UNIVERSIDADE DE LISBOA
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE INFORMÁTICA

Revisão e implementação de políticas de segurança centradas no utilizador

Francisco Antunes Alberto Amaro

Mestrado em Segurança Informática

Trabalho de Projeto orientado por:
Prof. Doutor Hugo Alexandre Tavares Miranda

2024

Agradecimentos

Gostaria de expressar a minha profunda gratidão a todos os que, de alguma forma, contribuíram para a realização deste projeto.

Ao Professor Hugo Alexandre Tavares Miranda, por tornar este projeto possível através da sua orientação, apoio e disponibilidade.

A toda a equipa da Direção de Serviços Informáticos da Faculdade de Ciências da Universidade de Lisboa pela forma como me acolheu.

À minha família, por sempre me ter apoiado e acreditado em mim.

Por fim, quero agradecer a todos os meus amigos, especialmente ao António, às Beatrizes, ao Francisco, ao Frederico, à Liliana, à Mariana, ao Nikhil, aos Pedros e ao Rodrigo.

Para a minha famílía.

Resumo

Os utilizadores (e os procedimentos que estes frequentemente adotam) são um dos mais relevantes vetores de ataque numa organização com um grande número de colaboradores em que os níveis de ligação e responsabilidade perante a organização são baixos.

A definição e implementação de políticas de segurança centradas no utilizador que permitam a deteção e mitigação eficaz e eficiente de ações que podem pôr em causa a segurança de toda a infraestrutura informática é em instituições com estas características, particularmente relevante. Para as apoiar, têm vindo a ser emanados de diferentes entidades um conjunto de recomendações e normativos legais que as auxiliam na definição das políticas e lhes dão suporte legal.

Definidas as políticas, é importante garantir que elas são efetivamente aplicadas, através do desenvolvimento de mecanismos que, sempre que possível, automatizem a sua verificação. Não menos importante, a definição das políticas deve ser acompanhada de estratégias de comunicação para a sua divulgação, que envolvam os utilizadores no estabelecimento de um ambiente mais confiável e seguro.

No âmbito deste projeto, foram realizadas diversas tarefas focadas nos utilizadores com o objetivo de reforçar a segurança informática da instituição. Isto incluiu a revisão das políticas e mecanismos de segurança, relacionadas com os utilizadores, em vigor em CIÊNCIAS ULisboa, bem como o desenvolvimento de sistemas para a deteção e resposta a violações dessas políticas. Adicionalmente, o processo de gestão de contas de utilizador foi simplificado através do desenvolvimento de novos mecanismos para criação de contas de utilizador e recuperação das respetivas credenciais.

Palavras-chave: Segurança Informática, Políticas de Segurança, Administração de Sistemas, Desenvolvimento de Aplicações, *Active Directory*.

Abstract

Users (and the procedures they often adopt) are one of the most relevant attack vectors in an organization with a large number of employees where the levels of connection and responsibility towards the organization are low.

The definition and implementation of user-centered security policies that allow the effective and efficient detection and mitigation of actions that could compromise the security of the entire IT infrastructure is particularly relevant in institutions with these characteristics. To support them, a set of recommendations and legal norms have been issued by different entities to assist in the definition of policies and provide legal support.

Once the policies are defined, it is important to ensure their effective application through the development of mechanisms that, whenever possible, automate their verification. Equally important is that the definition of policies should be accompanied by communication strategies for their dissemination, involving users in the establishment of a more reliable and secure environment.

In the scope of this project, various tasks focused on users were carried out with the aim of strengthening the IT security of the institution. This included reviewing the existing security policies and mechanisms related to users in CIÊNCIAS ULisboa, as well as developing systems for the detection and response to violations of these policies. Additionally, the user account management process was simplified through the development of new mechanisms for user account creation and credential recovery.

Keywords: Information Security, Security Policies, System Administration, Application Developing, Active Directory

Conteúdo

Lista de Figuras **xiii**

Lista de Tabelas **xv**

1 Introdução **1**

1.1 Motivação . . . 1
1.2 Objetivos . . . 2
1.3 Contribuições . . . 2
1.4 Estrutura do documento . . . 3

2 Instituição de Acolhimento **5**

2.1 Direção de Serviços Informáticos . . . 5
2.2 Contas de utilizador . . . 6
2.3 Aplicações de CIÊNCIAS ULisboa . . . 6
2.3.1 *Fénix* . . . 6
2.3.2 *Census* . . . 7
2.3.3 *SAP* . . . 7
2.3.4 BalcãoC . . . 8
2.3.5 *Cirrus* . . . 8
2.3.6 *Wazuh* . . . 8
2.4 Autenticação Centralizada . . . 8
2.5 *Active Directory* . . . 9
2.5.1 *Home Directories* . . . 9
2.5.2 *Organizational Units* (*OUs*) . . . 9
2.5.3 *Lightweight directory access protocol* (*LDAP*) . . . 9
2.6 Correio Eletrónico Institucional . . . 10
2.6.1 *Exchange* . . . 11

3 Conceitos e Trabalho Relacionado **13**

3.1 Documentos normativos . . . 13
3.1.1 Resolução do Conselho de Ministros n.º41/2018 . . . 13
3.1.2 Diretriz 2023/1 da Comissão Nacional da Proteção de Dados . . . 14

3.1.3 Diretiva *NIS2* (*Network and Information Security Directive*) 15
3.2 Verificação de identidade 15
3.2.1 Fatores de autenticação 16
3.2.2 Mecanismos para recuperação de palavra-passe 16
3.2.3 Comparação de mecanismos para recuperação de palavra-passe 18

4 Ferramentas de desenvolvimento **19**

5 Verificação Periódica de Políticas de Segurança **21**
5.1 Levantamento de requisitos 21
5.2 Solução 22
5.2.1 Itens 22
5.2.2 Pontuação 23
5.3 Avaliação 24
5.4 Trabalho Futuro 25

6 Gestão de Contas de Utilizadores **27**
6.1 Recuperação de Credenciais 27
6.1.1 Levantamento de requisitos 27
6.1.2 Decisões 28
6.1.3 Processo 28
6.1.4 Implementação 31
6.1.5 Auditoria 33
6.1.6 Segurança 35
6.1.7 Avaliação 37
6.2 Identificação de contas de utilizador anómalas 40
6.2.1 Levantamento de requisitos 40
6.2.2 Processo 41
6.2.3 Implementação 43
6.2.4 Segurança dos *Endpoints* 44
6.2.5 Avaliação 44
6.2.6 Trabalho Futuro 45
6.3 Criação de contas 46
6.3.1 Levantamento de requisitos 46
6.3.2 Formulários 48
6.3.3 Arquitetura 48
6.3.4 Auditoria 52
6.3.5 Implementação 52
6.3.6 Análise de Segurança 53
6.3.7 Avaliação 53

6.3.8 Trabalho Futuro 54

7 Conclusão **55**

Bibliografia **60**

Lista de Figuras

2.1 Exemplo de perfil no *Census* que mantém uma relação ativa com CIÊNCIAS ULisboa. 7
2.2 Entrada de *Active Directory* (com alguns dados omitidos). 10
2.3 Organização dos utilizadores em *OUs* no *Active Directory*. 10

3.1 Excerto da Resolução do Conselho de Ministros nº41/2018. 14
3.2 Excerto da Diretriz 2023/1 da Comissão Nacional da Proteção de Dados. 14
3.3 Excerto da Diretiva *NIS2* (*Network and Information Security Directive*). 15
3.4 Estrutura de um *URL token*. 17

5.1 Excerto do formulário. 22
5.2 Evolução da pontuação obtida no formulário. 24

6.1 Formulário inicial do pedido de recuperação de credenciais. 29
6.2 Fase inicial do pedido de recuperação de credenciais. 30
6.3 Fase final de recuperação de credenciais. 31
6.4 Formulário de recuperação de credenciais (Arquitetura). 32
6.5 Estados de um pedido de recuperação de credenciais. 34
6.6 *Logs* do sistema de recuperação de credenciais (com alguns dados omitidos). . . 35
6.7 *Logs* do sistema de recuperação de credenciais (com alguns dados omitidos). . . 36
6.8 Serviço do BalcaoC que dá acesso ao sistema de recuperação de credenciais. . . . 39
6.9 Arquitetura do sistema de identificação de contas de utilizador anómalas na instituição. 41
6.10 *URI* do verificador automático de coerência da informação. 42
6.11 Notificações enviadas. 43
6.12 Notificações de boas-vindas. 47
6.13 Formulários para a criação de contas de utilizador. 49
6.14 Relatório de criação de contas (com alguns dados omitidos). 50
6.15 Arquitetura do sistema de criação de contas. 51

Lista de Tabelas

3.1 Comparação de mecanismos para recuperação de palavra-passe. 18

5.1 Unidades de serviço. 23
5.2 Estado do formulário. 23
5.3 Coeficiente multiplicativo do formulário. 24

6.1 Campos da base de dados do mecanismo de recuperação de credenciais. 34
6.2 Estatísticas do sistema de recuperação de credenciais. 39
6.3 Campos da base de dados do mecanismo de identificação de contas de utilizador anómalas. 44
6.4 Estatísticas recolhidas do *Active Directory*. 45
6.5 Estatísticas referentes aos utilizadores sem vínculo válido no *Census*. 45
6.6 Estatísticas recolhidas do sistema de criação de contas. 54

Capítulo 1

Introdução

Os utilizadores, e os procedimentos que frequentemente adotam, são um dos principais vetores de ataque em organizações com inúmeros colaboradores, especialmente quando os níveis de compromisso e responsabilidade perante a organização são baixos. Comportamentos negligentes ou desinformados por parte dos utilizadores podem abrir portas para diversas ameaças informáticas, comprometendo a segurança da organização.

Quando uma organização é vítima de um ataque informático pode enfrentar um conjunto de consequências adversas. Estas consequências podem ser financeiras, com perdas significativas de receita; reputacionais, com danos à imagem pública da organização; legais, devido a possíveis violações de regulamentações de proteção de dados; e operacionais, afetando a continuidade e a eficiência dos serviços prestados.

Dada a gravidade destas potenciais consequências, é crucial que as organizações tomem medidas para prevenir e mitigar tais ataques. Estas medidas envolvem definir, implementar, verificar e atualizar continuamente um conjunto robusto de políticas e mecanismos de segurança. Só desta forma pode a organização continuar a proteger os seus recursos e a garantir um ambiente digital seguro e confiável para todos os seus utilizadores.

1.1 Motivação

As políticas e os mecanismos de segurança em vigor numa organização contribuem para a diminuição da superfície de ataque das organizações. Para as apoiar na sua definição e implementação, têm sido emanados, de diferentes entidades, um conjunto de recomendações e normativos legais.

Este projeto assenta na necessidade de contribuir para a segurança informática da instituição em que foi desenvolvido através da revisão e implementação de políticas de segurança centradas no utilizador, e através da implementação de novos mecanismos de segurança, mais simples e robustos.

Espera-se que estas melhorias tenham vários impactos positivos. Por um lado, a organização irá oferecer um ambiente, com uma grande variedade de recursos disponíveis, mais seguro e confiável para todos os seus utilizadores, diminuindo desta forma o risco de sofrer consequências adversas que possam surgir de um ataque informático. Por outro lado, pretende-se que estas melhorias promovam uma cultura de segurança informática na organização, sensibilizando e incentivando os

utilizadores para a importância da adoção de um conjunto de práticas seguras no seu dia a dia.

1.2 Objetivos

Este projeto é composto por vários objetivos interligados entre si, e que direta ou indiretamente têm o seu foco nos utilizadores.

O objetivo principal do projeto é a revisão das políticas e mecanismos de segurança em vigor em CIÊNCIAS ULisboa, bem como o desenvolvimento de mecanismos para a deteção e resposta a violações dessas políticas.

Neste processo de revisão de mecanismos de segurança, entendeu-se que o processo de gestão de contas de utilizador teria de ser alvo de intervenção, para possibilitar simultaneamente um maior grau de confiabilidade e de usabilidade. Isto resultou no desenvolvimento de novos mecanismos para criação de contas de utilizador e recuperação das respetivas credenciais.

Por fim, pretende-se que através destas políticas e mecanismos, cada conta de utilizador ativa na organização possa ser associada inequivocamente a uma pessoa que tenha um vínculo estabelecido com a organização que a justifique. Para atingir este objetivo foram implementadas medidas que impedem a criação de novas contas que não o respeitem, mas também mecanismos que detetem contas já existentes que não satisfazem este requisito.

1.3 Contribuições

As contribuições deste projeto incluem o estabelecimento de procedimentos para a definição e implementação de políticas de segurança na organização, com base em recomendações e normativos legais de diversas entidades.

Para garantir que estas políticas são efetivamente aplicadas, foi criado um formulário para autoavaliação sistemática da implementação de políticas de segurança na instituição.

Além disso, os mecanismos de gestão de contas de utilizadores foram simplificados, através do desenvolvimento de novos mecanismos para criação de contas de utilizador e recuperação das respetivas credenciais.

No novo mecanismo de recuperação de credenciais ou criação de contas e respetivos recursos, o utilizador apenas precisa de fornecer o número do seu documento de identificação e ter acesso ao seu dispositivo móvel ou à sua caixa de correio eletrónico pessoal.

Por fim, para assegurar que todas as contas de utilizador ativas na organização possam ser associadas inequivocamente a uma pessoa que tenha um vínculo ativo válido estabelecido com a organização, desenvolveu-se um sistema que deteta, notifica, e se necessário, encerra as contas de utilizador que não verificam esta condição.

1.4 Estrutura do documento

Este documento está organizado da seguinte forma. O capítulo 2 faz um enquadramento do trabalho realizado, apresentando a instituição de acolhimento. O enquadramento continua nos capítulos 3 e 4 respetivamente com a apresentação dos conceitos e o trabalho relevante, e das ferramentas utilizadas para a implementação do projeto.

O capítulo 5 introduz o trabalho realizado, apresentando o formulário para autoavaliação sistemática da implementação de políticas de segurança na instituição. A apresentação do trabalho realizado continua no capítulo 6, onde são descritos novos mecanismos de gestão de contas, incluindo aplicações para recuperação de credenciais de contas de utilizador, deteção de contas de utilizador anómalas na instituição e criação de contas de utilizador.

Por fim, o capítulo 7 apresenta as conclusões do trabalho realizado no âmbito projeto.

Capítulo 2

Instituição de Acolhimento

Neste capítulo são apresentadas informações relevantes sobre a Faculdade de Ciências da Universidade de Lisboa, instituição na qual este projeto foi realizado. Estas informações incluem dados sobre a sua dimensão, a sua infraestrutura informática, os serviços que disponibiliza e a sua direção de serviços informáticos.

CIÊNCIAS ULisboa tem uma forte componente tecnológica e foi um dos primeiros locais em Portugal com conectividade à Internet. A Universidade de Lisboa esteve desde o início da sua ligação à Internet e até 2005 interligada por meio de CIÊNCIAS ULisboa. Desde 2005 a ligação à FCCN (Fundação para o Cálculo Científico Nacional), que interliga todas as Instituições de Ensino Superior em Portugal, é realizada através da Reitoria da Universidade de Lisboa [1].

Como instituição de ensino superior, CIÊNCIAS ULisboa possui características muito específicas. Atualmente, conta com cerca de 5.000 alunos, com aproximadamente 1.000 novas inscrições e 1.000 conclusões de curso a cada ano letivo. Além disso, possui 700 colaboradores, dos quais cerca de 300 mudam anualmente [2]. Cada pessoa necessita de acesso a um conjunto variado de ferramentas e aplicações para desempenhar as suas funções. A Direção de Serviços Informáticos (DSI) é responsável por gerir esses recursos de forma eficaz.

2.1 Direção de Serviços Informáticos

De acordo com o Regulamento Orgânico de CIÊNCIAS ULisboa, a Direção de Serviços Informáticos (DSI) é responsável pela gestão, implementação, segurança, confiabilidade, suporte e promoção da utilização dos serviços e sistemas de informática no âmbito das atividades de CIÊNCIAS ULisboa. Dá também apoio ao planeamento dessas atividades e à tomada de decisão superior. Finalmente, é responsável pelo reporte às entidades competentes. A Direção de Serviços Informáticos é o serviço responsável pela arquitetura e evolução dos sistemas informáticos existentes, assumindo um carácter proativo no planeamento e desenvolvimento de novos sistemas que contribuam para a melhoria da qualidade e eficiência das atividades de CIÊNCIAS ULisboa [3, 4, 5].

A Direção de Serviços Informáticos integra atualmente 10 pessoas, distribuídas pelas suas unidades de serviço: Área de Serviços e Servidores, Área de Redes e Comunicações, Área de Aplicações e Desenvolvimento e Gabinete de Suporte ao Utilizador.

2.2 Contas de utilizador

Devido ao elevado número de alunos e colaboradores, bem como à sua constante rotatividade, a DSI precisa criar e desativar mais de mil contas por ano. Além disto, precisa de garantir ainda que estas contas têm acesso aos recursos necessários.

Para facilitar esta gestão, CIÊNCIAS ULisboa segrega as contas de utilizador em diferentes tipos:

Contas de aluno As contas de alunos são atribuídas a todos os estudantes, devidamente inscritos nos serviços académicos e estão associadas ao domínio *@alunos.fc.ul.pt*.

O *login* atribuído a este tipo de conta é do formato fcNNNNN@alunos.fc.ul.pt, onde NNNNN corresponde aos 5 algarismos do número de aluno. Por exemplo, se o número de aluno for 54440, o *login* do utilizador será fc54440@alunos.fc.ul.pt.

Contas de colaborador As contas de colaborador são atribuídas a todos os colaboradores (funcionários não docentes e não investigadores, docentes, investigadores, bolseiros de investigação, etc.) e estão associadas ao domínio *@fc.ul.pt*.

O *login* atribuído a esta conta é determinado por um algoritmo, que concatena a primeira letra do primeiro nome, a primeira letra do segundo nome e o último nome. Por exemplo, se o nome completo for António José Jacinto Gonçalves, o *login* será ajgoncalves@fc.ul.pt. Caso já exista um utilizador com o mesmo *login*, o número de letras do segundo nome é incrementado até se encontrar um disponível [6].

Contas institucionais As contas institucionais são atribuídas a unidades e grupos específicos afiliados a CIÊNCIAS ULisboa (unidades de investigação, departamentos, conferências, etc.) e estão associadas ao domínio *@fc.ul.pt*.

Conta temporaria de Conferência/Aulas As contas temporárias de conferência/aulas têm uma duração de até 2 meses e estão associadas ao domínio *@alunos.fc.ul.pt*.

Conta temporaria de Visitante As contas temporárias de visitante têm uma duração de até 2 meses e estão associadas ao domínio *@fc.ul.pt*.

2.3 Aplicações de CIÊNCIAS ULisboa

Nesta secção são apresentadas as várias aplicações de CIÊNCIAS ULisboa relevantes no âmbito deste projeto.

2.3.1 *Fénix*

O *Fénix*[1] é a aplicação de gestão académica. A principal responsabilidade de uma aplicação académica é gerir, eficientemente, toda a informação relacionada com as atividades académicas

[1] `https://fenix.ciencias.ulisboa.pt/`

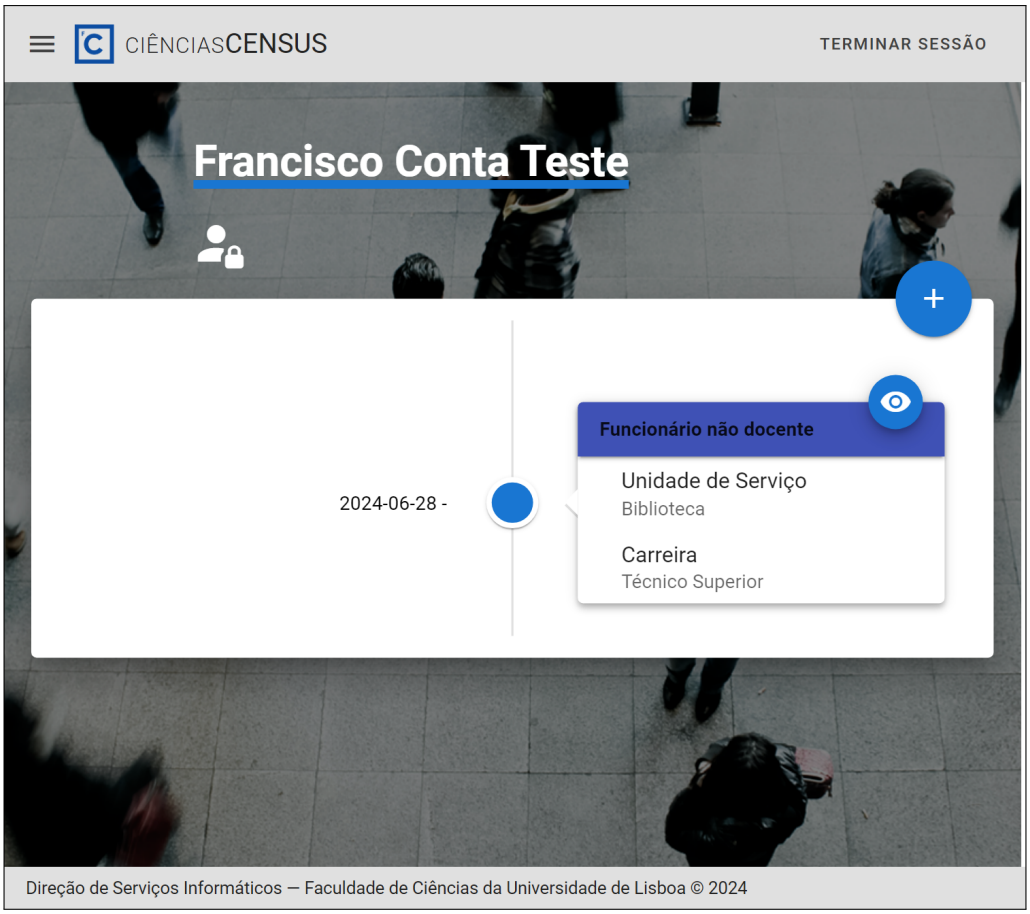


Figura 2.1: Exemplo de perfil no *Census* que mantém uma relação ativa com CIÊNCIAS ULisboa.

da escola, incluindo por isso (mas não limitado a) cursos, planos e unidades curriculares, aulas e sumários, espaços, classificações, pautas, docentes e alunos [7].

2.3.2 *Census*

O Census[2] é uma aplicação de gestão de recursos humanos. Esta serve como repositório das relações que todos os membros da CIÊNCIAS ULisboa mantêm ou mantiveram com a instituição, para além de relação de aluno. Isso inclui pessoal docente, não docente e investigador, bolseiros, colaboradores externos, visitantes, entre outros [8]. Na Fig. 2.1 está apresentado um exemplo de perfil que mantém uma relação ativa com a instituição, o utilizador em questão é um funcionário não docente, desempenha funções na biblioteca, está na carreira de técnico superior, iniciou funções a 28-06-2024 e não há data prevista para o encerramento de funções.

2.3.3 *SAP*

O SAP[3] é uma aplicação de gestão empresarial. No entanto, em CIÊNCIAS ULisboa, é utilizada uma instância em que um dos módulos é o de recursos humanos, que permite gerir de

[2] `https://census.ciencias.ulisboa.pt/`
[3] `https://sap.ulisboa.pt/`

forma eficiente as carreiras, os vencimentos, as ausências, as presenças e as férias dos funcionários.

No âmbito deste projeto, esta aplicação permite consultar determinados tipos de vínculos que os utilizadores mantêm com a instituição, e que, por esse motivo, justificam uma conta de utilizador. Além disso, permite verificar a coerência dos dados com outras aplicações, como, por exemplo, o *Census*.

2.3.4 BalcãoC

O BalcaoC[4] é uma aplicação que agrega todos os serviços disponibilizados por CIÊNCIAS ULisboa. O seu objetivo é simplificar o acesso a estes serviços, concentrando toda a informação num único ponto.

Esta aplicação apresenta toda a informação necessária para obter cada serviço, incluindo a informação que deverá prestar, o ponto de contacto, os formulários necessários e as condições que o requerente terá que satisfazer para o solicitar [9].

Adicionalmente, esta permite ainda receber, tratar e encaminhar os dados inseridos pelo utilizador ao preencher formulários associados a serviços *online*.

2.3.5 *Cirrus*

A *Cirrus*[5] é uma instanciação da *ownCloud*[6], sendo uma aplicação de armazenamento e partilha de ficheiros com uma interface *web* semelhante a serviços na nuvem como o *Google Drive* ou a *Dropbox*. Está disponível para toda a comunidade de CIÊNCIAS ULisboa [10].

2.3.6 *Wazuh*

CIÊNCIAS ULisboa possui uma instância do sistema de Gestão de Informações e Eventos de Segurança (*SIEM*) *Wazuh*[7]. Um *SIEM* auxilia as organizações a detetar, analisar e responder a ameaças à segurança antes que estas afetem as suas operações empresariais.

2.4 Autenticação Centralizada

CIÊNCIAS ULisboa utiliza na grande maioria dos seus serviços uma instância da plataforma *CAS*[8] que, em conjunto com o *Microsoft Active Directory*, oferecem um sistema de autenticação centralizado aos seus utilizadores.

O *CAS* disponibiliza um serviço de *single sign-on* que apresenta ao utilizador sempre a mesma página de autenticação (id.fc.ul.pt), independentemente do serviço acedido. Adicionalmente, este serviço de *single sign-on* garante que um único processo de autenticação é válido, durante um período predefinido de tempo, mesmo quando o utilizador alterna entre diferentes serviços [11].

[4] `https://balcaoc.ciencias.ulisboa.pt/`
[5] `https://cirrus.ciencias.ulisboa.pt`
[6] `https://owncloud.com/`
[7] `https://wazuh.com/`
[8] `https://apereo.github.io/cas/7.0.x/index.html`

O gestor de identidades do *Microsoft Active Directory* garante que a identidade de cada utilizador é partilhada por todos os serviços. O *Active Directory* também é responsável por monitorizar e gerir todos os acessos e respetivas autorizações [12].

Na instituição existem duas instâncias do serviço de diretório *Active Directory*: uma para o domínio @*alunos.fc.ul.pt* e outra para o domínio @*fc.ul.pt*. Conforme a política interna, os utilizadores ativos do domínio @*alunos.fc.ul.pt* devem ter uma matrícula ativa no *Fénix*, enquanto os do domínio @*fc.ul.pt* devem ter um dos vínculos que justifica a existência de conta, no *Census*.

2.5 *Active Directory*

O *Active Directory* é um serviço de diretório desenvolvido pela *Microsoft*, utilizado em ambientes *Windows*, que segue as diretrizes da norma X.500 [13] para serviços de diretório. Este serviço permite a autenticação de utilizadores, o armazenamento das suas contas e dados associados, bem como a consulta desses dados pelos utilizadores da rede, como ilustrado na Fig. 2.2. Esta tecnologia desempenha um papel essencial na administração e gestão de recursos de rede, como computadores, utilizadores, grupos e outros dispositivos, num ambiente distribuído [14].

2.5.1 *Home Directories*

O *Active Directory* também permite a gestão de *Home Directories*, ao armazenar os caminhos para diretórios remotos nos atributos do utilizador. As *Home Directories* são pastas pessoais *online* onde os utilizadores podem guardar qualquer tipo de ficheiros.

Estas pastas podem ser acedidas de diversas formas. O exemplo mais comum em CIÊNCIAS ULisboa, são os alunos que ao se autenticarem nos computadores dos laboratórios, têm no ambiente de trabalho um atalho para estas pastas. A vantagem é que todos os documentos destas pastas estarão sempre disponíveis, uma vez que estão guardados num servidor e não no computador local.

2.5.2 *Organizational Units* (*OUs*)

As *Organizational Units (OUs)* foram introduzidas nas diretrizes da norma X.500 [13] para serviços de diretório, permitindo a classificação de objetos nesse tipo de serviços. Como o *Active Directory* está conforme as diretrizes da norma X.500, permite organizar utilizadores em *Organizational Units (OUs)*. Na Fig. 2.3, observa-se, por exemplo, que a utilizadora *Elena Swift* pertence à *OU* de *Managers*. Uma das principais vantagens de organizar utilizadores em *OUs* é a facilidade de aplicar políticas de segurança a um grupo de utilizadores pertencentes à mesma *OU*.

Em CIÊNCIAS ULisboa, os utilizadores estão organizados em diversas *OUs* para uma gestão mais eficiente.

2.5.3 *Lightweight directory access protocol* (*LDAP*)

O *Lightweight Directory Access Protocol* (*LDAP*) é um protocolo aplicacional que permite aceder e gerir, através da rede, serviços de diretório, como, por exemplo, o *Active Directory* [15].

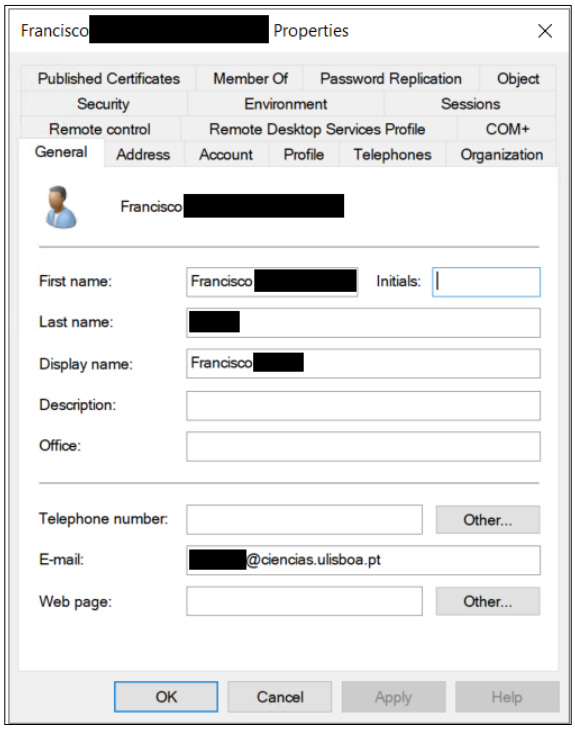


Figura 2.2: Entrada de *Active Directory* (com alguns dados omitidos).

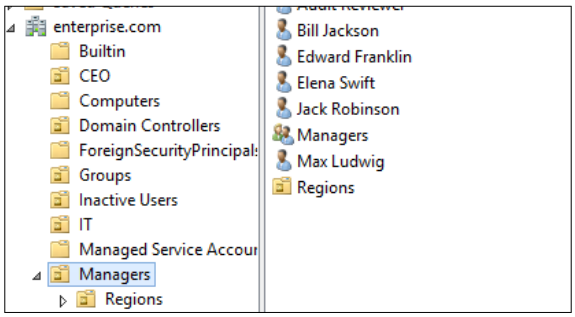


Figura 2.3: Organização dos utilizadores em *OUs* no *Active Directory*.

As bibliotecas usadas neste projeto, que permitem a gestão em rede do serviço de diretório *Active Directory*, recorrem a este protocolo.

2.6 Correio Eletrónico Institucional

CIÊNCIAS ULisboa disponibiliza um serviço de correio eletrónico institucional[9] para os seus utilizadores, entre os quais se incluem docentes, investigadores, bolseiros, funcionários e alunos.

A cada utilizador é atribuída uma quota, ou seja, uma capacidade máxima para armazenamento de mensagens, sendo em alguns casos, complementada com um sistema de arquivo, também este com uma quota [16].

O correio eletrónico recorre aos serviços do servidor *Microsoft Exchange on-premisses* para

[9] `https://webmail.ciencias.ulisboa.pt/`

receber e enviar mensagens.

2.6.1 *Exchange*

O *Microsoft Exchange Server* é um serviço de correio eletrónico desenvolvido pela *Microsoft* e utilizado em ambientes *Windows*. O *Exchange* utiliza o serviço de diretório *Active Directory* para armazenar os atributos necessários para o auxílio na gestão de caixas de correio, arquivos, contactos e calendários [17].

Capítulo 3

Conceitos e Trabalho Relacionado

A realização deste projeto versou uma componente administrativa e uma componente mais técnica. A primeira focou-se sobretudo em assegurar a conformidade das políticas e procedimentos da Direção de Serviços Informáticos (DSI) de CIÊNCIAS ULisboa com os normativos produzidos por entidades externas. Os documentos que materializam estes normativos são apresentados na Sec. 3.1. A segunda componente assentou num conjunto de princípios, técnicas e ferramentas que facilitaram a implementação das plataformas necessárias à reformulação dos procedimentos de autenticação dos utilizadores. A procura por soluções que aumentem a robustez e segurança do processo de mudança de credenciais é o foco da Sec. 3.2.

3.1 Documentos normativos

Para apoiar as organizações, têm sido emanados de diferentes entidades um conjunto de recomendações e normativos legais que as auxiliam na definição das políticas de segurança informática e lhes dão suporte legal.

3.1.1 Resolução do Conselho de Ministros n.º41/2018

A Resolução do Conselho de Ministros n.º41/2018 [18], cujo excerto é apresentado na Fig. 3.1, define orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação e procedimentos a adotar de modo a cumprir as normas do Regulamento Geral de Proteção de Dados.

Este documento inclui uma lista de orientações, que estão separadas por camadas (*front-end*, aplicacional e de base de dados). A cada uma destas orientações é atribuída uma classificação de obrigatoriedade ou de recomendação.

Alguns exemplos de orientações presentes neste documento abrangem, por exemplo, a capacidade para autenticar e autorizar todos os utilizadores, a atribuição de direitos de acesso e privilégio de forma restrita e controlada, a atribuição das credenciais de acesso de forma controlada e a revisão de direitos de acesso de utilizadores em intervalos regulares.

Arquitetura de segurança das redes e sistemas de informação

Requisitos técnicos

Notas:

FE — *Front-end*;
App — Camada Aplicacional
BD — Camada de Base de Dados

Requisito geral	Requisitos Específicos		Classificação
As aplicações cliente (exemplo, *Android*, IOS, WEB) devem ser desenvolvidas adotando práticas de desenvolvimento seguro.	FE	Seguir as boas práticas de desenvolvimento. Exemplo: *Open Web Application Security Project* (OWASP), no que respeita ao desenvolvimento de código seguro e de submissão desse código a testes de segurança.	Obrigatório.
		Utilização de sessões seguras com protocolo de Segurança.	Obrigatório.
		Recomenda-se o uso de *Transport Layer Security* (TLS), na sua versão mais recente.	Recomendado.
		Não guardar informação pessoal no *browser*, memória ou disco, para além do tempo da sessão e apenas na medida do necessário.	Obrigatório.

Figura 3.1: Excerto da Resolução do Conselho de Ministros nº41/2018.

B. Técnicas

i. Autenticação

a. Utilizar credenciais fortes com palavras-passe longas (pelo menos 12 caracteres), únicas, complexas e com números, símbolos, letras maiúsculas e minúsculas, alterando-as com frequência;

b. Equacionar, designadamente face à sensibilidade da informação, aos privilégios dos utilizadores ou à forma de acesso (*v.g.* remota), a aplicação de autenticação multifator;

Figura 3.2: Excerto da Diretriz 2023/1 da Comissão Nacional da Proteção de Dados.

3.1.2 Diretriz 2023/1 da Comissão Nacional da Proteção de Dados

A Diretriz 2023/1 da Comissão Nacional da Proteção de Dados [19], cujo excerto é apresentado na Fig. 3.2, contém recomendações de medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais, destinadas aos responsáveis pelos tratamentos e aos subcontratantes, pretendendo sensibilizá-los para as suas obrigações legais no domínio da segurança dos tratamentos e para a necessidade de realizarem um maior investimento nesta área.

Alguns exemplos de medidas organizativas presentes neste documento abrangem, por exemplo, a definição de políticas de gestão de palavras-passe seguras, impondo requisitos para o tamanho, a composição, a documentação e correção de vulnerabilidades de segurança detetadas sem demora, e a avaliação periódica das medidas de segurança, técnicas e organizativas, internas e proceder à sua atualização e revisão sempre que necessário.

As medidas técnicas presentes neste documento abrangem a autenticação, a infraestrutura e sistemas, a ferramenta de correio eletrónico, a proteção contra *malware*, a utilização de equipamentos em ambiente externo, o armazenamento de documentos em papel que contenham dados pessoais e o transporte de informação que integre dados pessoais. Isto traduz-se em medidas concretas no documento, como, por exemplo, a ativação e conservação dos registos de auditoria (*logs*) e o bloqueio de contas após várias tentativas inválidas de *login*.

Article 21

Cybersecurity risk-management measures

1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

Figura 3.3: Excerto da Diretiva *NIS2* (*Network and Information Security Directive*).

3.1.3 Diretiva *NIS2* (*Network and Information Security Directive*)

A Diretiva *NIS2* [20], cujo excerto é apresentado na Fig. 3.3, ainda não foi transposta para a legislação nacional. Esta diretiva, que atualiza a *NIS* [21], proveniente do Parlamento Europeu e do Conselho, foi publicada a 14 de dezembro de 2022 e estabelece uma legislação harmonizada sobre cibersegurança para toda a União Europeia.

A diretiva aplica-se apenas a entidades gestoras de serviços críticos, como empresas dos setores dos transportes, energia ou banca, e portanto não incluindo CIÊNCIAS ULisboa. A diretiva refere que estas entidades devem adotar medidas técnicas e organizacionais apropriadas e proporcionais, tais como a análise de riscos e políticas de segurança da informação, o tratamento e divulgação de vulnerabilidades e o uso de autenticação multifator.

3.2 Verificação de identidade

Nesta secção serão apresentados os vários fatores de autenticação existentes identificados em [22], os mecanismos que os implementam, e uma comparação entre os mesmos.

3.2.1 Fatores de autenticação

Os Fatores de Autenticação consistem em evidências que o utilizador disponibiliza para se autenticar num serviço. Abaixo estão descritos os fatores de autenticação mais comuns [22]:

Fator de autenticação baseado em conhecimento: Algo que o utilizador sabe, por exemplo, uma palavra-passe, um *PIN*, ou uma pergunta de segurança.

Fator de autenticação baseado em posse: Algo que o utilizador possui, por exemplo, um *token* ou um dispositivo móvel que lhe permita consultar *SMSs* ou receber chamadas.

Fator de autenticação baseado em inerência: Algo que o utilizador é. Este fator é determinado, por exemplo, através da recolha de um dado biométrico do utilizador, como a sua impressão digital, face, ou íris.

Fator de autenticação baseado em localização: Algum local no qual o utilizador se encontra. Este fator é determinado, por exemplo, através da recolha de um dado relativo à localização do utilizador, como a sua geolocalização, ou o seu *IP* de origem.

Fator de autenticação baseado em comportamento: Algo que o utilizador faz. Este fator é determinado, por exemplo, através da análise de como o utilizador se movimenta, usa o teclado, faz *swipe*, ou segura o dispositivo.

3.2.2 Mecanismos para recuperação de palavra-passe

A palavra-passe é um mecanismo de autenticação baseado em conhecimento. Para permitir a recuperação de uma palavra-passe, é necessário que o serviço tenha uma forma alternativa de autenticar o utilizador, por meio de um mecanismo que implemente pelo menos um dos fatores de autenticação, por exemplo, dos apresentados na secção 3.2.1. Esta autenticação pode ser feita, por exemplo, através de *URL tokens*, *PINs*, métodos *offline* ou perguntas de segurança [23].

***URL tokens*:** Um *URL Token* é uma chave de autenticação composta por vários caracteres, que está incluída num *URL*, conforme ilustrado na Fig. 3.4. Ao receber o *URL Token*, o utilizador precisa apenas de clicar nele para ser automaticamente redirecionado para uma página de alteração de credenciais.

Este mecanismo só garante eficácia e segurança, quando cumpre um conjunto de requisitos [23, 24, 25, 18], que abrange vários critérios, nomeadamente: a geração, o armazenamento, as associações, a extensão, a validade e a comunicação do mesmo.

Os requisitos de geração segura estabelecem que cada *URL token* deve ser criado aleatoriamente por algoritmos criptográficos seguros. Em trabalhos anteriores foram descobertas vulnerabilidades em *websites* que utilizavam métodos pouco seguros para essa geração [23, 25]. Após a criação, é essencial que o armazenamento seja seguro, recorrendo a técnicas de criptografia, como *hashing*, *salting* e/ou *peppering*. *Hashing* é uma função unidirecional que

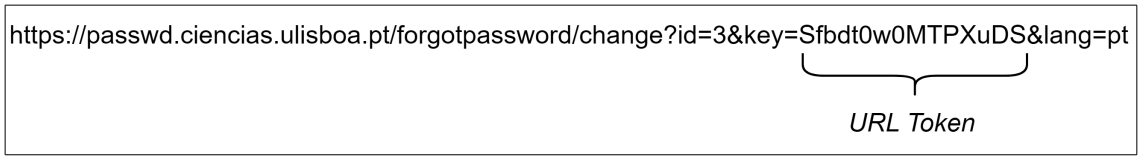


Figura 3.4: Estrutura de um *URL token*.

converte um valor noutro valor. Por ser uma função unidirecional este processo é irreversível. O *hashing* é o método preferencial para armazenar palavras-passe. *Salting* e *peppering* são mecanismos que são usados para prevenir ataques de dicionário e ataques de força bruta, através da adição de uma cadeia de caracteres aleatória a um dado antes deste ser processado por uma função de *hash*.

Cada *URL token* deve estar associado a um único utilizador, garantindo que cada pessoa tem, no máximo, um *URL token* válido de cada vez [25]. Para prevenir ataques de força bruta, é necessário que o *token* seja suficientemente extenso. Além disso, cada *token* deve ter um prazo de validade estipulado, evitando assim vários tipos de ataques, como os de força bruta ou repetição. Estudos anteriores recomendaram que esse período de validade seja bastante reduzido, preferencialmente não superior a 5 minutos, conforme estipulado na Resolução do Conselho de Ministros nº 41/2018 [18].

A comunicação do *URL token* deve ser feita por um canal alternativo, como *SMS* ou *e-mail*. Esses canais contribuem para a segurança do sistema, uma vez que funcionam como fatores de autenticação baseados em posse, garantindo que apenas o utilizador pretendido tem acesso ao *SMS* ou *e-mail* que contém o *URL token*.

***PINs*:** Os *PINs* são números, compostos por 6 a 12 dígitos, enviados ao utilizador por um canal secundário, por exemplo, por *SMS* [23]. Os *PINs*, neste contexto, implementam um fator de autenticação baseado em posse.

Métodos *offline*: Os métodos *offline* permitem que o utilizador recupere a sua palavra-passe sem solicitar um *URL token* ou um *PIN*. Os códigos de *backup* são um exemplo de método *offline*. Estes códigos são atribuídos ao utilizador no momento do seu registo, e o objetivo é que o utilizador os guarde seguramente, até que precise deles para recuperar a sua palavra-passe [23].

Perguntas de segurança: Este mecanismo consiste no utilizador definir a resposta a algumas perguntas pessoais (ex.: "Qual é o nome do seu melhor amigo de infância?") durante o processo de registo da sua conta. Quando é necessário recuperar o acesso à mesma, o utilizador apenas necessita de responder acertadamente a essas perguntas.

As perguntas de segurança foram usadas por empresas como a *Google*, *Microsoft* e o *Yahoo* como mecanismo para recuperação de palavra-passe.

Mecanismo	Confidencialidade	Usabilidade	Implementação
Pergunta de Segurança			√
PIN	√		√
Método Offline	√		√
URL Token	√	√	√

Tabela 3.1: Comparação de mecanismos para recuperação de palavra-passe.

3.2.3 Comparação de mecanismos para recuperação de palavra-passe

A comparação de mecanismos para recuperação de palavra-passe está apresentada na Tab. 3.1.

As perguntas de segurança têm um baixo nível de segurança, confiabilidade e usabilidade, apresentando várias vulnerabilidades. Há respostas comuns a vários utilizadores, o universo de respostas possíveis a algumas destas questões é bastante limitado, as respostas estão muitas vezes publicamente disponíveis. Este mecanismo é ainda vulnerável a ataques de engenharia social e a ataques de inferência social. Além disso, os utilizadores sentem dificuldade em memorizar as respostas às perguntas de segurança. Posto isto, o uso das perguntas de segurança como mecanismo para recuperação de palavra-passe é amplamente desaconselhado por múltiplas autoridades, incluindo a *NIST*[1] através da diretriz *NIST SP 800-63* [23, 26, 27, 28, 29].

Os *PINs* requerem que o utilizador os copie, e introduza numa página de recuperação de credenciais, reduzindo desta forma a usabilidade deste mecanismo. Além disso, os *PINs* são compostos apenas por números, enquanto os *URL tokens* são compostos por caracteres alfanuméricos. Ou seja, um *URL Token* com o mesmo número de caracteres que um *PIN* tem mais combinações possíveis, logo é ainda mais seguro.

Os métodos *offline* requerem que o utilizador os guarde seguramente até que precise deles, o que pode implicar um baixo grau de usabilidade.

O mecanismo para recuperação de palavra-passe mais recomendado pelos investigadores na área da segurança informática é o *URL token*. Este método caracteriza-se por ser de simples e rápida implementação, por apresentar uma elevada taxa de sucesso entre os utilizadores [23, 30, 28].

[1] `https://www.nist.gov/about-nist`

Capítulo 4

Ferramentas de desenvolvimento

Para desenvolver os novos mecanismos no âmbito deste projeto foram utilizadas as linguagens de programação: *PHP*[1] e *Python*[2]. Além disso, foi necessário recorrer a *Powershell*[3], para usar módulos exclusivos, que permitem gerir serviços *Active Directory* e o *Exchange*.

Em linha com as políticas de desenvolvimento da DSI, de forma a simplificar o processo de programação de novos mecanismos, recorreu-se às seguintes *frameworks* para aplicações *web*: *Laravel*[4] (*PHP*), *Vue.js*[5], *Tailwind*[6], *InertiaJS*[7]. No entanto, em alguns casos em que foi necessário simplesmente desenvolver *APIs web* optou-se pela *framework Flask*[8] (*Python*), caracterizada por ter uma arquitetura simples e minimalista.

Por fim, ao longo do desenvolvimento do projeto, foram utilizadas outras ferramentas, cada uma com funções específicas: gestão de bases de dados com o *MySQL*[9], edição de código com o *Visual Studio Code*[10], controlo de versões com o *GitLab*[11], e gestão de containerização de aplicações com o *Docker*[12].

Neste projeto foram ainda usadas interfaces de programação de aplicações *API*. Uma *API* é a forma pela qual uma aplicação solicita um serviço de outra aplicação. Um *endpoint* da *API* é o local em que essas solicitações (conhecidas como chamadas *API*) são atendidas [31]. No âmbito do projeto, recorreu-se, por exemplo, a *APIs* de aplicações de CIÊNCIAS ULisboa como o *Fénix*[13] e o *Census*,[14] para obter os dados pessoais dos utilizadores e o vínculo que mantêm com a instituição.

[1] `https://www.php.net/`
[2] `https://www.python.org/`
[3] `https://learn.microsoft.com/en-us/powershell/`
[4] `https://laravel.com/`
[5] `https://vuejs.org/`
[6] `https://tailwindcss.com/`
[7] `https://inertiajs.com/`
[8] `https://flask.palletsprojects.com/en/3.0.x/`
[9] `https://www.mysql.com/`
[10] `https://code.visualstudio.com/`
[11] `https://about.gitlab.com/`
[12] `https://www.docker.com/`
[13] `https://fenix.ciencias.ulisboa.pt/`
[14] `https://census.ciencias.ulisboa.pt/`

Capítulo 5

Verificação Periódica de Políticas de Segurança

Durante o levantamento de requisitos para um sistema, é comum que as questões de segurança não sejam explicitamente abordadas. No entanto, espera-se que qualquer aplicação seja projetada de forma a mitigar as ameaças e vulnerabilidades que possam surgir durante a sua operação.

É essencial, contudo, dispor de uma forma de verificar se um sistema foi, de facto, concebido para lidar com essas potenciais ameaças. As duas abordagens mais comuns para essa avaliação são [32]:

Formulários Conjunto de critérios que permite avaliar a segurança informática de uma aplicação. Os formulários permitem que uma instituição converta as suas políticas de segurança num conjunto estruturado de itens, que podem ser utilizados para avaliar a segurança do sistema.

Análise de vulnerabilidades Avaliação que verifica se uma aplicação está exposta a um conjunto específico de ameaças conhecidas, considerando a origem, o motivo, as ações, o impacto e as medidas de mitigação associadas a cada ameaça.

No caso da análise de vulnerabilidades, Ciências ULisboa já dispõe de mecanismos automáticos para realizar essa tarefa. No entanto, até agora, a instituição não contava com um formulário que permitisse uma avaliação sistemática da segurança.

Por essa razão, a DSI decidiu criar um formulário específico para este propósito. Ficou estabelecido que as várias unidades de serviço da DSI deveriam preenchê-lo em conjunto, como uma forma de autoavaliação do cumprimento das políticas de segurança. Além disso, foram definidos objetivos a serem alcançados com o uso desse formulário, com o intuito de reforçar a segurança informática na instituição.

5.1 Levantamento de requisitos

As instituições públicas têm de estar em conformidade com um conjunto de recomendações e normativos legais referentes a políticas que permitam a deteção e mitigação eficaz e eficiente de ações que podem pôr em causa a segurança de toda a infraestrutura informática. Destes documentos,

					Data	**dez/23**	
					Pontos	**326/900 (36,22%)**	
Unidade	VS	Elemento	Classificação	X	Estado	Pontos	Obs
AAD	VS0	Plataformas desenvolvidas internamente validadas pelas boas práticas da OWASP.	Obrigatório	3	Maioria (2)	6	
A2S	VS1	Política que proíbe a recolha de dados pessoais em sistemas de informação acessórios.	Obrigatório	2	Nunca (0)	0	
A2S	VS2	Utilização de sessões seguras nos sistemas de informação nucleares.	Obrigatório	3	Totalidade (4)	12	
A2S	VS3	Utilização de sessões seguras nos sistemas de informação acessórios.	Obrigatório	2	Maioria (2)	4	
A2S/AAD	VS4	Utilização de TLS, na sua versão mais recente, na comunicação entre front-end <-> backend nos sistemas de informação nucleares.	Recomendado	2	Alguns (1)	2	

Figura 5.1: Excerto do formulário.

destaca-se a Resolução do Conselho de Ministros nº41/2018 [18] e a Diretriz/2023/1 da Comissão Nacional da Proteção de Dados [19].

Além disso, a Direção de Serviços Informáticos (DSI) da Faculdade de Ciências da Universidade de Lisboa necessita de avaliar sistematicamente as políticas de segurança em vigor na instituição, para efeitos de monitorização regular, controlo de qualidade e para cumprimento das obrigações legais.

5.2 Solução

Para suprir estas necessidades, foi elaborado no âmbito do trabalho desenvolvido no projeto um formulário, cujo excerto é apresentado na Fig. 5.1, com mais de 100 itens, que cobre e integra os requisitos constantes na Resolução do Conselho de Ministros n.º 41/2018 [18] e na Diretriz/2023/1 da Comissão Nacional da Proteção de Dados [19], para verificar o nível de cumprimento das políticas de segurança na DSI.

5.2.1 Itens

O formulário é composto por itens. A maioria dos itens foi adaptada dos documentos normativos citados anteriormente, no entanto, alguns deles surgiram de objetivos definidos internamente pela DSI.

Cada item está associado a uma unidade de serviço (as siglas de cada unidade de serviço estão apresentadas na Tab. 5.1), atribuindo-lhe a responsabilidade pelo cumprimento de determinado objetivo. Esta associação também facilitou a revisão e validação dos itens por parte de cada unidade de serviço, garantindo serem relevantes e aplicáveis às suas operações específicas.

Adicionalmente, cada item no formulário possui um identificador único, uma designação, uma classificação, um coeficiente multiplicativo, um estado, uma pontuação e uma observação.

Unidade de serviço	
Sigla	Designação
AAD	Área de Aplicações e Desenvolvimento
A2S	Área de Serviços e Servidores
ARC	Área de Redes e Comunicações
GSU	Gabinete de Suporte ao Utilizador
DSI	Direção de Serviços Informáticos

Tabela 5.1: Unidades de serviço.

Estado	Valor
Nunca	0
Ocasional	1
Frequente	2
Sempre	4

Tabela 5.2: Estado do formulário.

5.2.2 Pontuação

Para quantificar o nível de cumprimento das políticas de segurança, o formulário está associado a um sistema de pontuação, que é vantajoso. A projeção do nível de cumprimento num indicador numérico permite quantificar a situação em cada instante e estipular objetivos de pontuação, que irão exigir aos colaboradores maior auto-controlo, esforço e espírito de equipa.

A pontuação de cada item do formulário é o produto do coeficiente multiplicativo pelo valor associado ao estado.

Os estados, apresentados na Tab. 5.2, indicam o grau de cumprimento do item, e estão associados a um valor numérico. Os coeficientes multiplicativos, apresentados na Tab. 5.3 dependem de dois critérios, o tipo de sistema e a classificação do item.

Foram considerados dois tipos de sistema. Os sistemas nucleares são aqueles que ou contém dados pessoais, ou são centrais ao funcionamento da Faculdade. Incluem-se nesta definição: *Fénix*, *Moodle*, Portal de CIÊNCIAS ULisboa, *SAP*, *Census*, Correio eletrónico e sistema de autenticação. Os restantes são sistemas acessórios.

Foram consideradas duas classificações possíveis para os itens: recomendado ou obrigatório. A classificação dos itens adaptados da Resolução do Conselho de Ministros n.º 41/2018 [18] foi mantida conforme a atribuída nesse documento. A classificação dos itens adaptados da Diretriz/2023/1 da Comissão Nacional de Proteção de Dados [19] foi recomendatória, uma vez que este documento contém apenas recomendações. Por fim, os itens que surgiram de objetivos definidos pela própria DSI foram classificados como obrigatórios caso estivessem associados a sistemas nucleares; caso contrário, foram classificados como recomendados.

Pontuação		
Sistema	Classificação	Coeficiente multiplicativo
Sistema de informação nuclear	Obrigatório	3
	Recomendado	2
Sistema de informação acessório	Obrigatório	2
	Recomendado	1

Tabela 5.3: Coeficiente multiplicativo do formulário.

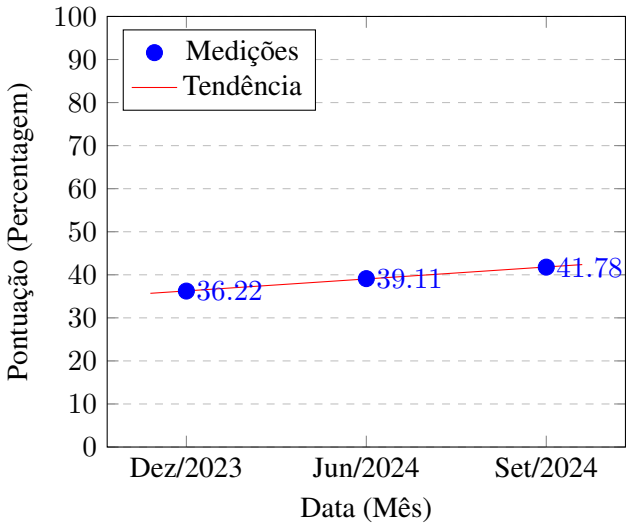


Figura 5.2: Evolução da pontuação obtida no formulário.

5.3 Avaliação

A DSI estabeleceu como objetivo preencher coletivamente o formulário, a cada quadrimestre, aumentando em 1% a sua classificação relativamente à anterior, sendo que a classificação inicial não poderia ser inferior a 30%.

Na Fig. 5.2 está apresentada a evolução da pontuação obtida no formulário. A DSI começou com uma pontuação inicial de 36,22% em dezembro de 2024, alcançou uma pontuação de 39,11% no mês de junho seguinte, e alcançou uma pontuação de 41.78% em setembro de 2024. Esta evolução, embora ligeira, é positiva e notória, e cumpre o objetivo estabelecido pela DSI.

Desta forma, o formulário teve um impacto positivo na segurança informática de CIÊNCIAS ULisboa. Através da mudança de estado dos itens VS16, VS39, VS40 VS54 e VS71 alcançaram-se várias melhorias na segurança informática da instituição. As palavras-passe de todos os utilizadores cumprem agora a nova Política de Palavras-passe (mais restrita) nos sistemas de informação nucleares. Adicionalmente, foi feito um levantamento de todos os ativos críticos, que contêm dados pessoais. Além disso, foi elaborado um documento interno na DSI para cobrir as medidas de segurança, técnicas e organizativas aplicáveis aos tratamentos de dados pessoais, internas da DSI. Em relação à deteção de ameaças na defesa perimétrica da infraestrutura da instituição, foi

implementada uma instância do *SIEM Wazuh*.

5.4 Trabalho Futuro

Conforme forem surgindo novos documentos normativos ou novas políticas internas, o formulário necessitará de ser revisto. Desta forma, o formulário estará sempre em atualização por forma a responder a alterações ou melhorias às políticas de segurança.

O objetivo interno da DSI de aumentar, a cada quadrimestre, 1% a sua classificação relativamente à anterior deverá continuar a ser cumprido.

Capítulo 6

Gestão de Contas de Utilizadores

A gestão eficiente de contas de utilizadores é crucial para garantir a segurança, a privacidade e o acesso adequado aos recursos da instituição.

No decorrer do projeto foram revistos vários processos, que tinham pontos a melhorar, associados à gestão de contas. Nomeadamente a criação, recuperação, correção e o encerramento de contas de utilizador. Estes processos foram reestruturados para incorporar práticas recomendadas de segurança informática, automação de tarefas repetitivas e melhorias na interface com o utilizador. Neste capítulo serão apresentados em detalhe as alterações a estes processos.

6.1 Recuperação de Credenciais

Os mecanismos *online* de recuperação de credenciais simplificam consideravelmente o problema da escala, que no caso de CIÊNCIAS ULisboa é não negligenciável devido aos mais de 6.000 utilizadores ativos. Até ao ano letivo de 2022/2023 o sistema que estava em vigor solicitava o endereço de correio eletrónico e o número de identificação civil do utilizador, e permitia a recuperação de palavra-passe por meio de perguntas de segurança e *pins*. As perguntas e os *pins* revelavam-se pouco eficazes, uma vez que poucos eram os utilizadores que os definiam. Para além deste problema de usabilidade, este sistema apresentava uma vulnerabilidade conhecida internamente pela Direção de Serviços Informáticos.

No ano letivo de 2022/2023, os pedidos de recuperação de palavra-passe passaram, por razões técnicas, a ter de ser acompanhados e processados manualmente pela equipa de suporte da DSI. Para além do aumento do consumo de recursos humanos, a indisponibilidade da mudança de palavra-passe *online* resultou na insatisfação dos utilizadores.

Conjugado com a decisão de CIÊNCIAS ULisboa de remover os serviços do Portal CIÊNCIAS ULisboa, a DSI decidiu então renovar o sistema de recuperação de credenciais, em vez de reestabelecer o funcionamento do anterior.

6.1.1 Levantamento de requisitos

O novo mecanismo de recuperação de credenciais teria de cumprir vários requisitos. Primeiramente, era necessário que este fosse mais seguro, o que implicaria, por exemplo, a mitigação da

vulnerabilidade existente. Adicionalmente, era desejável a substituição do fator de autenticação baseado em perguntas de segurança e *pins*, que como discutido na Sec. 3.2.3, apresentava uma baixa confidencialidade e usabilidade. Além disso, era necessário, que os utilizadores recuperassem as suas credenciais mesmo que desconhecessem o seu *login*. Por fim, outro dos requisitos era que o sistema obrigasse as novas palavras-passe a respeitarem a política de segurança da instituição.

6.1.2 Decisões

Para o mecanismo estar conforme os requisitos levantados e considerando a discussão apresentada na Sec. 3.1, escolheu-se adotar um fator de autenticação baseado em *URL tokens*, em detrimento das perguntas e *PINs* utilizados anteriormente.

Adicionalmente, decidiu-se permitir que o utilizador recuperasse as suas credenciais fornecendo apenas o seu número de identificação civil. Desta forma os utilizadores que se esquecessem tanto do *login* quanto da palavra-passe conseguiriam recuperar as suas credenciais. Além disso, esta abordagem possibilitaria que utilizadores com múltiplas contas de utilizador recuperassem todas as suas credenciais de uma só vez.

Por fim, este serviço foi adicionado ao BalcaoC[1] para que mais utilizadores o possam encontrar e obter informações a seu respeito.

6.1.3 Processo

O processo de recuperação de credenciais foi dividido em duas etapas.

Submissão do pedido

A primeira etapa consiste no preenchimento, pelo utilizador, do formulário inicial,[2] apresentado na Fig. 6.1. Neste formulário o utilizador insere o seu número de identificação civil e escolhe o meio de contacto (correio eletrónico ou *SMS*) para receber o *URL token* que lhe permitirá recuperar as suas credenciais.

A arquitetura desta etapa é ilustrada na Fig. 6.2. Primeiramente, os valores submetidos no formulário são higienizados. Em seguida, verifica-se na base de dados local se há pedidos recentes pendentes associados ao número de identificação civil fornecido. Como discutido mais à frente esta verificação tem por objetivo impedir que sejam realizados pedidos sucessivos. Depois, obtêm-se os contactos pessoais do utilizador a partir do *Fénix*, *Census* ou *Active Directory*. Posteriormente, identificam-se as contas existentes no *Active Directory* associadas ao número de identificação civil fornecido. Por fim, cria-se o pedido na base de dados local e envia-se uma notificação ao utilizador, utilizando o meio de contacto que ele selecionou, contendo o seu *login* (endereço de correio eletrónico institucional), o *URL token* que permitirá a recuperação das credenciais e um alerta relativamente à importância de completar este processo rapidamente [33]. A decisão de incluir este alerta na notificação deve-se a, em estudos anteriores, se ter verificado que muitos utilizadores

[1] Acessível em `https://balcaoc.ciencias.ulisboa.pt/servico/mudar-password`
[2] Acessível em `https://passwd.ciencias.ulisboa.pt/`

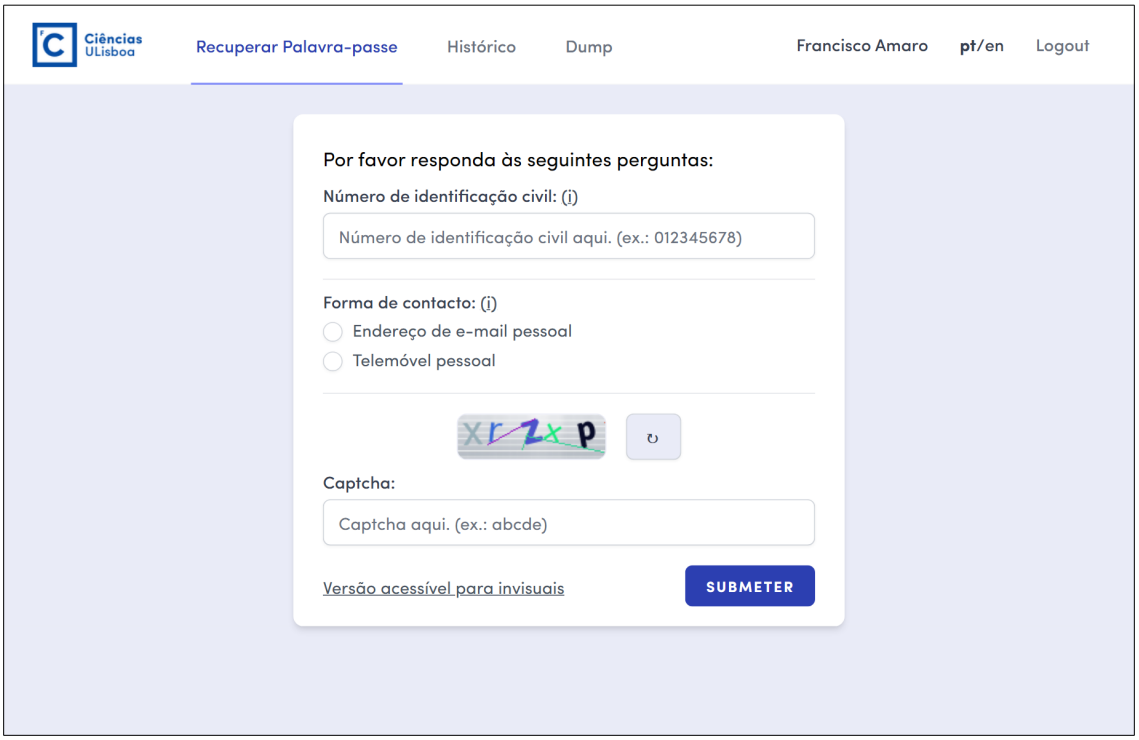


Figura 6.1: Formulário inicial do pedido de recuperação de credenciais.

demoravam vários dias para concluir o processo de recuperação de credenciais [33]. Esta demora estava associada a vários fatores: os utilizadores estarem ocupados, não utilizarem frequentemente a plataforma e não estarem preocupados ou não compreenderem os riscos a que estavam sujeitos [33]. Esta negligência agrava os riscos de segurança, dado que os pedidos permanecem ativos.

Definição de credenciais

A segunda etapa consiste no preenchimento pelo utilizador do formulário final, apresentado na Fig. 6.3, quando segue o *URL* que lhe foi entregue. Neste formulário, o utilizador, insere a sua nova palavra-passe duas vezes, para evitar erros de digitação.

A arquitetura desta etapa é ilustrada na Fig. 6.4. Primeiramente, os valores submetidos neste formulário são higienizados. Em seguida, verifica-se na base de dados local se há algum pedido associado ao *URL token* fornecido. Depois, é verificado se o *URL token* continua válido e nunca foi usado. Posteriormente, identificam-se as contas existentes no *Active Directory* associadas ao número de identificação civil fornecido. Após isto, desbloqueiam-se essas contas de utilizador, que podem estar bloqueadas devido a vários processos de autenticação falhados, e alteram-se as suas credenciais. Por fim, atualiza-se o pedido na base de dados local e envia-se uma notificação ao utilizador, através do mesmo meio utilizado na 1.ª etapa, alertando-o de que o processo de recuperação de credenciais está concluído.

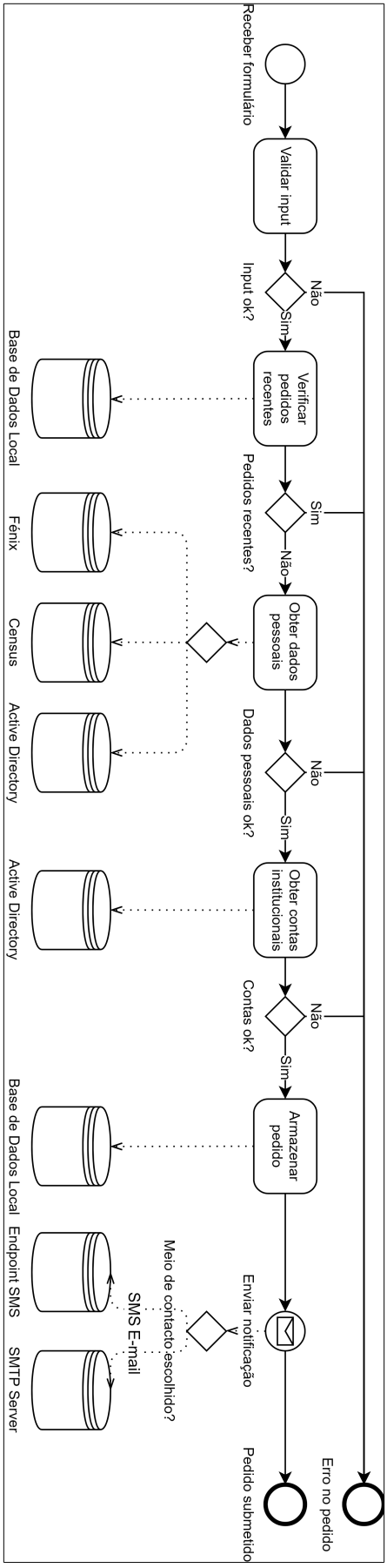


Figura 6.2: Fase inicial do pedido de recuperação de credenciais.

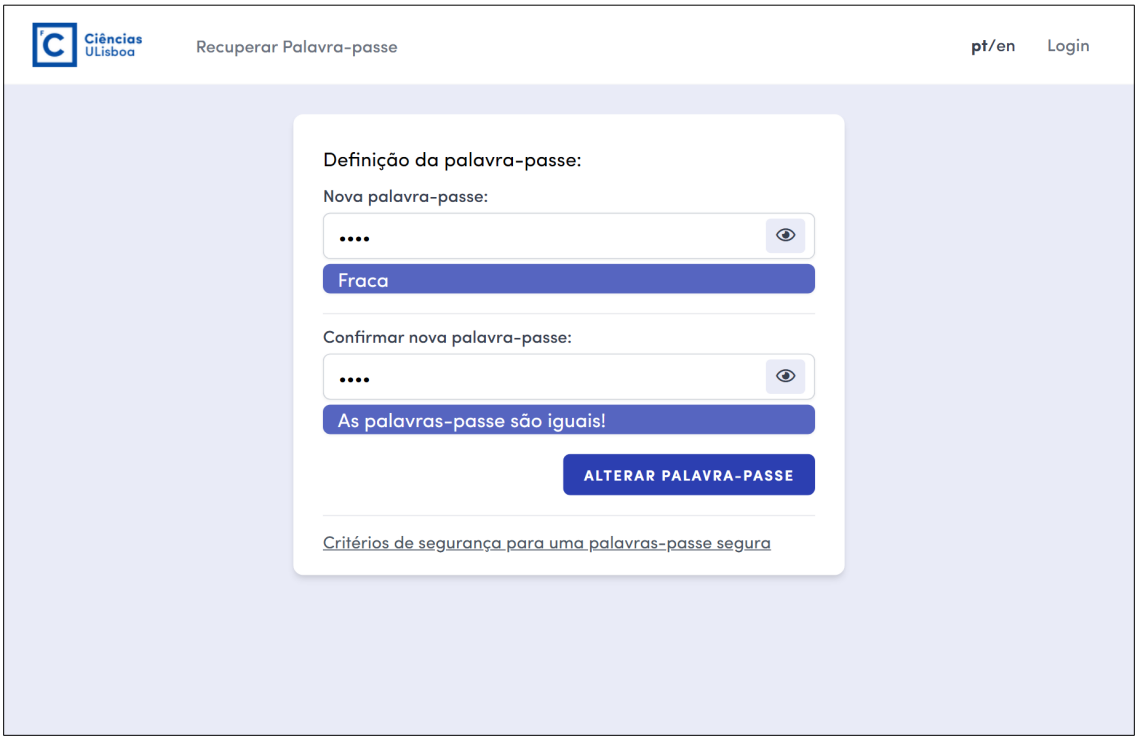


Figura 6.3: Fase final de recuperação de credenciais.

6.1.4 Implementação

Em linha com as políticas de desenvolvimento da DSI, o servidor foi desenvolvido utilizando a *framework Laravel Inertia*[3] e integrado num *container Docker*, juntamente com um servidor de base de dados *MySQL*. Atualmente, existem duas instâncias do sistema: uma em ambiente de qualidade e outra em ambiente de produção. Ambas as instâncias são instaladas automaticamente através de *pipelines* integradas com o *GitLab* da DSI.

Ao implementar este sistema foi necessário prevenir o acesso ilegítimo a dados e informações pessoais dos utilizadores. Como tal, o sistema, independentemente da validade dos dados inseridos, devolve sempre uma resposta genérica, que não revela nenhuma informação acerca do estado do pedido. As informações relativas ao pedido são sempre enviadas por um canal alternativo apenas ao dono da conta, caso esta exista. Evita-se assim que terceiros tomem conhecimento sobre a existência de uma relação com CIÊNCIAS ULisboa de alguém que conheçam o número de identificação civil.

Para a alteração de credenciais, o sistema utiliza as funções do *Lightweight Directory Access Protocol* (*LDAP*) disponibilizadas pelo *PHP*, e uma conta de utilizador com privilégios especiais, para comunicar com o serviço de diretório *Active Directory*. Esta comunicação inclui a definição e a verificação das credenciais, assegurando a conformidade com a política interna.

No código, as variáveis sensíveis, como as credenciais de acesso a *APIs*, foram armazenadas num ficheiro de configuração.

De forma a garantir que a nova palavra-passe cumpre os requisitos da política interna, o

[3] `https://laravel.com/`

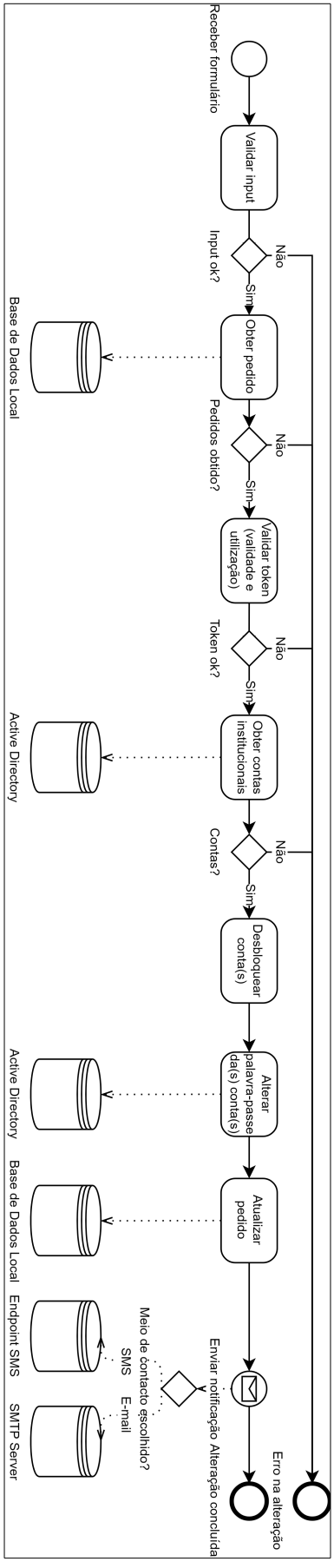


Figura 6.4: Formulário de recuperação de credenciais (Arquitetura).

sistema utiliza, numa primeira fase, uma conta com privilégios especiais para atribuir uma palavra-passe temporária ao utilizador. De seguida, o sistema autentica-se como o utilizador com essa palavra-passe temporária e, por fim, tenta definir a palavra-passe escolhida pelo utilizador. Desta forma, cabe ao serviço *Active Directory* validar a conformidade da palavra-passe com as políticas estabelecidas. Contudo, esta abordagem apresenta algumas limitações: se o utilizador estiver apenas a alterar as credenciais e continuar a definir palavras-passe fracas, poderá perder o acesso à sua conta, já que será atribuída uma palavra-passe temporária, desconhecida para o utilizador. Além disso, o *Active Directory* regista o histórico das credenciais mais recentes para impedir a reutilização de palavras-passe. No entanto, se o utilizador repetir o processo várias vezes, poderá eventualmente conseguir reutilizar uma palavra-passe anterior.

Adicionalmente, para comunicar com os serviços de CIÊNCIAS ULisboa, nomeadamente o *Fénix* e *Census*, o sistema recorre a *APIs* disponibilizadas pelos mesmos.

Estados

Os estados do Pedido de Recuperação de credenciais, também ilustrados no diagrama de transição de estados da Fig. 6.5, são:

Pedido efetuado: O utilizador submete corretamente um pedido de recuperação de credenciais;

Pedido verificado: O utilizador acede ao *URL token*, que ainda está válido e não utilizado, e interage com a página, comprovando desta forma a sua autenticidade;

Pedido concluído: O utilizador altera as suas credenciais, concluindo desta forma, o processo de recuperação de credenciais;

Pedido Não Verificado Expirado: O *URL token* excede o prazo de validade e nunca foi acedido;

Pedido Verificado Expirado: O *URL token* excede o prazo de validade, tendo sido acedido pelo menos uma vez.

Para além destes estados, foram definidos os estados de erro que não estão ilustrados na figura. Todos os estados de erro assinalam o encerramento do processo. Diferem por registarem a razão pela qual o processo terminou com erro e desta forma ajudarem a diagnosticar anomalias.

Base de dados

Para a manutenção do estado entre os 2 passos de um pedido foi utilizada uma base de dados relacional *MySQL*. Os campos da base de dados estão apresentados na Tab. 6.1.

6.1.5 Auditoria

Os registos de atividades (*logs*) são guardados na base de dados, durante um ano. A remoção destes registos é implementada através de uma chamada à base de dados, sempre que a página é carregada.

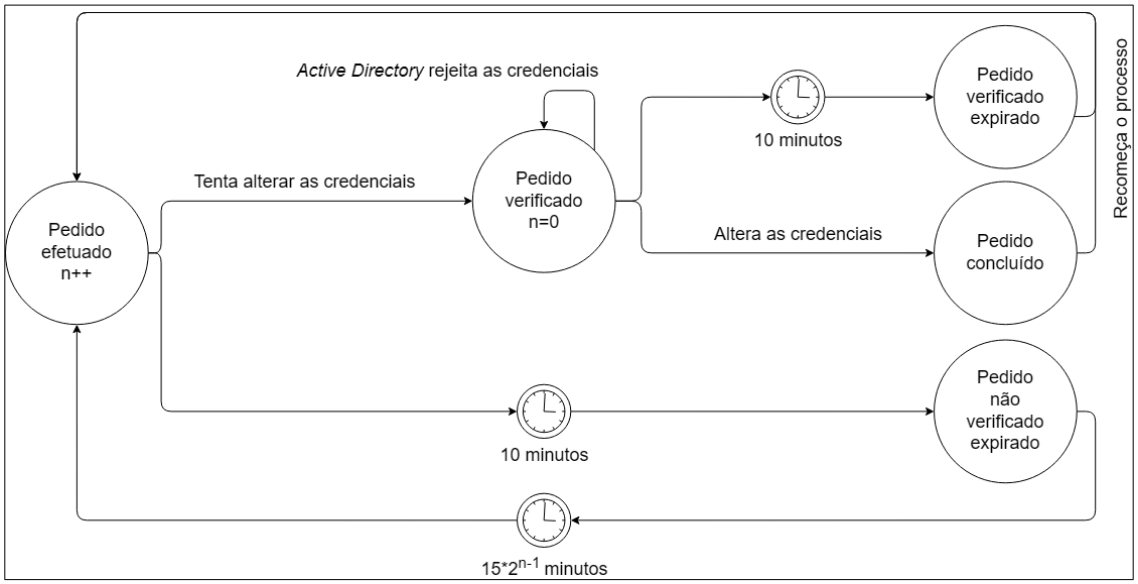


Figura 6.5: Estados de um pedido de recuperação de credenciais.

Descrição	Campo	Tipo de Dados
Identificador do pedido	*ID*	Inteiro
Número do documento de identificação	Documento de identificação	*String*
Nome do utilizador	Nome	*String*
Meio de contacto que o utilizador escolheu	Meio de contacto	Enumerado
Contacto do utilizador	Contacto	*String*
E-mail institucional do utilizador	*E-mail* institucional	*String*
Token do pedido cifrado	*Token*	*String*
Data de criação do pedido	Criado em	*Timestamp*
IP com que o utilizador criou o pedido	Criado por	*String*
Data de conclusão do pedido	Concluído em	*Timestamp*
IP com que o utilizador concluiu o pedido	Concluído por	*String*
Estado do pedido	Estado	Enumerado
Informação adicional do pedido	Informação adicional	*String*

Tabela 6.1: Campos da base de dados do mecanismo de recuperação de credenciais.

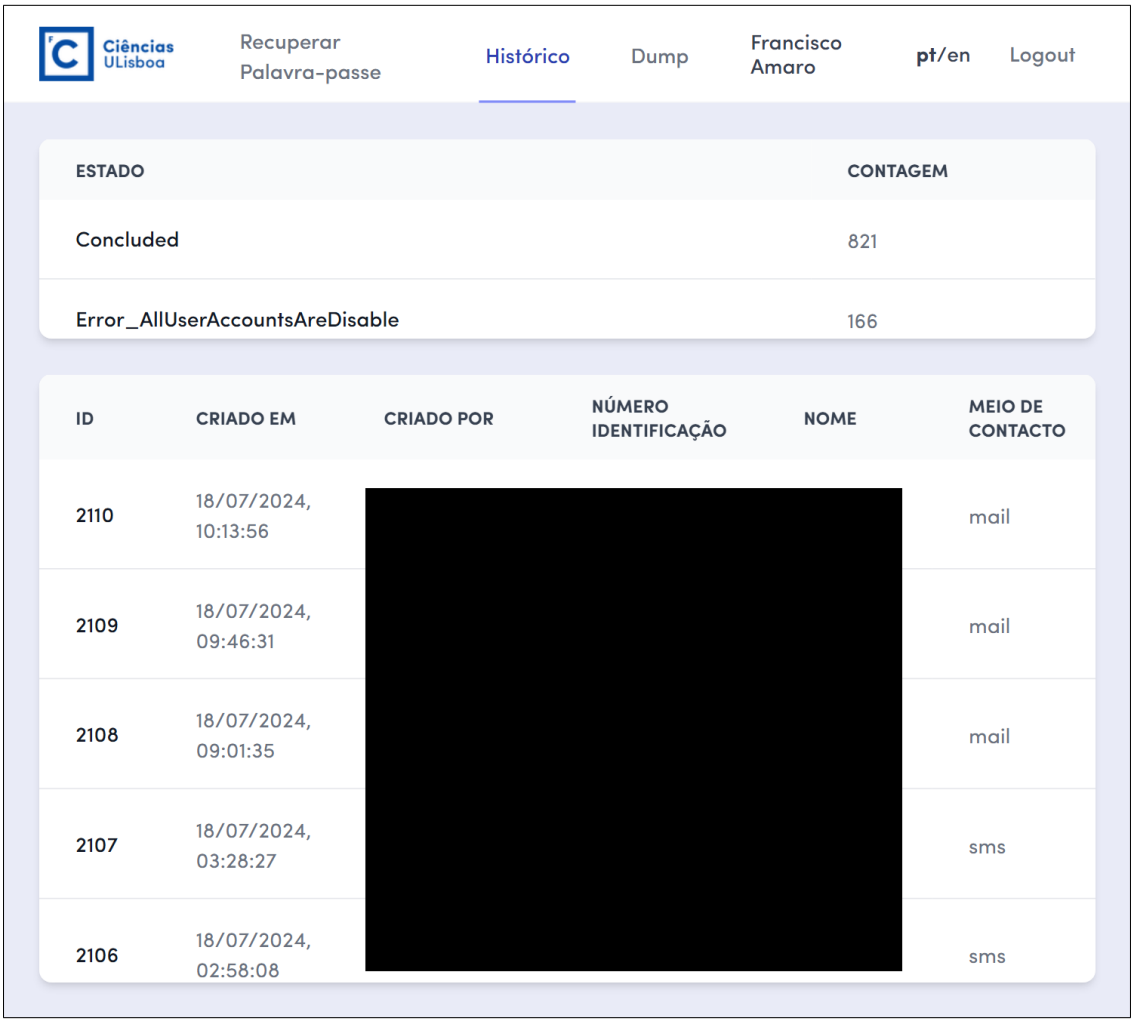


Figura 6.6: *Logs* do sistema de recuperação de credenciais (com alguns dados omitidos).

Além disso, para possibilitar a monitorização da aplicação e o acompanhamento dos *tickets* relacionados com pedidos de recuperação de *credenciais* pela equipa de suporte, foram criadas duas páginas de apoio, com acesso restrito aos colaboradores da DSI. Uma, ilustrada na Fig. 6.6, apresenta uma tabela que exibe parte do conteúdo da base de dados, permitindo visualizar o estado de cada pedido. A outra, ilustrada na Fig. 6.7 apresenta os ficheiros de *logs*.

6.1.6 Segurança

Sendo este um sistema crítico para a instituição, é especialmente importante garantir que a recuperação de credenciais é segura, uma vez que um ataque informático bem-sucedido pode comprometer as contas dos utilizadores de CIÊNCIAS ULisboa.

Para monitorizar e proteger a máquina em ambiente de produção e os respetivos *containers*, instalou-se um agente *Wazuh*, que comunica com o servidor *Wazuh* (*SIEM*, apresentado na Sec.2.3.6), na máquina. Este agente é usado para recolher *logs* e responder a alguns tipos de ameaças, por exemplo, injeção de código *SQL* [34].

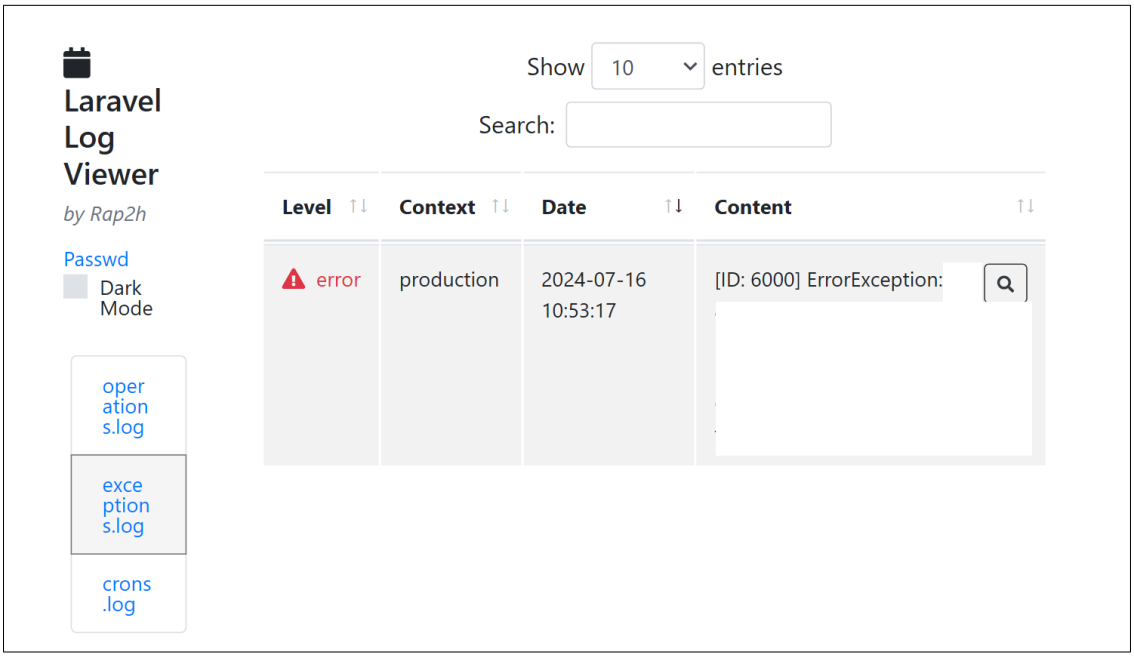


Figura 6.7: *Logs* do sistema de recuperação de credenciais (com alguns dados omitidos).

Cenários de Ataque

No desenho e implementação da aplicação foram consideradas respostas aos seguintes cenários de ataque:

Ataque de força bruta para criar pedidos Caso um atacante realize um ataque de força bruta para submeter pedidos, será bloqueado. Este bloqueio pode ocorrer por meio de um *captcha* que protege o formulário inicial. Adicionalmente, a submissão de pedidos para o mesmo utilizador é bloqueada por um tempo de espera de $15 * 2^n$ minutos, onde n é o número de pedidos realizados pelo mesmo utilizador nas últimas 24 horas.

Além desses controlos, o atacante terá mais dificuldade em saber se iniciou ou não um pedido com sucesso, dado que a resposta à criação de um pedido de recuperação de credenciais é sempre a mesma, independentemente de o número de identificação civil fornecido existir ou não no sistema.

Ataque de força bruta para explorar *URL Tokens* gerados A segurança deste sistema depende das características dos *URL tokens* usados. Optou-se por *URL tokens* compostos por 15 caracteres alfanuméricos e com uma validade de 10 minutos.

Cada carácter de um *URL token* pode ser formado por 62 caracteres diferentes (alfanuméricos maiúsculos e minúsculos e algarismos), o que implica que um *URL token* é um de 62^{15} combinações possíveis.

Posto isto, caso o atacante realize um ataque de força bruta para explorar *URL tokens* gerados, terá de explorar um que ainda não tenha expirado e que não tenha sido usado. Dadas as características dos *URL Tokens* enunciadas acima, este torna-se um processo mais complexo.

Além disso, o atacante nunca saberá se alterou uma palavra-passe com sucesso, dado que a resposta a uma conclusão de um pedido de recuperação de credenciais é sempre a mesma, independentemente do *URL token* fornecido existir ou não no sistema.

SQL Injection Ataques de *SQL Injection*, que ocorrem quando utilizadores fornecem *inputs* maliciosos, são prevenidos através da higienização desses *inputs*, da utilização de *prepared statements* nas comunicações com a base de dados e da cifra dos *URL tokens* na base de dados.

LDAP Injection Ataques de *LDAP Injection*, que ocorrem quando utilizadores fornecem *inputs* maliciosos, são prevenidos através da higienização desses *inputs*.

Desrespeito pelas políticas de palavras-passe Se um utilizador introduzir uma palavra-passe que não cumpre as políticas estabelecidas, o serviço de diretório *Active Directory* rejeitará a alteração das credenciais até que a palavra-passe cumpra os requisitos de segurança.

6.1.7 Avaliação

Este sistema está em produção desde Abril de 2024. Ao colocá-lo em produção surgiram alguns problemas que tiveram de ser corrigidos. Alguns desses problemas foram:

Funcionários não docentes e não investigadores Havia utilizadores que, ao tentar recuperar as suas credenciais, não conseguiam, pois não possuíam perfil no *Fénix*, impedindo o sistema de obter os seus contactos pessoais. Para corrigir este problema, o sistema passou a recolher também contactos pessoais do *Census* e da *Active Directory*.

Contas de utilizador inativas Havia utilizadores que tentavam recuperar as credenciais de contas inativas. Para corrigir este problema, passou a ser enviada uma notificação informando-o de que todas as suas contas estavam inativas e que, por esse motivo, não se poderia dar continuidade ao processo.

Contas de utilizador bloqueadas Havia utilizadores que tentavam recuperar as suas credenciais de contas bloqueadas. As contas de utilizador ficam bloqueadas quando um utilizador erra a sua palavra-passe várias vezes consecutivas. Para corrigir este problema, o mecanismo passou a desbloquear as contas de utilizador no momento em que é definida a nova palavra-passe. Este desbloqueio não subverte o propósito do bloqueio inicial porque o algoritmo de alteração de palavra-passe confirma a identidade do utilizador.

Contas de utilizador em *OUs* sem permissão Em CIÊNCIAS ULisboa os utilizadores estão organizados por *Organizational Units* (*OUS*).

Alguns dos utilizadores que tentavam recuperar as suas credenciais pertenciam a determinadas *OUs*, para as quais o utilizador com que a plataforma acedia à *Active Directory* não tinha permissão para recuperar credenciais. Para corrigir este problema, foram adicionadas mais permissões à conta de *Active Directory* utilizada pelo sistema.

Utilizadores *Fénix* Havia vários utilizadores que apenas tinham contas no *Fénix*, ou seja, eram candidatos a ciclos de estudos em CIÊNCIAS ULisboa sem conta no serviço *Active Directory*, mas ainda assim tentavam usar este sistema de recuperação de credenciais. Para corrigir este problema, foi adicionada uma nota no serviço do BalcãoC para redirecionar esses utilizadores para o serviço correto, conforme apresentado na Fig. 6.8.

Notificações ilimitadas Havia utilizadores que tentavam recuperar as suas credenciais, selecionando como método de contacto o dispositivo móvel. Em alguns casos, estes utilizadores conseguiam submeter pedidos imediatamente após o anterior expirar, sem ter de aguardar o *timeout* esperado. Isto ocorria porque, ao enviar notificações via *SMS* para dispositivos *Android*, estes mostravam automaticamente uma pré-visualização do *website* no *SMS*, fazendo com que os pedidos atualizassem o seu estado para verificados. Para corrigir este problema, os pedidos passaram apenas a atualizar o seu estado para verificados caso o utilizador aceda ao *URL token* e interaja com a página. A interação é registada quando o utilizador tenta submeter o formulário.

Envio de notificações Havia casos em que o servidor *SMTP* estava indisponível, e o envio da notificação via correio eletrónico ao utilizador falhava. Quando o utilizador tentava repetir o pedido, era bloqueado pelo *timeout* acionado para evitar pedidos em massa. Para resolver este problema, caso tenha havido uma exceção no envio da notificação via correio eletrónico no pedido anterior, o utilizador não terá de aguardar para repetir o pedido.

Tempo insuficiente Inicialmente, os utilizadores dispunham de um período de 5 minutos para submeter um pedido e concluí-lo. No entanto, este período revelou-se insuficiente, uma vez que começaram a surgir muitos pedidos expirados seguidos de pedidos concluídos pelo mesmo utilizador. Para resolver este problema, o tempo foi aumentado para 10 minutos.

A Tab. 6.2 apresenta algumas estatísticas recolhidas entre abril e agosto de 2024. Estes resultados incluem já a definição da 1.ª palavra-passe pelos novos alunos inscritos em CIÊNCIAS ULisboa por via do Concurso Nacional de Acesso no ano letivo de 2024/2025.

A Tab. 6.2 mostra que apenas 50% dos pedidos foram concluídos com sucesso. As 3 principais razões de insucesso totalizam quase 40% dos restantes pedidos e explicam-se por diversos motivos.

Os pedidos verificados expirados devem-se, em grande parte, à introdução de palavras-passe consideradas fracas, sendo consequentemente rejeitadas pelo serviço de diretório *Active Directory*, ou a utilizadores pertencentes a (*OUs*) especiais, para as quais a conta utilizada pelo mecanismo de alteração de credenciais não dispõe das permissões necessárias para modificar.

Adicionalmente, o número de *timeouts* está relacionado com utilizadores que submetem múltiplos pedidos consecutivos, na expectativa de uma notificação imediata. Por fim, o número de pedidos inválidos, que resulta da ausência de contactos associados às contas de utilizador, deve-se ao fato de os utilizadores não saberem o número do documento de identificação com o qual estão registados nos sistemas de informação de CIÊNCIAS ULisboa, acabando por inserir um número que não está associado a nenhuma conta.

Figura 6.8: Serviço do BalcaoC que dá acesso ao sistema de recuperação de credenciais.

Estatísticas			
Estado		Contagem	Percentagem
Concluídos		2974	50,51%
Expirado	Verificado	171	2,90%
	Não verificado	600	10,19%
Erro	Contas de utilizador desativadas	232	3,94%
	Enviar notificação	6	0,10%
	Timeout	616	10,47%
	Conta de utilizador não existe no *Active Directory*	250	4,25%
	Inexistência de contactos associados à conta de utilizador	1039	17,64%
Total		5888	100,00%

Tabela 6.2: Estatísticas do sistema de recuperação de credenciais.

6.2 Identificação de contas de utilizador anómalas

O processo de criação de contas de utilizador em CIÊNCIAS ULisboa sofreu várias alterações ao longo do tempo. Anteriormente, as contas de aluno eram atribuídas apenas aos estudantes inscritos em ciclos de estudos. Para as restantes contas, o candidato a utilizador tinha de submeter um pedido. Esse pedido era validado por um membro da comunidade, indicado pelo candidato, e posteriormente pela equipa de suporte da DSI. Após a validação, a conta era criada sem que o processo verificasse automaticamente a correção da informação constante de todos os campos do pedido.

Para as contas já existentes, não existiam verificações automáticas para confirmar se o utilizador mantinha algum tipo de vínculo com a instituição. Ou seja, após o término do vínculo dos utilizadores com a instituição não havia um processo automático que encerrasse as contas de utilizador.

Como resultado, surgiram situações anómalas nas contas de utilizador da instituição. Havia ex-alunos e ex-funcionários, por exemplo, aposentados, que continuavam com contas de utilizador ativas. Adicionalmente, havia funcionários que não estavam registados na plataforma *Census*, ou que não tinham o perfil do *Census* atualizado com todos os vínculos com a instituição, o que levantava questões sobre a necessidade de manter essas contas ativas. Por fim, ocorreram também casos em que um funcionário tinha mais do que uma conta de utilizador, uma vez que o processo de criação de contas não impedia a criação de múltiplas contas de utilizador associadas à mesma pessoa.

Um dos objetivos deste trabalho era definir os mecanismos que permitem garantir que todos os utilizadores com contas ativas na instituição mantivessem um vínculo válido com a mesma e que os dados nas várias plataformas de CIÊNCIAS ULisboa onde estivessem registados fossem corretos e coerentes entre si. No limite, a solução irá consistir em corrigir, sempre que possível automaticamente, as situações irregulares e, em último caso, desativar as contas de utilizadores que já não mantiverem vínculo com a instituição. A implementação desta solução contribuirá para aumentar a segurança informática, uma vez que ao garantir que apenas as contas necessárias permanecem ativas, reduz a superfície de ataque. Adicionalmente, a desativação de contas não utilizadas liberta espaço de armazenamento, contribuindo para uma gestão eficiente de recursos.

6.2.1 Levantamento de requisitos

Ao redefinir as políticas relacionadas com a gestão do ciclo de vida dos utilizadores, que implicam uma revisão dos direitos de acesso de utilizadores em intervalos regulares, a DSI (Direção de Serviços Informáticos) estabeleceu como meta realizar um levantamento abrangente das contas de utilizador existentes em CIÊNCIAS ULisboa.

Este levantamento seria efetuado através de vários serviços de diretório. Isto inclui o diretório *fc.ul.pt*, que contém todas as contas de utilizador com o domínio *@fc.ul.pt* e que devem estar associadas a um perfil no *Census*. Seria também consultado o diretório *alunos.fc.ul.pt*, que abrange contas com o domínio *@alunos.fc.ul.pt* e que devem estar associadas a um perfil no *Fénix*.

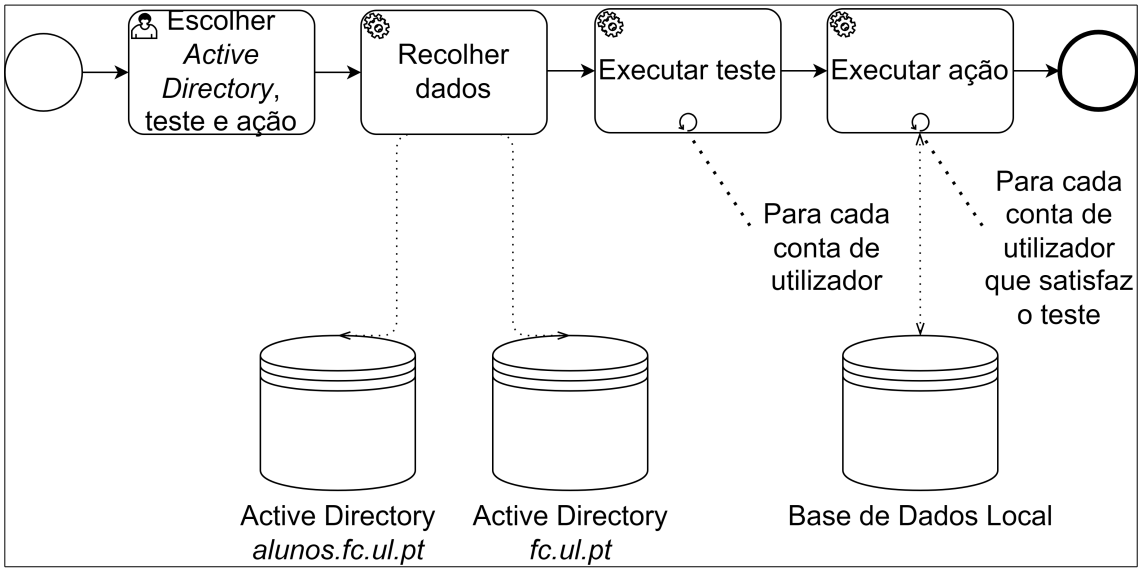


Figura 6.9: Arquitetura do sistema de identificação de contas de utilizador anómalas na instituição.

Após este levantamento, seriam verificadas quais dessas contas deveriam continuar ativas, quais deveriam ser corrigidas, e quais deveriam ser encerradas. Por fim, esperava-se que este processo fosse invocado de forma automática diariamente, para contribuir para um ambiente informático seguro na instituição.

6.2.2 Processo

Para satisfazer os requisitos definidos foi desenvolvido um protótipo de aplicação que inclui um conjunto de testes e ações automatizadas. Este protótipo serve como proposta para resolver as irregularidades relacionadas com as contas de utilizador na instituição.

A arquitetura da aplicação está presente na Fig. 6.9. No primeiro passo, o utilizador escolhe, através de um *URI*, apresentado na Fig. 6.10, o serviço de diretório *Active Directory* onde deseja fazer o levantamento de utilizadores, o teste que deseja realizar e a ação que deseja tomar através dos seus respetivos identificadores numéricos. A sintaxe da invocação é `https://servidor/api/endpoint/task/activedirectory/<codigoAD>/test/<codigoTeste>/action/<codigoAcao>`, onde <*codigoAD*> corresponde ao identificador numérico do serviço de diretório *Active Directory* desejado, <*codigoTeste*> refere-se ao identificador numérico do teste pretendido, e <*codigoAcao*> é o identificador numérico da ação a executar.

Em seguida, a aplicação recolhe os dados do serviço de diretório escolhido e realiza o teste e a ação indicada pelo utilizador.

Testes

O sistema disponibiliza uma série de testes para assegurar a validade e a coerência dos dados:

Identificação unívoca dos utilizadores Garantir que todas as contas tenham um documento de identificação associado, uma vez que várias aplicações em CIÊNCIAS ULisboa utilizam esse

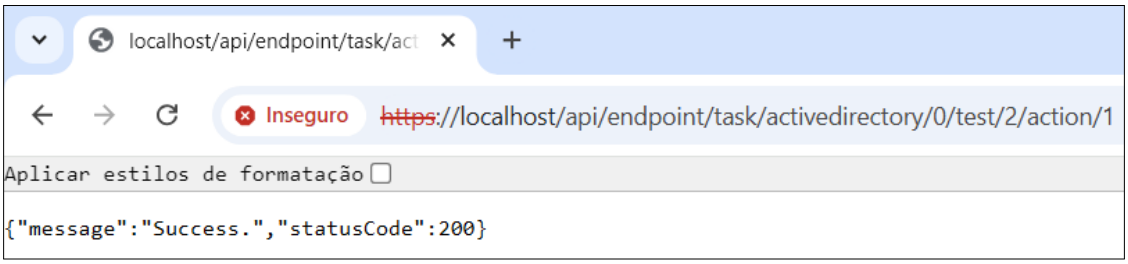


Figura 6.10: *URI* do verificador automático de coerência da informação.

dado para identificar os utilizadores.

Ausência de atividade recente Identificar contas ativas que não apresentam atividade recente.

Múltiplas contas de utilizador A existência de indivíduos com várias contas de utilizador no mesmo serviço de diretório.

Ausência de vínculo válido com a instituição Todas as contas devem ter um vínculo válido com a instituição. Para os alunos, isso implica a necessidade de uma matrícula ativa no *Fénix*. Para as restantes contas, é necessário que o vínculo seja válido no *Census*.

As contas que deveriam possuir um vínculo válido no *Census* podem manifestar essa irregularidade de diversas formas. Primeiramente, podem existir contas que não estão associadas a nenhum perfil no *Census*. Além disso, algumas contas podem estar associadas a um perfil no *Census*, mas não terem nenhum vínculo ativo com a instituição. Também pode haver contas com vínculos ativos no *Census* que deveriam estar inativos, como funcionários aposentados cujo perfil não foi atualizado. Por fim, podem surgir contas com dados incoerentes, associadas, por exemplo, a um perfil no *Census* com um documento de identificação inexistente, formado por caracteres inválidos ou diferente daquele utilizado em outras aplicações de CIÊNCIAS ULisboa.

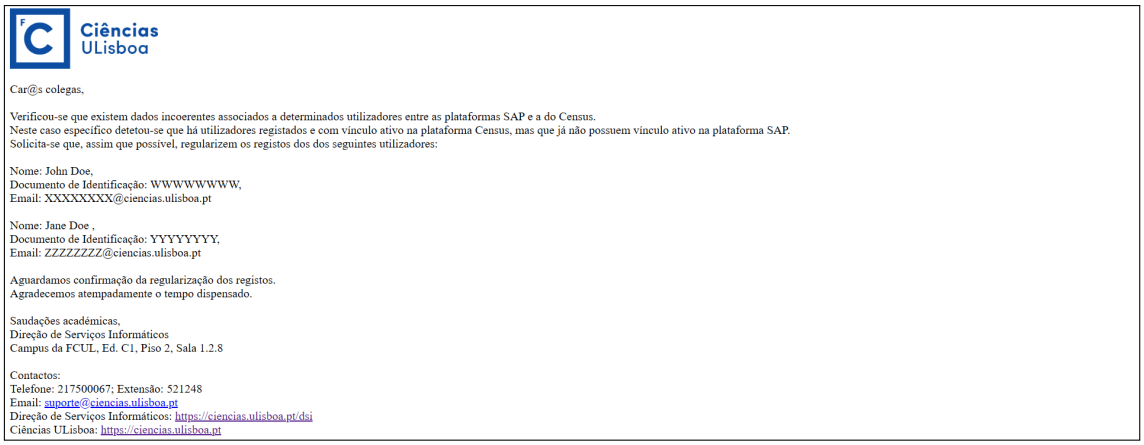
Ações

Em sequência dos testes, existem ações cujo objetivo é corrigir e, em último caso, encerrar as contas que se encontram em situação anómala. Em alguns casos, poderá ser preferível guardar o resultado de um teste num ficheiro.

A outra ação disponível notifica o utilizador e/ou entidade responsável e, se necessário, encerra a conta irregular. Inicialmente, notifica-se o utilizador e/ou a entidade responsável pela conta para resolver a irregularidade num determinado período. Se a irregularidade persistir numa próxima invocação da ação, o próximo passo será desativar a conta do utilizador.

Para os utilizadores com dados incoerentes entre o *Census* e o *SAP*, a entidade responsável será notificada, como mostrado na Fig. 6.11a. Se a irregularidade não for resolvida num determinado período, a conta do utilizador será encerrada.

Se um utilizador não tiver perfil no *Census*, será notificado diretamente, como ilustrado na



Ciências ULisboa

Car@s colegas,

Verificou-se que existem dados incoerentes associados a determinados utilizadores entre as plataformas SAP e a do Census.
Neste caso específico detetou-se que há utilizadores registados e com vínculo ativo na plataforma Census, mas que já não possuem vínculo ativo na plataforma SAP.
Solicita-se que, assim que possível, regularizem os registos dos dos seguintes utilizadores:

Nome: John Doe,
Documento de Identificação: WWWWWWWW,
Email: XXXXXXXX@ciencias.ulisboa.pt

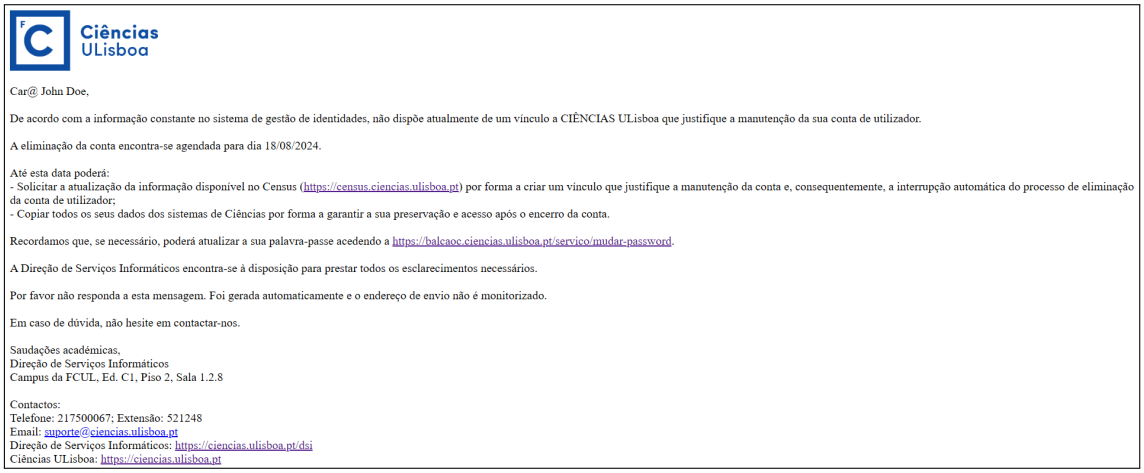
Nome: Jane Doe ,
Documento de Identificação: YYYYYYYY,
Email: ZZZZZZZZ@ciencias.ulisboa.pt

Aguardamos confirmação da regularização dos registos.
Agradecemos atempadamente o tempo dispensado.

Saudações académicas,
Direção de Serviços Informáticos
Campus da FCUL, Ed. C1, Piso 2, Sala 1.2.8

Contactos:
Telefone: 217500067; Extensão: 521248
Email: suporte@ciencias.ulisboa.pt
Direção de Serviços Informáticos: https://ciencias.ulisboa.pt/dsi
Ciências ULisboa: https://ciencias.ulisboa.pt

(a) Exemplo de mensagem de correio eletrónico enviada à entidade responsável.



Ciências ULisboa

Car@ John Doe,

De acordo com a informação constante no sistema de gestão de identidades, não dispõe atualmente de um vínculo a CIÊNCIAS ULisboa que justifique a manutenção da sua conta de utilizador.

A eliminação da conta encontra-se agendada para dia 18/08/2024.

Até esta data poderá:
- Solicitar a atualização da informação disponível no Census (https://census.ciencias.ulisboa.pt) por forma a criar um vínculo que justifique a manutenção da conta e, consequentemente, a interrupção automática do processo de eliminação da conta de utilizador;
- Copiar todos os seus dados dos sistemas de Ciências por forma a garantir a sua preservação e acesso após o encerro da conta.

Recordamos que, se necessário, poderá atualizar a sua palavra-passe acedendo a https://balcaoc.ciencias.ulisboa.pt/servico/mudar-password.

A Direção de Serviços Informáticos encontra-se à disposição para prestar todos os esclarecimentos necessários.

Por favor não responda a esta mensagem. Foi gerada automaticamente e o endereço de envio não é monitorizado.

Em caso de dúvida, não hesite em contactar-nos.

Saudações académicas,
Direção de Serviços Informáticos
Campus da FCUL, Ed. C1, Piso 2, Sala 1.2.8

Contactos:
Telefone: 217500067; Extensão: 521248
Email: suporte@ciencias.ulisboa.pt
Direção de Serviços Informáticos: https://ciencias.ulisboa.pt/dsi
Ciências ULisboa: https://ciencias.ulisboa.pt

(b) Exemplo de mensagem de correio eletrónico enviada ao utilizador.

Figura 6.11: Notificações enviadas.

Fig. 6.11b. Caso a irregularidade não seja resolvida dentro do prazo estabelecido, a sua conta será encerrada.

6.2.3 Implementação

Este sistema foi desenvolvido em *Python*, utilizando a *framework Flask* para possibilitar o acesso através duma *API web*. Para garantir uma gestão eficiente, o sistema foi integrado em um *container Docker*, que inclui um servidor de base de dados *MySQL*.

No código, as variáveis sensíveis, como as credenciais de acesso a *APIs*, foram armazenadas num ficheiro de configuração.

Para a comunicação com a *Active Directory*, o sistema utiliza as funções do *Lightweight Directory Access Protocol* (*LDAP*) disponibilizadas pela biblioteca *ldap3*[4] do *Python*. Adicionalmente, para comunicar com os serviços de CIÊNCIAS ULisboa, nomeadamente o *SAP*, *Fénix* e *Census*, o sistema recorre a *APIs* disponibilizadas pelos mesmos.

[4] `https://ldap3.readthedocs.io/`

Descrição	Campo	Tipo de Dados
E-mail do utilizador	*E-mail*	*String*
Estado do utilizador	Estado	*String*
Data em que a entrada foi atualizada	Data	*Timestamp*

Tabela 6.3: Campos da base de dados do mecanismo de identificação de contas de utilizador anómalas.

Base de dados

Para manter estado e permitir auditorias, foi utilizada uma base de dados relacional *MySQL* com uma tabela para cada ação.

Cada tabela é composta pelos campos apresentados na Tab. 6.3. Além disso, esta estrutura foi pensada para evitar que o utilizador seja notificado repetidamente pela mesma irregularidade, permitindo o registo do estado das ações aplicadas.

Modularidade

Para facilitar a implementação futura de novos testes e ações, o código foi estruturado modularmente. Como tal, apenas é necessário que o programador programe o teste ou a ação desejada, seguindo a interface dos restantes, e que o inclua no módulo/pasta do projeto correspondente (módulo dos testes ou módulo das ações). Um desafio particular é a passagem de informação dos utilizadores identificados nos testes para as ações. Na estrutura definida, o estado é entregue através da comunicação com a base de dados da aplicação.

6.2.4 Segurança dos *Endpoints*

Este é um sistema crítico para a instituição. Como tal, é especialmente importante garantir que o mesmo é seguro, uma vez que um ataque informático bem-sucedido pode comprometer o encerramento automático das contas de utilizador existentes em CIÊNCIAS ULisboa, e por sua vez a sua infraestrutura informática.

Um sistema de identificação de contas de utilizador anómalas robusto é essencial para mitigar riscos e garantir a segurança dos utilizadores.

Os *Endpoints* disponibilizados pela *API* do sistema estão numa rede isolada e estão disponíveis via comunicação *HTTPS* protegida por autenticação.

6.2.5 Avaliação

As estatísticas recolhidas da realização dos testes utilizando este sistema estão apresentadas na Tab. 6.4 e na Tab. 6.5. Estes dados resultam da aplicação de todos os testes desenvolvidos para o sistema, aplicados exclusivamente aos utilizadores com contas ativas.

As estatísticas mostram um número considerável de utilizadores com contas ativas em situação irregular em CIÊNCIAS ULisboa, que se dividem em várias categorias. Há diversas contas sem atividade, mas que ainda se mantêm ativas, muitas das quais pertencem a utilizadores que já não

Critério	Domínio			
	fc.ul.pt	alunos.fc.ul.pt	Total	% Total
Contas	8484	28143	36627	100%
Contas inativas	5871	20064	25935	71%
Contas ativas	2613	8079	10692	29%
Contas sem atividade (+3 meses)	151	808	959	3%
Utilizadores com múltiplas contas			342	1%
Utilizadores sem vínculo válido *Fénix*		1891	1891	5%
Utilizadores sem vínculo válido *Census*	1171		1171	3%
Utilizadores sem número de identificação civil	489	82	571	2%

Tabela 6.4: Estatísticas recolhidas do *Active Directory*.

Critério	Contagem
Contas sem perfil no *Census*	378
Contas sem relação ativa no *Census*	732
Contas com relação ativa no *Census*, mas que deveria estar inativa	23
Contas sem um número de identificação civil válido no *Census*	38

Tabela 6.5: Estatísticas referentes aos utilizadores sem vínculo válido no *Census*.

têm vínculo com a instituição. Além disso, foram encontrados casos de utilizadores com múltiplas contas no mesmo domínio, uma situação permitida pelo sistema anterior de criação de contas. Também foram identificados vários utilizadores sem número de identificação civil, devido, por exemplo, à criação manual de contas no serviço de diretório. Por fim, há um número significativo de utilizadores sem um vínculo válido com a instituição, uma situação que resulta não só da ausência até então de processos automáticos de verificação e encerramento de contas, mas também do sistema anterior de criação de contas.

Apesar disto, o sistema atualmente apenas envia notificações via correio eletrónico para o servidor de *SMTP* de testes, pelo que ainda nenhum utilizador foi alertado nem desativado.

6.2.6 Trabalho Futuro

A aplicação deve começar por ser colocada em ambientes de qualidade e produção, e deve ser executada automaticamente todos os dias, com os testes e ações já desenvolvidos e configurados. Ao colocá-la em produção, esta deve ser configurada, através das variáveis de ambiente (por exemplo: o endereço do servidor *SMTP* de produção para o envio de *e-mails*), para notificar e desativar efetivamente os utilizadores.

É necessário evitar que o mesmo utilizador seja notificado por anomalias relacionadas. Isto significa que, caso o utilizador tenha uma anomalia A (por exemplo, ausência de perfil *Census*), que por sua vez causa a anomalia B (por exemplo, ausência de vínculos ativos no *Census*), este utilizador apenas deve ser notificado pela anomalia A.

Adicionalmente, deve ser possível definir exceções às regras, ou seja, deve haver um mecanismo que possibilite que as entidades responsáveis por determinada conta de utilizador, prolonguem o prazo até ao encerramento da conta de utilizador. Esta decisão deve-se a uma política interna da instituição. Por fim, devem ainda ser desenvolvidos mais testes e ações.

6.3 Criação de contas

Tal como descrito na secção anterior, ao realizar o levantamento das contas de utilizadores existentes na instituição, verificou-se que o sistema antigo de criação de contas tolerava várias situações anómalas. Em primeiro lugar, havia centenas de contas que não podiam ser associadas inequivocamente a um perfil do *Census* com um vínculo válido ativo. Adicionalmente, existiam utilizadores com múltiplas contas na instituição.

Assim, além de resolver as situações anómalas herdadas do passado, era também crucial impedir que esses problemas ocorressem na criação de novas contas. Em linha com a iniciativa da DSI de remoção de serviços do Portal CIÊNCIAS ULisboa, foi decidido renovar o sistema de criação de contas de utilizador, em vez de corrigir o anterior.

6.3.1 Levantamento de requisitos

O novo sistema de criação de contas de utilizador teria de cumprir vários requisitos.

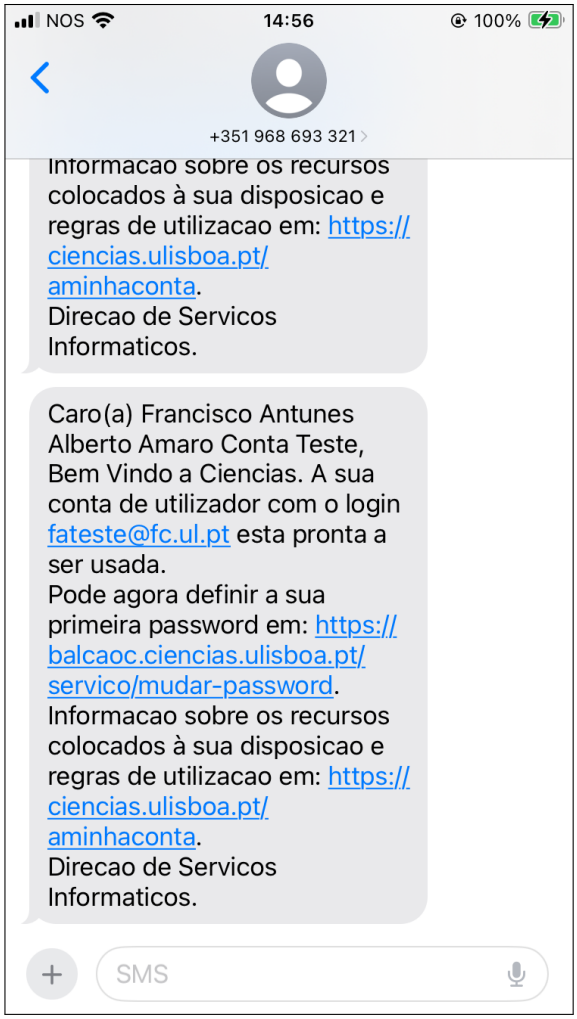
Primeiramente, apenas seriam criadas contas para utilizadores registados no *Fénix* com uma matrícula ativa ou para colaboradores registados no *Census* com um vínculo ativo com a instituição. Adicionalmente, o sistema deveria permitir a criação de contas de utilizador exclusivamente através do número de identificação civil, assegurando, assim, a validade dos dados associados a cada utilizador.

Havia dois casos de uso previstos para a criação de contas. Deveria ser possível que um utilizador não autenticado pudesse solicitar a criação de uma conta de utilizador. Além disso, deveria ser possível ainda que um utilizador autenticado pudesse solicitar a criação de um conjunto de contas. Este caso de uso, poderia, por exemplo, ser usado pela direção académica no início de cada ano letivo para criar as contas de utilizador para os novos alunos.

O sistema permitiria, no máximo, a existência de uma conta por utilizador em cada domínio, *@alunos.fc.ul.pt* e *@fc.ul.pt*. E, quando fosse necessário, o sistema apenas reativaria as contas existentes. O sistema deveria criar contas no *Active Directory*, e todos os recursos disponibilizados aos utilizadores, incluindo, caixas de entrada, arquivos e *home directories*.

Por fim, após a criação ou reativação de uma conta, o utilizador deveria ser notificado simultaneamente por correio eletrónico e *SMS*, tal como apresentado na Fig. 6.12. Esta abordagem assegura que, na eventualidade de faltar um dos contactos ou ocorrer uma falha no envio de uma notificação, exista um meio alternativo que aumente a probabilidade de sucesso na entrega.

(a) Mensagem de correio eletrónico de abertura de contas.



(b) *SMS* de boas-vindas.

Figura 6.12: Notificações de boas-vindas.

6.3.2 Formulários

Para criar uma conta de utilizador, foram definidos dois formulários no BalcaoC, apresentados na Fig. 6.13. Ambos os formulários são semelhantes, no entanto, há ligeiras diferenças:

Criação de uma conta de utilizador O formulário[5], apresentado na Fig. 6.13a, permite que um utilizador não autenticado solicite a criação de uma conta de utilizador.

Criação de um conjunto de contas de utilizador O formulário[6], apresentado na Fig. 6.13b, permite que um utilizador autenticado solicite a criação de um conjunto de contas. Após a submissão deste formulário o utilizador recebe uma mensagem de correio eletrónico com o relatório da criação de contas de utilizador. Um exemplo é apresentado na Fig. 6.14.

Após submissão, nenhum dos formulários devolve informação acerca do pedido. Esta informação é enviada, apenas por canal alternativo. Desta forma, previne-se o acesso indevido a dados de terceiros, em particular informações sobre a existência ou não de uma relação com CIÊNCIAS ULisboa, por meio destes formulários.

6.3.3 Arquitetura

A arquitetura deste processo está ilustrada na Fig. 6.15. Inicialmente, os valores submetidos através deste formulário são higienizados. Para cada número de identificação civil obtêm-se os respetivos dados pessoais e vínculo com CIÊNCIAS ULisboa a partir do *Fénix* e do *Census*.

Se o utilizador tiver uma matrícula ativa no *Fénix*, será concedida permissão para a criação de uma conta de aluno. Da mesma forma, se o utilizador tiver um perfil com um vínculo ativo no *Census*, será permitida a criação de uma conta de colaborador. Caso ambas as condições sejam satisfeitas, ambas as contas serão criadas, isto porque, estes dois tipos de contas de utilizador têm acesso a recursos distintos, e atualmente, na instituição, ainda não é possível combinar os recursos de colaborador e aluno numa única conta de utilizador.

Antes de proceder à criação da conta, verifica-se se o utilizador já possui uma conta. Se o utilizador tiver uma conta inativa, esta será reativada. Caso o utilizador já possua uma conta ativa, nenhuma ação adicional será tomada. Se o utilizador ainda não possuir uma conta, procede-se então à criação da mesma e à inclusão em grupos de *Active Directory* caso necessário.

Adicionalmente, é verificado se o utilizador tem permissão para possuir recursos específicos, através do domínio e dos grupos de *Active Directory* a que pertence. Caso se verifique, são criados os recursos adicionais, nomeadamente a *Home Directory*, a caixa de entrada de correio eletrónico, o arquivo e uma *quota* do *Cirrus*. Finalmente, caso alguma conta tenha sido criada ou reativada, o utilizador será notificado via correio eletrónico e *SMS* para definir as suas credenciais através do sistema de recuperação de credenciais, descrito na Sec. 6.1.

[5] `https://balcaoc.ciencias.ulisboa.pt/servico/criar-conta-utilizador`
[6] `https://balcaoc.ciencias.ulisboa.pt/servico/criar-contas-utilizador`

(a) Formulário para a criação de uma conta de utilizador.

(b) Formulário para a criação de um conjunto de contas de utilizador.

Figura 6.13: Formulários para a criação de contas de utilizador.

Ciências ULisboa

Caro Francisco Amaro,

O pedido de criação de contas recebido a 07/25/2024 14:38:46 teve os seguintes resultados:

a) Número total de contas solicitadas: 1
b) Número de contas criadas com sucesso: 0 (os titulares foram notificados da criação da conta por SMS e/ou email para os endereços registados no Fénix ou Census).
c) Número de contas reativadas: 0 (titulares de contas que tiveram previamente uma relação com Ciências e que foram notificados da reativação da conta por SMS e/ou email para os endereços registados no Fénix ou Census).
d) Número de contas ativas: 0 (titulares de contas que se encontram ativas e para os quais não foi enviada notificação).
e) Número de contas não criadas por inexistência de permissões: 0 (as contas não foram criadas por não ter sido possível encontrar no Fenix ou Census um motivo para a sua criação. A lista de contas nesta situação encontra-se abaixo).
f) Número de contas não criadas por inexistência de contactos: 0 (as contas não foram criadas por não ter sido possível encontrar no Fenix ou Census um contacto para a sua notificação. Depois de carregar um contacto (telemóvel ou email) o pedido de criação de conta deve ser repetido. A lista de contas nesta situação encontra-se abaixo).
g) Número de contas não criadas por não se ter encontrado informação sobre o utilizador: 1 (os números de identificação para os quais não foi encontrado registo no Fénix ou Census é indicado abaixo).
h) Número de contas não criadas devido à inserção de dados em formato incorreto: 0 (o número de identificação civil fornecido contém caracteres inválidos).
i) Número de contas não criadas devido à tentativa de reativação de contas de utilizadores que não têm nenhuma conta: 0 (o utilizador tentou reativar a sua conta mas não possui nenhuma conta).
j) Número de contas não criadas por outros problemas: 0 (a lista de contas e uma descrição técnica do problema segue abaixo. A equipa de suporte foi colocada em CC nesta mensagem para que se inicie a despistagem do problema).

- Lista de nomes e/ou documentos de identificação da alínea g)
0123456789

- Detalhes
[Mensagem #0]:

[Mensagem #1]:

[Mensagem #2]:

Saudações académicas,
Direção de Serviços Informáticos
Campus da FCUL, Ed. C1, Piso 2, Sala 1.2.8

Contactos:
Telefone: 217500067; Extensão: 521248
Email: suporte@ciencias.ulisboa.pt
Direção de Serviços Informáticos: https://ciencias.ulisboa.pt/dsi
Ciências ULisboa: https://ciencias.ulisboa.pt/

Figura 6.14: Relatório de criação de contas (com alguns dados omitidos).

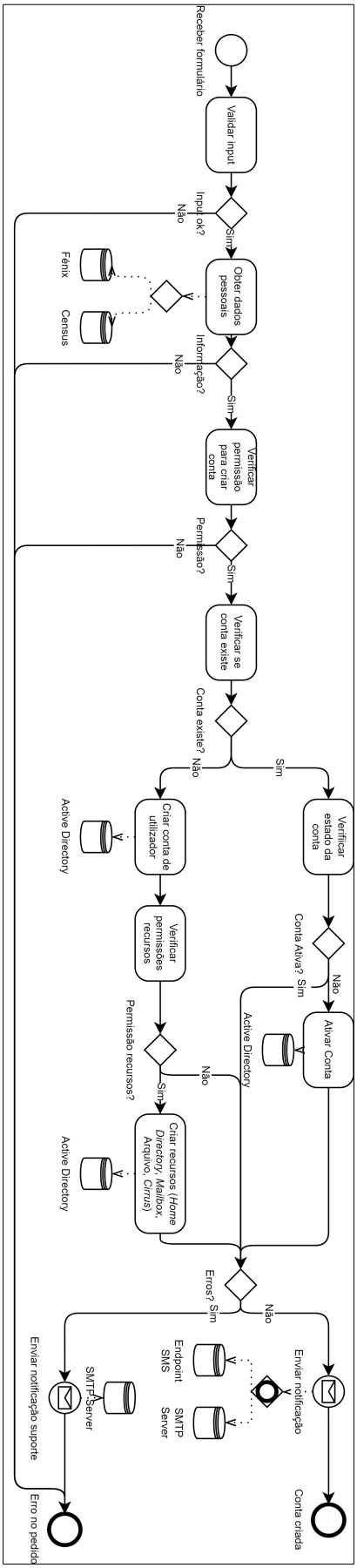


Figura 6.15: Arquitetura do sistema de criação de contas.

6.3.4 Auditoria

Para possibilitar uma auditoria o sistema gera registos das suas atividades. Irão ser guardados num ficheiro, registos relativamente a cada processo de criação de conta de utilizador. Estes registos incluem informações relativamente a tentativas de criação de conta, contas criadas, contas reativadas e exceções que possam ter ocorrido nestes processos.

Para facilitar o acompanhamento dos pedidos de criação de contas pela equipa de suporte, foi criada uma página de apoio. O acesso a esta página é restrito por rede, utilizador e palavra-passe. A página apresenta os registos dos pedidos e permite consultar o estado de cada um, incluindo o número de documento de identificação fornecido, o erro associado (em caso de falha) e o identificador da conta criada quando o processo é bem-sucedido.

6.3.5 Implementação

Há funcionalidades de gestão do *Active Directory* e do *Exchange* que apenas estão disponíveis em sistemas operativos *Windows* através de *powershell*. Como tal, este sistema teve forçosamente de ser desenvolvido em ambiente *Windows*.

Para a comunicação com a *Active Directory*, o sistema utiliza o módulo *Active Directory* do *Powershell*. Adicionalmente, para comunicar com os serviços de CIÊNCIAS ULisboa, nomeadamente o *Fénix* e *Census*, o sistema recorre a *APIs* disponibilizadas pelos mesmos. Além disso, no código, as variáveis sensíveis, como as credenciais de acesso a *APIs*, foram armazenadas num ficheiro de configuração.

O sistema foi implementado em *Python* utilizando a *framework Flask* para permitir o acesso ao mesmo por uma *API web*. Esta *API web* por sua vez invoca um *script powershell* que procede à criação da conta de utilizador.

A instalação deste sistema em *containers* apresentou vários desafios. Quando o *Docker* foi lançado, inicialmente era focado exclusivamente em *containers Linux*, o que fez com que as primeiras imagens *Docker* fossem baseadas nesse sistema. Só após alguns anos do lançamento do *Docker* é que a *Microsoft* introduziu o suporte para *containers Windows* [35, 36]. Como resultado, a maioria das imagens e da documentação disponíveis para *Docker* ainda são baseadas em sistemas *Linux*. Apesar dessas limitações, e da decisão de não incluir certas funcionalidades ou optar por alternativas, o sistema foi integrado com sucesso em um *container Windows* no *Docker*, o que facilitou a sua gestão. No entanto, devido à menor popularidade dos *containers Windows*, há algumas funcionalidades que ainda não estão disponíveis. Por exemplo, não foi possível incluir uma imagem do servidor *MySQL* no *container*[7], nem projetar determinados ficheiros do *container* para a máquina *host*[8]. Além disso, não foi viável a utilização de modos de rede específicos[9].

Atualmente, existem duas instâncias do sistema: uma em ambiente de qualidade e outra em ambiente de produção. A primeira permite testar novas funcionalidades, a segunda é aquela que

[7] `https://hub.docker.com/r/mysql/mysql-server/`

[8] `https://docs.docker.com/reference/cli/docker/container/run/#/mount-volume--v--read-only`

[9] `https://docs.docker.com/engine/network/drivers/host/`

está disponível para o público.

6.3.6 Análise de Segurança

Para um sistema crítico para a instituição, é especialmente importante garantir que o mesmo é seguro, uma vez que um ataque informático bem-sucedido pode comprometer as contas de utilizador criadas em CIÊNCIAS ULisboa e por sua vez a sua infraestrutura informática. Um sistema de criação de contas de utilizador robusto é essencial para mitigar riscos e garantir a segurança dos utilizadores.

Nesta secção está presente uma análise de segurança do sistema.

Formulários Todos os campos dos formulários são higienizados.

Endpoints Os *Endpoints* disponibilizados pela *API* do sistema estão numa rede isolada e têm uma versão *HTTPS* protegida por autenticação.

Agente *Wazuh* Para monitorizar a máquina em ambiente de produção e os respetivos *containers*, instalou-se um agente *Wazuh*, que comunica com o servidor *Wazuh*, na máquina. Este agente é usado para recolher *logs* e responder a alguns tipos de ameaças, por exemplo, injeção de código *SQL* [34].

6.3.7 Avaliação

Este sistema está em produção desde julho de 2024. Desde esse mês até agosto de 2024, foram recolhidas algumas estatísticas, referentes aos pedidos de criação de contas, que estão disponíveis na Tab. 6.6. Esses pedidos foram realizados tanto pelos próprios utilizadores quanto por terceiros.

Essas estatísticas podem ser explicadas da seguinte forma:

Utilizadores novos 803 utilizadores criaram uma conta de utilizador.

Utilizadores reativados 16 utilizadores reativaram a sua conta de utilizador.

Utilizadores que já tinham uma conta de utilizador ativa 8 utilizadores foram impedidos de criar uma conta de utilizador, porque já possuíam uma ativa.

Utilizadores sem permissão 11 utilizadores foram impedidos de criar uma conta de utilizador, porque não tinham um vínculo válido com a instituição. Isto é, não tinham uma matrícula válida no *Fénix*, nem uma relação válida ativa no *Census*.

Para o ano letivo de 2024/2025, todas as contas dos novos alunos, totalizando mais de 800, foram criadas através deste novo mecanismo. No entanto, ao processar um elevado volume de utilizadores num curto espaço de tempo, surgiu uma limitação: formou-se uma fila para o envio de *SMS*, devido ao elevado número de notificações de boas-vindas e de definição de credenciais a serem enviadas simultaneamente. Como resultado, alguns pedidos de definição das primeiras credenciais expiraram antes que os *SMS* fossem efetivamente enviados.

Critério	Contagem	Percentagem
Utilizadores novos	803	95,82%
Utilizadores reativados	16	1,91%
Utilizadores que já tinham uma conta ativa	8	0,95%
Utilizadores sem permissão	11	1,32%
Total	838	100,00%

Tabela 6.6: Estatísticas recolhidas do sistema de criação de contas.

6.3.8 Trabalho Futuro

Este sistema de criação de contas ainda tem algumas limitações, como tal, é usado em simultâneo com o sistema antigo. Dos vários tipos de contas existentes na instituição, apenas é possível usá-lo para criar contas de aluno e colaborador, ficando de fora contas institucionais, temporárias de conferência/aulas e contas temporárias de visitante. Desta forma, será necessário, no futuro, alargar este sistema para esses casos de uso.

Além disso, por limitações dos *containers windows* houve várias funcionalidades que não foram possíveis incluir desde o início, por exemplo, uma base de dados *MySQL* no *container*. Assim, será necessário incluir por meio de formas alternativas uma base de dados, interna ou externa, para que se possa incluir uma página de gestão de utilizadores associada a este sistema.

Capítulo 7

Conclusão

Este projeto permitiu realizar um conjunto de tarefas que contribuem para a segurança informática da instituição. Além disso, permitiu ainda adquirir e aprofundar competências de desenvolvimento em múltiplas tecnologias, em administração de sistemas, em interação com o utilizador, em documentos normativos referentes à segurança informática e por fim, proporcionou o confronto com um ambiente de trabalho.

Apesar de CIÊNCIAS ULisboa sempre ter tido como prioridade a garantia de um ambiente digital seguro e confiável para todos os seus utilizadores, nunca teve um mecanismo que permitisse autoavaliar o cumprimento das políticas de segurança da DSI. Este projeto desenvolveu um mecanismo que não só permite essa autoavaliação, como também sensibiliza os colaboradores para a importância do cumprimento das políticas de segurança, e acaba consequentemente por contribuir para o seu cumprimento.

Adicionalmente, já existiam mecanismos *online* que permitiam a recuperação de credenciais e a criação de contas de utilizadores. No entanto, estes mecanismos utilizavam métodos datados e com vulnerabilidades conhecidas. Este projeto renovou os processos de criação de conta e alteração de credenciais que estão agora bastante mais robustecidos.

Outra preocupação fundamental foi garantir que as contas de utilizadores ativas na instituição tivessem um vínculo que as justificasse, e que os seus dados fossem coerentes entre os diferentes serviços de CIÊNCIAS ULisboa. Anteriormente, não havia mecanismos automáticos para a deteção e resolução destas incongruências, o que dificultava a gestão de contas de utilizadores. Este projeto implementou um verificador automático de coerência de informação, que visa facilitar essa gestão, identificando e corrigindo essas situações, como, por exemplo, através da notificação e do encerramento das contas que não cumprem os critérios estabelecidos.

Por fim, o trabalho realizado neste projeto permitiu oferecer aos utilizadores um ambiente informático ainda mais confiável, com serviços mais simples e seguros, que tiveram muita adesão por parte dos utilizadores. Além disso, contribuiu para mitigar os riscos que anteriormente existiam na instituição, reforçando a segurança e a eficiência dos seus sistemas.

Bibliografia

[1] Faculdade de Ciências da Universidade de Lisboa. Rede. https://ciencias.ulisboa.pt/pt/rede-0, 2024. [Online - Accessed on 03-07-2024].

[2] Faculdade de Ciências da Universidade de Lisboa. Estatísticas. https://ciencias.ulisboa.pt/pt/estatisticas, 2024. [Online - Accessed on 03-07-2024].

[3] Faculdade de Ciências da Universidade de Lisboa. Direção de Serviços Informáticos. https://ciencias.ulisboa.pt/pt/direcao-servicos-informaticos, 2024. [Online - Accessed on 03-07-2024].

[4] Faculdade de Ciências da Universidade de Lisboa. Despacho n.º 11913/2021. https://ciencias.ulisboa.pt/pt/estatutos-e-regulamentos-organicos, 2021. [Online - Accessed on 03-07-2024].

[5] Faculdade de Ciências da Universidade de Lisboa. Despacho n.º 602/2022. https://ciencias.ulisboa.pt/pt/estatutos-e-regulamentos-organicos, 2022. [Online - Accessed on 03-07-2024].

[6] Faculdade de Ciências da Universidade de Lisboa. Criação de Conta de Colaborador. https://ciencias.ulisboa.pt/pt/registar, 2024. [Online - Accessed on 22-07-2024].

[7] Faculdade de Ciências da Universidade de Lisboa. Fénix FAQ - Perguntas Frequentes Sobre o Fénix. https://ciencias.ulisboa.pt/pt/faq-fenix, 2024. [Online - Accessed on 03-07-2024].

[8] Faculdade de Ciências da Universidade de Lisboa. Census: Perguntas e Respostas. https://census.ciencias.ulisboa.pt/faq, 2024. [Online - Accessed on 03-07-2024].

[9] Faculdade de Ciências da Universidade de Lisboa. Sobre o Balcão C. https://balcaoc.ciencias.ulisboa.pt/sobre, 2024. [Online - Accessed on 03-07-2024].

[10] Faculdade de Ciências da Universidade de Lisboa. Serviço de Partilha de Ficheiros. https://ciencias.ulisboa.pt/node/7090, 2024. [Online - Accessed on 03-07-2024].

[11] Faculdade de Ciências da Universidade de Lisboa. Contas de Utilizador. https://ciencias.ulisboa.pt/pt/contas-de-utilizador, 2024. [Online - Accessed on 03-07-2024].

[12] Faculdade de Ciências da Universidade de Lisboa. Suporte a Infraestruturas Informáticas. https://ciencias.ulisboa.pt/pt/suporte-a-infraestruturas-informaticas-de-id-em-ciencias, 2024. [Online - Accessed on 03-07-2024].

[13] Telecommunication Standardization Sector of the International Telecommunication Union. X.500 standard. https://web.archive.org/web/20190104231951/http://www.x500standard.com/, 2019. [Online - Accessed on 26-07-2024].

[14] Microsoft. Active Directory Domain Services Overview. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview, 2022. [Online - Accessed on 03-07-2024].

[15] Red Hat. What is lightweight directory access protocol (LDAP) authentication? https://www.redhat.com/en/topics/security/what-is-ldap-authentication, 2022. [Online - Accessed on 19-07-2024].

[16] Faculdade de Ciências da Universidade de Lisboa. Correio Eletrónico. https://ciencias.ulisboa.pt/pt/correio-eletronico, 2024. [Online - Accessed on 03-07-2024].

[17] Microsoft. What is a Microsoft Exchange account? https://support.microsoft.com/en-us/office/what-is-a-microsoft-exchange-account-47f000aa-c2bf-48ac-9bc2-83e5c6036793, 2024. [Online - Accessed on 03-07-2024].

[18] Conselho de Ministros. Resolução do Conselho de Ministros n.º 41/2018. https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/41-2018-114937034, 2018. [Online - Accessed on 03-07-2024].

[19] Comissão Nacional de Proteção de Dados. Diretriz/2023/1. https://www.cnpd.pt/decisoes/diretrizes/, 2023. [Online - Accessed on 03-07-2024].

[20] União Europeia. Diretiva NIS2 (Network and Information Security Directive). https://eur-lex.europa.eu/eli/dir/2022/2555, 2022. [Online - Accessed on 03-07-2024].

[21] União Europeia. Diretiva NIS (Network and Information Security Directive). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L1148, 2016. [Online - Accessed on 23-07-2024].

[22] The Open Web Application Security Project (OWASP). Multifactor Authentication Cheat Sheet. https://cheatsheetseries.owasp.org/cheatsheets/Multifactor_Authentication_Cheat_Sheet.html, 2024. [Online - Accessed on 05-07-2024].

[23] The Open Web Application Security Project (OWASP). Forgot Password Cheat Sheet. https://cheatsheetseries.owasp.org/cheatsheets/Forgot_Password_Cheat_Sheet.html, 2024. [Online - Accessed on 05-07-2024].

[24] The Open Web Application Security Project (OWASP). Password Storage Cheat Sheet. https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html, 2024. [Online - Accessed on 05-07-2024].

[25] Tommaso Innocenti, Seyed Ali Mirheidari, Amin Kharraz, Bruno Crispo, and Engin Kirda. You've got (a reset) mail: A security analysis of email-based password reset procedures. In Leyla Bilge, Lorenzo Cavallaro, Giancarlo Pellegrino, and Nuno Neves, editors, *Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 1–20, Cham, 2021. Springer International Publishing.

[26] The Open Web Application Security Project (OWASP). Choosing and Using Security Questions Cheat Sheet. https://cheatsheetseries.owasp.org/cheatsheets/Choosing_and_Using_Security_Questions_Cheat_Sheet.html, 2024. [Online - Accessed on 05-07-2024].

[27] Stuart Schechter, A.J. Brush, and Serge Egelman. It's no secret: Measuring the security and reliability of authentication via 'secret' questions. In *Proceedings of the 2009 IEEE Symposium on Security and Privacy*. IEEE Computer Society, May 2009.

[28] Joseph Bonneau, Elie Bursztein, Ilan Caron, Rob Jackson, and Mike Williamson. Secrets, lies, and account recovery: Lessons from the use of personal knowledge questions at google. In *Proceedings of the 24th International Conference on World Wide Web*, WWW '15, page 141–150, Republic and Canton of Geneva, CHE, 2015. International World Wide Web Conferences Steering Committee.

[29] National Institute of Standards and Technology. NIST special publication 800-63: Digital identity guidelines. https://pages.nist.gov/800-63-3/, 2017. [Online - Accessed on 19-07-2024].

[30] The Open Web Application Security Project (OWASP). Testing for Weak Password Change or Reset Functionalities. https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/09-

Testing_for_Weak_Password_Change_or_Reset_Functionalities, 2024. [Online - Accessed on 05-07-2024].

[31] Cloudfare. What is an API endpoint? https://www.cloudflare.com/learning/security/api/what-is-api-endpoint/, 2024. [Online - Accessed on 15-07-2024].

[32] Dinesh Chandra Verma. *Principles of Computer Systems and Network Management*. Springer, New York, 2010.

[33] Jun Ho Huh, Hyoungshick Kim, Swathi S.V.P. Rayala, Rakesh B. Bobba, and Konstantin Beznosov. I'm too busy to reset my linkedin password: On the effectiveness of password reset emails. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, page 387–391, New York, NY, USA, 2017. Association for Computing Machinery.

[34] Wazuh. Wazuh agent. https://documentation.wazuh.com/current/installation-guide/wazuh-agent/index.html, 2024. [Online - Accessed on 26-07-2024].

[35] Taylor Brown. Bringing Docker To Windows Developers with Windows Server Containers. https://learn.microsoft.com/en-us/archive/msdn-magazine/2017/april/containers-bringing-docker-to-windows-developers-with-windows-server-containers, 2017. [Online - Accessed on 10-09-2024].

[36] Microsoft. Linux containers on Windows 10. https://learn.microsoft.com/en-us/virtualization/windowscontainers/deploy-containers/linux-containers, 2023. [Online - Accessed on 10-09-2024].

[37] Faculdade de Ciências da Universidade de Lisboa. Datacenter. https://ciencias.ulisboa.pt/pt/datacenter, 2024. [Online - Accessed on 03-07-2024].