantagens: permite personalizar o acesso de acordo com o nível de privilégio do utilizador em questão (ex: alunos, docentes ou técnicos);
  - Desvantagens: requer uma gestão contínua das permissões, o que pode ser complexo e exigente em ambientes com muitos utilizadores;

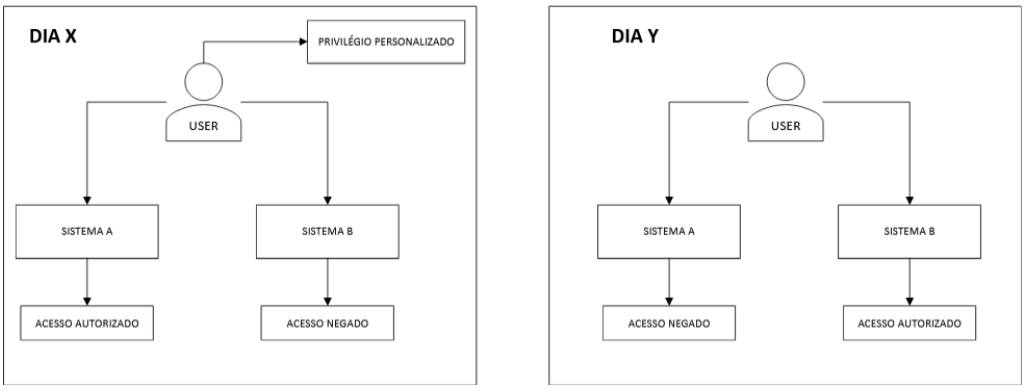


**Figura 3.1:** *IBAC*

- Em RBAC, ou *Role-Based Access Control*, os acessos são atribuídos consoante funções ou papéis dentro de uma instituição (por exemplo, se for aluno, fica com os

acessos iguais aos restantes utilizadores no grupo de alunos, aplicando-se o mesmo aos restantes cargos, docentes, técnicos, entre outros). O responsável consegue, de uma maneira mais simples, atribuir permissões a grupos de funções em vez de o fazer individualmente (figura 3.2).

  - Vantagens: reduz a complexidade da gestão de acessos e permite um controlo mais eficiente, especialmente em casos que existe um número elevado de utilizadores;
  - Desvantagens: caso haja necessidade de adaptar acessos específicos para um utilizador dentro de uma função, este método deixa de ser válido pois é necessário fazê-lo individualmente[12, 13].


**Figura 3.2:** *RBAC*
(Fonte: [14])

- ABAC (*Attribute-Based Access Control*) – permite definir as permissões com base numa combinação de atributos do utilizador, como função, departamento, nível de autorização (figura 3.3).

  - Vantagens: proporciona um nível elevado de flexibilidade e pode ser ajustado para necessidades específicas, permitindo uma personalização completa de acessos;
  - Desvantagens: é complexo de implementar e requer uma gestão rigorosa de atributos e políticas, o que pode ser um desafio em ambientes académicos ou ambientes empresariais de grande dimensão[15].

### 3.2.4 Estratégias e tecnologias de um controlo de acessos

As estratégias e tecnologias de controlo de acessos desempenham um papel fundamental na proteção de infraestruturas críticas, permitindo uma gestão eficiente e segura dos recursos físicos e digitais. A sua implementação não só protege os acessos não autorizados como também permite a continuidade das operações e integridade dos sistemas.

#### A importância da existência de um controlo de acessos

O controlo de acesso e a monitorização constituem elementos-chave da segurança em infraestruturas críticas, permitindo a restrição de entrada apenas a pessoas autorizadas

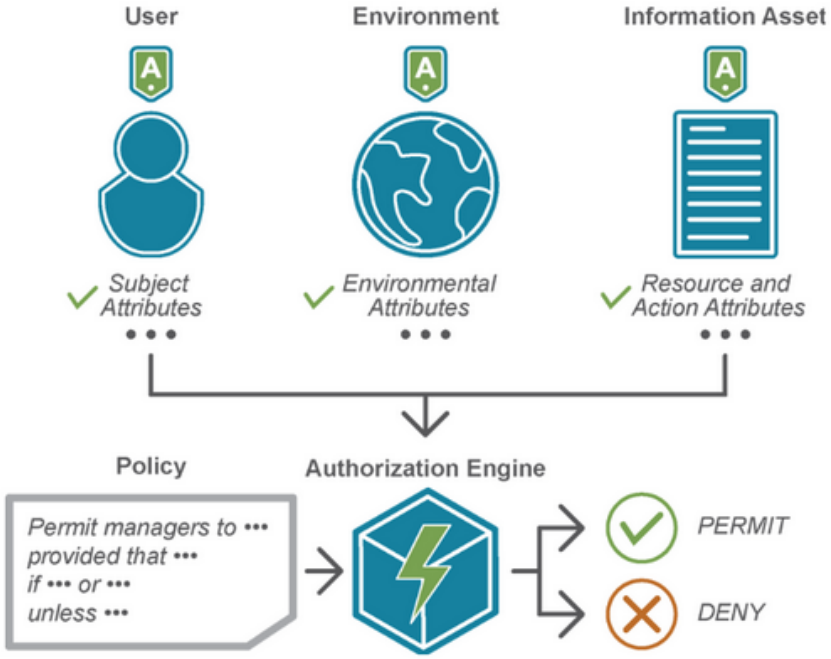


**Figura 3.3:** *ABAC*
(Fonte: [16])

e o acompanhamento das atividades realizadas. Os principais objetivos a cumprir num sistema de controlo de acessos incluem:

- Proteção de recursos e equipamentos: prevenir o uso não autorizado dos equipamentos de rede garantindo que apenas pessoas com autorização específica acedam aos recursos críticos;
- Garantia de segurança e integridade: proteger a infraestrutura contra danos físicos
- Responsabilização: criar registos detalhados de acessos e atividades permitindo, assim, uma análise de auditoria mais rigorosa que permita, em caso de falha ou perda do sistema, apurar responsáveis.

### 3.2.5 Requisitos para um sistema de controlo de acessos

Para que seja eficaz, um sistema de controlo de acessos deve cumprir requisitos específicos que garantam tanto a segurança física quanto lógica. Abaixo e de forma sintetizada, apresenta-se os principais requisitos a ter em conta:

- Monitorização em tempo real;
- Registo de entrada e saídas;
- Flexibilidade e escalabilidade;
- Conformidade com as Políticas de Segurança Institucionais.

### 3.2.6 Análise de Riscos em Sistemas de Acesso

A segurança em sistemas de controlo de acessos constitui um dos pilares fundamentais na protecção de recursos físicos e digitais. Estes sistemas visam garantir que apenas utilizadores autorizados possam aceder a determinados espaços ou funcionalidades, protegendo assim informação sensível ou zonas restritas.

A autenticação pode basear-se em três factores principais:

- Algo que o utilizador possui (ex.: cartão, chave, *token*);
- Algo que o utilizador sabe (ex.: código PIN, palavra-passe);
- Algo que o utilizador é (ex.: impressão digital, reconhecimento facial).

A autenticação de dois fatores (2FA) consiste na combinação de dois destes elementos, aumentando o nível de segurança. Neste projeto, é utilizada a combinação de um cartão NFC (algo que o utilizador possui) com um código PIN (algo que o utilizador sabe), o que segue as boas práticas de segurança recomendadas por normas como a *ISO/IEC 27001*.

## 3.3 Comunicações I²C e SPI

Para permitir a comunicação entre microcontroladores e dispositivos periféricos, são frequentemente utilizados protocolos de comunicação digital como o I²C e o SPI[6].

### I²C (Inter-Integrated Circuit)

O protocolo I²C é utilizado em sistemas embebidos devido à sua simplicidade e eficiência na comunicação entre dispositivos. Trata-se de um protocolo de comunicação série síncrona que utiliza apenas duas linhas: a linha de dados (*SDA*[7]) e a linha de relógio (*SCL*[8]). [17]

Entre as principais vantagens do protocolo I²C destacam-se:

- Redução significativa do número de fios necessários, o que simplifica a construção de circuitos;
- Facilidade na expansão do sistema, bastando adicionar novos dispositivos ao barramento com endereços distintos;
- Comunicação bidirecional entre *master-slave*;
- Compatibilidade com uma vasta gama de sensores, ecrãs LCD, entre outros[17].

[6] SPI – *Serial Peripheral Interface*
[7] SDA – *Serial Data Line*
[8] SCL – *Serial Clock Line*

Apesar das suas vantagens, o I²C tem algumas limitações, nomeadamente em termos de velocidade de transmissão, que é inferior à de outros protocolos como o SPI. As frequências típicas variam entre 100 kHz (modo padrão) e 400 kHz (modo rápido), podendo alcançar até 1 MHz ou 3,4 MHz em modos mais avançados. Para além disso, uma vez que todos os dispositivos partilham o mesmo barramento, podem ocorrer interferências em ambientes elétricos ruidosos ou em sistemas com muitos dispositivos[17].

### SPI (Serial Peripheral Interface)

O SPI é um protocolo de comunicação síncrona em série, amplamente utilizado em sistemas embutidos devido à sua elevada velocidade e simplicidade. Este protocolo utiliza tipicamente quatro fios:

- **MOSI**[9]: linha de dados do *master* para o *slave*;
- **MISO**[10]: linha de dados do *slave* para o *master*;
- **SCK**[11]: sinal de relógio gerado pelo *master*;
- **SS**[12], também designado por CS[13] linha para selecionar o *slave* activo.

A arquitetura do SPI segue um modelo *master–slave*, com o *master* a controlar o relógio e a seleção dos *slaves*. Esta configuração permite comunicação *full-duplex*[14], em que o *master* envia e recebe dados simultaneamente – uma vantagem em relação ao I²C, cujo funcionamento é *half-duplex*[15].

As principais vantagens do SPI são:

- **Simplicidade de *hardware*** – o protocolo é simples de implementar, não requer resistências de *pull-up* e dispensa qualquer forma confirmação de receção[18];
- **Configuração flexível** – suporta múltiplos *slaves* através de linhas SS dedicadas, sem necessidade de endereçamento interno como no I²C[19];
- **Compatibilidade** com inúmeros periféricos – como sensores, memórias *flash*, cartões SD[16], ecrãs LCD/TFT e módulos NFC[19].

[9] MOSI – *Master Out Slave in*
[10] MISO – *Master In Slave Out*
[11] SCK – *Serial Clock*
[12] SS – *Slave Select*
[13] CS – *Chip Select*
[14] *full-duplex* é um modo de transmissão de dados que pode ocorrer em ambas as direções em simultâneo através do mesmo canal de comunicação.
[15] *half-duplex* é um modo de transmissão de dados que pode ocorrer em ambas as direções mas apenas alternadamente.
[16] SD – *Secure Digital*

Contudo, o SPI também apresenta algumas limitações:

- **Exige mais fios** – cada *slave* adicional requer uma linha SS independente[20];
- Ausência de **mecanismos de verificação** de erros como ACK[17]/NACK[18][21];
- Não permite *hot-swap*, ou seja, os dispositivos devem ser ligados antes da comunicação e estar ligados até à substituição.

## 3.4 Arquiteturas cliente-servidor em sistemas embutidos

O modelo cliente-servidor é amplamente utilizado em sistemas distribuídos. Neste modelo, o cliente envia pedidos e o servidor responde com os dados ou validações necessárias. As principais vantagens desta arquitetura são[22]:

- Centralização da lógica de autenticação;
- Facilidade de atualização de permissões e dados de utilizadores;
- Registo centralizado dos acessos efetuados.

Este modelo é particularmente eficaz quando utilizado com micro-controladores com capacidade de comunicação por Wi-Fi, como o ESP8266 ou o ESP32, que suportam protocolos como HTTP.

## 3.5 Validação remota e privacidade dos dados

A validação remota dos dados de autenticação, sem que estes sejam armazenados localmente no dispositivo, é uma medida fundamental para garantir a segurança e a privacidade dos utilizadores. Este tipo de validação[23]:

- Minimiza os riscos em caso de acesso físico ao equipamento;
- Facilita o cumprimento do Regulamento Geral de Protecção de Dados (RGPD);
- Permite que a lógica de controlo e segurança seja implementada e mantida centralmente.

[17] ACK – *Acknowledgement*
[18] NACK – *Negative Acknowledgement*

## 3.6 Princípios de usabilidade em sistemas interativos

O sistema de autenticação deve ser intuitivo, claro e eficiente, mesmo para utilizadores sem formação técnica. Segundo os princípios da usabilidade[24]:

- O sistema deve apresentar o estado atual de forma clara (ex.: "Aproxime o cartão");
- As mensagens devem ser compreensíveis e em língua natural;
- Deve existir validação local de erros simples, como por exemplo garantir que o PIN tem quatro dígitos antes de o enviar.

Estes cuidados melhoram significativamente a experiência do utilizador, reduzindo erros e aumentando a eficácia do sistema.

## 3.7 Análise de riscos em sistemas de controlo de acessos

A análise de riscos permite identificar potenciais falhas de segurança e adoptar medidas de mitigação. No contexto de um sistema de controlo de acessos como o aqui proposto, os principais riscos incluem [25]:

- **Clonagem de cartões NFC** – pode ser minimizada utilizando cartões com níveis de segurança superiores (ex.: MIFARE DESFire) e validação centralizada;
- **Interceção de dados na comunicação** – pode ser mitigada com a utilização de HTTPS e autenticação de mensagens;
- **Sabotagem física do sistema** – previsível através da proteção física do *hardware* (ex.: caixas seladas, sensores de intrusão).

Uma abordagem proativa à segurança é essencial para garantir a confiança e a fiabilidade do sistema.

## 3.8 Comparação entre tecnologias de autenticação

A seleção da tecnologia de autenticação mais adequada para um sistema de controlo de acessos deve ter em conta múltiplos critérios, entre os quais se destacam a segurança, a facilidade de utilização, o custo de implementação e a escalabilidade. Nos últimos anos, têm sido adotadas diversas soluções tecnológicas em ambientes institucionais e corporativos, cada uma com características distintas e níveis de fiabilidade variáveis.

Entre as opções mais comuns encontram-se tecnologias como NFC, RFID de baixa frequência, códigos QR e mecanismos biométricos. Cada uma destas soluções apresenta

vantagens e limitações que devem ser consideradas em função do contexto específico de aplicação[26].

A tabela 3.1 apresenta uma síntese comparativa entre estas tecnologias, analisando os principais parâmetros associados ao seu desempenho e adequação prática.

**Tabela 3.1:** *Comparação entre tecnologias de autenticação*
(Fonte: [27])

| **Tecnologia** | **Segurança** | **Facilidade de Utilização** | **Custo** |
|---|---|---|---|
| NFC (com PIN) | Elevada | Elevada | Médio |
| RFID (125kHz) | Baixa | Elevada | Baixo |
| Código QR | Média | Média | Muito baixo |
| Biometria | Muito elevada | Elevada | Elevado |

Assim, a seleção da tecnologia ideal deve considerar cuidadosamente o nível de protecção necessário, as características dos utilizadores, o orçamento disponível e a infraestrutura tecnológica existente.

# Capítulo 4

# Estado da Arte

O controlo de acessos em infraestruturas tem evoluído significativamente em Portugal nos últimos anos. Este avanço deve-se à crescente necessidade de garantir a segurança de equipamentos de elevado valor, proteger dados sensíveis e melhorar a eficiência na gestão de espaços. Este capítulo apresenta o estado da arte em tecnologias de controlo de acessos, destacando exemplos de locais onde estas já foram implementadas ou estão em processo de implementação no contexto nacional.

## 4.1 Tecnologias de controlo de acessos: panorama geral

As tecnologias de controlo de acessos utilizadas atualmente variam desde sistemas físicos tradicionais até soluções avançadas que integram *hardware*, *software* e algoritmos vários, incluindo de inteligência artificial. Em Portugal, diversas instituições têm adotado este tipo de soluções, especialmente em universidades, empresas tecnológicas e hospitais, onde a proteção de infraestruturas críticas é essencial. Os principais tipos de sistemas implementados incluem:

- Cartões Eletrónicos e *RFID*: Amplamente usados em instituições de ensino e empresas para garantir o controlo de entradas e saídas. Estes sistemas registam automaticamente as interações, facilitando auditorias e monitorizações.
- Sistemas Biométricos: Tecnologias como reconhecimento facial, impressão digital e leitura da íris são cada vez mais comuns em ambientes onde a segurança é crítica, graças à sua capacidade de identificar de forma única cada utilizador.
- Controlo Baseado em Aplicações Móveis: O uso de *smartphones* como credenciais de acesso tem vindo a ganhar terreno. Estes sistemas utilizam aplicações móveis para autenticação, fornecendo maior flexibilidade e reduzindo os custos associados a cartões físicos.

- Sistemas Integrados com Monitorização em Tempo Real: Integração de câmaras de vigilância e sensores IoT[1] que, aliados aos sistemas de controlo de acessos, fornecem uma visão em tempo real do espaço e notificam anomalias automaticamente.

## 4.2 Exemplos de Implementação de Controlo de Acessos

Portugal tem dado passos significativos na adoção de sistemas avançados de controlo de acessos, especialmente em ambientes críticos, como hospitais, universidades, centros de dados e infraestruturas de transportes. Estas iniciativas têm como objetivo melhorar a segurança, a eficiência na gestão de acessos e a proteção de recursos sensíveis. Seguem-se alguns exemplos detalhados.

### 4.2.1 Universidade do Minho

A Universidade do Minho, no âmbito da modernização das suas infraestruturas, implementou um sistema de controlo de acessos nas suas residências universitárias. O projeto foi concluído em agosto, sendo que, a partir deste ano letivo, as entradas e saídas nas residências passaram a ser feitas exclusivamente através de leitura biométrica. Esta iniciativa foi realizada no contexto da operação POCER-SAS[2]

Este sistema digital de controlo de acessos foi instalado nas portas principais e em cada bloco das residências universitárias, permitindo um controlo mais eficiente das entradas e saídas. Além disso, foi implementado um sistema de fechaduras eletrónicas na residência Professor Lloyd Braga, similar ao utilizado na residência dos Combatentes, permitindo aos residentes o acesso aos quartos através de cartões eletrónicos ou telemóveis com tecnologia Bluetooth. A introdução deste sistema tem como objetivos melhorar a segurança e promover uma gestão mais eficiente das instalações.

Carlos Almeida, Diretor do Departamento de Apoio Social, destacou que esta foi uma oportunidade para modernizar as infraestruturas tecnológicas das residências universitárias. Sublinhou, ainda, que a implementação do novo sistema facilita o acesso e a circulação dos residentes, aumentando a comodidade e contribuindo para uma melhor gestão das infraestruturas. Além disso, afirmou que as novas ferramentas proporcionam uma gestão mais eficiente, ajudando na melhoria da qualidade do serviço prestado[28].

A implementação deste sistema de controlo de acessos nas residências universitárias da Universidade do Minho demonstra um exemplo eficaz de como tecnologias de ponta podem ser integradas na gestão de infraestruturas críticas, assegurando não só maior segurança, mas também maior eficiência nos processos administrativos e operacionais da instituição[28].

[1] IoT – *Internet of Things*

[2] POCER-SAS – Programa Operacional de Capacitação e Eficiência de Recursos dos Serviços de Ação Social

### 4.2.2 Imprensa Nacional Casa da Moeda

O INESC TEC[3], desenvolveu uma solução inovadora para o Cartão de Cidadão, integrando um algoritmo biométrico avançado que utiliza impressões digitais, com o objetivo de reforçar a segurança na autenticação da identidade do titular. Este sistema de controlo de acessos é um exemplo relevante de como as tecnologias biométricas estão a ser aplicadas em infraestruturas críticas e processos de verificação de identidade.

O Cartão de Cidadão é um documento duplo, físico e eletrónico, que permite aos cidadãos portugueses realizar diversas operações sem necessidade de interação presencial, como assinar documentos eletrónicos e autenticar-se em sistemas públicos e privados. O novo sistema desenvolvido pelo INESC TEC incorpora um algoritmo biométrico de alta segurança, utilizando a tecnologia MoC[4], que garante que as impressões digitais sejam processadas diretamente no próprio cartão. Este processo elimina a necessidade de extrair ou transferir os dados biométricos para outros sistemas, garantindo maior proteção e confidencialidade das informações pessoais.

Este algoritmo foi implementado pela INCM[5], que é a entidade responsável pela produção do Cartão de Cidadão. A solução foi desenvolvida ao longo de dois anos por uma equipa multidisciplinar composta por vários centros de investigação do INESC TEC. A sua implementação veio responder à crescente necessidade de autenticação segura no contexto de serviços digitais e transações eletrónicas, especialmente nas áreas de serviços públicos e de segurança.

O sistema foi apresentado publicamente durante a Mostra de Inovação organizada pela INCM, evidenciando as vantagens desta tecnologia tanto no setor público quanto em áreas privadas que exigem um elevado nível de segurança[29].

A implementação do Cartão de Cidadão com biometria avançada serve como exemplo de boas práticas na utilização de tecnologias para garantir a segurança e a privacidade de dados sensíveis, além de possibilitar a melhoria da eficiência em serviços digitais. Este sistema biométrico pode ser considerado um modelo para futuras implementações em outros sistemas de controlo de acessos em Portugal e além-fronteiras, especialmente no que diz respeito à verificação remota de identidade e à gestão de dados pessoais de forma segura[29].

### 4.2.3 Porter Keyless System

A Porter Systems desenvolveu uma solução inovadora para controlo de acessos que visa simplificar o processo de abertura de portas, dispensando a tradicional chave. Através de um sistema de cilindro automatizado que substitui o modelo europeu de cilindro de fechadura, os utilizadores podem abrir portas utilizando apenas um *smartphone*. A

[3]INESC TEC – Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência
[4]MoC – *Match-On-Card*
[5]INCM – Imprensa Nacional Casa da Moeda

aplicação móvel, compatível com sistemas Android e IOS, permite que o acesso à porta seja autorizado via Bluetooth, utilizando um código gerado de forma única e de curta duração[30].

A principal vantagem desta solução é a facilidade de instalação, uma vez que não exige modificações estruturais complexas como a eletrificação das portas ou a instalação de sistemas biométricos. A inovação está no uso de baterias recarregáveis de longa duração, que suportam cerca de 3000 ciclos de utilização, ou seja, aproximadamente um ano e meio de uso[30].

O código gerado para desbloquear a porta é único e não pode ser reutilizado. Mesmo que um potencial atacante consiga clonar o sinal de comunicação, o código gerado já teria sido descartado, impedindo o acesso não autorizado.

A solução Porter Keyless System foi implementada nos Edifícios Centrais do Óbidos Parque — Parque Tecnológico de Óbidos. Esta tecnologia foi aplicada nos ambientes do parque tecnológico, utilizando *smartphones* para abrir portas sem necessidade de chaves físicas[30].

### 4.2.4 Comunicações RFID para identificação e controlo de presenças – Politécnico de Leiria

O projeto "*Comunicações RFID para Identificação e Controlo de Presenças*", desenvolvido no Politécnico de Leiria, surgiu da necessidade de modernizar e simplificar o registo de assiduidade dos estudantes em sala de aula, substituindo métodos tradicionais como registos em papel ou chamadas orais. Este objetivo foi especialmente relevante devido às restrições de contacto físico impostas pela pandemia de COVID-19. A solução apresenta um dispositivo portátil, de baixo custo e fácil utilização, que recorre a diversas tecnologias de identificação para proporcionar flexibilidade, segurança e eficiência no processo[31]. Entre as tecnologias incorporadas no projeto destaca-se:

- RFID – sistema de identificação que utiliza ondas de rádio para reconhecer de forma única cada utilizador ou objeto. A tecnologia permite registos automáticos e rápidos, adequados para ambientes de sala de aula.
- NFC (*Near-Field Communication*) – tecnologia de curto alcance (até 10 cm), utilizada como alternativa para situações em que os estudantes se esqueçam dos cartões RFID. Permite a integração com objetos pessoais, como porta-chaves, facilitando a identificação.
- Impressão digital – método baseado em características únicas dos relevos dos dedos, assegurando elevada precisão na identificação. São utilizados sensores modernos, como sensores capacitivos ou por ultrassom, que captam a impressão digital e a transformam em dados para validação.

- Bluetooth – comunicação sem fios de curto alcance que utiliza o padrão BLE[6] para garantir transferências de dados seguras e económicas em termos de consumo de energia.

O dispositivo foi concebido para resolver limitações dos sistemas existentes, como falta de manutenção e problemas de atualização de equipamentos. Além disso, elimina erros e danos nos registos manuais, garantindo maior fiabilidade no controlo de presenças. A portabilidade do dispositivo permite que os docentes o utilizem facilmente em diferentes salas e laboratórios[31].

Este projeto responde a uma exigência regulamentar do Politécnico de Leiria, que determina a necessidade de um mínimo de 75% de presença em sala de aula para acesso à avaliação contínua. Ao integrar múltiplas tecnologias de identificação, a solução assegura que todos os estudantes, independentemente das suas preferências ou limitações, possam ser identificados de forma eficaz e segura[31].

A escolha de componentes eletrónicos acessíveis permite que o sistema seja escalável, servindo de base para futuras melhorias e possíveis adaptações a outras áreas de controlo de acessos, tanto em ambientes educacionais como empresariais.

## 4.3 Tendências e desafios em Portugal

A implementação de sistemas de controlo de acessos em Portugal tem acompanhado as principais tendências tecnológicas globais, destacando-se pela incorporação de soluções inovadoras e sustentáveis. Esta evolução é impulsionada pela necessidade crescente de proteger infraestruturas críticas e melhorar a eficiência operacional em diversos sectores, desde o educacional ao empresarial.

A utilização de algoritmos de Inteligência Artificial para prever comportamentos suspeitos e gerar alertas em tempo real tem vindo a crescer adotada em Portugal, incluindo no domínio da segurança e do controlo de acessos. Um estudo da Microsoft revela que uma em cada cinco empresas portuguesas já utiliza soluções de cibersegurança baseadas em IA[7], demonstrando uma crescente integração desta tecnologia na proteção de infraestruturas críticas[32].

A integração de sistemas de controlo de acessos com plataformas de gestão académica e empresarial é outra tendência em crescimento no país. Diversas instituições de ensino superior e empresas têm adotado esta abordagem para simplificar a emissão de permissões e gerir acessos temporários de forma mais eficiente.

Agregado a isto, existe o tema sustentabilidade, que nos últimos anos tem sido um dos temas centrais na adoção de novas tecnologias em Portugal. A transição dos tradici-

[6]BLE – *Bluetooth Low Energy*
[7]IA – *Artificial Intelligence*

onais cartões físicos para soluções digitais baseadas em aplicações móveis é um exemplo desta prioridade. O impacto ambiental associado ao fabrico e descarte de cartões físicos é significativo, devido ao uso de materiais não biodegradáveis, como plásticos e metais, bem como ao consumo de energia e emissões de gases de efeito estufa durante os processos de produção. Além disso, o descarte inadequado destes cartões contribui para a poluição ambiental, principalmente em aterros sanitários.

No entanto, as soluções digitais podem oferecer vantagens tanto ambientais quanto operacionais. A utilização de aplicações móveis elimina a necessidade de produção e gestão de cartões físicos, reduzindo custos e complexidade administrativa. Estes sistemas permitem um maior controlo, facilitando a emissão e a atualização de permissões em tempo real, enquanto promovem práticas mais sustentáveis e alinhadas com as preocupações ambientais atuais.

Por outro lado, a utilização de dispositivos móveis apresenta desafios de segurança intrínsecos. Estes dispositivos podem ser vulneráveis a ameaças como *malware*, ataques de *phishing* e perda ou roubo físico, comprometendo a integridade das credenciais armazenadas. Além disso, a falta de atualização regular de sistemas operativos e a partilha inadequada de dispositivos podem aumentar os riscos de acesso não autorizado. Estas vulnerabilidades exigem que as organizações implementem medidas rigorosas de cibersegurança para mitigar potenciais riscos.

# Capítulo 5

# Análise experimental

Foi necessário realizar uma fase de testes exploratórios com os diversos componentes e tecnologias envolvidos. Estes testes tiveram como principal objetivo consolidar os conhecimentos práticos necessários para a implementação do sistema, bem como identificar possíveis limitações ou desafios técnicos.

## 5.1 Preparação inicial do hardware

Antes da realização do primeiro teste funcional, foi essencial compreender detalhadamente o papel de cada pino do microcontrolador *Arduino Nano*. Para garantir uma correta ligação dos diversos módulos ao *hardware*, recorreu-se à análise de um esquema explicativo do *pinout*, o qual permitiu identificar com precisão as funções de entrada, saída digital, alimentação e comunicação (*SPI*, $I^2C$).

Este passo preliminar revelou-se crucial para evitar erros de ligação durante a montagem e assegurar o funcionamento esperado dos componentes logo nas fases iniciais de teste. A Figura 5.1 apresenta o diagrama de *pinout* utilizado como referência.

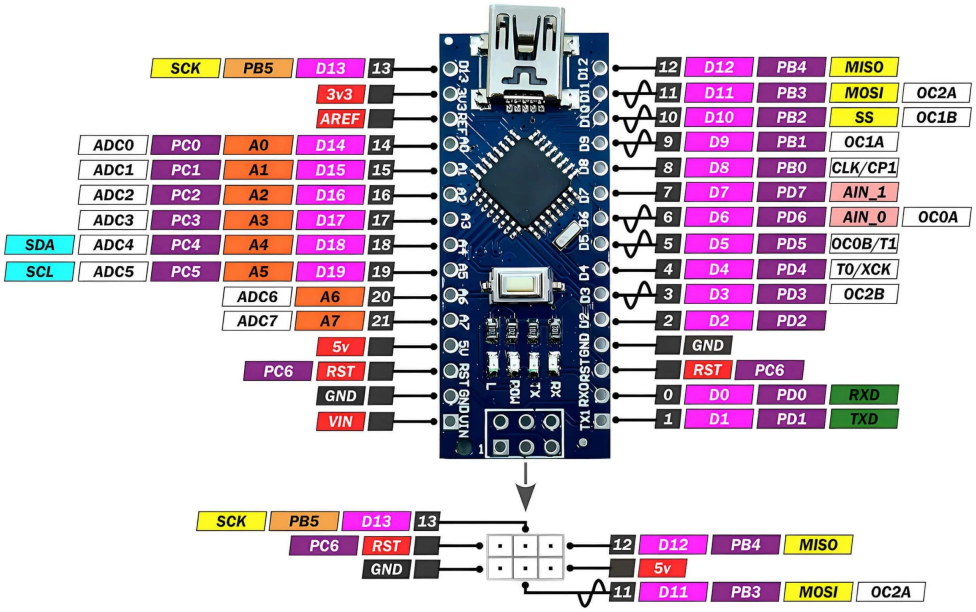


**Figura 5.1:** *Pinout do microcontrolador Arduino Nano.*

O primeiro teste realizado foi o clássico exemplo *Blink*, que consiste em programar o Arduino para piscar um led em intervalos de tempo regulares. Esta experiência serviu para confirmar que o micro-controlador estava a funcionar corretamente, que o ambiente de desenvolvimento (IDE Arduino) estava configurado, e que a comunicação com o computador era estável.

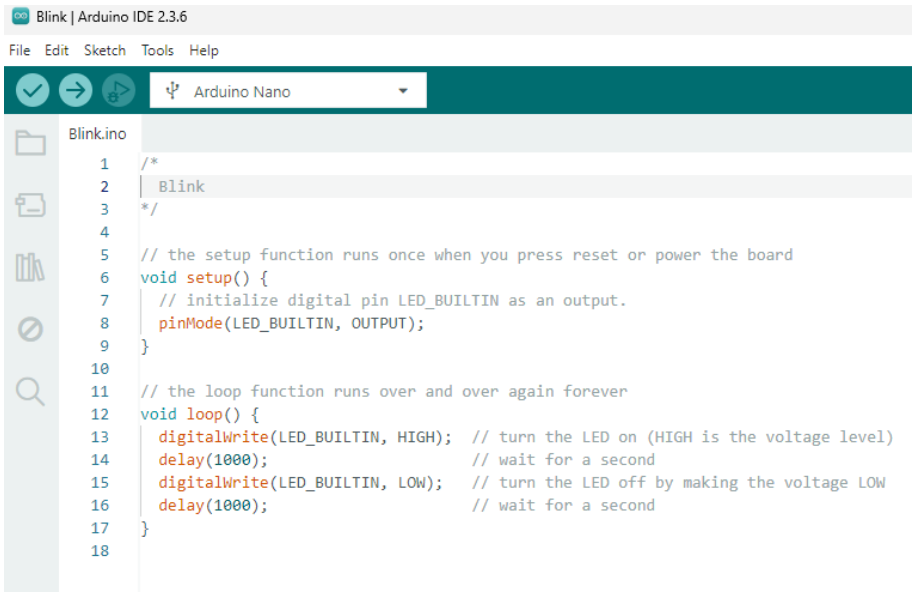


**Figura 5.2:** *Teste Blink*

### Integração entre o leitor NFC e o ecrã LCD

Após a validação individual dos módulos, procedeu-se à montagem conjunta do leitor NFC PN532 e do ecrã LCD 16x2 com interface I²C, de modo a simular uma experiência de utilização mais próxima da realidade final do sistema.

Na figura 5.3 observa-se o LCD a apresentar a mensagem inicial "*Aproxime o cartão*", instruindo o utilizador a iniciar o processo de autenticação, conforme mostrado na figura 5.4.


**Figura 5.3:** *Mensagem apresentada no LCD no início do processo de autenticação*

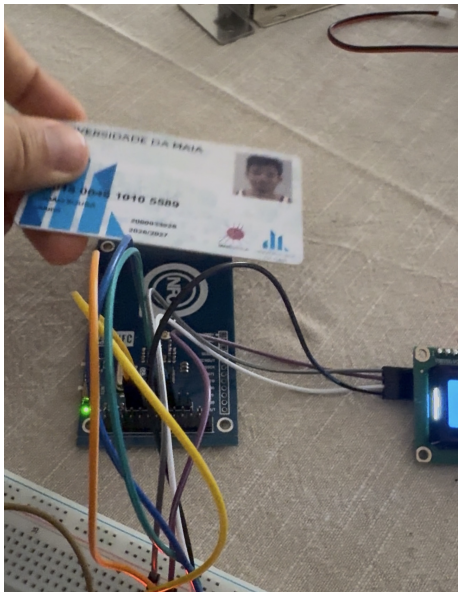

**Figura 5.4:** *Cartão NFC*

Ao aproximar um cartão NFC válido, o leitor PN532 deteta a presença do mesmo e procede à leitura do seu identificador único (UID). Esta ação é imediatamente refletida no LCD, como ilustrado na Figura 5.5, onde surge a mensagem "*Cartão lido*".

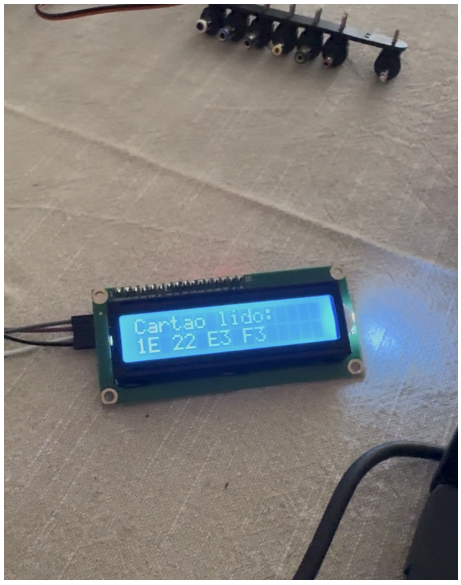


**Figura 5.5:** *Confirmação visual da leitura do cartão NFC com sucesso.*

Simultaneamente, no *Serial Monitor* da Arduino IDE, é possível visualizar o UID do cartão lido, como mostrado na Figura 5.6. Esta informação será posteriormente utilizada para verificação das permissões junto do servidor remoto.

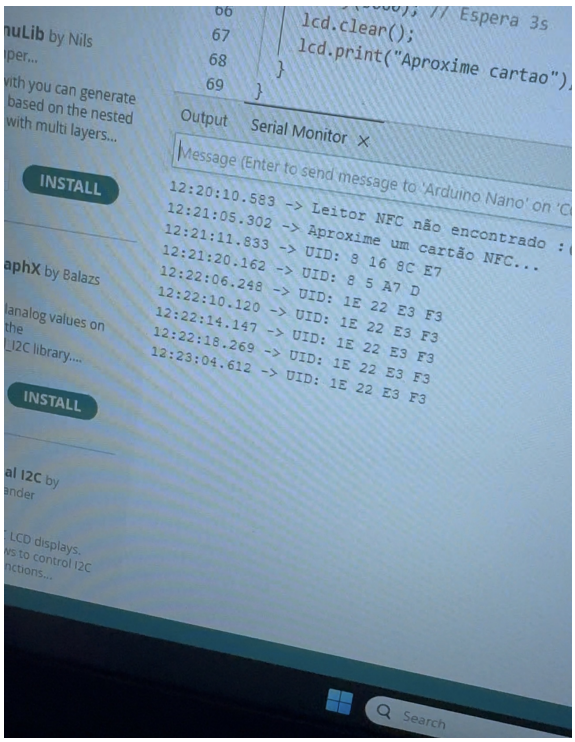


**Figura 5.6:** *UID do cartão NFC lido apresentado no Serial Monitor.*

Este teste reforçou a importância do *feedback* visual ao utilizador e demonstrou a estabilidade da leitura NFC em conjunto com a apresentação de mensagens no visor, um passo fundamental para a implementação do sistema completo de autenticação.

Foi também feito um conjunto de experiências com o módulo ENC28J60, responsável pela ligação do Arduino à rede. Através deste módulo, foram enviados pedidos HTTP simulados para servidores locais, com o intuito de testar a comunicação, estruturação de mensagens e interpretação de respostas. Ferramentas como o *Serial Monitor* auxiliaram nesta fase.

Durante esta fase, foram consolidados diversos conceitos fundamentais:

- Leitura e escrita em pinos digitais e analógicos;
- Utilização de bibliotecas externas no Arduino;
- Manipulação de strings e conversão de dados;
- Compreensão do protocolo SPI e $I^2C$;
- Estruturação de mensagens HTTP e conceitos básicos de redes;
- Utilização de simuladores e ferramentas auxiliares (por exemplo *serial monitor*, fonte de alimentação).

Em resumo, esta fase experimental foi essencial para garantir o bom funcionamento individual de cada componente e para adquirir a confiança necessária antes da integração no sistema completo.

# Capítulo 6

# Plano de trabalho

Neste capítulo apresenta-se o plano de trabalho a adotar na realização do projecto, identificando as fases principais, as atividades previstas e a sua calendarização.

## 6.1 Planeamento

O planeamento deste projecto está estruturado em duas fases principais: a fase de estudo e a fase de implementação.

A fase de estudo tem como principal objetivo a análise preliminar e a fundamentação teórica e técnica do projeto, de forma a assegurar que as decisões a tomar na fase seguinte estejam devidamente sustentadas. Esta fase será subdividida nas seguintes etapas:

- **Levantamento de opções**: identificação e recolha das várias abordagens, metodologias e tecnologias aplicáveis à problemática em estudo;
- **Análise de opções**: avaliação comparativa das alternativas identificadas, com base em critérios como viabilidade técnica, custos, tempo de desenvolvimento e adequação aos requisitos do projeto;
- **Testes de viabilidade**: provas de conceito ou protótipos simplificados, com o intuito de validar as soluções consideradas mais promissoras;
- **Análise de resultados**: interpretação dos dados obtidos durante os testes, com vista à fundamentação da escolha da abordagem a adotar;
- **Revisão do planeamento**: atualização do planeamento inicial com base nas conclusões obtidas, ajustando prazos e recursos de acordo com as necessidades identificadas.

Após a fase de estudo, inicia-se a fase de implementação, centrada na execução prática do projecto, seguindo as decisões previamente tomadas. Esta fase está organizada nas seguintes etapas:

- **Aprovisionamento**: aquisição os recursos materiais e tecnológicos necessários para o desenvolvimento do projeto;
- **Desenvolvimento**: implementação da solução definida, incluindo a programação, integração de componentes e construção do produto final;
- **Testes**: verificação do correto funcionamento da solução implementada, através de testes técnicos e funcionais que permitam avaliar a sua fiabilidade e desempenho;
- **Análise de resultados**: avaliação dos testes realizados, com identificação de eventuais falhas, oportunidades de melhoria e verificação do cumprimento dos objetivos estabelecidos.

Estas fases, bem como as respetivas atividades, estarão representadas no gráfico de Gantt na figura 6.2, permitindo uma visualização clara da distribuição temporal do trabalho, da interdependência entre tarefas e da duração prevista de cada etapa. Este instrumento de planeamento será fundamental para o acompanhamento do progresso do projeto, permitindo reajustar estratégias sempre que necessário.

## 6.2 Representação visual do planeamento

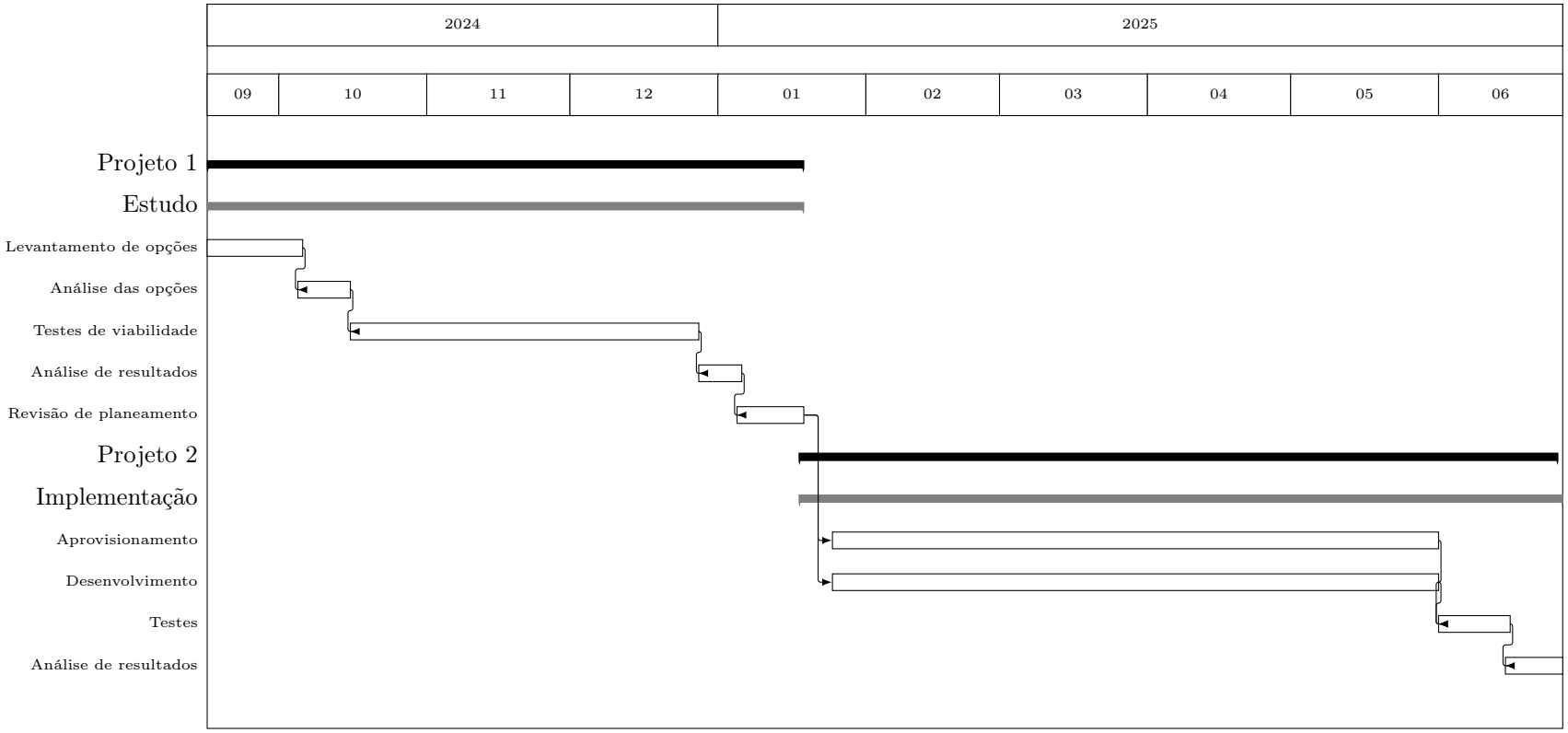


**Figura 6.1:** *Gráfico de Gantt com o faseamento do projeto*

# Capítulo 7

# Proposta de Solução

## 7.1 Proposta

A proposta de solução visa controlar o acesso físico a uma sala através de um sistema eletrónico baseado em autenticação dupla (cartão NFC[1] + código PIN[2]). O sistema será implementado com um microcontrolador (Arduino), dispositivos periféricos (leitor NFC, teclado matricial, LCD[3], relé) e comunicação com um serviço remoto (Forge), responsável por validar os dados de autenticação e gerir os acessos dos utilizadores.

### 7.1.1 Arquitetura geral

O sistema será composto por *hardware* local para identificação e controlo do trinco, e por um serviço remoto que valida os dados e guarda os registos. A autenticação será feita da seguinte forma:

1. Leitura do cartão NFC do utilizador.
2. Introdução de um código PIN atribuído ao cartão.
3. Envio dos dados para um servidor remoto (Forge).
4. Validação da permissão de entrada com base no UID[4] e PIN.
5. Abertura do trinco se for autorizado ou apresentação de mensagem de erro se não for.

[1] NFC – *Near-Field Communication*
[2] PIN – *Personal Identification Number*
[3] LCD – *Liquid Crystal Display*
[4] UID – *Unique Identifier*

### 7.1.2 Componentes da solução

Nesta secção, apresentam-se os principais componentes físicos e lógicos que integram a solução desenvolvida. Cada elemento desempenha um papel específico na identificação e validação dos utilizadores, bem como no controlo de acesso ao espaço. De seguida, descrevem-se os módulos utilizados, as suas funções e a forma como comunicam entre si para assegurar o funcionamento eficaz e seguro do sistema.

#### Módulo NFC

Será utilizado um módulo como o MFRC522, conectado ao Arduino via SPI, para ler o UID (identificador único) do cartão NFC da instituição. Este UID serve como identificador do utilizador no sistema.

- **Função:** Leitura de cartão NFC
- **Saída:** UID(string).

#### Teclado matricial

Um teclado matricial 4x4 permitirá ao utilizador introduzir um código PIN após a leitura do cartão. Este PIN é previamente atribuído ao utilizador no sistema Forge.

- **Função:** Entrada de PIN do utilizador.
- **Validação local:** Apenas formato (ex: 4 dígitos).
- **Validação lógica:** Realizada remotamente.

#### Ecrã LCD

O visor escolhido oferece visualização de 16 colunas e duas linhas de caracteres (vulgo LCD 16x2), totalizando até 32 caracteres visíveis em simultâneo, possui um *interface* $I^2C$. Será usado para comunicar com o utilizador, apresentando mensagens como:

- `Aproxime o cartão`
- `Insira o código`
- `Acesso autorizado`
- `Utilizador não válido`

### Módulo de comunicação

Para permitir a comunicação HTTP com o serviço Forge, será utilizado o módulo **ENC28J60**, que fornece conectividade Ethernet via *interface* SPI com o Arduino. Este módulo permite ao sistema enviar os dados de autenticação através de pedidos HTTP ao servidor remoto.

- **Protocolo:** HTTP GET ou POST
- **Formato:** URL *encoded*

**Exemplo de dados enviados (formato POST ou GET):**

```
" uid=04A1B2C3D4&pin=1234 "
```

**Resposta esperada do servidor:**

```
" valid=1&nome=Joao%20Silva "
```

O Arduino irá interpretar apenas se o valor de `valid` é `1` (acesso autorizado) ou `0` (acesso negado), simplificando o processamento e mantendo a compatibilidade com os seus recursos limitados.

### Servidor Forge (API HTTP)

O sistema Forge já existente será utilizado para:

- Validar o par UID + PIN;
- Verificar se o utilizador tem acesso à sala;
- Registar os acessos com hora/data.

O Arduino irá apenas enviar os dados e interpretar a resposta de autorização.

### Relé e trinco elétrico

Caso a resposta do servidor seja positiva, será ativado um **relé** que permite a passagem de corrente para um **trinco elétrico**, destrancando a porta temporariamente.

- **Tempo de abertura:** aproximadamente 5 segundos.
- **Segurança:** só abre após validação dupla.

### 7.1.3 Fluxo do sistema

1. LCD mostra: "`Aproxime o cartão`";
2. NFC lê UID;
3. LCD mostra: "`Insira o código`";
4. Utilizador introduz PIN no teclado;
5. Dados são enviados via HTTP para o Forge;
6. Servidor responde com `valid: true` ou `false`;
7. Se válido: relé ativa trinco e LCD mostra "`Acesso autorizado`";
8. Se inválido: LCD mostra "`Utilizador não válido`".

### 7.1.4 Segurança

A autenticação dupla (cartão + PIN) garante maior segurança contra acessos indevidos. Nenhum dado sensível (como o PIN) é guardado localmente no Arduino. Todas as validações são centralizadas no Forge, dificultando fraudes e facilitando a gestão de permissões.

### 7.1.5 Vantagens da solução

- Simples de operar para o utilizador;
- Integração com infraestrutura existente (Forge);
- Escalável para outras portas ou zonas da instituição;
- Maior controlo e histórico de acessos.

# Capítulo 8

# Implementação

Este capítulo descreve o processo de implementação do sistema de controlo de acesso baseado em dupla validação: código numérico e cartão NFC. A implementação abrange a montagem do *hardware*, o desenvolvimento do *firmware* no micro-controlador, a integração dos diversos módulos e a configuração do servidor para comunicação remota.

Todas as decisões técnicas foram orientadas para garantir simplicidade de uso, robustez e segurança.

## 8.1 Montagem do hardware

A montagem do sistema teve início com a validação dos seguintes componentes principais (ver figura 8.1):

- Microcontrolador **Arduino Nano**;
- Módulo leitor NFC **PN532**;
- Teclado matricial **4x4**;
- Ecrã LCD 16x2 com interface I²C;
- Módulo de relé de **2 canais**;
- Trinco electromagnético (solenóide);
- Fonte de alimentação externa 12 V/2 A.


**Figura 8.1:** *Componentes principais organizados antes da montagem.*

A montagem presente na figura 8.2 foi executada interligando os componentes conforme o esquema apresentado na figura 8.3. O relé foi ligado aos pinos digitais `D5` e `D6`, sendo `D5` dedicado ao controlo do trinco.

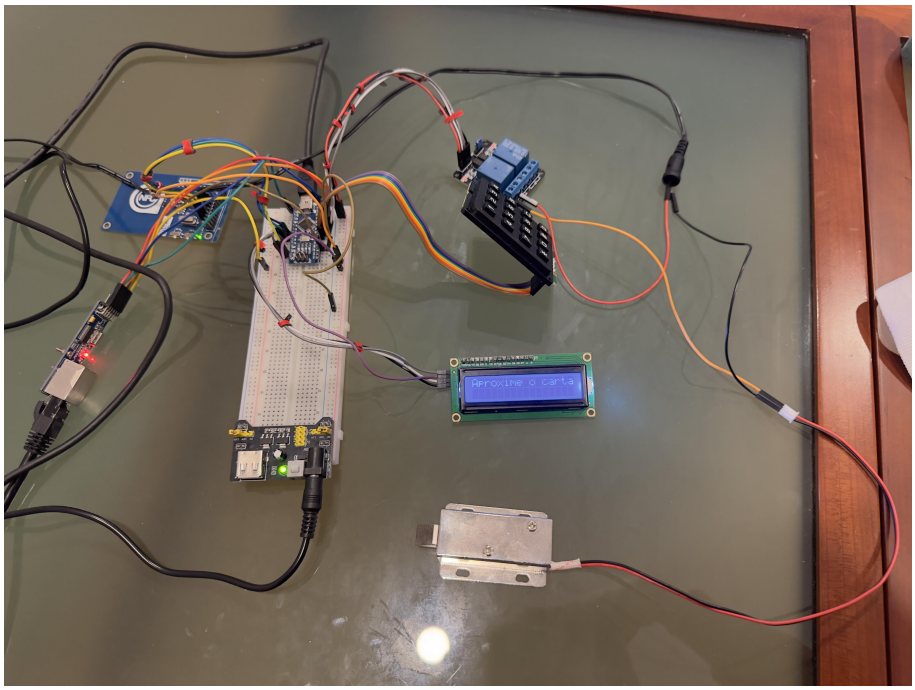


**Figura 8.2:** *Ligação dos módulos ao Arduino Nano*

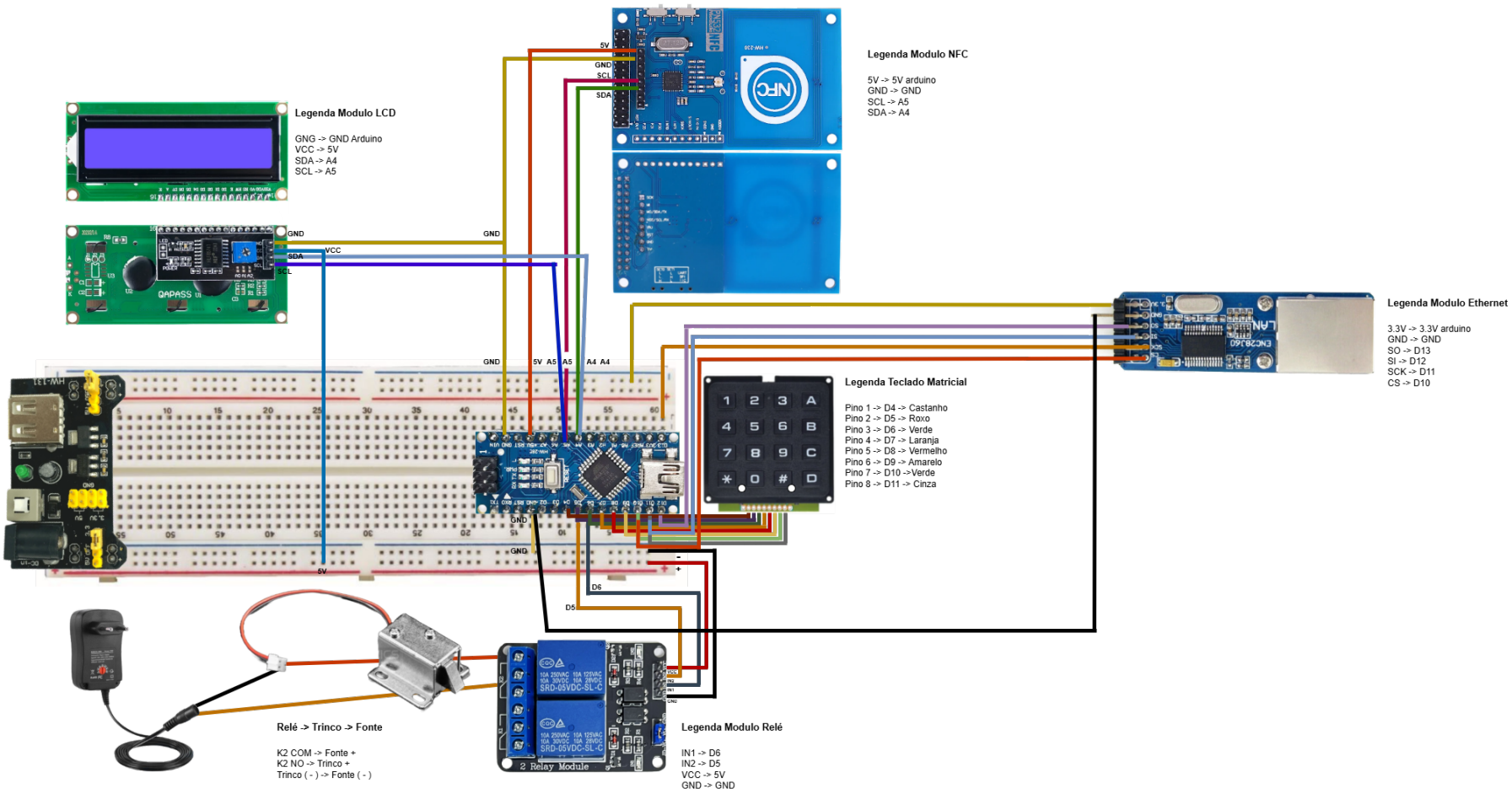


**Figura 8.3:** *Esquema de ligações*

## 8.2 Programação do sistema

O *firmware* foi implementado em C++ no *software* Arduino IDE, seguindo uma lógica que integra a leitura do cartão NFC e a comunicação com o servidor para autenticação. O sistema funciona de forma contínua, realizando as seguintes operações principais:

1. Configuração dos periféricos: preparação do LCD, do leitor NFC, do relé e do *interface* Ethernet;
2. Deteção e leitura do UID do cartão NFC quando este é aproximado;
3. Envio do UID para o servidor via Ethernet para validação;
4. Ativação do relé caso o servidor confirme que o cartão está autorizado, apresentando mensagens informativas no LCD ao longo do processo.

### 8.2.1 Arranque do sistema

Na função `setup()`, configura-se o LCD, o leitor NFC, o relé e a rede Ethernet:

**Excerto 8.1:** *Configuração inicial no* `setup()`

```
lcd.init();
lcd.backlight();

pinMode(RELAY_PIN, OUTPUT);
digitalWrite(RELAY_PIN, HIGH); // Rele desligado

nfc.begin();
nfc.SAMConfig();

if (Ethernet.begin(mac) == 0) {
    Ethernet.begin(mac, ipArduino); // IP fixo se o DHCP falhar
}
```

### 8.2.2 Leitura e validação do UID NFC

O UID é lido do cartão NFC, convertido em *string* e enviado para o servidor para validação:

**Excerto 8.2:** *Leitura do UID e comunicação com o servidor*

```
if (nfc.readPassiveTargetID(...)) {
    String uidStr = ""; // Construcao da string do UID

    if (client.connect(servidor, 80)) {
```

```
5           client.print("GET /verifica.php?uid=");
6           client.print(uidStr);
7           client.println(" HTTP/1.1");
8           // ...
9       }
10  }
```

### 8.2.3 Resposta do servidor e controlo do relé

Se o servidor responder com "`sim`", o relé é ativado e a mensagem no LCD é atualizada:

**Excerto 8.3:** *Activação do relé após validação*

```
1  if (autorizado) {
2      lcd.clear();
3      lcd.print("Autorizado!");
4      digitalWrite(RELAY_PIN, LOW); // Rele ligado
5      delay(3000);
6      digitalWrite(RELAY_PIN, HIGH); // Rele desligado
7  }
```

## 8.3 Servidor PHP

O servidor recebe o UID através de um pedido `GET`, verifica se está autorizado e responde ao Arduino:

**Excerto 8.4:** *Código de exemplo de validação do UID no servidor*

```
1  <?php
2  $uid = $_GET['uid'] ?? '';
3
4  $uids_autorizados = ["1e 22 e3 f3"];
5
6  if (in_array(trim($uid), $uids_autorizados)) {
7      echo "sim";
8  } else {
9      echo "nao";
10 }
11
12 file_put_contents('estado.txt', date('Y-m-d H:i:s') . " - $uid\n"↩
       , FILE_APPEND);
13 ?>
```

## 8.4 Mensagens no LCD

Durante o processo, o LCD apresenta mensagens para o utilizador, tais como:

- `"Aproxime o cartão"`;
- `"Autorizado!"`;
- `"Cartão inválido"`.

## 8.5 Infraestrutura da plataforma de testes

Para suportar e validar o sistema de controlo de acessos em condições mais próximas do ambiente real, foi criada uma infraestrutura virtual baseada numa VM[1] utilizando a ferramenta VirtualBox. Esta VM simula o servidor *backend* responsável pela receção e verificação das autenticações provenientes do Arduino.

O objetivo principal desta infraestrutura é permitir testes isolados, flexíveis e reproduzíveis, sem necessidade de equipamentos físicos adicionais, garantindo ainda maior controlo sobre a rede e os serviços executados.

### 8.5.1 Configuração da máquina virtual

A máquina virtual foi configurada com os seguintes parâmetros:

- Memória RAM: 2 GB;
- Armazenamento em disco: 40 GB, com reserva dinâmica;
- Sistema operativo: Ubuntu Server 22.04 LTS, versão estável e suportada a longo prazo (LTS);
- Modo de rede: *Bridge*, permitindo que a VM receba um endereço IP da mesma rede do computador e do Arduino, facilitando a comunicação direta entre os dispositivos;
- *Software* instalado: Apache2 (servidor HTTP) com arranque automático ao iniciar o sistema.

### 8.5.2 Estrutura de pastas do servidor

O *backend* foi estruturado com simplicidade, organizando os ficheiros PHP[2] num diretório específico, acessível ao Apache. A estrutura ficou definida da seguinte forma:

[1] VM – *Virtual Machine*
[2] PHP – *Hypertext Preprocessor*

```
var/www/html/
|- verifica.php        % Script para validar UID recebido do Arduino apos registado no estado.txt
|- estado.php          % Script que le e apresenta o conteudo do ficheiro estado.txt
|- estado.txt          % Ficheiro de registo de acessos
```

### 8.5.3 *Scripts* de validação – PHP

O ficheiro `verifica.php` foi desenvolvido para receber o UID enviado pelo Arduino e devolver uma resposta simples: `sim` ou `nao`, consoante o UID esteja autorizado.

**Bloco de código:** *Script* `verifica.php`

```php
<?php
$uid_recebido = $_GET['uid'] ?? '';

$uid_autorizado = '1e 22 e3 f3 ';
$estado = '';

if (strtolower(trim($uid_recebido)) === strtolower(trim($uid_autorizado))) {
    $estado = "Autorizado";
    echo "sim";
} else {
    $estado = "Invalido";
    echo "nao";
}

file_put_contents("estado.txt", $estado . " - UID: " . $uid_recebido . " - " . date("Y-m-d H:i:s") . "\n");
?>
```

**Figura 8.4:** *Código verifica.php*

O ficheiro `estado.php` foi desenvolvido para ler e apresentar o conteúdo de um ficheiro chamado `estado.txt` se ele existir. Caso contrário, mostra a mensagem "`Nenhum estado registado ainda`".

verifica.php × estado.php ×

C: > phpcompartilhado > estado.php

```php
<?php
if (file_exists("estado.txt")) {
    echo nl2br(file_get_contents("estado.txt"));
} else {
    echo "Nenhum estado registado ainda.";
}
?>
```

**Figura 8.5:** *Código do ficheiro* `estado.php`

### Verificação de conectividade

Após a atribuição dos endereços IP aos dispositivos envolvidos no sistema – computador (`192.168.1.3`), Arduino (`192.168.1.4`) e servidor (`192.168.1.2`) – foram realizados testes

para assegurar a comunicação correta entre estes.

Utilizando a máquina *host* da VM, foram executados comandos `ping` direcionados ao servidor e ao Arduino, com o intuito de validar a acessibilidade e a estabilidade da ligação de rede.

A Figura 8.6 apresenta uma captura de ecrã com os resultados destes testes, demonstrando o tempo de resposta dos dispositivos. Estes testes são fundamentais para garantir que a comunicação entre o *hardware* e o *backend* se processa de forma fiável, elemento crítico para o funcionamento do sistema de controlo de acesso.

```
PS C:\Users\jpcouto> ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=3ms TTL=64
Reply from 192.168.1.2: bytes=32 time=1ms TTL=64
Reply from 192.168.1.2: bytes=32 time<1ms TTL=64
Reply from 192.168.1.2: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms
PS C:\Users\jpcouto> ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\jpcouto> ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.3: Destination host unreachable.
Reply from 192.168.1.4: bytes=32 time=29ms TTL=64
Reply from 192.168.1.4: bytes=32 time=8ms TTL=64
Reply from 192.168.1.4: bytes=32 time=8ms TTL=64
```

**Figura 8.6:** *Verificação de conectividade entre o computador, o servidor e o Arduino.*

### Verificação da ligação inicial à rede e ao servidor

Antes de iniciar os testes funcionais de autenticação, foi necessário confirmar que o microcontrolador se encontrava corretamente ligado à rede e que conseguia comunicar com o servidor remoto. Para esse efeito, foi utilizada a consola do *Serial Monitor* da *Arduino IDE*, onde foram impressas mensagens com o IP atribuído dinamicamente ao dispositivo, bem como o resultado da tentativa de ligação à máquina virtual (VM) responsável pelo processamento dos pedidos.

A figura 8.7 apresenta uma captura de ecrã do *Serial Monitor*, demonstrando o sucesso

na obtenção de um endereço IP válido e a confirmação da ligação estabelecida com o servidor remoto.

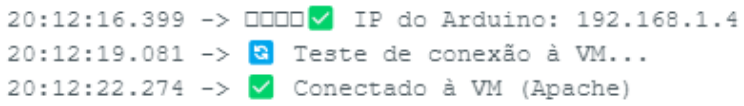


**Figura 8.7:** *Atribuição de IP ao Arduino e verificação da ligação à VM via Serial Monitor.*

### Resultados dos testes de autenticação

Após estabelecida a ligação de rede, iniciaram-se os testes de autenticação. Para isso, foram simuladas situações com cartões autorizados e não autorizados. O Arduino comunicava com o servidor e este, se autorizado, devolvia um resultado. Este resultado era apresentado no browser através de uma resposta textual simples – "`autorizado`" ou "`nao_autorizado`" – conforme o caso.

As figuras 8.8 e 8.9 apresentam uma captura de ecrã ilustrando ambos os cenários. Esta verificação visual permitiu comprovar que a comunicação estava funcional e que o sistema conseguia autenticar corretamente os utilizadores com base nas suas credenciais.


**Figura 8.8:** *Resultado da autenticação apresentado no browser para cartões válidos.*

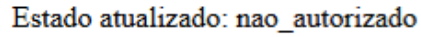


**Figura 8.9:** *Resultado da autenticação apresentado no browser para cartões inválidos.*

Estes testes revelaram tempos de resposta satisfatórios, confirmando que a troca de dados entre o microcontrolador e o servidor se realiza de forma fiável e em tempo útil, aspeto essencial para um sistema de controlo de acessos eficiente.

# Capítulo 9

# Desvios de Procedimento

Durante a execução do projeto, foram identificados alguns desvios relativamente ao planeamento inicial, devido a limitações técnicas e decisões tomadas em resposta a dificuldades encontradas. A seguir descreve-se as principais situações em que a implementação não seguiu o caminho inicialmente previsto.

## 9.1 Implementação incompleta do teclado matricial

No planeamento inicial estava prevista a utilização simultânea do leitor NFC e do teclado matricial para garantir uma dupla autenticação baseada no cartão e num código numérico introduzido pelo teclado. No entanto, devido ao elevado consumo de memória do *firmware* no Arduino Nano, não foi possível implementar ambos os componentes em conjunto sem comprometer a estabilidade e o funcionamento do sistema.

Esta limitação levou à decisão de privilegiar a autenticação por cartão NFC, deixando a integração do teclado matricial como uma melhoria futura, conforme descrito no capítulo de trabalho futuro. O recurso limitado de memória do micro-controlador impediu a coexistência das bibliotecas necessárias ao funcionamento simultâneo dos dois módulos, originando conflitos que inviabilizaram a implementação final com dupla autenticação via *hardware*.

## 9.2 Alterações no planeamento do desenvolvimento do *firmware*

Durante a fase de desenvolvimento do *firmware*, foram identificadas várias dificuldades técnicas que obrigaram a ajustar o planeamento inicial. Embora o projeto previsse a implementação de funcionalidades avançadas, como a integração completa do teclado matricial para dupla autenticação e uma gestão mais complexa das comunicações, a realidade do ambiente de desenvolvimento impôs algumas limitações significativas.

Uma das principais restrições encontradas foi a capacidade limitada de memória do micro-controlador utilizado, que dificultou a implementação simultânea de todos os módulos previstos, especialmente o teclado matricial aliado ao leitor NFC. A tentativa de incluir ambas as funcionalidades gerou conflitos e instabilidade no sistema, obrigando a optar por uma solução simplificada que garantisse o funcionamento básico e fiável do controlo de acessos.

Além disso, a gestão do tempo de processamento e a resposta do sistema foram fatores críticos para garantir uma experiência de utilização fluída. Assim, foram simplificadas certas rotinas de comunicação e autenticação para minimizar atrasos e garantir a resposta em tempo real necessária ao sistema.

Estas alterações implicaram a renúncia temporária a algumas funcionalidades inicialmente planeadas, dando prioridade à robustez e estabilidade do sistema como um todo. O compromisso passou por assegurar a implementação de um sistema funcional, testável e seguro dentro das capacidades técnicas disponíveis, deixando abertas futuras melhorias para versões posteriores.

Este desvio do planeamento original ilustra a importância da adaptação contínua face às restrições técnicas e operacionais, bem como a necessidade de equilibrar as funcionalidades desejadas com a viabilidade prática durante o desenvolvimento.

## 9.3 Infraestrutura de testes e recursos utilizados

No planeamento inicial, previa-se que os testes fossem realizados com recurso a equipamentos físicos, incluindo servidores e dispositivos de rede, para simular o ambiente real do sistema de controlo de acessos.

Durante a implementação, optou-se pela utilização de uma máquina virtual com Ubuntu Server em vez de Alpine Linux (que é a distribuição primária usada nos *containers* com os vários serviços do Forge) para simular o servidor *backend*. Esta abordagem proporcionou maior facilidade de prototipagem, permitindo configurar e replicar rapidamente o ambiente de testes, sem depender de *hardware* físico.

A virtualização garantiu o isolamento do ambiente, evitando impactos noutros recursos da rede, e facilitou o acompanhamento do desempenho do servidor.

Esta alteração, não prevista inicialmente, permitiu uma melhor utilização dos recursos disponíveis e acelerou o desenvolvimento, demonstrando a importância da capacidade de adaptação ao longo do projeto.

Para versões futuras, recomenda-se a continuação do uso de infraestruturas virtualizadas, complementadas por equipamentos físicos sempre que necessário para testes específicos relacionados com o *hardware*.

## 9.4 Atrasos e ajustes no cronograma

Durante o desenvolvimento do projeto, surgiram algumas dificuldades técnicas que provocaram atrasos em determinados prazos, sobretudo nas fases de desenvolvimento e testes. A ligação entre os diferentes componentes de hardware revelou-se mais complexa do que o previsto, o que exigiu mais tempo para resolver os problemas e garantir que o micro-controlador e o servidor comunicavam corretamente.

A utilização do micro-controlador Arduino Nano revelou limitações significativas ao nível da memória disponível, impedindo a coexistência das bibliotecas necessárias ao funcionamento simultâneo de múltiplos dispositivos. Como resultado, a autenticação através do teclado foi adiada para iterações futuras, tendo-se privilegiado a estabilidade funcional do sistema.

Face a estes imprevistos, foi necessário reajustar o ritmo das tarefas, dando prioridade à resolução cuidada dos problemas, de modo a assegurar que o sistema fosse estável e fiável. Apesar dos atrasos, optou-se por manter o foco na qualidade do produto final, dando preferência à segurança e ao bom funcionamento, em detrimento do cumprimento rigoroso do calendário inicialmente definido.

# Capítulo 10

# Discussão de resultados

O sistema implementado permitiu validar a viabilidade de um modelo de controlo de acessos baseado em autenticação eletrónica, recorrendo a cartões NFC e comunicação remota com um servidor para verificação de credenciais. Esta abordagem revelou-se eficaz na substituição dos métodos tradicionais baseados em chaves físicas, ao garantir um nível superior de segurança, possibilitar a rastreabilidade dos acessos e assegurar uma maior escalabilidade do sistema para futuras expansões.

Durante a fase experimental, o sistema foi sujeito a 18 execuções consecutivas, que visaram testar a robustez da comunicação entre os componentes, a estabilidade do *firmware* implementado no micro-controlador e a integração com o *backend* virtualizado. Estas execuções tiveram por objetivo identificar eventuais falhas ou limitações que pudessem comprometer o funcionamento contínuo e fiável do controlo de acessos.

A análise dos resultados permitiu não só validar o funcionamento geral do sistema, como também identificar pontos críticos relacionados com a memória do micro-controlador, dependências de bibliotecas e configurações da rede virtual. Estes aspetos foram fundamentais para compreender os desafios práticos associados à implementação e para orientar possíveis melhorias futuras.

A Tabela 10.1 apresenta os resultados obtidos durante as execuções, com especial destaque para as falhas registadas, que são colocadas no topo da tabela para maior visibilidade. As restantes execuções ocorreram sem anomalias, confirmando a estabilidade e fiabilidade da solução dentro do ambiente testado.

**Tabela 10.1:** *Resultados dos testes de autenticação e comunicação com o servidor*

| Teste | Resultado | Observações |
|---|---|---|
| 1 | Falha | Ausência da biblioteca do módulo Ethernet no código do Arduino |
| 2 | Falha | Tentativa de integração do teclado matricial excedeu a memória disponível no Arduino Nano |
| 3 | Falha | Máquina virtual com o servidor não configurada em modo *bridged*, impossibilitando a comunicação com os dispositivos da rede local |
| 4 | Sucesso | Funcionamento estável após correção da falha do teste 1 |
| 5 | Sucesso | Comunicação com o servidor validada com sucesso |
| 6 | Sucesso | Sistema autenticou corretamente cartão autorizado |
| 7 | Sucesso | Operação estável com leitura de cartões e resposta do servidor |
| 8 | Sucesso | Comunicação estabelecida após reconfiguração da VM |
| 9 | Sucesso | Sistema validado com utilizadores simulados |
| 10 | Sucesso | Sem anomalias |
| 11 | Sucesso | Sem anomalias |
| 12 | Sucesso | Sem anomalias |
| 13 | Sucesso | Sem anomalias |
| 14 | Sucesso | Sem anomalias |
| 15 | Sucesso | Sem anomalias |
| 16 | Sucesso | Sem anomalias |
| 17 | Sucesso | Sem anomalias |
| 18 | Sucesso | Sem anomalias |

As falhas registadas decorreram de limitações técnicas enfrentadas durante o desenvolvimento. A primeira, relacionada com a ausência da biblioteca do módulo Ethernet, foi prontamente identificada e corrigida, permitindo o prosseguimento dos testes. A segunda, de natureza estrutural, resultou da insuficiência de memória do microcontrolador Arduino Nano, impossibilitando a inclusão simultânea das bibliotecas necessárias ao funcionamento do teclado matricial. Por último, a terceira falha teve origem na configuração da máquina virtual que alojava o servidor, a qual se encontrava em modo NAT[1]. Tal impediu a comunicação com os dispositivos físicos na mesma rede, sendo necessário alterar a configuração para modo *bridged*.

Apesar destes constrangimentos, os resultados revelaram um desempenho estável do sistema na maioria dos testes, evidenciando a eficácia da abordagem adotada. A sequência de sucessos obtida após a resolução das falhas demonstra que a solução é tecnicamente viável e constitui uma base sólida para futuras extensões, como a integração de autenticação multi-fator, protocolos de comunicação segura e funcionalidades de gestão remota.

[1]NAT – *Network Address Translation*

# Capítulo 11

# Trabalho futuro

Sendo que o sistema implementado, devido a imprevistos relacionados com limitações de *hardware*, cumpre apenas parcialmente os requisitos essenciais de controlo de acessos, existem várias melhorias possíveis que podem ser consideradas em versões futuras.

### Separação das funcionalidades de autenticação e abertura

Numa futura iteração do sistema, deverá ser considerada a utilização de dois microcontroladores distintos (por exemplo, dois Arduinos) para reforçar a segurança física do sistema. Atualmente, o mesmo Arduino executa a leitura dos dados de autenticação e o controlo do trinco elétrico, o que representa uma vulnerabilidade em caso de acesso físico ao dispositivo.

A proposta passa por manter um microcontrolador exposto (junto ao leitor NFC e teclado), responsável apenas pela recolha dos dados de autenticação (UID e PIN), e um segundo microcontrolador colocado em local seguro e inacessível do exterior, que recebe a validação do sistema de autenticação integrado no Forge da Universidade da Maia e executa, caso aplicável, a abertura do trinco.

Esta divisão garante que, mesmo que um atacante tente manipular o primeiro Arduino, não conseguirá ativar o mecanismo de abertura da porta, uma vez que esse controlo estará delegado a um segundo dispositivo isolado.

### Implementação da dupla autenticação com teclado matricial

Devido ao excesso de memória ocupada pelo *firmware* final, não foi possível implementar a dupla autenticação com teclado matricial em conjunto com o sistema NFC. Futuramente, será importante otimizar o código ou utilizar *hardware* com maior capacidade para incluir esta funcionalidade, aumentando a segurança do sistema ao exigir simultaneamente a introdução do PIN e a autenticação via cartão NFC.

### Segurança da comunicação com o servidor

Outra possibilidade de evolução será a adopção de protocolos de comunicação seguros, como HTTPS, em substituição do HTTP simples atualmente utilizado. Isto protegeria os dados transmitidos entre o microcontrolador e o serviço Forge contra ataques como *man-in-the-middle*, especialmente em redes Wi-Fi abertas ou vulneráveis.

### Ligação ao serviço de autenticação do Forge

A integração direta com o serviço Forge da Universidade da Maia, que inclui suporte de autenticação centralizada dos seus utilizadores, está prevista para futuras versões. Esta funcionalidade não foi incluída nesta fase, uma vez que o acesso à base de dados de autenticação se encontra restringido a outros membros da equipa responsável pela gestão do sistema, não tendo sido possível obter permissões adequadas durante o período de desenvolvimento.

Quando implementada, esta ligação permitirá validar credenciais diretamente contra os registos institucionais, garantindo coerência com o sistema de autenticação existente e centralizando a gestão de acessos a nível institucional.

### Gestão remota e monitorização em tempo real

Será vantajoso, em futuras versões, estender a funcionalidade de gestão de utilizadores, já existente no serviço Forge, integrando campos adicionais relacionados com o controlo de acessos físicos. Isto irá permitir associar a cada utilizador algumas informações como:

- Identificadores de cartões NFC;
- Códigos PIN associados;
- Permissões de acesso a zonas específicas (pavilhões ou salas);
- Horários autorizados de entrada;

Ao reutilizar a infraestrutura atual de gestão de utilizadores, evita-se a duplicação de dados e garante-se uma administração centralizada e coerente das permissões. Esta abordagem permitirá ainda, em futuras versões, a integração com *interfaces* gráficos (por exemplo, aplicações *web* ou móveis) para:

- Consultar registos de entrada de forma visual e com filtros;
- Atribuir ou revogar permissões dinamicamente;
- Receber notificações de acessos inválidos ou tentativas suspeitas.

### Sistema de energia redundante

A inclusão de uma fonte de energia de *backup* (como uma bateria ou UPS[1] de baixo consumo) aumentaria a resiliência do sistema em caso de falha de corrente elétrica. Isto é particularmente importante em ambientes onde o acesso não pode ser interrompido por motivos de segurança ou continuidade de serviço.

### Expansão multiporta

Deverá ser equacionada a expansão do sistema para controlar múltiplos pontos de acesso dentro da mesma instituição, garantindo a centralização da autenticação e a sincronização das permissões em todas as portas. Isto pode ser conseguido através da replicação do sistema com instâncias independentes que comunicam com o mesmo servidor central.

### Sistema de controlo para saída da sala

Futuramente, poderá ser implementado um sistema específico para controlar a saída da sala, complementando o sistema de entrada atualmente em uso. Ter um mecanismo dedicado para a saída, como um segundo leitor NFC ou teclado, permitiria registar de forma segura e autónoma a saída dos utilizadores, aumentando o controlo sobre o fluxo dentro do espaço e prevenindo saídas não autorizadas ou situações de emergência. Este sistema de controlo de saída poderá estar integrado com o sistema principal, mantendo a coerência e segurança do controlo de acessos.

[1] UPS – *Uninterruptible Power Supply*

# Capítulo 12

# Conclusões

O presente trabalho teve como principal objetivo o desenvolvimento de um sistema de controlo de acessos físicos mais seguro, fiável e adequado às necessidades do Laboratório 10 da Universidade da Maia, substituindo o tradicional uso de chaves mecânicas por um sistema eletrónico baseado em autenticação por cartão NFC.

Ao longo do processo de conceção e implementação, foi possível validar a viabilidade técnica desta solução, demonstrando que é possível aplicar tecnologias de baixo custo, como micro-controladores e leitores NFC, para reforçar a segurança física em ambientes académicos. O sistema desenvolvido permite identificar de forma unívoca os utilizadores, controlar o acesso em tempo real e manter registos auditáveis das entradas autorizadas.

Contudo, o desenvolvimento enfrentou diversas limitações técnicas, nomeadamente ao nível da capacidade de memória do micro-controlador utilizado (Arduino Nano), o que impediu a concretização de todas as funcionalidades inicialmente previstas, como a dupla autenticação com teclado matricial. A instabilidade gerada pela tentativa de integrar múltiplos módulos levou à necessidade de simplificar o sistema e priorizar a estabilidade e o funcionamento seguro da solução base.

Ainda assim, os resultados obtidos demonstram que a abordagem adotada foi eficaz na criação de uma infraestrutura funcional e escalável, que poderá servir como base para futuras iterações. A utilização de uma infraestrutura de testes virtualizada contribuiu significativamente para a flexibilidade e rapidez no desenvolvimento, destacando-se como uma boa prática a considerar em projetos semelhantes.

Em termos de impacto, esta solução representa um contributo relevante para a melhoria da segurança na instituição, promovendo uma gestão de acessos mais controlada, eficiente e rastreável. Além disso, abre caminho para a implementação de funcionalidades avançadas, como a separação física de módulos críticos, a comunicação segura com o servidor, a integração com plataformas de gestão e a expansão para múltiplos pontos de acesso.

Em conclusão, este projeto demonstrou que é possível criar uma solução de controlo de acessos física robusta e tecnicamente sólida com recursos limitados, desde que acompa-

nhada de uma abordagem cuidadosa, adaptável e orientada para a segurança. O trabalho realizado estabelece uma base sólida para melhorias futuras, respondendo aos desafios atuais e antecipando as necessidades emergentes da instituição.

# Referências


[1] CISA. *Critical Infrastructure Sectors*. 2023.

[2] Techfusion. *Segurança Física e Logica*. 2023.

[3] Microsoft. *O que é a proteção de dados?* 2024.

[4] Anastasiya Novikava. *Cybersecurity in education: back to school, back to risks*. 2024.

[5] CNCS. *Quadro nacional de referência para a cibersegurança*. 2019.

[6] CNCS. *Glossário*. 2024.

[7] Codima. *RFID o que é? Para que serve?* 2024.

[8] CDVI. *O que é o controlo de acesso?* 2024.

[9] Microsoft. *O que é a autenticação?* 2024.

[10] Sérgio Lopes Lavos. «Implementação de um Sistema de gestão de segurança de informação (SGSI) baseado na norma ISO/TEC 27001 na EIB SA». Em: Escola Superior de Tecnologia e Gestão. 2023.

[11] Adminlp2m. *Exploring and Empowering Identity-Based Access Control (IBAC)*. 2024.

[12] imperva. *Role-Based Access Control (RBAC)*. 2024.

[13] Red Hat. *What is role-based access control (RBAC)?* 2024.

[14] Alexander Babko. *Role-based Access Control vs Attribute-based Access Control: Which to Choose*. 2024.

[15] Keith Casey. *What Is Attribute-Based Access Control (ABAC)?* 2020.

[16] Axiomatics. *Intro to Attribute Based Access Control (ABAC)*. 2018.

[17] Prodigy Technovations. *Introduction to I2C Protocol*. 2024.

[18] Piyu Dhaker. *Introduction to SPI Interface*. 2018.

[19] Smoothieware. *Serial Peripheral Interface*. 2016.

[20] TotalPhase. *SPI Background*. 2023.

[21] MikeGrusin. *What is SPI ?: The Basics of Serial Peripheral Interface*. 2024.

[22] Omar S. Saleh Muhammad Ehsan Rana. *High assurance software architecture and design*. 2022.

[23] OWASP. *Insecure Data Storage*. 2025.

[24] Jakob Nielsen. *10 Usability Heuristics for User Interface Design*. 2024.

[25] S. M. S. Shahriar et al. «Security Issues in Near Field Communications (NFC)». Em: International Journal of Advanced Computer Science. 2020.

[26] Polimek. *QR Codes vs. Traditional and Advanced Security Technologies: A Comparative Analysis*. 2024.

[27] Asset infinity. *Barcode vs QR Code vs RFID vs NFC vs BLE vs GPS: Which One Is Better?* 2019.

[28] Ana Marques. «Residências universitárias já dispõem de novo sistema de controlo de acessos». Em: Universidade do Minho. 2024.

[29] Eunice Oliveira. «Cartão do Cidadão tem algoritmo INESC TEC». Em: Universidade do Porto. 2018.

[30] Joel Ribeiro. *Porter Systems lança solução inovadora para abertura de portas e controlo de acessos*. 2018.

[31] Rui Miguel Baptista Peixoto. «Comunicações RFID para Identificação e Controlo de Acessos». Em: Instituto Politécnico de Leiria. 2021.

[32] Microsoft. *Uma em cada cinco empresas já recorre a soluções de cibersegurança baseadas em IA*. 2024.