UNIVERSIDADE
LUSÓFONA

Plataforma de Gestão de Identidades e Acessos

Trabalho Final de curso

Diogo Agostinho

Rui Ribeiro

Trabalho Final de Curso | LEI | Data 26/06/2020

Direitos de cópia

Índice

Índices de Quadros, Figuras, Tabelas, Equações, source code exemplo....

Resumo

O presente relatório foi elaborado como parte integrante da unidade curricular do Trabalho Final de Curso lecionada no âmbito da Licenciatura de Engenharia Informática, pretendo espelhar parte da criação de um protótipo de plataforma de Gestão de Identidades e Acessos(IAM), baseado em Open Source.

Como se pretende demonstrar neste relatório, subjacentes à prática desenvolvida em ambas as valências estão metodologias voltadas para a aprendizagem pela descoberta, investigação, assentes, sempre que possível, na utilização e manipulação de recursos fornecidos.

Constam deste relatório sete grandes capítulos, o primeiro capítulo dedicado á identificação do problema, onde será descrito o enquadramento prático e a envolvente do problema em análise.

O relatório apresenta um segundo capítulo, levantamento e analise dos requisitos, onde será identificado detalhadamente as características da solução a produzir sobre a forma de requisitos. Neste sentido, apresenta-se a lista de requisitos propostos, onde é indicado o cumprimento, parcial ou integral, ou não implementação de cada um.

O terceiro capítulo é a viabilidade e relevância do projeto, que se focara no resultado final do TFC, tomando por base a solução concreta produzida e os resultados dos testes de validação, visto ser este o produto a entregar ao 'cliente'.

No quarto capítulo é sobre a Solução Desenvolvida onde serão apresentadas as principais opções técnicas do desenvolvimento, modelos conceptuais relevantes, fundamentação teórica, validação técnica da solução desenvolvida e o destaque as alterações que decorram dos resultados dos testes.

O quinto capítulo, Benchmarking , destina-se à análise comparativa da solução proposta inicialmente face a alterativas e potenciais concorrentes existentes em mercado.

O presente relatório tem um sexto capítulo, o Método e planeamento onde é descrito o método de trabalho seguido no desenvolvimento do projeto.

E por fim um capítulo onde é descrito detalhadamente os resultados, outputs e uma análise comparativa dos resultados face ao proposto inicialmente, mostrando diferenças entre a proposta e resultados.

O objetivo deste trabalho final de curso é desenvolver um protótipo de uma plataforma de gestão de identidades e acessos voltada para a faculdade que terá como âmbito a criação e gestão da conta dos utilizadores e a possível integração com outros sistemas.

Palavras-chave: IAM, Gestão de Identidades e Acessos, protótipo, plataforma, sistemas.

Abstract (em Inglês)

This report was prepared as part of the Final Course Work unit taught in the context of the Degree in Computer Engineering, I intend to mirror part of the creation of a prototype platform for Identity and Access Management (IAM), based on Open Source.

As we intend to demonstrate in this report, underlying the practice developed in both valences are methodologies focused on learning by discovery, research, based, whenever possible, on the use and manipulation of resources provided.

There are five main chapters in this report, the first dedicated to the identification of the problem, where the practical framework and the environment of the problem under analysis will be described, as well as a comparative analysis of the results compared to what was initially proposed, showing differences between the proposal and the results.

The report presents a second chapter, survey and analysis of the requirements, where the characteristics of the solution to be produced on the form of requirements will be identified in detail. In this sense, the list of proposed requirements is presented, where compliance, in part or in full, or non-implementation of each is indicated.

The third chapter is the feasibility and relevance of the project, which will focus on the final result of the TFC, based on the concrete solution produced and the results of the validation tests, since this is the product to be delivered to the 'client'.

The fourth chapter is about the Developed Solution where the main technical options of the development, relevant conceptual models, theoretical background, technical validation of the developed solution and highlighting the changes that result from the test results will be presented.

The fifth chapter, Benchmarking , is aimed at the comparative analysis of the solution initially proposed against changes and potential competitors in the market.

This report has a sixth chapter, Method and Planning, where the working method followed in the development of the project is described.

And finally a chapter where the results, outputs and outcomes are described in detail.

The objective of this final course work is to develop a prototype of an identity and access management platform focused on the faculty that will have as its scope the creation and management of the user account and the possible integration with other systems.

Keywords: IAM, Identity and Access Management, prototype, platform, systems .

1 Identificação do Problema

1.1. Introdução

A infraestrutura global de informação - a Web - conecta partes remotas em todo o mundo através do uso de redes de larga escala, confiando em protocolos e serviços a nível de aplicação, tais como a recente tecnologia de serviços Web. As empresas estão a aproveitar cada vez mais os recursos computacionais disponíveis na Web através do uso de tecnologias de computação em cloud e virtualização. Assim, à medida que a riqueza das nossas vidas no ciberespaço começa a paralelizar a nossa experiência no mundo físico, espera-se que haja infraestruturas e sistemas de informação e comunicação mais convenientes. Esperamos, por exemplo, que as nossas preferências e perfis pessoais estejam prontamente disponíveis quando fazemos compras pela Web, sem ter de entrar repetidamente.

Em tal cenário, a tecnologia de gestão de identidades digital é fundamental para personalizar e melhorar a experiência do utilizador, proteger a privacidade, sustentar a responsabilidade nas transações e interações e cumprir com os controlos regulatórios. A identidade digital pode ser definida como a representação digital da informação conhecida sobre um indivíduo ou organização específica.

A identidade digital pode incluir informações atributivas sobre um indivíduo, tais como nome, número de Segurança Social (SSN), ou número de passaporte. Além disso, também pode incorporar informações biométricas, tais como características da íris ou impressões digitais, e informações sobre as atividades do utilizador, incluindo pesquisas na Web. A identidade digital também pode incluir identificadores, como nomes de login e pseudônimos, usados por indivíduos ao interagirem com sistemas de computador ou com outros indivíduos no "mundo virtual".

1.2. Ecossistema de Identidades

A combinação de necessidades individuais, soluções empresariais, políticas públicas, padrões e tecnologias está assim a impulsionar a formação da identidade "Ecossistema" . O Ecossistema emergente gera interesses crescentes na gestão das identidades digitais na sociedade da informação. Assim, espera-se que o mercado de gestão de identidades cresça rapidamente.

A segurança e a privacidade são problemas universais, que exigem bases de identidade sólidas. A gestão da informação de identidade digital levanta uma série de desafios devido aos requisitos conflituosos de segurança e privacidade. Por um lado, essa informação precisa ser compartilhada para acelerar e facilitar a autenticação dos utilizadores e o controle de acesso.

As credenciais do utilizador comprometidas costumam servir como ponto de entrada na rede de uma organização e nos seus ativos de informações. As empresas usam a gestão

de identidade para proteger os seus ativos de informações contra as ameaças crescentes de ransomware, hackers criminais, phishing e outros ataques de malware. Espera-se que os custos globais de danos ao ransomware excedam US $ 5 bilhões este ano, um aumento de 15% em relação a 2016, previu a Cybersecurity Ventures.

1.3 Desafios na Gestão da Identidade

A gestão da identidade digital deve encontrar o melhor equilíbrio entre usabilidade, segurança e privacidade. Várias soluções de identidade estão a ser propostas, cada uma adotando abordagens diferentes com objetivos diferentes. As soluções atuais não são necessariamente interoperáveis ou complementares, e às vezes sobrepõem se. Portanto, é fundamental estabelecer as bases para uma compreensão holística das áreas problemáticas e abordagens sinergéticas para soluções inovadoras, tais como diretrizes, metodologias, ferramentas e padrões técnicos.

O desafio é importar uma abordagem semelhante para o ambiente digital online, ou seja, criar credenciais de identidade digital seguras, confiáveis e que possam ser usadas em diferentes ecossistemas e entidades. Isso permite que indivíduos usem a mesma credencial de identidade para assinar nas redes de mais de uma empresa a fim de realizar transações.

Entre as principais questões a serem abordadas na gestão da identidade como uma disciplina essencial para as empresas e a sociedade, incluem-se por exemplo:

- Como disponibilizar as identidades apenas aos indivíduos ou serviços certos, no momento e local certos;
- Como estabelecer a confiança entre as partes envolvidas nas transações de identidade;
- Como evitar o abuso de identidade;
- Como tornar estas disposições possíveis de uma forma escalável, utilizável e rentável.

A IDentity and Access Management (IAM) é uma parte crítica de qualquer plano de segurança da empresa, pois está inextricavelmente vinculado à segurança e à produtividade das organizações na atual economia digitalmente habilitada, é um processo crítico no sentido de proteger os sistemas, dados e aplicações da organização de acessos não autorizados. Em muitas organizações, os utilizadores às vezes têm mais privilégios de acesso do que o necessário.

Muitos governos exigem que as empresas se preocupem com a gestão de identidades. Regulamentos como Sarbanes-Oxley, Gramm-Leach-Bliley e HIPAA responsabilizam as organizações pelo controlo do acesso às informações dos clientes e funcionários. Os sistemas de gestão de identidades podem ajudar as organizações a cumprir esses regulamentos.

À medida que os novos funcionários ingressam na empresa, enfrenta-se o dilema de garantir que eles recebam direitos sobre todos os sistemas e recursos necessários para realizar seu trabalho no dia em que ingressarem na empresa. Da mesma forma, quando

uma pessoa muda de posição dentro da empresa, o acesso que não é mais relevante deve ser revogado e o acesso necessário para seu novo cargo deve ser concedido. Para a situação de utilizadores que saem da empresa ou são rescindidos, é ainda mais imperativo que as permissões sejam endereçadas. O acesso a aplicativos e dados confidenciais deve ser desativado / removido em tempo hábil, com rastreabilidade para evitar as consequências de um utilizador insatisfeito. Sem um sistema para automatizar esses processos, é quase impossível obter o que foi dito acima de maneira oportuna e consistente.

A gestão das contas e privilégios dos utilizadores - user access management - não está a tornar-se mais fácil. Á medida que as empresas externalizam os seus processos de negócios pela Internet para clientes e parceiros comerciais, por consequência expandem o número e os tipos de utilizadores com os quais devem trabalhar.

Assim, mais utilizadores necessitam de acesso a recursos de TI; os ambientes de plataforma permanecerão complexos e heterogéneos; e os serviços Web estão a impulsionar a necessidade de gerir as transações, bem como o acesso dos utilizadores aos recursos de TI. Assim, as empresas já não podem gerir eficazmente o acesso dos utilizadores ao ambiente de TI heterogéneo (por exemplo, repositórios de informação de identidade de utilizadores externos e internos, bases de dados, sistemas operativos e aplicações) para múltiplos fins de acesso, tais como funções empresariais, regras de gestão de senhas e políticas de acesso ao horário de trabalho.

As empresas precisam de assegurar que os utilizadores sejam devidamente identificados e que estas identidades são validadas para os recursos de TI - isto é autenticação. Precisam de saber que os utilizadores só podem aceder o que a sua função lhes permite aceder dentro da empresa - isto é autorização. Eles precisam de ter uma visão consolidada, empresarial e forma de gerir o utilizador acesso - isto é administração. Finalmente precisam de assegurar que as atividades associadas ao acesso dos utilizadores (administração e aplicação em tempo real) são registadas para o acompanhamento diário, fins regulamentares e investigativos - isto é auditoria. Estes são os quatro "A's" de segurança da informação (ver Figura 1) serão fornecidas pelas tecnologias emergentes do IAM.

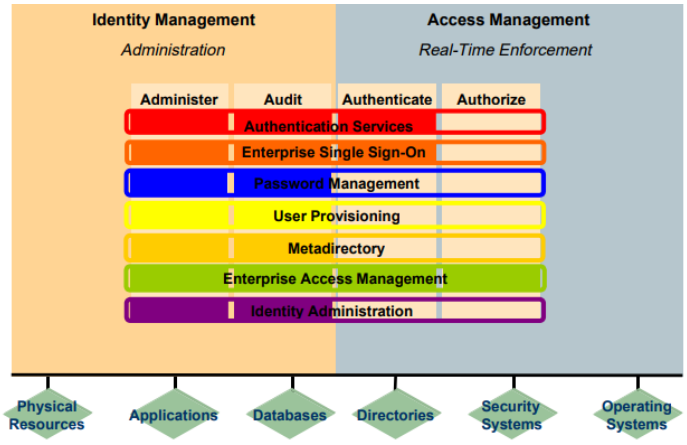

Figura 1 User Identities, Transactions, Roles, Policies and Privileges

2 Levantamento e análise dos Requisitos

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 1	Instalação de máquina virtual Linux(Centos 7) ligada á Cloud(Digital Ocean)	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 2	Instalação de pacotes de pré-requesitos	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 3	Atualizar os serviços hosts	Alta	Intergral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 4	Instalação da DataBase(MariaDB)	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 5	Instalação do OpenIAM via docker	Alta	Não implementado

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 6	Instalação do OpenIAM via RPM(solução á não implementação do requisito funcional 5)	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 6	Iniciar os serviços do OpenIAM	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 7	Efetuar login no OpenIAM pela primeira vez	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 8	Alterar a password padrão	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 9	Efetuar Auto-Registo	Alta	Parcial

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 10	Alterar a password padrão	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 11	Personalizar a página de boas-vindas pré definida	Media	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 12	Personalizar a página de informações	Media	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 13	Personalizar a exibição do cabeçalho de pesquisa	Media	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 14	Alterar senha	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 15	Alterar senha para um sistema gerido	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 17	Revogar o acesso dos funcionários	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 18	Gerir utilizadores	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 19	Criando um novo utilizador	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 20	Editar um utilizador	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 21	Definir o estado do utilizador	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 22	Definir direitos do menu para o utilizador	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 23	Adicionar direitos para um utilizador	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 24	Remover direitos para um utilizador	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 25	Ressincronizando senhas	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 26	Revogar tokens do OAuth 2.0	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 27	Definindo campos para configurar conectores	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 28	Modificar conectores predefinidos	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 29	Criar uma política de atributo	Media	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 30	Desenvolver uma Política de Atributos	Media	Parcial

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 31	Criar um sistema gerenciado	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 32	Incluir atributos para o sistema gerenciado	Alta	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 33	Definir mapas de política para a inserção nos sitemas de destino	Media	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 34	Implementar conectores remotos(Ldap, remote DataBase)	Media	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 35	Criar uma política de atributo	Media	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 36	Criar organização (ULHT)	Media	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 37	Criar grupos (Alunos e Professores)	Media	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 38	Criar Menus diferentes para cada grupo	Media	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 39	Gerir os direitos dos utilizadores para cada grupo	Media	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 40	Alterar icons dos menus do grupo	Media	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 41	Criar submenus para cada Menu de cada grupo	Media	Integral

Referencia	Descrição	Prioridade	Cumprimento
Requisito funcional 42	Inserção e atualização de utilizadores nos sistemas de destino(OpenLdap e DB na máquina virtual)	Media	Integral

Foram melhorados alguns dos requisitos funcionais já implementados, a maior parte dos requisitos foram implementados permitindo o melhoramento da própria plataforma sendo que os requisitos não implementados ou apenas parcialmente cumpridos são requisitos de menor importância que não teriam grande impacto a utilização da plataforma ou até não faziam sentido num âmbito da plataforma sendo esta voltada para a faculdade.

3 Viabilidade e Pertinência

No meu ver o projeto em si apresenta um grande nível de viabilidade após a conclusão do TFC e não apenas como projeto académico devido para alem de ser um tema de grande relevância para o funcionamento e gestão de qualquer empresa nos dias que correm, os sistemas de gestão de identidade e acesso podem aumentar a produtividade dos negócios. Os recursos de gestão central dos sistemas podem reduzir a complexidade e o custo e proteger as credenciais e o acesso do utilizador. Ao mesmo tempo, os sistemas de gestão de identidade permitem que os funcionários sejam mais produtivos (mantendo-se seguros) numa variedade de ambientes, trabalhando em casa, no escritório ou no trânsito. Um sistema IAM completo pode adicionar uma camada importante de proteção, garantindo uma aplicação consistente de regras e políticas de acesso do utilizador numa organização. Mais empresas estão a oferecer mais componentes de IAM porque as atividades dos mercados do IAM são relacionadas com a gestão do acesso dos utilizadores, e as empresas querem para gerir o acesso dos utilizadores a partir de uma instalação comum e integrada. A implementação da gestão de identidade e acesso e das práticas recomendadas associadas pode oferecer uma vantagem competitiva significativa de várias maneiras e feito da maneira correta pode ser um catalisador essencial na construção de negócios bem-sucedidos na era da transformação digital. O IAM atende às necessidades de missão crítica para garantir acesso adequado aos recursos em ambientes de tecnologia cada vez mais heterogêneos e para atender a requisitos de conformidade cada vez mais rigorosos. Atualmente, a maioria das empresas precisa conceder aos utilizadores fora da organização acesso a sistemas internos. Abrir a sua rede para clientes, parceiros, fornecedores, contratados e, é claro, funcionários pode aumentar a eficiência e reduzir os custos operacionais. Os sistemas de gestão de identidade podem permitir que uma empresa estenda o acesso aos seus sistemas de informações numa variedade de aplicativos locais, aplicativos móveis e ferramentas SaaS sem comprometer a segurança. Ao fornecer maior acesso a pessoas de fora, pode impulsionar a colaboração em toda a organização, aumentando a produtividade, a satisfação dos funcionários, a pesquisa e desenvolvimento e, finalmente, a receita. Os sistemas IAM pode reforçar a conformidade regulamentar, fornecendo as ferramentas para implementar políticas abrangentes de segurança, auditoria e acesso. Muitos sistemas agora fornecem recursos projetados para garantir que uma organização esteja em conformidade. As Plataforma de Gestão de Identidades e Acessos tão em crescimento para empresas de todos os tamanhos e indústrias. Saber com que produto começar e terminar na implementação geral, e porquê de poder ajudar a reduzir o investimento em fornecer-lhe uma infraestrutura segura de controlo de acessos.

4 Solução Desenvolvida

4.1 Tecnologias Fundamentais e Processos

Uma solução abrangente para a gestão da identidade (IDM) é crucial para o uso eficaz e seguro das identidades digitais nas transações e outras atividades realizadas no mundo cibernético. IDM inclui todas as atividades relacionadas com a gestão de identidades digitais, nomeadamente o estabelecimento, gestão, uso e revogação de identidades. Como na maioria dos casos, estas atividades envolvem múltiplas partes de diferentes domínios de administração com diferentes requisitos, IDM tem que combinar diferentes tecnologias, processos, procedimentos e políticas. Normalmente não existe um sistema único capaz de suportar todas as funções do IDM e, como tal, as soluções IDM são muitas vezes soluções integradoras; ou seja, resultam da integração de diferentes sistemas e técnicas. Embora existam muitas abordagens diferentes à gestão da identidade, ela envolve essencialmente dois processos fundamentais: o processo de identificação de uma pessoa e a emissão de uma credencial de identidade para refletir essa identidade ("identificação"), e o processo de verificação posterior de que uma determinada pessoa que apresenta essa credencial e afirma ser essa pessoa previamente identificada é, de facto, essa pessoa ("autenticação").

Uma vez que a identidade de um indivíduo é autenticada com sucesso, um terceiro processo, referido como "autorização", é usado pelo negócio que depende da identidade autenticada para determinar que direitos e privilégios são concedidos a essa pessoa - por exemplo, se essa pessoa deve ter acesso a um website, a um banco de dados, a um bar, a um aeroporto área de embarque, etc. Uma credencial é normalmente um conjunto de atributos de identidade e afirmações sobre um assunto específico emitidas por um fornecedor de identidade, referido como emissor de credenciais. O emissor é crucial para uma parte confiável na decisão de aceitar ou não uma credencial fornecida por um sujeito, como o emissor atesta a integridade e possivelmente a validade do conteúdo da credencial. Note que, neste contexto, integridade refere-se à garantia de que a credencial não foi adulterada; como tal, técnicas como assinaturas digitais e infraestruturas PKI podem ser usadas para garantia de integridade.

A validade é um requisito mais difícil na medida em que exige que o que é afirmado na credencial seja verdadeiro; ou seja, que tenha sido submetido a um processo de garantia. Como diferentes processos de garantia podem ser adotados por diferentes provedores de identidade, dependendo também do conteúdo e propósito das credenciais, uma credencial pode conter informações, chamadas de nível de garantia, transmitindo indicações sobre o processo de garantia específico adotado na emissão da credencial. Os sujeitos também podem emitir credenciais que podem ser úteis em muitos casos. Por exemplo, um utilizador pode usar essa credencial para indicar seus hobbies num Web site. Portanto, de acordo com , podemos classificar as credenciais nos seguintes tipos: • Credencial validada: assinada digitalmente após a validação da credencial; • Credencial autenticada: assinada digitalmente, mas não validada; • Credencial em bruto: assinada digitalmente pelo próprio sujeito e não é validada. Outra classificação interessante de credenciais é feita pelo NIST . Esta classificação foi concebida para credenciais físicas, tais como

passaportes e cartas de condução. No entanto, é interessante no nosso contexto porque identifica claramente propósitos e requisitos para diferentes classes de credenciais. À medida que a tecnologia e sua aplicação evoluem, a criação das contrapartidas eletrônicas destas credenciais exigirá determinar como estes propósitos e requisitos podem ser abordados no mundo cibernético. Um requisito importante ao utilizar tais certificados é a capacidade de verificar a assinatura digital do emissor, a fim de determinar a integridade dos certificados. Tal requisito é abordado pela Infraestrutura de Chave Pública (PKI), uma infraestrutura (distribuída) que fornece as funções e os serviços necessários para suportar a vida útil dos certificados de chave pública e a sua utilização .A gestão dos certificados de chave pública envolve vários processos e funções. A noção de certificado de atributo, que é uma abordagem para implementar credenciais de identidade, é muito semelhante à noção de certificado de chave pública - a principal diferença é que o primeiro pode codificar uma grande variedade de atributos de identidade, em vez de apenas chaves públicas. Single sign-on (SSO) refere-se ao uso do mesmo nome de login para se conectar a vários sistemas dentro da mesma empresa, conhecido como SSO empresarial (ESSO); ou através de várias empresas, conhecido como SSO multi-domínio; ou mesmo através da Web para clientes interagindo através de navegadores com aplicativos baseados na Web, conhecido como SSO baseado na Web. Além disso, um sistema baseado em SSO permite que um sujeito entre com suas credenciais apenas uma vez dentro de uma sessão e acesso a múltiplos recursos e serviços sem ter que ser solicitado a autenticação novamente. Como tal, o SSO é útil para reduzir os custos administrativos da conta de gestão. O IAM como prática de segurança é uma tarefa crucial para qualquer empresa. Está cada vez mais alinhado aos negócios e, além de conhecimentos técnicos, requer habilidades de negócios. Existem vários componentes num sistema IAM: provisionamento (ou integração), gestão de contas, controlo de identidades, identificação (ou autenticação), controlo de acesso (ou autorização) e associação de identidades.

O IAM é uma área ampla, portanto, esses componentes podem ser divididos em subcomponentes específicos. Por exemplo, apenas o provisionamento se concentra no provisionamento de entrada / saída de contas do utilizador, provisionamento just-in-time, fluxos de trabalho de aprovação, enquanto a gestão de contas fala sobre gestão de contas privilegiadas, gestão de credenciais, gestão dos utilizadores / grupos / funções. O Identity Manager permite que se faça as seguintes atividades: • Controlo do fluxo de dados entre os sistemas conectados. • Determinar quais dados são compartilhados, qual dos sistemas é a fonte autorizada para um dado, e como os dados são interpretados e transformados para atender aos requisitos de outros sistemas. 20 Também incluído como parte da administração atividades é a capacidade de abstrair e correlacionar automaticamente dados de HR, gestão de relacionamento com clientes e email sistemas (e outras "lojas de identidade"), e dos sistemas geridos. A realização é feita de várias maneiras tais como: - Em resposta a uma solicitação de self-service - por exemplo, o self-registration. - Uma solicitação de line management - por exemplo, o gerente tem um novo funcionário que começa a trabalhar em determinada data ou um utilizador precisa ter acesso a uma aplicação - Uma mudança em um sistema de HR - por exemplo, rescisão do contrato de trabalho . Uma carga para efeitos de uma nova aplicação ou fusão/aquisição. Estas atividades devem ser monitoradas para fins regulatórios e investigativos(reports)

4.2 Arquitetura

4.2.1 Introdução

A arquitetura de software recebeu atenção crescente como um importante subcampo de engenharia de software. A definição de uma arquitetura de software correta é um fator de sucesso para o design e desenvolvimento de sistemas. Uma boa arquitetura de software pode ajudar a garantir que um sistema satisfaça os requisitos essenciais em áreas como desempenho, confiabilidade, portabilidade, escalabilidade e interoperabilidade. No entanto, se a arquitetura não for bem definida, pode ser ineficiente, e em último recurso desastrosa para o projeto.

OpenIAM apresenta uma arquitetura unificada. Forte integração com AD, Exchange, Google e Office365.

A integração da gestão de utilizadores é a consolidação dos dados do utilizador e da autorização em vários sistemas num repositório centralizado de utilizadores. Todos os dados da gestão de utilizadores são mantidos centralizados num único sistema.

Isso pode ajudar a facilitar a administração do utilizador, mas também reduzir redundâncias de dados e sobrecargas de gestão, aumentar a transparência e melhorar a privacidade da segurança.

A sincronização Lightweight Directory Access Protocol (LDAP) integra dados de gestão de utilizadores de vários sistemas (SAP e não SAP) num sistema SAP Web AS ABAP.

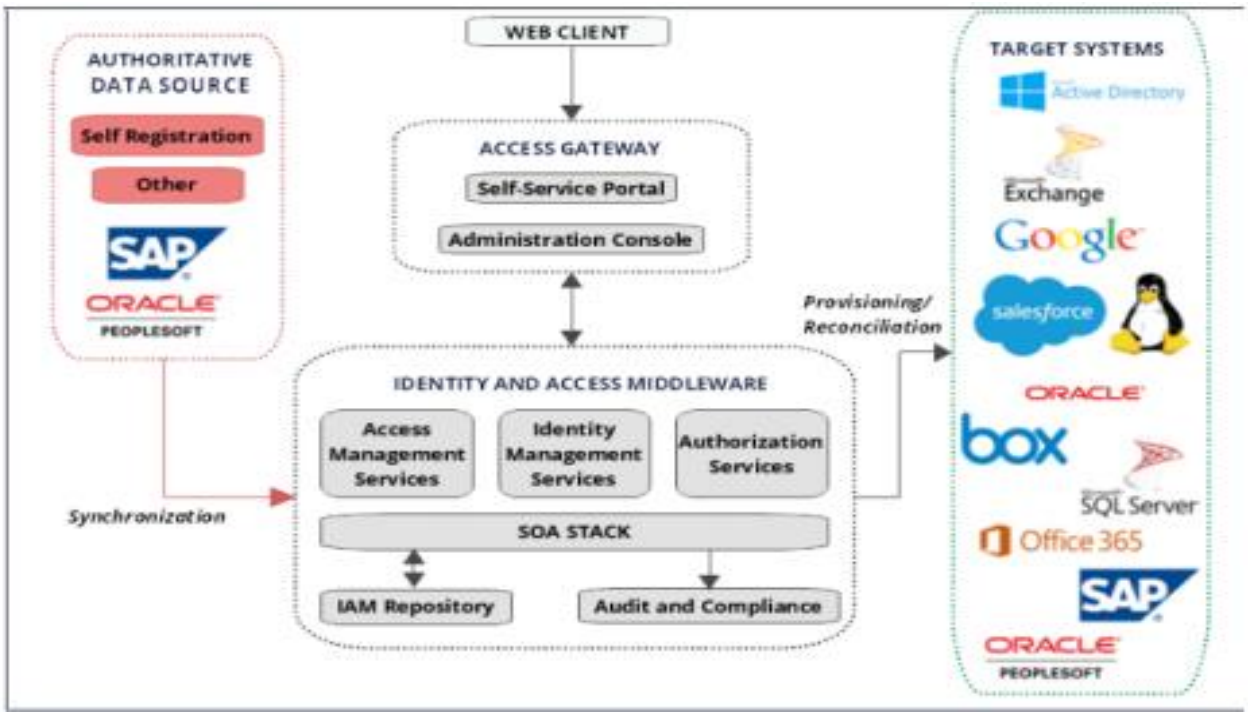

Figura 2 Arquitetura

4.2.2 Utilizadores

Os utilizadores apenas podem ser criados pelo administrador ou em caso de haver a possibilidade de um "Sefl-Registration" essa aprovação apenas podes ser feita pelo administrador.

Sempre que um utilizador é criado ou aprovado não quer dizer que esteja ativo, isto é, pode ser necessário(se assim for implementado) a necessidade de efetuar um primeiro login na plataforma para se proceda assim, automaticamente, á sua ativação no sistema este tipo de abordagem foi inserido na plataforma, mas podendo ser opcional conforme como é pensado. O administrador pode ser alterar as credenciais deste utilizador sempre que necessário ou o próprio utilizador pode fazê-lo sendo por vezes necessário a verificação e aceitação do administrador dependendo da informação que estejam a ser alterada.

4.2.2.1 Credenciais

O administrador tem acesso a um menu onde é possível criar utilizadores onde apresenta credenciais "gerais" como o First Name, Last Name e se for um aluno também o Número de aluno(ver Figura 3).

Figura 3 Credenciais Básicas

A seguir temos uma página onde podemos introduzir informação mais detalhada como o estado do utilizador, temos também o First Name, Last Name caso não tenha sido inserido na página anterior, temos outros campos em relação ao nome, temos o género(Masculino ou Feminino), a data de nascimento, a fotografia do utilizador, entre outros(ver Figura 4)

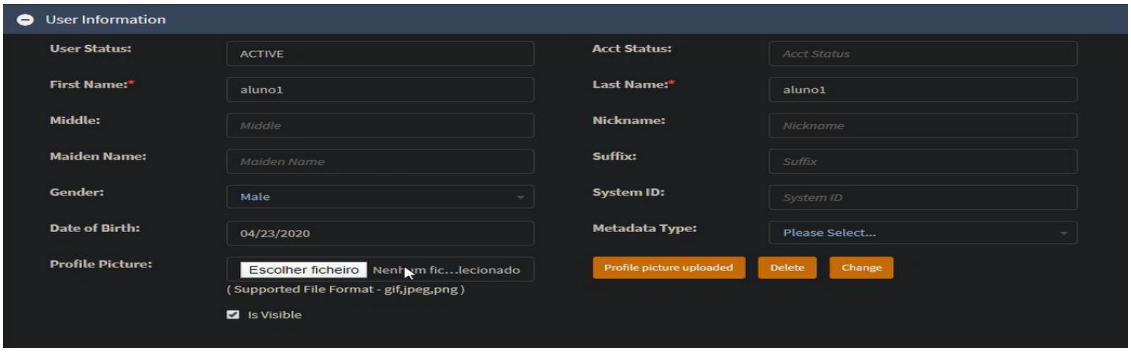

Figura 4 User Information

Temos também outras informações relevantes como o email, contactos(email e numero de telemóvel) e em relação a organização(ULHT) temos a start date e a end date (ver Figura 5) que podem ser especialmente importantes para a gestão de acessos onde isto fara com que aquele utilizador só tenha acesso a plataforma a partir do start date que introduzirmos(ver figura 6) e deixe de ter acesso a plataforma a partir da data introduzida no end date sendo que estas credenciais podem ser sempre alteradas caso necessário sobretudo o end date, como por exemplo no caso de um aluno a fazer uma licenciatura(3 anos) o end date poderá ser a data atual mas somando os 3 anos isto fara com que a conta depois de completar estes 3 anos seja bloqueada(não sendo eliminada porque pode ser utilizada mais tarde, noutra ocasião por exemplo se o aluno mais tarde volte a faculdade para completar o mestrado, etc) mas caso o aluno por algum motivo demore mais que estes 3 anos esta credencial tem de ser alterada para evitar assim o bloqueio da conta.

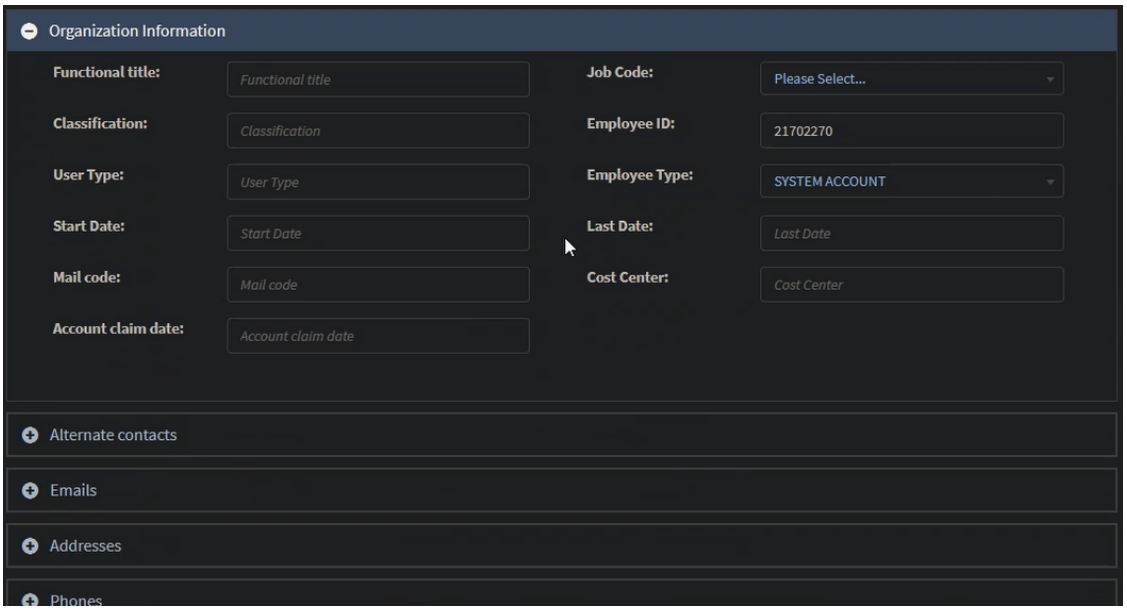

Figura 5 Organization Information

Figura 6 Peding Start Date

4.2.2.2 Direitos do utilizador

Direitos é a funcionalidade para conceder acesso aos utilizadores apropriados. A arquitetura de direitos do OpenIAM é um gráfico multicamada e hierárquico(ver Figura 7) entre utilizadores, grupos, funções e recursos. Um utilizador pode ser um membro direto ou indireto de um grupo ou função e pode ter, direta ou indiretamente, direito a um recurso. Esse é o mecanismo de direitos e está no centro da arquitetura do OpenIAM . A gestão de direitos garante que o acesso seja concedido apenas aos utilizadores

apropriados. Esse recurso utiliza componentes de provisionamento e gestão de função. Os direitos são usados, por exemplo, para autorizar utilizadores, grupos ou funções ao provedor de serviços. Isso concede a todos os membros a hierarquia de membros para o logon único (SSO) neste aplicativo.

Os cenários possíveis para o direito centrado no utilizador são os seguintes:

-Um utilizador pode ser membro de um ou vários grupos. Um utilizador também é um membro indireto de todos os grupos, funções e recursos associados a um determinado grupo.

-Um utilizador pode ser um membro de uma ou várias funções. Um utilizador também é um membro indireto de todas as funções e recursos associados a uma determinada função.

-Um utilizador pode ter direito a um ou vários recursos. Um utilizador também é um membro indireto de todos os recursos associados a um determinado recurso.

Embora o princípio hereditário se aplique a todas as entidades acima, só é possível verificar se um utilizador é membro de um grupo ou função ou se tem direito a um recurso. O sistema não faz distinção entre associação direta e indireta. Um relacionamento indireto é tão válido quanto um relacionamento direto.

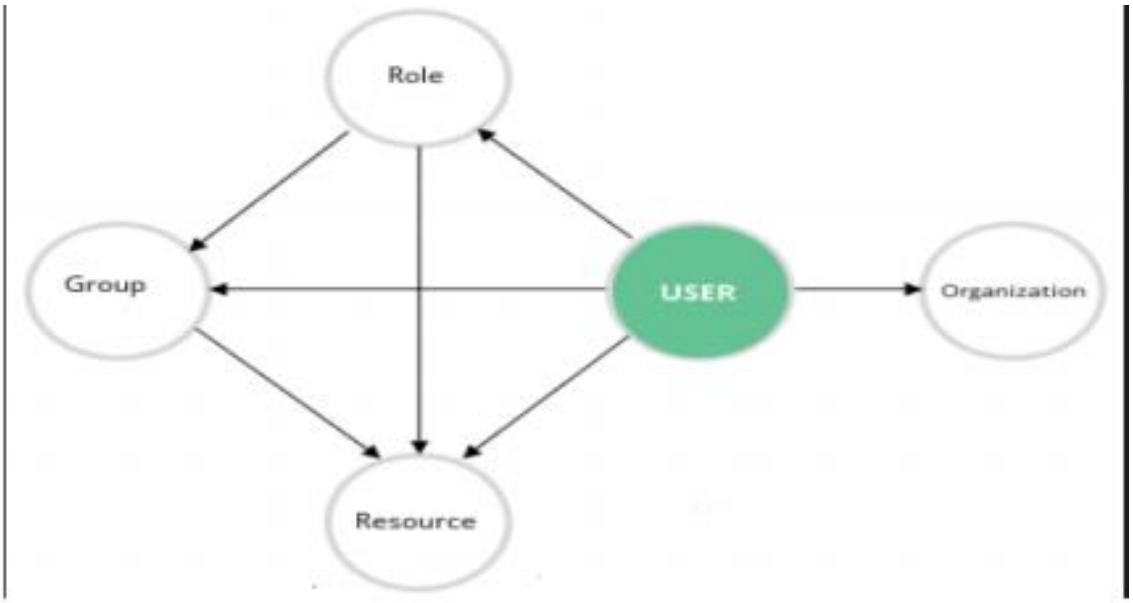

Figura 7 Arquitetura de direitos

4.2.2.3 Gestão de acessos a menus para o utilizador

O administrador pode conceder ou remover direitos de acesso a menus no aplicativo Web para um utilizador existente usando o recurso de direitos ao menu. Esses direitos garantem que o utilizado tenha direitos de acesso a um menu especificado, isto é garantir que o

utilizador tem apenas acesso aquilo que é fundamental e necessário não dando a possibilidade de ter mais acessos daqueles devia sendo isto uma regra fundamental para a criação deste tipo de plataformas como já foi referido em capítulos anteriores.

Os direitos de menu são classificados como não autorizados, menus públicos, explicitamente autorizados, implicitamente ou uma combinação de menus públicos, explicitamente autorizados e implicitamente, conforme mostrado na figura abaixo:

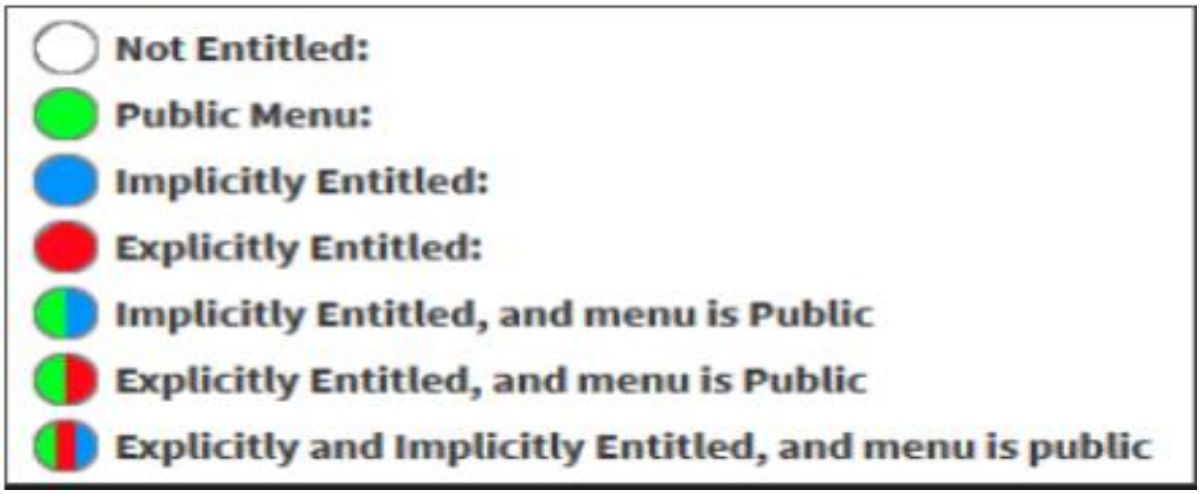

Figura 8 Direitos de Menu

Onde os importantes a reter são:

“Not entitled” são os menus aos quais um utilizador não tem acesso concedido

“Public menus” estão disponíveis para todos os utilizadores(são os menus normalmente que todo o tipo de utilizadores podem ter acesso quando se pensa numa plataforma de gestão de acessos com um menu referente a visualização dos seus próprios dados ou edição dos mesmo). Todos os utilizadores recém-criados têm acesso a esses menus por padrão(menus públicos). No entanto estes menus podem ser sempre configurados sempre que se achar que não pode ser mais publico por exemplo quando se cria um novo tipo de utilizadores e estes não podem ter acesso a esses menus.

“Explicit entitlements” são direitos de acesso concedidos explícita e diretamente a um utilizador. Os direitos explícitos são geridos a partir dos direitos do Menu para a página do utilizador.

“Implicit entitlements” Estes direitos de acesso são concedidos indiretamente ao utilizador por meio de associação de função, grupo ou organização.

A atribuição explícita de um item de menu pode não conceder acesso implícito aos itens do submenu que estão na árvore do menu com direitos explícitos. O direito implícito depende da função do utilizador, grupo e associação à organização.

Em baixo está um exemplo de uma “Menu tree”, isto é, se da aos utilizadores os acessos que lhe devem ser devidamente atribuídos.

Figura 9 Menu Tree

4.2.2.4 Importância da criação de grupos

Um grupo é um conjunto de utilizador, sistemas ou outros grupos aos quais podem ser concedidas coletivamente permissões de acesso. Os direitos de acesso concedidos a um grupo são aplicados a todas as entidades dentro do grupo. Grupos são geralmente usados para modelar a estrutura organizacional. Os grupos podem ter uma hierarquia (grupos filho ou pai) e podem ser atribuídos a organizações. Um grupo pode ser vinculado a um tipo de metadados, um sistema gerenciado e um recurso de administrador.

Um grupo pode ter uma ou várias funções filhas. Um grupo herda todos os direitos diretos e indiretos das funções filho.

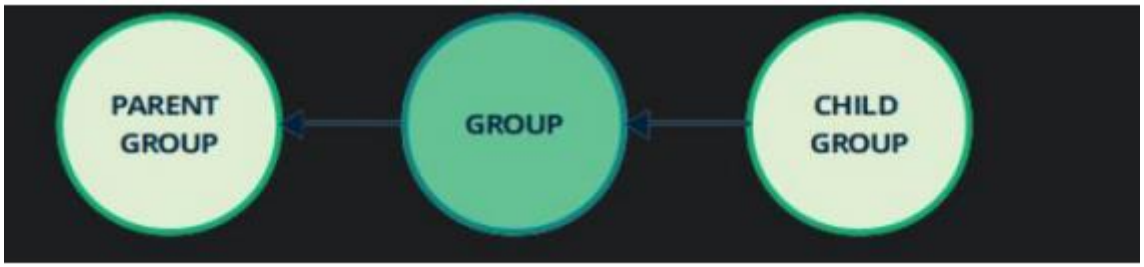

Figura 10 Arquitetura grupos

Mas porque a criação de grupos pode ser importante para gerir acessos? A resposta é simples, vamos imaginar o caso concreto da faculdade onde todos os anos entram milhares de alunos, o tempo perdido a dar acessos individuais a cada um destes alunos seria imenso e para alem disso poderia dar azos a enganos podendo haver alunos com mais permissões que outros o que do ponto de vista da Gestão de acessos seria completamente errado então se criarmos grupos, na criação de um novo aluno bastava introduzi-lo logo nesse grupo e adquiria o acesso(indireto) aos menus daquele grupo havendo assim uma homogeneização de todos os alunos diminuindo a possibilidade de

haver alunos com mais permissões que outros, sendo que apenas herdavam acessos do grupo e estando todos no mesmo grupo a possibilidade de isto acontecer era mínima para não dizer impossível no entanto os alunos deixariam de ter acessos diretos(Explicit entitlements), isto seria um problema? A resposta seria não, sendo que o sistema não faz distinção de acessos diretos de acessos indiretos sendo um acesso indireto tão valido como um acesso direto, não iria haver nenhum impacto para a plataforma e o modo como gere os acessos, apenas traz benefícios.

4.2.3 Autenticação/Login

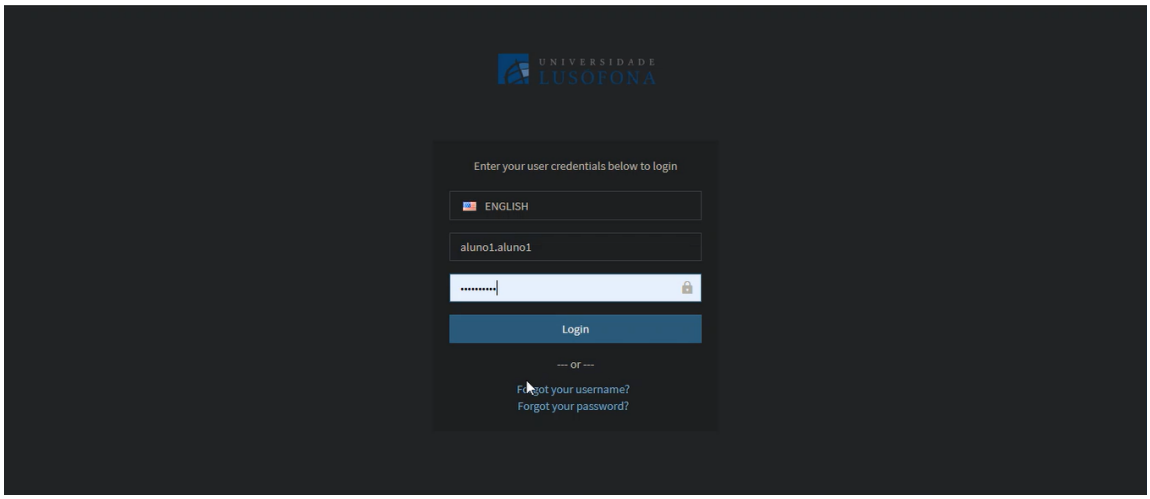

Figura 11 Login

Autenticação é o método de validação da identidade genuína de um utilizador. Um utilizador é autenticado usando uma política de autenticação, que é um conjunto de condições que devem ser cumpridas antes que o utilizador o tenha acesso ao sistema. Um provedor de autenticação implementa um protocolo para verificar uma identidade que deseja se conectar a um sistema.

Um utilizador precisa ser autenticado apenas uma vez (logon único (SSO)) e transmitir um token de segurança. Um provedor de autenticação verifica um token de segurança como uma alternativa para autenticar explicitamente um utilizador num domínio de segurança.

O OpenIAM suporta vários tipos de provedores de autenticação como o do Facebook, Google, SAML.

Neste caso o utilizado foi o Cliente OAuth ,sendo esta utilizado para a integração com outras aplicações, que permite usar o padrão aberto OAuth 2.0 para executar a autenticação do utilizador.

O OAuth é uma estrutura de autorização que permite que os aplicativos obtenham acesso limitado às contas dos utilizadores num serviço HTTP. Funciona delegando a

autenticação de utilizadores ao serviço que hospeda a conta do próprio utilizador, e autorizando aplicações de terceiros a aceder a conta do utilizador. O OAuth 2 fornece fluxo de autorização para aplicações web e desktop, e para dispositivos móveis

O cliente é a aplicação que quer aceder a conta do utilizador. Antes de fazer isso, deve ser autorizada pelo utilizador, e a autorização deve ser validada pela API

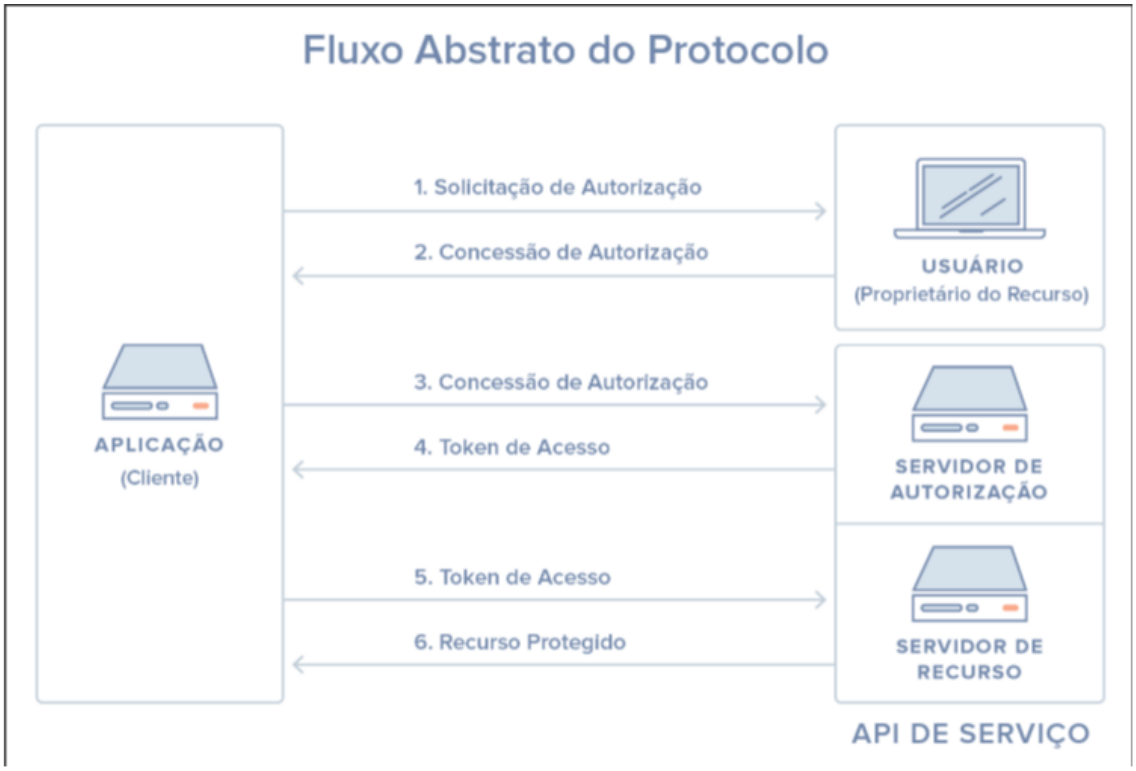

Figura 12 OAuth Geral

-A aplicação solicita autorização para aceder recursos do serviço do utilizador

-Se o utilizador autorizar a solicitação, a aplicação recebe uma concessão de autorização

-A aplicação solicita um token de acesso ao servidor de autorização (API) através da autenticação de sua própria identidade, e da concessão de autorização

-Se a identidade da aplicação está autenticada e a concessão de autorização for válida, o servidor de autorização (API) emite um token de acesso para a aplicação. A autorização está completa.

-A aplicação solicita o recurso ao servidor de recursos (API) e apresenta o token de acesso para autenticação

-Se o token de acesso é válido, o servidor de recurso (API) fornece o recurso para a aplicação

O fluxo real desse processo será diferente dependendo do tipo de concessão de autorização em uso, mas essa é a ideia geral.

No caso específico do OpenIAm o tipo de concessão é o Código de autorização que é o é o mais comumente usado porque é otimizado para aplicações do lado servidor, onde o código fonte não é publicamente exposto, e a confidencialidade do Segredo do Cliente pode ser mantida. Este é um fluxo baseado em redireccionamento, o que significa que a aplicação deve ser capaz de interagir com o agente do utilizador (i.e. o navegador web do utilizador) e receber códigos de autorização da API que são roteados através do agente do utilizador.

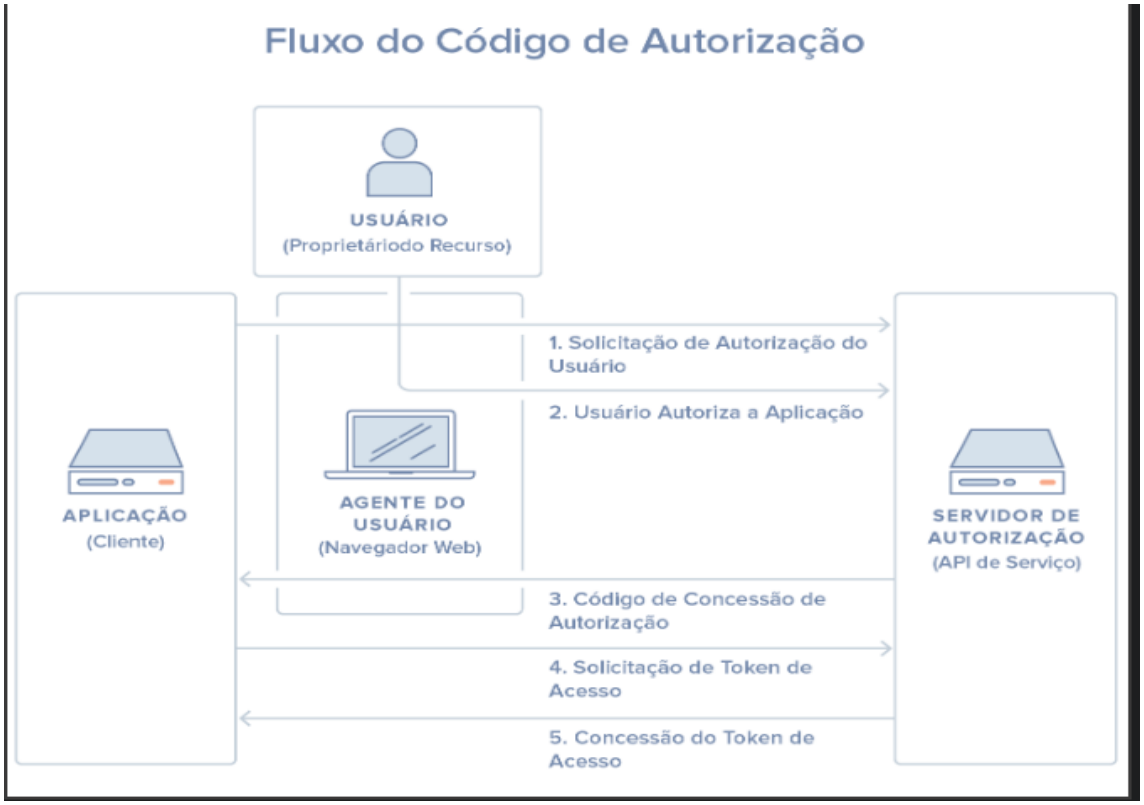

Figura 13 OAuth codigo de autorização

Onde o utilizador, primeiramente, recebe um link de código de autorização que é o seguinte:

http://206.189.27.237:8080/idp/oauth2/token/authorize

Em seguida o utilizador clica no link, deve primeiro fazer login no serviço, para autenticar a sua identidade (a menos que ele já esteja logado). Em seguida será solicitado pelo serviço a autorizar ou negar o acesso da aplicação à sua conta.

Se o utilizador clica em “Authorize Application”, o serviço redireciona o agente do utilizador para a URI de redireccionamento da aplicação, que foi especificada durante o registo do ciente, juntamente com um código de autorização.

A aplicação solicita um token de acesso da API, passando o código de autorização juntamente com detalhes de autenticação, incluindo o segredo do cliente, para o endpoint de token da API.

Se a autorização é válida, a API irá enviar uma resposta contendo o token de acesso (e opcionalmente, um token de atualização) para a aplicação.

Onde a reposta seria algo como isto:


```
{
"expired": false,
"client_id": "92BF26DD50D748668730F7639C4A0D3D",
"user_id": "3000",
"access_token": "Lf_Sc-YeKHB8rsGfiGcLMKJOxbTGmpbdYs5wK3i7ZhINrjJlTOHEuV-phwJ1wE7.MjWqDcx8Lpri",
"expires_in": 1709,
"expires_on": 1531332707193,
"scopes": [
{
"scopeId": "c42a190a6488010b01648810b83a005a",
"name": "dev1 - /idp/oauth2/token/info"
},
{
"scopeId": "c42a190a6488010b01648810bdfd0096",
"name": "dev1 - /idp/rest/api/*"
},
{
"scopeId": "c42a190a6488010b01648810be2a0098",
"name": "dev1 - /webconsole/rest/api/*"
},
{
"scopeId": "c42a190a6488010b01648810be6d009b",
"name": "dev1 - /selfservice/rest/api/*"
},
{
"scopeId": "c42a190a6488010b01648810be96009d",
"name": "dev1 - /selfservice-ext/rest/api/*"
},
{
"scopeId": "c42a190a6488010b01648810bebf009f",
"name": "dev1 - /webconsole-idm/rest/api/*"
```


Assim a aplicação está autorizada! Pode usar o token para aceder a conta do utilizador através da API do serviço, limitada ao scope de acesso, até que o token expire ou seja revogado. Se um token de atualização foi emitido, ele poderá ser utilizado para solicitar um novo token de acesso se o token original expirou.

Depois que um token de acesso expira, utilizá-lo para realizar uma solicitação irá resultar em um erro “Token Inválido”. Nesse ponto, se um token de atualização foi incluído quando o token de acesso original foi emitido, ele pode ser usado para solicitar um token de acesso renovado do servidor de autorização.

Esta tipo de autenticação é especialmente importante quando queremos integrar a nossa plataforma com outros serviços externos que não pertençam ao próprio sistema o a outros sistemas que pertençam a faculdade como por exemplo usar a conta da plataforma para se registar num sistema que disponibiliza cursos que tenham parceria com a faculdade permitindo assim o acesso aos dados do utilizador em questão limitado pelo scope que queiramos tendo por exemplo apenas acesso a dados do como o nome completo, email, numero de aluno, etc .

Em relação ao login na própria plataforma é feita através da política de senha default do próprio Sistema onde ´necessário o username do utilizador e a sua password no entanto o

Sistema não verifica apenas estas credenciais também verificando o estado da conta do utilizador para perceber se a conta se encontra ativa ou bloqueada podendo assim revogar o acesso á plataforma a utilizadores que já não devem ter acessos a mesma, caso a conta se encontra bloqueada ira mostrar um aviso. Outro facto importante e relacionando com o descrito em cima em relação á integração da plataforma com outras aplicações usando o sistema de autorização OAuth a partir do momento em que uma conta é bloqueada todos esses tokens são revogados impedindo assim a utilização da conta na própria plataforma, mas também o acesso dessa conta bloqueada noutras aplicações.

Caso seja a primeira vez que o utilizador entra na conta ira aparecer uma pagina chamada de IT Use Policy onde só é possível avançar caso o utilizador em questão aceite os termos da mesma(ver figura 14).No entanto existe outro pormenor interessante em relação ao aparecimento deste IT use Policy que é que sempre que é alterado aparecesse outra vez que os utilizadores fizerem login outra vez no sistema mantendo-se assim sempre informados sobre os termos e condições da plataforma que estão a aceder, estes termos e condições são os mesmo que estão no site da Lusófona apenas traduzidos para inglês .

Figura 14 IT Use Policy

4.2.4 Sistemas Gerenciados

A configuração de sistemas gerenciados faz parte do processo de provisionamento, que é a criação e o gerenciamento sincronizados do utilizador durante seu ciclo de vida em diferentes sistemas. A solução do controlo de identidade OpenIAM automatiza essa tarefa de gerir identidades em vários dispositivos e aplicativos usados. O processo de provisionamento consiste em integrar aplicativos de identidade e utilizador de terceiros usando conectores, configurar sistemas gerenciados, configurar o mapeamento de políticas de atributos para definir como os atributos no gerador de identidades são mapeados para os atributos em um sistema gerenciado e reconciliar alterações de dados em um sistema de destino para atualizar o OpenIAM.

Para isto existe a Synchronization(sincronização) que permite sincronizar dados de uma ou mais fontes autorizadas para um conjunto de sistemas gerenciados. A configuração de

sincronização permite monitorar mudanças no sistema de origem e, em seguida, atualizar os sistemas de destino em intervalos periódicos agendados(Batch tasks)

Por exemplo, pode se sincronizar as informações dos alunos. As informações do aluno no sistema podem conter dados para especificar itens, como número do aluno e nome. O OpenIAM permite desenvolver scripts, descritos mais adiante nesta seção, que capturam regras de negócios para tomar decisões de sincronização com base nesses atributos. Com base nessas regras definidas, o OpenIAM o gestor de identidades pode provisionar utilizadores apenas nos sistemas aos quais eles precisam aceder. Além disso, pode -se definir com que frequência esses scripts são executados usando o Cron ou definindo uma data exata para a sincronização executar. Isso permite que a monitorização ativa do sistema em busca de alterações e publicar essas alterações nos sistemas de destino, conforme apropriado. Portanto, pode-se provisionar um novo utilizador no sistema de destino ou desabilitar um utilizador quase em tempo real.

O principal objetivo da regra customizada para script correspondente é localizar e retornar um utilizador correspondente usando algum valor de atributo proveniente do sistema de destino. A regra personalizada para correspondência pode ser usada, por exemplo, se os dados forem salvos em diferentes formas para utilizadores no sistema de destino e no OpenIAM . A figura abaixo mostra um exemplo quando o formato de identidade principal do utilizador (primaryIdentity) no OpenIAM é igual do formato de identidade do utilizador (uid) no LDAP. Portanto, podemos corresponder pela identidade do utilizador Neste exemplo, a correspondência pode ser feita usando o campo uid(que é basicamente o “FirstName”.”LastName”, que tem o mesmo formato que o primaryIdentity campo no OpenIAM .

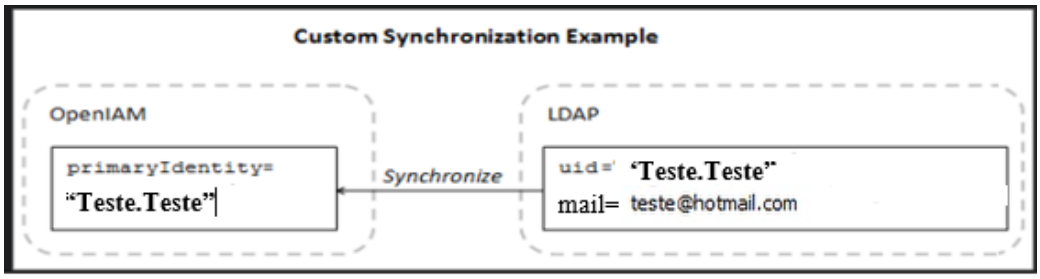

Figura 15 Ldap syncronization

No caso específico da sincronização para outros sistemas foi usado o Ldap e o OpenLdap(é um software OpenSource que implementa o protocolo LDAP) toda esta sincronização é feita sempre que existe uma inserção de um novo utilizador(aluno ou professor) ou atualização dos mesmos quer seja feita pelo administrador quer seja pelo utilizador.

O Ldap vai funcionar basicamente como uma segunda base de dados que nos possibilita manter atualizados todos os sistemas sem que haja uma ligação direta entre eles sendo assim o sistema de destino que atualizara todos os outros Sistemas a ele ligados.

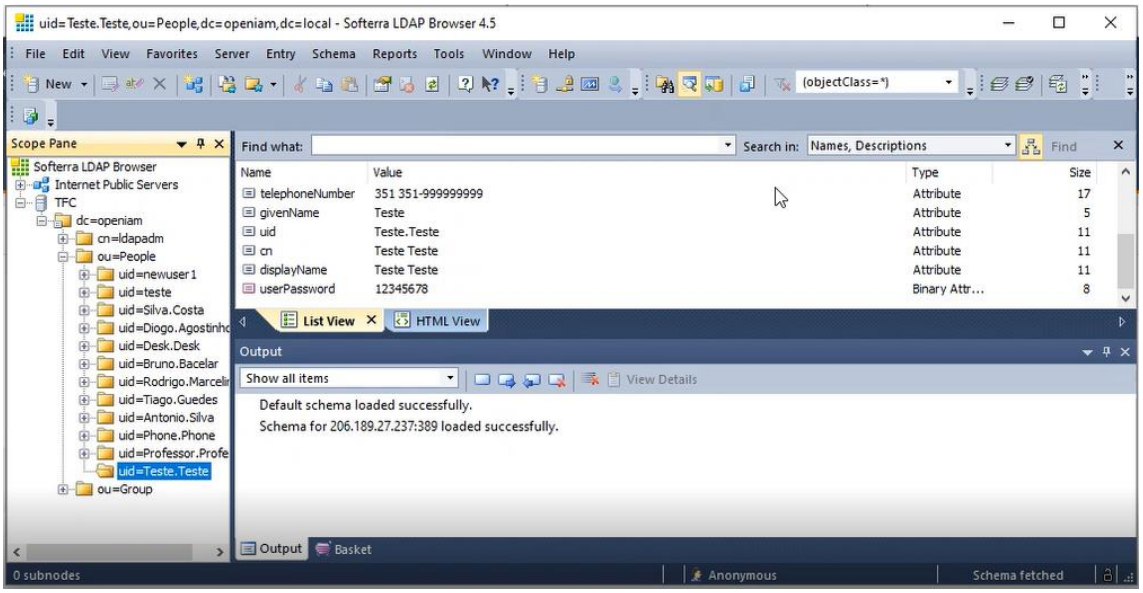

Figura 16 Ldap

Na implementação do OpenLdap temos de ter em atenção á inserção dos dados na base Ldap que será feita por meio de arquivos ldif (LDAP Data Interchange Format), um arquivo de texto comum que pode ser criado ou alterado com editores de texto convencionais, obedecendo-se, apenas, o schema do diretório.

Os schema basicamente são arquivos padrões .Sungaila (2008) afirma que “um esquema é um conjunto de regras que define atributos, classes de objetos, e controles indicando onde cada dado pode ser armazenado”. Já Malère (2008) explica um schema como sendo uma estrutura de objetos que especifica a lista total de atributos permitidos e necessários para uma entrada de dados no serviço de diretório. Os schemas permitem manter a consistência dos dados. Uma importante característica desses arquivos é serem extensíveis e assim pode-se adicionar mais atributos ou classes em função das necessidades. Para usar um schema é necessário incluí-lo no arquivo de configuração slapd.conf. Os schemas definem:

-quais as classes de objetos (object classes) podem ser inseridas num diretório; -quais os atributos de uma determinada classe de objetos;

-os valores possíveis para os atributos;

Se um objeto (entrada) não obedecer às regras do schema, ele não pode ser inserido no diretório. Portanto cada entrada estará condicionada a uma hierarquia de armazenamento dos dados na base LDAP. Isto é especificado através do Distinguished Name (DN).

As funções do arquivo ldif são:

-importar dados para o diretório

-alterar objetos existentes

-criar o backup do diretório

-replicação do diretório

Outra parte importante dos Sistemas gerenciados é em relacionada com a Reconciliation(reconciliação) que é usada para detetar ou monitorar alterações nos utilizadores no sistema de destino e atualizar o OpenIAM ou qualquer outro sistema. Essas alterações podem ser: criação, modificação ou exclusão de uma conta no sistema de destino. A reconciliação compara o conteúdo do índice da conta com o que cada recurso contém atualmente.

A reconciliação pode ser usada para preencher previamente a base de dados OpenIAM com utilizadores existentes.

O gestor de identidade do OpenIAM (IDM) é capaz de reconhecer várias situações de reconciliação, que podem ocorrer durante o processo de reconciliação:

-IDM (excluído) e sistema destino (existe) - o utilizador é excluído no IDM e existe no sistema de destino.

-IDM (existe) e sistema destino (existe) - o utilizador existe no IDM e existe no sistema de destino.

-IDM (existe) e sistema destino (não existe) – o utilizador existe no IDM e não existe no sistema de destino.

-IDM (não existe) e sistema destino (existe) - o utilizado não existe no IDM e existe no sistema de destino.

A resposta para as situações listadas acima pode ser uma das seguintes:

-Fazer nada

Adicionar registo ao IDM a partir do recurso - Cria um utilizador IDM a partir de uma entrada do sistema de destino. O mapeamento é fornecido por um script Groovy.

-Excluir do recurso - exclui a entrada do sistema de destino.

-Desativar (ou alterar o status no recurso) -Desativar (ou alterar o status no recurso)

-Excluir do IDM - exclui a identidade de um utilizador para o sistema de destino

-Remover do IDM

-Desativar (ou alterar o status no IDM)

-Adicionar registo ao recurso do IDM - Cria uma entrada no sistema de destino com os dados fornecidos pelo utilizador do IDM. O mesmo mapeamento usado no provisionamento é usado.

-Atualizar IDM do recurso

-Atualizar recurso do IDM - fornece a capacidade de mesclar os dados do sistema de destino e do IDM usando um script Groovy. Todos os dados do utilizador do IdM, que não são substituídos por esse script, são transferidos para o sistema de destino.

No caso dos scripts que são usados para a reconciliação são feitos em groovy.

Pode-se especificar quatro scripts Groovy diferentes para cada caso de reconciliação:

-IDM (excluído) e sistema destino (existe)

-IDM (existe) e sistema destino (existe)

-IDM (existe) e sistema destino (não existe)

-IDM (não existe) e sistema destino (existe)

Cada script Groovy implementa a interface PopulationScript.java com o único método

```
public int execute(Map<String, String> line, ProvisionUser pUser);
```

É necessário primeiro procurar o utilizador na plataforma através deste script:

```
import groovy.json.JsonSlurper
import org.openiam.idm.searchbeans.UserSearchBean
import org.openiam.idm.srvc.recon.service.AbstractIDMSearchScript
public class UserSearchScript extends AbstractIDMSearchScript {
    @Override
      public UserSearchBean createUserSearchBean(Map<String, Object> bindingMap) {
         def bean = new UserSearchBean()
            if (updatedSince) {
                bean.updatedSince = updatedSince
             def obj = new JsonSlurper().parseText(searchFilter)
                if (obj in Map) {
                  obj.keySet().each {
                        key->   if (bean.properties.find{key}) {
                          bean."${key}" = obj."${key}"
                          }
                      }
                }
             }
           return bean
   }
}
```

Figura 17 Script SearchUser

Cada registo (utilizador) do sistema de destino é representado por um mapa de pares de nomes e valores de atributos. O segundo parâmetro na função de execução é provUser, que se precisa de preencher com os valores do mapa. Se o utilizador já existir no OpenIAM , ele será preenchido com valores da base de dados OpenIAM . Assim sempre pode-se comparar valores antigos com os novos.

Aqui está o exemplo do PopulationScript :

```
public int execute(Map<String, String line, ProvisionUser pUser){
        for( String key: line.keySet()){
            switch(key){
              case "NumeroAluno":
                    pUser.numeroAluno=line.get("NumeroAluno")
                    break
              }
      }
return 0
}
```

Figura 18 Population Script

Também é necessario fornecer um provisionUser válido após a reconciliação de cada registo e retornar 0 se tudo estiver correto.

Depois que o provUser é passado para o provisioningService , o utilizador é criado / atualizado com os novos valores do sistema de destino. Por exemplo, aqui está um trecho de código que adiciona um atributo personalizado ao utilizador:

```
def addAttribute(ProvisionUser pUser, String attributeName, String attributeValue) {
        def userAttr = new UserAttribute(attributeName, attributeValue)
          if (!pUser.userAttributes.containsKey(attributeName)) {
             userAttr.operation = AttributeOperationEnum.ADD
           } else {
              if (userAttr.value != attributeValue) {
                 userAttr.operation = AttributeOperationEnum.REPLACE
              }
        }
       pUser.userAttributes.put(attributeName, userAttr)
}
```

Figura 19 Provisioning Service

O provisionamento e o desaprovisionamento são considerados os principais recursos de uma solução IdM. Refere-se à funcionalidade que permite a gestão do ciclo de vida do utilizador e da conta em diferentes sistemas com base num conjunto de regras ou funções (se estiver usando o provisionamento baseado em função). As contas do utilizador podem ser criadas automaticamente com permissões diferentes, com base nas suas funções ou regras.

Quando usado um conjunto com o recurso Sincronização no OpenIAM, é possível integrar-se a uma fonte autorizada e automatizar a gestão completa do ciclo de vida do utilizador.

Para ativar o provisionamento e o desprovisionamento do OpenIAM, precisamos examinar dois componentes principais: -Serviço de provisionamento - determina quais sistemas uma pessoa deve ser provisionada e os direitos que ela deve ter nesses aplicativos.

-Conectores - Serviços que se comunicam com o aplicativo final (sistemas como LDAP, Active Directory, Office365, Google, Azure, AWS ou aplicativos personalizados)

Os conectores comunicam com o serviço de provisionamento por meio de um message bus, conforme mostrado no diagrama abaixo. Os conectores podem ser implantados independentemente do restante do OpenIAM para fornecer flexibilidade, escalabilidade e segurança. Por exemplo, a solução principal do OpenIAM pode ser implantada na cloud e o conector pode estar no local.

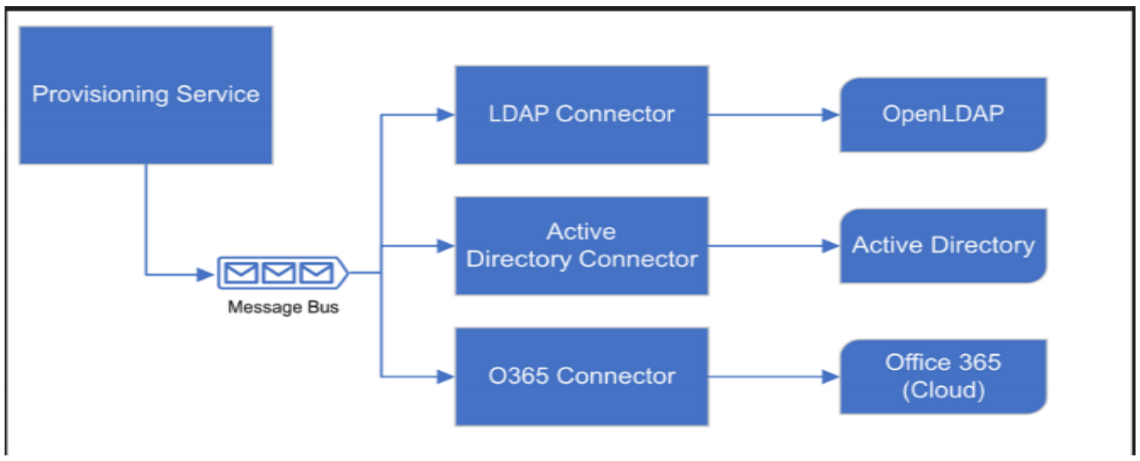

Figura 20 Provisionamento

4.2.5 Batch Tasks

O Batch Tasks é a execução de programas (tarefas) sem intervenção manual. No OpenIAM , as tarefas em lote podem ser agendadas usando tarefas Cron ou executadas uma vez em uma data exata. As tarefas podem ser definidas na forma de um script Groovy ou Spring Bean. Um exemplo de tarefa orientada a lotes é quando uma conta é bloqueada por algum motivo, uma notificação é enviada; se ocorrer um evento de auditoria, publique esse evento.

Outra Batch Tasks importante é relativa a eliminação ou desativação de uma conta pela pela data de termino de acesso á plataforma(ver figura 19) que é executada todos os dias á meia noite verificando a variável "Last Date" de todas as contas e caso essa data já tenha passado bloqueia a conta do utilizador só podendo ser ativada novamente pelo administrador.

Figura 21 Batch Tasks

Para alem da desativação da conta pela "Last Date" também temos outra tarefa importante relativa á ativação da conta pela "Start Date" isto permite que o utilizador só consiga fazer login na plataforma depois dessa data, tal como o a da tarefa de bloqueio de contas a de ativação de contas também é executada todos os dias á meia noite isto imposto pela Cron(00***)

4.2.6 Resumo da arquitetura

Na figura 21 encontra-se um resumo da arquitetura implementada onde vai existir dois portais(duas paginas web) uma para o administrador(webconsole) e outra para os utilizadores(self-service) que serão encaminhada para o servidor da plataforma, ao fazer o login a plataforma tem de verificar primeiramente a validação da password usando a

politica de senha implementada neste caso para o login na própria plataforma a usada é a default do próprio OpenIAM.

Depois vai haver conexão com os sistemas Ldap através do ldap conector(falado anteriormente) e através do DB Connector para outra Base de dados criada na própria máquina virtual

No caso da Base de dados externa á plataforma é usado um jbdc que é uma interface de programação de aplicativos (API) para a linguagem de programação Java , que define como um cliente pode aceder a uma base de dados. É uma tecnologia de acesso a dados baseada em Java usada para conectividade de banco de dados Java. Faz parte da plataforma Java Standard Edition , da Oracle Corporation . Fornece métodos para consultar e atualizar dados numa Base de Dados que é orientado para Base de dados relacionais . Uma ponte JDBC para ODBC permite conexões com qualquer fonte de dados acessível por ODBC no ambiente host da Java virtual achie (JVM).

A base de dados(mariadb) foi criada com o nome de lusofona e utilizamos um conector para fazer a conexão da plataforma com o base de dados assim- jdbc:mysql:// 206.189.27.237:3306/lusófona

Para permitir que esta conexão é feita e que a inserção é eficaz temos de garantir a correspondência das variáveis do OpenIAM com as das Base de dados, para isto não é necessário que os nomes sejam iguais mas que ao configurarmos o sistema que as variáveis que queremos introduzir correspondam as tabelas da Base de dados que é o nosso sistema de destino.

Esta correpondecia é feita através do Policy Maps para todos os atributos do sistema de destino basta para isso selecionarmos o User Policy do sistema que estamos a utilizar neste caso da Base de dados e preencher o atribute name com o atributo da base de dados OpenIAM e preencher o policy que corresponde aquele atributo na base de dados externa(ver figura 22)

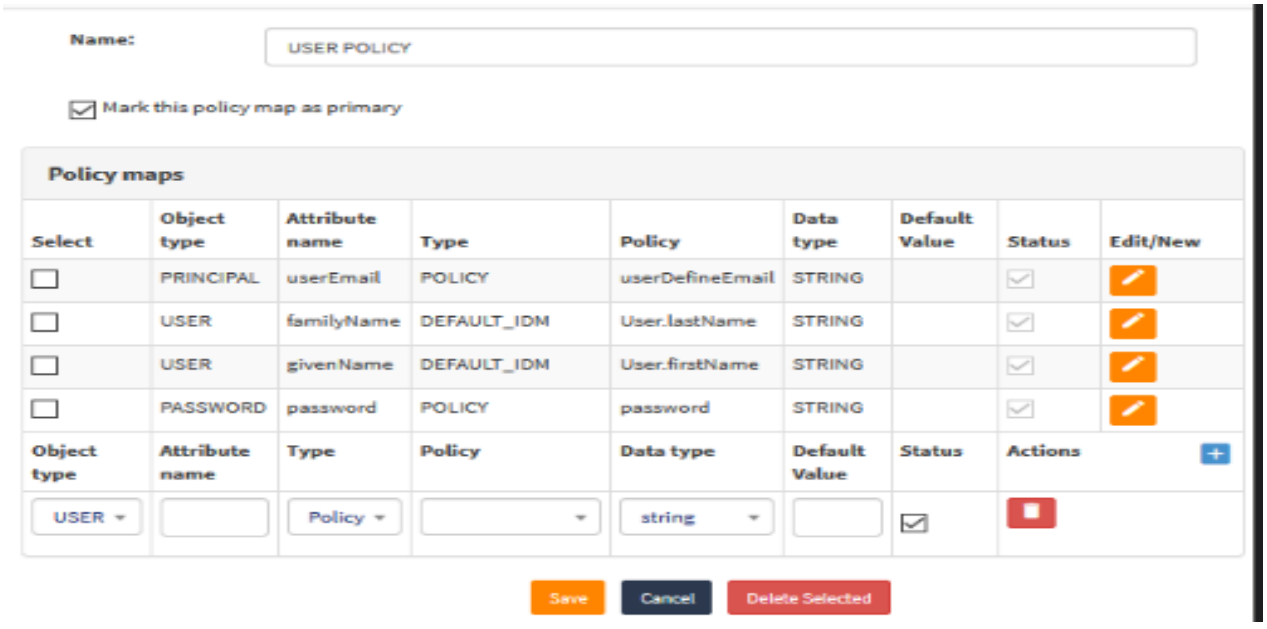

Figura 22 Policy Maps

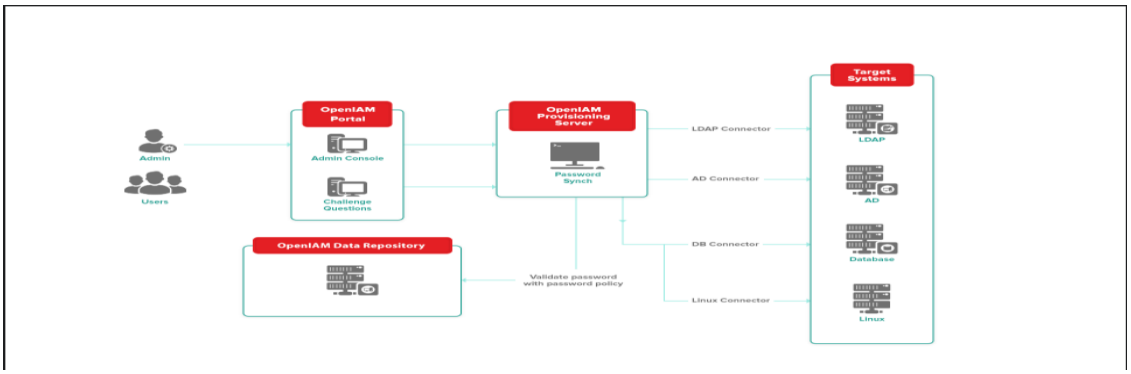

Figura 23 Resumo Arquitetura

5 Benchmarking

5.1 O que é Gestão da Identidade?

Existem várias definições diferentes de identidade no contexto da gestão da identidade digital. Por exemplo, Pfitzmann e Hansen definem identidade como: "Uma identidade de uma pessoa individual pode compreender muitas identidades parciais, cada uma das quais representa a pessoa em um contexto ou papel específico. Uma identidade parcial é um subconjunto de valores de atributos de uma identidade completa, onde uma identidade completa é a união de todos os valores de atributos de todas as identidades dessa pessoa".

As identidades podem ser categorizadas de muitas maneiras a partir de diferentes perspetivas, uma vez que as discussões sobre identidade abrangem uma ampla gama de disciplinas, incluindo sociologia, psicologia e filosofia, bem como ciência da computação. Através da pesquisa sobre trabalhos sobre identidade na ciência da computação, Nabeth descobriu que as identidades são conceitualizadas principalmente a partir de perspetivas estruturais e de processo. De uma perspetiva estrutural, uma identidade é vista como uma representação ou um conjunto de atributos que caracterizam a pessoa . De uma perspetiva de processo, uma identidade é conceitualizada para fins de identificação como "um conjunto de processos relativos à divulgação de informações sobre a pessoa e o uso dessa informação".

Uma identidade consiste em três tipos diferentes de dados: identificador, credenciais e atributos.

- **Identificadores**: Uma série de dígitos, caracteres e símbolos ou qualquer outra forma de dados utilizados para identificar um sujeito. Os identificadores podem ser scoped por tempo e/ou espaço. Por exemplo, um URI é globalmente único ao longo do tempo. Pseudónimos podem ser temporais e eficazes apenas para um serviço específico. Alguns exemplos são nomes de contas de utilizador, passa, números de telemóvel, números de funcionários, pseudónimos e URI.
- **Credenciais**: Um conjunto de dados que fornecem provas de reivindicações sobre partes ou identidades inteiras. Uma credencial pode ser gerada com base em uma ou mais credenciais. Alguns exemplos são senhas, certificados digitais, impressões digitais, bilhetes Kerberos e afirmações SAML.
- **Atributos**: Um conjunto de dados que descreve as características de um sujeito. Os dados incluem a informação fundamental para identificar um sujeito (por exemplo, nome completo, domicílio e data de nascimento), suas preferências, e a informação gerada como resultado de suas atividades. Alguns exemplos são dados/nomes de família, domicílios, idades, gêneros, papéis, títulos, afiliações, registos de atividades e reputações.

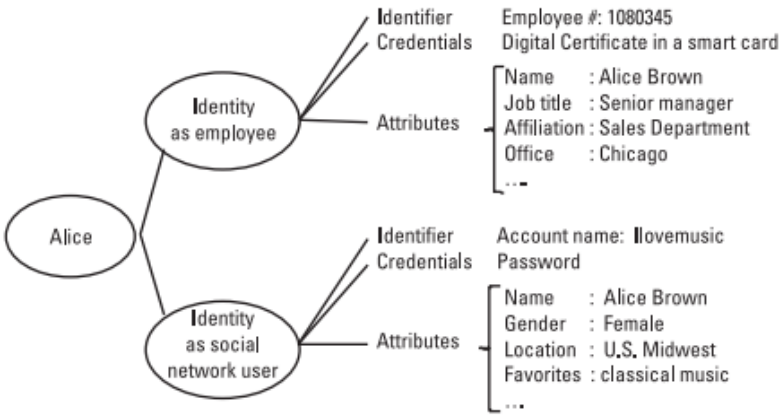

Figura 24 As identidades consistem em identificadores, credenciais e atributos

Há recomendações de padronizações de conceitos de gestão de identidade, que consideram a informação existente numa entidade suficiente para identificar essa identidade num contexto particular. Definem a informação de uma entidade em três tipos de dados: identificadores, credenciais e atributos. A gestão de informações de uma identidade baseando-se em identificadores (por exemplo, o endereço de correio eletrónico, telefone, identificador único de utilizador), credencias (certificados digitais, dados biométricos, *tokens*) e atributos (por exemplo, regras de negócio, privilégios de acesso, localização) já recebeu outras abordagens.

Cada vez mais os serviços são baseados em contextos e regras, são acedidos a partir de qualquer lugar, a qualquer momento, tornando a gestão de informação contida na identidade, vulnerável a questões de segurança. Existem também desafios como a interoperabilidade dos sistemas, num contexto heterogéneo que é necessário ligar-se entre si.

Do ponto de vista do processo, a identidade é formada através da identificação de um conjunto de processos relacionados à divulgação de informações sobre a pessoa e ao uso dessa informação.

Podem ser terceiros a definir uma identidade. A identidade é gerada com base em quem tem e controla as identidades. Este conceito de abordagem de identidade composta por três níveis: a *minha identidade*, a *nossa identidade* e a *identidade por terceiros*. A *minha identidade*, é como um identificador central. Pode ser exposto e anónimo, e é a pessoa própria que controla o acesso dos outros. É também considerada a verdadeira identidade e são criadas quanto o objeto pessoa natural nasce. A *nossa identidade* não pertence à pessoa nem à identidade que nos fornece. Esta identidade existe por meio de acordos de terceiros (por exemplo, a identidade como funcionário de uma instituição e que se mantêm enquanto existir um acordo entre a instituição e o funcionário). A identidade por terceiros é uma identidade que é criada internamente, normalmente por uma empresa com interesses comerciais identificados, sem o consentimento explicito do sujeito. Neste tipo

de identidade, as empresas criam conjunturas de identidades dos utilizadores, mesmo com a pouca informação que têm do utilizador, utilizando dados com o IP, localização demográfica e *cookies* do computador (por exemplo, um serviço de pesquisa web, que cria um modelo de utilizador com base nas pesquisas para aquele IP).

Finalmente, introduzimos a federated identity management. A federated identity management é uma forma de gerir as identidades, permitindo a um sujeito de identidade estabelecer ligações entre as suas identidades, cada uma das quais pode ser utilizada para um serviço diferente, através de fronteiras geográficas e organizacionais. O estabelecimento de uma ligação lógica entre as identidades é chamado de federação de identidades. A federated identity management está se tornando importante à medida que pessoas, organizações e sociedades interagem e colaboram entre si com mais frequência numa escala.

Um sistema de gestão de identidade tem de ter capacidade para adicionar ou remover o aprovisionamento ou não aprovisionamento da informação. Para isso, deverá assegurar políticas de autenticação e políticas de acesso à informação, sistemas, dados e funcionalidades.

5.2 Objetivo da Gestão de Identidades e Acessos

A Gestão de Identidades e Acessos (IAM) na TI corporativa é sobre como definir e gerenciar as funções e os privilégios de acesso dos utilizadores individuais da rede e as circunstâncias nas quais os utilizadores recebem (ou negam) esses privilégios. Esses utilizadores podem ser clientes (gestão de identidade do cliente) ou funcionários (gestão de identidade do funcionário). Os objetivos principais dos sistemas IAM é uma identidade digital por indivíduo. Depois que a identidade digital for estabelecida, ela deverá ser mantida, modificada e monitorada ao longo de cada utilizador " aceder ao ciclo de vida".

Assim, o objetivo principal da gestão de identidades é conceder acesso aos ativos corporativos certos aos utilizadores certos no contexto certo, desde a integração do sistema do utilizador até autorizações de permissão até a exclusão desse utilizador conforme necessário em tempo hábil.

Os sistemas IAM fornecem aos administradores as ferramentas e tecnologias para alterar a função de um utilizador, rastrear atividades do utilizador, criar relatórios sobre essas atividades e aplicar políticas continuamente. Esses sistemas foram projetados para fornecer um meio de administrar o acesso do utilizador em toda a empresa e garantir a conformidade com as políticas corporativas e os regulamentos governamentais.

As soluções IAM resolvem duas funções principais: administração e aplicação em tempo real. As soluções de gestão de identidade atendem à necessidade das empresas de administrar (criar, modificar e excluir) contas de utilizadores, perfis de utilizadores e políticas corporativas em todo o ambiente de TI heterogêneo através de uma combinação de funções de utilizadores e regras de negócios.

5.3 Gestão de Identidades e Acessos na IoT

A Internet of Things (IoT) está a destacar-se em ambientes de consumo e de negócios. A CSA criou o Grupo de Trabalho da IoT (WG) para se concentrar no fornecimento de orientações relevantes aos interessados que estão a implementar soluções IoT. Este Capítulo centra-se em considerações para a gestão da identidade e do acesso(IAM) à IoT.

5.3.1 Introdução

A IoT introduz a necessidade de gerir exponencialmente mais identidades do que os sistemas IAM existentes são necessários para suportar. A indústria da segurança está a assistir a uma mudança de paradigma, em que o IAM já não se preocupa apenas em gerir pessoas, mas também em gerir as centenas de milhares de "coisas" que podem estar ligadas a uma rede. Em muitos casos, estas “coisas” são ligadas intermitentemente e podem ser necessárias para comunicar com outras “coisas”, com dispositivos móveis e com a infra-estrutura back end. Alguns começaram a referir-se a este novo ecossistema de identidade como a Identidade das Coisas (IDoT). O IDoT refere-se às relações entre dispositivos e seres humanos, dispositivos e aplicação/serviços. Está se a experimentar a “significant rowth” em ambientes de consumo e empresariais.

5.3.2 A indústria só agora está a iniciar a mudança para a concepção e implantação da IoT

Por conseguinte, é um momento oportuno para considerar a forma como o IAM IoT se relaciona com outros serviços de segurança necessários para uma empresa ligada à Internet of Things. Isto inclui serviços como a gestão de ativos e de chaves criptográficas. Em alguns casos, os fornecedores de soluções IoT começaram mesmo a integrar o IAM como subproduto da ligação dos ativos da IoT.

Há também uma tendência para a Gestão da Relação de Identidade (IRM), liderada pela iniciativa Kantara. A Iniciativa Kantara definiu um conjunto de pilares IRM que se centram, em parte, nos consumidores e nas “coisas” sobre os empregados; à escala da Internet sobre a escala das empresas; e sem fronteiras sobre o perímetro. Estes pilares são altamente aplicáveis ao que é necessário para apoiar o IAM IoT. As organizações devem manter-se informadas sobre as novas politicass IRM da nossa indústria.

Existem outros desafios associados à gestão da identidade e do acesso na IoT. Estes incluem a necessidade de repensar o que a autenticação multi-factores (MFA) implica e a necessidade de definir convenções de nomes para os ativos de uma organização em rede. De acordo com um relatório da Comissão Europeia sobre as identidades da IoT, elaborado pelo Grupo de Peritos na Internet of Things, "as questões do fornecimento de endereços únicos não colidentes num esquema global exigem uma infraestrutura que suporte dispositivos altamente dinâmicos que aparecem e desaparecem da rede em qualquer momento, se movimentam entre redes locais e/ou privadas diferentes e têm a

flexibilidade necessária para identificar o seu utilizador de forma única ou ocultar a sua identidade, preservando assim privacidade conforme necessário.

5.3.3 Porque estamos num estado tão novo em relação ao IAM da IOT

É igualmente importante estar a par do trabalho de normalização nesta área. A IETF, por exemplo, está a trabalhar numa série de tipos de informação sob a égide da Autenticação e Autorização para Ambientes Constrangidos. A IETF ACE está a trabalhar em alterações aos protocolos IoT existentes, como o protocolo CoAP Delegado, que "especifica como com os recursos limitados podem delegar tarefas definidas relacionadas com autenticação e autorização em dispositivos menos limitados, chamados gestores de autorização, limitando assim os requisitos de hardware da solução de segurança para os ambientes limitados pelos dispositivos".

5.3.4 Orientações sumárias para a gestão da identidade e do acesso na IoT

Integre a sua implementação da IoT nos quadros de governação existentes do IAM e do GRC na sua organização. As considerações devem incluir os seguintes passos:

-Definir um espaço de nomes comum para dispositivos IoT.

-Estabeleça um ciclo de vida de identidade extensível que possa ser aplicado às coisas na sua organização e que possa ser adaptado com base na vida útil do dispositivo e no identificador necessário.

-Dentro do ciclo de vida de identificação, estabeleça processos de registo claros para os dispositivos IoT.

-O rigor do processo de registo deve ser ditado pela sensibilidade dos dados tratados por um determinado dispositivo IoT.

-Determinar o nível de proteção da segurança (confidencialidade, autenticação, autorização) a aplicar aos fluxos de dados únicos dos sensores e outros componentes da IoT.

-Estabelecer procedimentos claros de autenticação e autorização para o acesso local a dispositivos IoT (p. ex., acesso administrativo local).

-Definir as proteções de privacidade necessárias para categorias de dados diferentes.

-O estabelecimento de uma definição-quadro de referência para estabelecer as proteções da privacidade da informação identificável pessoalmente (ICP) ajudará nestas definições.

-Determinar e documentar se as organizações externas têm acesso a determinadas categorias de dados.

-Definir como efetuar a autenticação e autorização dos dispositivos IoT que são apenas intermitentemente ligados à rede.

-Identificar os requisitos de controlo de acesso que se aplicam à IoT de acordo com a sua política de controlo de acesso da organização.

Não se deve utilizar recursos da IoT sem alterar as palavras-passe por defeito para acesso administrativo. Se possível, não implementar dispositivos IoT apenas com capacidades de acesso local. Pelo contrário, tente integrar todos os recursos da IoT no sistema IAM empresarial. Note-se que esta orientação não se aplica aos dispositivos IoT baseados no consumidor que estejam ligados à rede da empresa. Novos conceitos semelhantes aos exigidos para o registo de dispositivos pelo BYOD teriam de ser aplicados a esse segmento de dispositivos IoT.

Avaliar uma mudança para a Gestão da Relação de Identidade (IRM) em vez do tradicional IAM. O IRM é mais adequado à IoT do que os tradicionais IAM e baseia-se num conjunto de pilares que incluem o foco nos consumidores e nas coisas através dos empregados, a escala da Internet em relação à escala das empresas e o Borderless em relação ao perímetro. Identifique e avalie as soluções dos fornecedores IRM como um possível ajuste para os seus requisitos de identidade de Internet das coisas.

Deve desenhar-se os esquemas de autenticação e autorização com base nos modelos de ameaça a nível do sistema. Avaliar a implementação de cada fabricante individual e escolher fornecedores que tenham aderido às normas aplicáveis e/ou procurado orientação ou seguindo as melhores práticas de grupos de segurança da indústria, tais como BuildItSecure.ly e OWASP. Ter em conta as vulnerabilidades do sistema.

Implemente uma lógica mais restritiva nos seus fluxos de trabalho(Workflow) de gestão da identidade, de modo a restringir proactivamente o acesso a sistemas e dispositivos relacionados com a IoT, caso uma pessoa não tenha tido os pré-requisitos necessários, tal como especificado no seu quadro de governação do acesso. Exemplos de pré-requisitos incluem a formação e a verificação dos antecedentes.

Example IoT Protocols and Authentication Options

Protocol	m2m Authentication Options	Discussion
HTTP/ REST	Basic Authentication (cleartext) (TLS methods) OAUTH2	HTTP/REST typically requires the support of the TLS protocol for authentication and confidentiality services. Although Basic Authentication (where credentials are passed in the clear) can be used under the cover of TLS, this is not a recommended practice. Instead attempt to stand up a token-based authentication approach such as OAUTH 2

Figura 25 IoT Protocols and Authentication Options

5.4 Concorrência nos softwares de gestão de identidades

Existem vários softwares de gestão de identidade tais como OpenIAM, (já explicado), Shibboleth, WSO2 Identity Server, MidPoint, Soffid, Apache Syncope e Gluu, em baixo vão ser apresentados todos as suas vantagens e desvantagens.

5.4.1 WSO2 Identity Server

O WSO2 Identity Server pode ser usado para simplificar as atividades relacionadas à gestão de identidade e acesso (IAM) na empresa. O produto é baseado em padrões abertos e princípios de OpenSource. O WSO2 Identity Server vem com recursos de integração fáceis de usar que ajudam a conectar aplicativos, repositórios de utilizadores, diretórios e sistemas de gestão de identidades.

O WSO2 Identity Server permite que as empresas atinjam o logon / logon único (SSO), federação de identidades, autenticação forte, administração de identidades, gestão de contas, provisionamento de identidades, controlo de acesso refinado, segurança da API, monitoramento, relatórios e auditoria. O WSO2 Identity Server permite conectar e reutilizar ativos de TI novos e existentes de maneira segura.

As principais vantagens do WSO2 Identity Server sobre a concorrência são ser 100% de OpenSource (o código-fonte e os binários são divulgados sob a licença de código aberto Apache 2.0 mais amigável para negócios), a capacidade de integrar-se facilmente a qualquer estrutura de gestão de identidade baseada na cloud ou local ou usar o armazenamento. APIs bem definidas e bem documentadas e vários conectores prontos disponíveis no WSO2 Connector Store para fazer isso rapidamente, inúmeros modelos de fluxo de trabalho, modelos de política, amostras e arquiteturas de referência disponíveis para ajudar a reduzir esforços redundantes e permitir implementações mais rápidas da solução IAM, suporte para protocolos de federação de identidade heterogênea (com base em padrões abertos) e transformação e mediação de token entre eles, liberdade para arquitetos e desenvolvedores escolherem mecanismos da federação, protocolos de autenticação e formatos padrão e formatos de token para atender às suas necessidades, capacidade de automatizar operações de gestão com APIs REST e SOAP integradas, facilidade de implantação, operações de gestão amigáveis e baixo custo de manutenção, arquitetura orientada a componentes e suporte a cloud e contêiner permitem implantar recursos do IAM usando uma topologia de sua escolha, com base em suas necessidades, de maneira segura, escalável e adaptável, os scripts e ferramentas readymade ajudam a implantações rápidas, garantindo a capacidade de entrar no mercado rapidamente com sua solução, inovação contínua que ajuda a criar soluções de identidade e acesso à prova de futuro, ciclos de atualização rigorosos e frequentes do produto e suporte de ferramentas de ponta para gerenciar implantações do IAM com as melhores práticas do DevOps, práticas abrangentes de limpeza de segurança e testes de penetração para garantir o mais alto nível de qualidade e segurança do conjunto de produtos IAM e teste e ajuste proativos de desempenho e inovação em torno de aprimoramentos de desempenho.

5.4.2 midPoint

O midPoint, desenvolvido pela Evolveum , é uma solução de OpenSource para “Identity Governance and Administration” e, portanto, software para Identity and Access Management (IAM). Como uma solução completa, fornece todas as ferramentas e possibilidades de configuração necessárias que um departamento de TI precisa para estabelecer um novo IAM e oferece serviços de consultoria, integração, implementação e suporte para o midPoint. que permite que as empresas, organizações e negócios de vários setores otimizem a gestão do ciclo de vido do utilizador, gerem logs de auditoria de atividades relacionadas ao acesso, configuram a estrutura organizacional dentro da plataforma, criam e aplicam políticas de senha, fluxos de trabalho de aprovação e implementação de gestão de direitos de um local.

O Evolveum midPoint suporta a integração com outos sistemas de gestão de identidades e aplicativos de gestão de serviços TI.

5.4.3 Shibboleth

O Shibboleth é um projeto de OpenSource que fornece recursos de logon único e permite que os sites tomem decisões de autorização informadas para acesso individual a recursos online protegidos de maneira a preservar a privacidade, permite que as pessoas entrem usando apenas uma identidade em vários sistemas executados por associações de diferentes organizações ou instituições. As associações são frequentemente universidades ou organizações de serviço público.

5.4.4 Soffid

O Soffid fornece experiência completa de Logon único e recursos completos de gestão de identidade e acesso por orquestração centralizada de identidades do utilizador com base em políticas. Tudo entregue por uma solução completa de OpenSource.

O Soffid fornece uma ferramenta de configuração única para o administrador e fornece um portal de autoatendimento fácil de usar para os utilizadores finais. Uma ferramenta única para todos melhorarem a produtividade do utilizador. Usa padrões de segurança de última geração. A gestão de identidade e acesso fornece uma nova visão sobre segurança, não mais baseada na visão de firewall antiga, mas centrada em quem, quando e como o utilizador está ligado a recursos específicos para melhorar a segurança externa e interna .

Permite a opção de gerir todos os ativos de TI não com base em sua localização, mas com base em quem os acede, fornecendo a flexibilidade perfeita para a infraestrutura de TI moderna das empresas modernas que estão migrando para o ambiente móvel e na cloud. Os utilizadores finais não precisam mais entrar em contato com o suporte de TI quando perdem suas credenciais ou desejam novas permissões. Com o Soffid, tudo é gerenciado a partir do portal de autoatendimento, levando a uma importante redução no custo de suporte .

Soffid regista todas as ações executadas por todos os utilizadores e administradores em qualquer objeto Soffid ou sistema de destino, e todas essas informações são auditáveis a qualquer momento. Recursos completos de auditoria e conformidade legal sempre disponíveis no mesmo conjunto de produtos Soffid.

A recertificação de acesso é um controlo de TI que envolve a auditoria de privilégios de acesso do utilizador para determinar se eles estão corretos e aderem às políticas internas da organização e aos regulamentos de conformidade.

5.4.5 Apache Syncope

O Apache Syncope é um sistema de OpenSource para gerir identidades digitais em ambientes corporativos, implementado na tecnologia Java EE e lançado sob a licença Apache 2.0.

O Apache Syncope permite gerir todo o ciclo de vida da identidade - sejam utilizadores, grupos ou outros. Com opções de implantação na cloud ou local, oferece recursos avançados para fluxos de aprovação, notificações de eventos, execução e programação de tarefas utilitárias, provisionamento e reconciliação.

O Syncope suporta utilizadores de sincronização para contas e funções para grupos. Nada mais. Não há suporte para a estrutura organizacional e parece que estender o Syncope para esse fim está longe de ser trivial.

O Syncope possui uma consola (web) separado e um mecanismo de provisionamento "principal" que se comunica por uma interface REST. Eles devem ser implantados como dois aplicativos da web. Exceto pelo fato de que o Syncope quase não possui estrutura interna de componentes. Existem apenas três componentes "núcleo", "consola" e "comum". Enquanto os componentes são divididos internamente em pacotes, exceto pela interface REST, parece haver muito poucas interfaces internas. Definitivamente, isso terá um impacto negativo na capacidade de manutenção futura de projetos baseados em Syncope.

O Syncope é um sistema pequeno e agradável. Mas não é totalmente fácil entender como isso funciona. Uma boa documentação é realmente necessária. No entanto, a documentação é um dos problemas duradouros do projeto Syncope. De alguma forma, a documentação melhorou em no ano passado, mas ainda é muito insuficiente. A documentação não está completa e não é muito consistente, o que dificulta a leitura. A falta de documentação torna quase impossível usar o Syncope sem o suporte da equipa de desenvolvimento.

De facto, o Syncope é o mais OpenSource de todos os projetos avaliados. Possui uma estratégia clara de OpenSource. É uma parte da Apache Foundation, portanto, é quase certo que essa estratégia permanecerá inalterada. Existem listas de discussão ativas que são usadas abertamente para discutir tudo sobre o Syncope - incluindo planos e decisões de design. Isso é realmente único entre todos os projetos avaliados.

5.4.6 Gluu

O Gluu é uma plataforma de gestão de identidade e acesso (IAM) para logon único na web e móvel (SSO), autenticação de dois fatores e gestão de acesso à API, é um software OpenSource.

O Gluu ofereçe SSO (logon único) sem protocolo e com protocolo cruzado a qualquer aplicativo que utilize o Gluu para fazer login, tem a infraestrutura de autenticação SAML ou OpenID Connect de clientes e parceiros para gerir credenciais externas e simplificar o acesso a recursos protegidos.

Tem também suporte para registo e login no Google, Facebook, GitHub ou qualquer outro IDP de consumidor popular. As páginas e solicitações voltadas ao público, como login e solicitações de consentimento do OAuth 2.0, usam um design responsivo para apresentar uma experiência fluida do utilizador em todos os dispositivos.

5.4.7 Fornecedores de gestão de identidades e acessos

O cenário de fornecedores de gestão de identidades e acessos é bastante movimentado, consistindo de provadores de pureplay, como Okta e OneLogin, e de grandes fornecedores, como IBM, Microsoft e Oracle(ver figura 6)

Com tudo o software de identidade escolhido vai ser como foi referido num capítulo anterior vai ser o OpenIAm sendo na minha opinião o mais completo de todos sendo que muitas dos outros referidos também eram bastante validos e poderiam ser usados.

Figura 26 Magic Quadrant for Acess Management

6 Método e planeamento

6.1 Modelo Sequencial Linear

É consoante as especificidades do projeto que o modelo de procedimento de engenharia de software é escolhido. Essa escolha assenta na natureza do projeto, nos métodos que vão ser aplicados, nas ferramentas a serem utilizadas e no calendário de entregas.

Neste modelo de desenvolvimento de software é sugerida uma abordagem sistemática e sequencial para o desenvolvimento de software, que se inicia ao nível da análise, desenho, código, testes e suporte, como apresentado na figura 27.

• **Análise e definição dos requisitos**- Nesta etapa o levantamento de requisitos é focado no software, ou seja, estabelecem-se os requisitos do produto que se deseja desenvolver, a finalidade, o comportamento, o desempenho e as funcionalidades necessárias das interfaces.

• **Desenho técnico e funcional**- O design de software é, na verdade, um processo de múltiplos passos que se concentra em quatro atributos distintos de um programa: estrutura de dados, arquitetura de software, representações de interface e detalhes processuais (algorítmicos)

• **Implementação**- É nesta fase que todo o trabalho técnico e funcional é traduzido para código, ou seja, implementado. Sugere-se neste modelo que no início seja incluído um teste unitário nos módulos desta etapa para as unidades de código produzidas serem testadas.

• **Testes**- Após a codificação inicia-se o programa de testes, que se centra em dois pontos essenciais: os componentes internos do software (testes aplicacionais) e as funcionalidades externas (testes funcionais). Desta forma é assegurado que todas as funções foram testadas, e que produzem os outputs esperados, coincidentes com os requisitos especificados.

• **Suporte**- É nesta etapa que é feita a correção de erros que não foram detetados na implementação. O software após a entrega tem de estar adaptado para acomodar mudanças no seu ambiente externo (por exemplo mudança de dispositivo periférico, melhorias funcionais necessárias, aumento de desempenho). O suporte/manutenção de software reaplica cada uma das fases anteriores para um programa existente em vez de um novo.

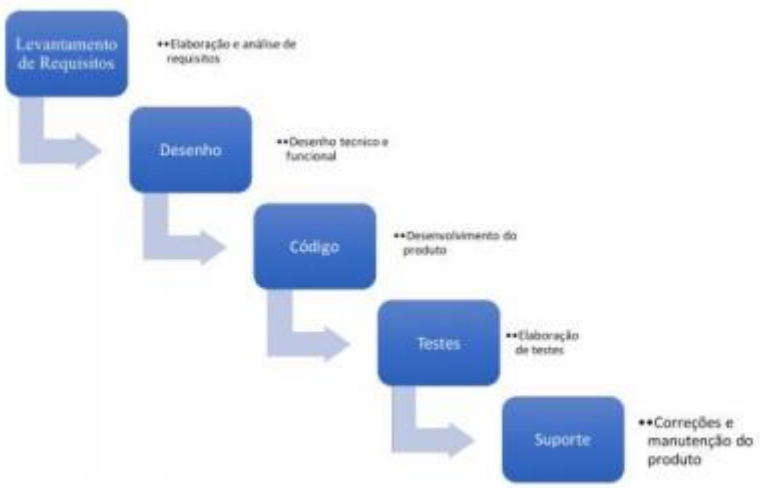

Figura 27 Modelo Sequencial Linear

6.2 Trabalho realizado

Depois de toda esta tecnologia referida o protótipo foi assente num Sistema de serviços cloud, dando um ambiente mais empresarial ao próprio protótipo usando uma máquina virtual em Linux através do Digital Ocean.

• Revisão do trabalho relacionado

O trabalho de pesquisa ajudou-me a compreender a finalidade do projeto e quais os objetivos que teriam de ser levados em conta para a implementação do componente do projeto do IAM. Também permitiu a análise de casos de sucesso e insucesso de implementações de soluções idênticas, permitindo uma maior perceção e cuidado em aspetos mais críticos de desenvolvimento da solução. Para além de todo o trabalho de pesquisa realizado anteriormente foi importante seguir e fazer o guião do próprio OpenIAM onde abordam os principais conceitos para a criação de um protótipo deste tipo.

• Enquadramento do projeto

Durante as primeiras semanas ocorreu o período de adaptação ao projeto que me foi atribuído. As minhas principais tarefas consistiram em pesquisas sobre o tema do projeto e analisar as várias soluções existentes no mercado. Perceber também o controlo de acessos por um CRM(Customer relationship management), o CRM refere-se à tecnologia e aos processos que uma organização usa para gerir os seus contatos, tanto externos quanto internos tais como: Assinantes de listas de e-mail, Leads de vendas, Oportunidades de vendas, Clientes, Funcionários, CRM é uma abordagem que coloca o cliente como principal foco dos processos de negócio, com o intuito de perceber e antecipar suas necessidades, para então atendê-los da melhor forma, contudo existe diferenças entre estratégia de CRM com Sistemas de CRM que é o que vai ser abordado, sendo que sistemas de CRM são aplicativos de informação desenvolvidos com o objetivo de auxiliar na gestão do relacionamento com o cliente. Conceitualmente, dá-se o nome de CRM à

gestão deste relacionamento, e de sistemas de CRM aos sistemas empregados para a gestão deste relacionamento.

Os benefícios de implantar CRM inclui o aumento das receitas a partir do melhor foco nos potenciais clientes, aumento da participação nos gastos dos clientes atuais, e retenção de clientes por períodos mais longos. Estas vantagens são quantificadas por meio de bancos de dados que ajudam as empresas a compreender melhor os seus clientes e a utilizar esse conhecimento para promover a lealdade e otimizar o valor do cliente no tempo. As táticas de CRM também podem reduzir custos, resultando numa maior 53 rentabilidade. Outra tecnologia estudada e analisada que é essencial para a continuação do projeto foi o Active directory.

Foi importante também perceber posteriormente á instalação do OpenIAM como funciona toda esta arquitetura, que por si só apresenta uma grande complexidade havendo pontos chaves e conceitos que tem de ser entendidos para uma implementação mais eficaz.

• Leitura de documentação Gestão de Identidade

Existem inúmeras abordagens de conceitos e implementações de sistemas de gestão de identidade. A leitura de conceitos de identidade digital e de casos de estudo de implementações de Sistemas de Gestão do Utilizador, permitiu o levantamento de um conjunto de riscos a ter em conta na implementação do projeto em causa.

• Configurações

Nesta etapa o meu objetivo foi instalar e configurar o produto e perceber toda a sua arquitetura, realizar o guião disponível no próprio site do OpenIAM para ajudar os desenvolvedores destas plataformas a terem uma introdução para perceberem conceitos chaves e por fim a criação de protótipo básico e da realização de um vídeo onde esse protótipo se foca na gestão de acessos isto é o que o utilizador pode ou não ter acesso.

• Criação do Protótipo

Desde da ultima entrega houve bastante progressos em termos da configuração e aplicação dos conceitos provenientes da leitura da documentação que foi bastante importante perceber o funcionamento e a arquitetura do sistema mas também pode se perceber a sua complexidade de realização , tendo que ao longo do tempo aprimorar o conhecimento e desenvolver certas “skills” no desenvolvimento deste tipo de plataformas que contem um grande conjunto de riscos a terem em conta na sua implementação.

Foi então criado um protótipo onde inicialmente foram apenas a criação de grupos, utilizadores e gerir os acessos de cada um e numa etapa final ligar toda a plataformas a outros Sistemas

• Testes

Nesta fase foi pedido a colegas da faculdade que entrassem em contras previamente feitas por mim e que testassem os acessos que tinham que mudassem as suas passwords, credenciais e etc, e que para alem disso essas mudanças de passwords foram verificadas nos outros sistemas quer no Ldap quer na Base de dados externa.

7 Resultados

Nesta secção vou fazer uma análise comparativa face ao proposto no primeiro relatório, entregue no primeiro momento de avaliação e também a demonstração dos resultados. Nesta fase o suposto, como apresentado quer por escrito no relatório quer complementado pela apresentação de um Cronograma em relatórios anteriores, era a realização de um protótipo de uma Plataforma IAM virado para faculdade.

Na parte de desenvolvimento, sendo que todos os requisitos importantes para a realização de um protótipo foram realizados na integra, os que foram apenas realizados parcialmente ou não implementados foi pela sua importância querendo incidir no que é o mais importante.

Em relação ao próprio projeto apresentado inicialmente era realizar um protótipo de uma Plataforma de IAM onde fossem geridos os acessos e as identidades de utilizadores baseadas nas suas permissões não permitindo que haja utilizadores do mesmo tipo com permissões a mais(abuso de permissões) ou a menos e que estas permissões estejam conformidade com o tipo de informação que necessitam não tendo mais permissões do que aquelas necessárias(autorização) como por exemplo um aluno não ter permissões para pesquisar alunos ou ter acesso a dados de outros alunos na própria plataforma mas um professor já poder ter acesso a esses dados como por exemplo uma lista de alunos para poder atribuir notas e estarem logo disponíveis no lado do aluno mas não tendo apenas acesso aos dados do aluno que sejam estreitamente necessárias para atribuir as avaliações não tendo acesso a dados pessoais do aluno que não sejam relevantes para as avaliações , para alem disso foram criadas ligações(que será explicado noutro capitulo) que permitiram ligar a plataforma a outras plataformas exteriores, serviços ou ate mesmo Base de dados(excluindo a própria Base de dados da Plataforma) conseguindo manter uma sincronização em todos os sistemas que queiramos permitindo colmatar incoerências e “transportar” informações e acessos de utilizadores sem que haja ligações diretas entre estes sistemas relevando assim simplificação da solução. Toda esta sincronização é feita assim que haja uma inserção de um novo utilizador, atualização das informações de um utilizador quer fosse por parte do próprio administrador, quer fosse feita pelo próprio utilizador, sendo esta parte importante em relação á coerência dos dados permitindo assim que todos os sistemas tenham os dados atualizados.

Em termo de resultados foram positivos, quer por ter enriquecido a parte teórica do trabalho devido a implementação do próprio protótipo, este enriquecimento foi mais notório na explicação da arquitetura como toda a plataforma se procede, mesmo com os problemas iniciais de instalação que foram ultrapassados acho que como o trabalho se procedeu a seguir foi bastante bom e produtivo em face a grande dificuldade da criação deste tipo de plataformas.

Em relação aos resultados obtidos foi a verificação que tipos de utilizadores diferentes(alunos, professores) tinhas acessos diferenciados verificado pelas figuras abaixo:

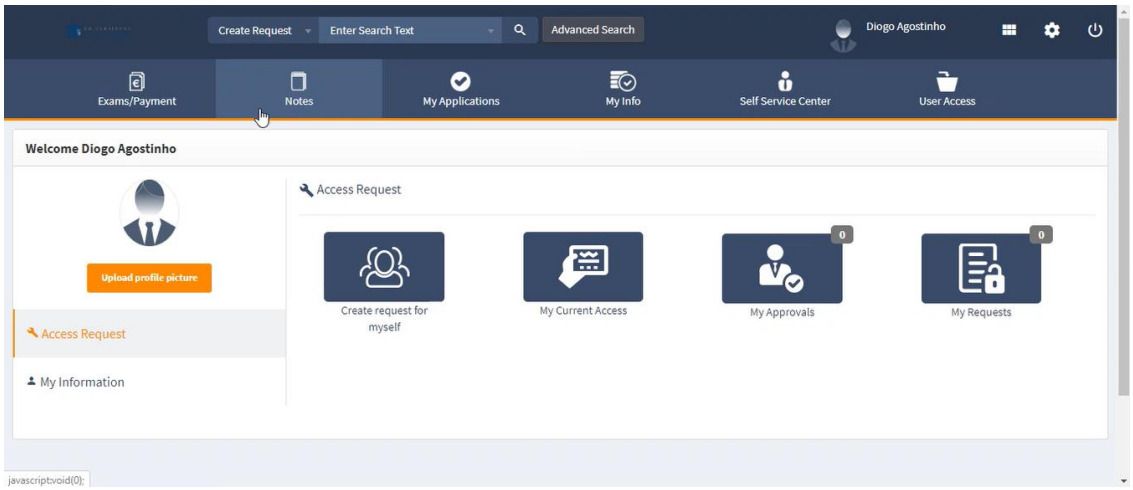

Figura 28 Aluno

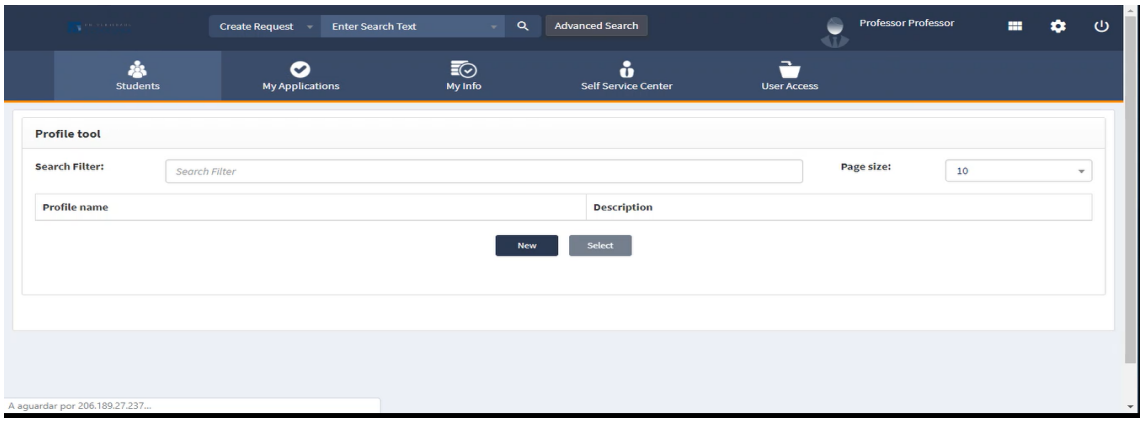

Figura 29 Professor

Através destas duas imagens podemos ver que uma é referente a um aluno e outra referente a um professor e também constatamos que ambos tem acessos a menus diferentes onde por exemplo o aluno tem acesso as notas e ao calendário/pagamento dos exames e o professor tem apenas acesso a uma lista de alunos.

Para alem desta gestão de acessos também foram obtidos resultados nas vertentes da integração da plataforma com outros Sistemas nomeadamente com LDAP

Nas figuras em baixo podemos verificar a mudança de credenciais(neste caso a password) assim que uma atualização no OpenIAM é imediatamente alterada no sistema(LDAP) como foi dito em cima.

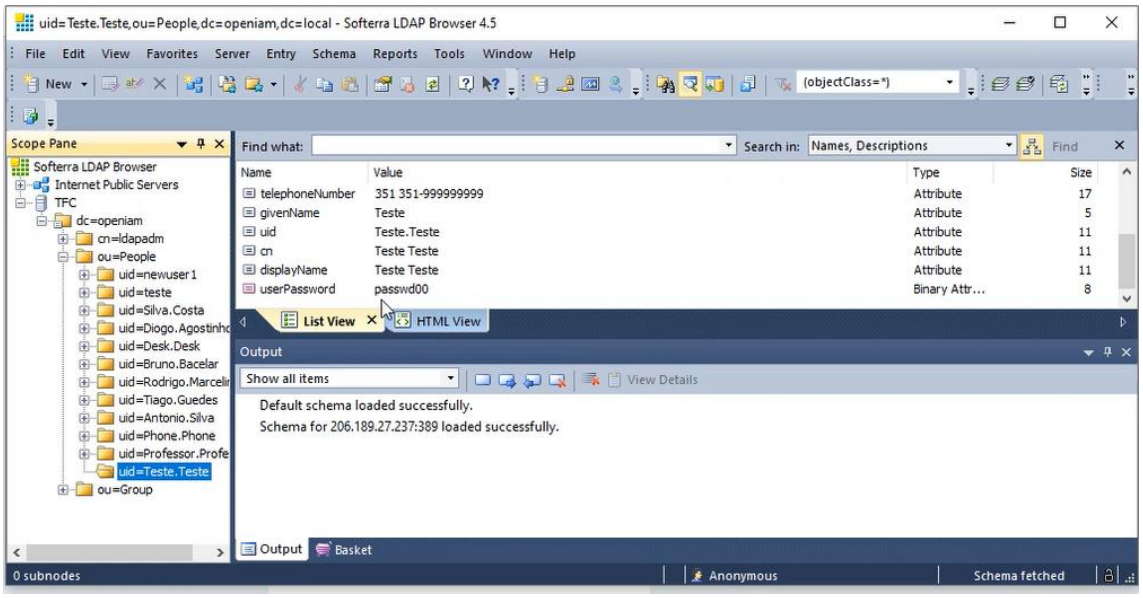

Figura 30 Ldap antes

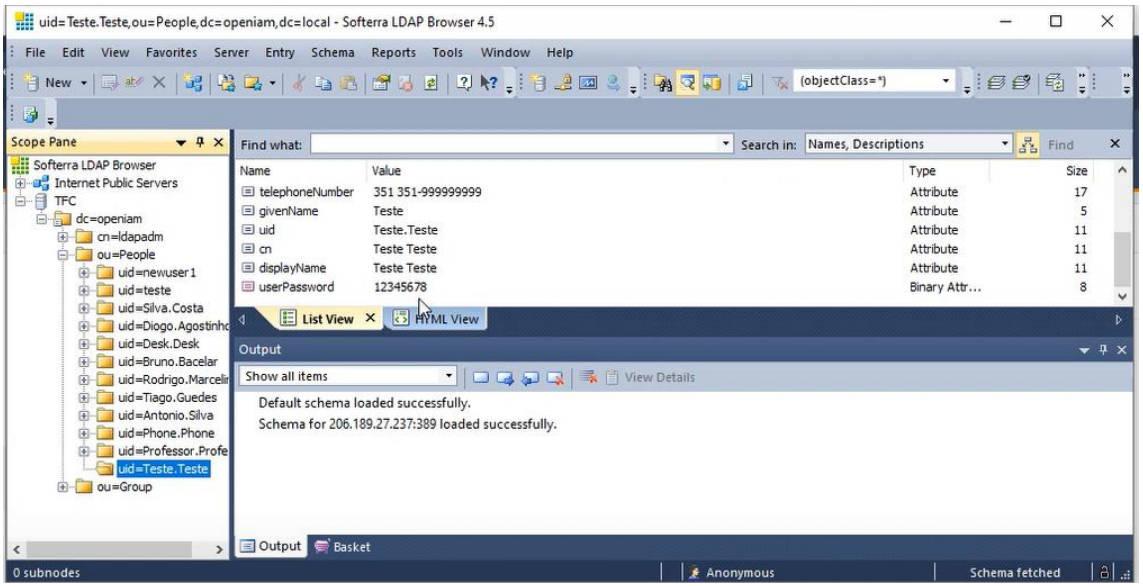

Figura 31 Ldap depois

Link Para o vídeo complementar do Protótipo da plataforma:
https://www.youtube.com/watch?v=-poa1_um2_k&feature=youtu.be

8 Conclusão e trabalhos futuros

Em relação a conclusão do trabalho foi importante perceber que estas plataformas são bastante complexas e trazem riscos associados que devem pesar na equação quando se pretende desenvolver uma plataforma destas quer seja para uma empresa ou para uma faculdade no entanto acho importantíssimo o desenvolvimento deste tipo de plataformas para empresa/faculdades porque facilita e muito o trabalho dos profissionais que la trabalham mas no caso dos alunos pode também facilitar a forma como a informação é disposta e como a podem aceder.

Este tipo de Plataformas como permite a ligação entre vários sistemas que é perfeito para grandes empresas que quer necessitam de vários sistemas ou que disponham de outras empresas ligadas a si.

O factor segurança também é importante para o desenvolvimento destas plataformas onde tem de haver um conjunto de regras que tem de ser muito bem definidas quer para a visualização de informação sobre os utilizadores presentes na plataforma, quer na passagem desta informação para outros sistemas quer também nos próprios acessos dos utilizadores na plataforma que não podem ser mais do que aqueles que deviam, dando apenas acesso aquilo que é estritamente necessário para a realização do seu trabalho quer enquanto estudante quer como funcionário, no caso especifico da faculdade.

Neste momento a faculdade não dispões de uma plataforma desta contudo com este trabalho espero conseguir com que a faculdade explore esta hipótese e que pense bem que é uma ótima altura para mudar e no meu ver para mudar para melhor e que uma plataforma destas faz muito sentido no âmbito escolar como num âmbito empresarial, sendo que é muito usado principalmente por empresas estrangeiras e com um grande nível eficiência e aumento de produtividade das mesmas.

Bibliografia

Bertino, E., & Takahashi, K. (2011). Identity Management: Concepts, Technologies, and Systems. Artech House.

Gartner. (2016). Identity and Access Management (IAM). Obtido de Gartner: http://blogs.gartner.com/it-glossary/identity-and-access-management-iam/

Microsoft. (2016). What is LDAP. Obtido de Microsoft Developer Network: https://msdn.microsoft.com/en-us/library/aa367036(v=vs.85).aspx

Nabeth, T. (2009). Identity of Identity. Em K. Rannenberg, D. Royer, & A. Deuker (Edits.), The Future of Identity in the Information Society (pp. 19-69). New York: Springe

Pfitzmann, A., & Hansen, M. (10 de 09 de 2010). Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management—A Consolidated Proposal for Terminology. Obtido de Technische Universität Dresden: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management—A Consolidated Proposal for Terminology

Margaret Rouse and Linda Rosencrance. identity and access management (IAM). Advances in access governance strategy and technology: https://searchsecurity.techtarget.com/definition/identity-access-management-IAM-system

Prabath Siriwardena. Identity Architect Ground Rules: Ten IAM Design Principles: https://wso2.com/whitepapers/identity-architect-ground-rules-ten-iam-design-principles/

NetIQ® Identity Manager(2018). Overview and Planning Guide: https://www.netiq.com/documentation/identity-manager-47/pdfdoc/idm_overview_planning/idm_overview_planning.pdf

"Things" will force makeover of enterprise ID, access management by John Fontana

http://www.zdnet.com/article/things-will-force-makeover-of-enterprise-id-access-managemen t/

Deploy360@IETF92, Day 2: DNSSEC, DANE, IPv6, IoT and Homenet http://www.internetsociety.org/deploy360/blog/2015/03/deploy360ietf92-day-2/

Managing the Authorization to Authorize in the Lifecycle of a Constrained Device https://datatracker.ietf.org/doc/draft-gerdes-ace-a2a/?include_text=1

Expert Group on the Internet of Things (IoT-EG) http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1752

The shift from IAM to Identity Relationship Management by Joni Brennan, Kantara Initiative http://www.scmagazine.com/the-shift-from-iam-to-identity-relationship-management/article/3 38758/

Identity Relationship Management by Kantara Initiative https://kantarainitiative.org/irmpillars/

Anexos

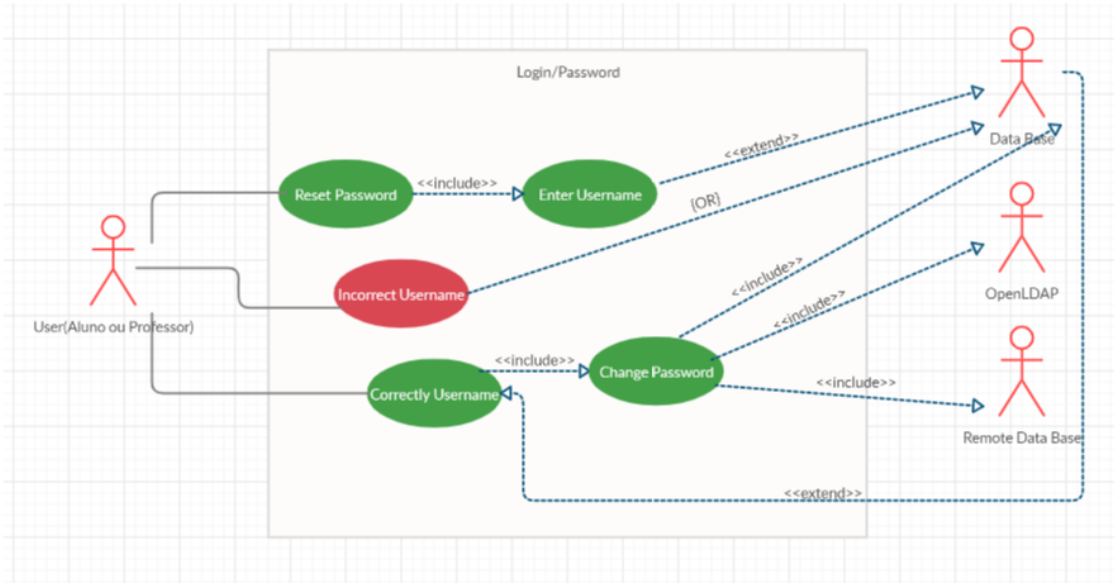

Figura 32 Change Password

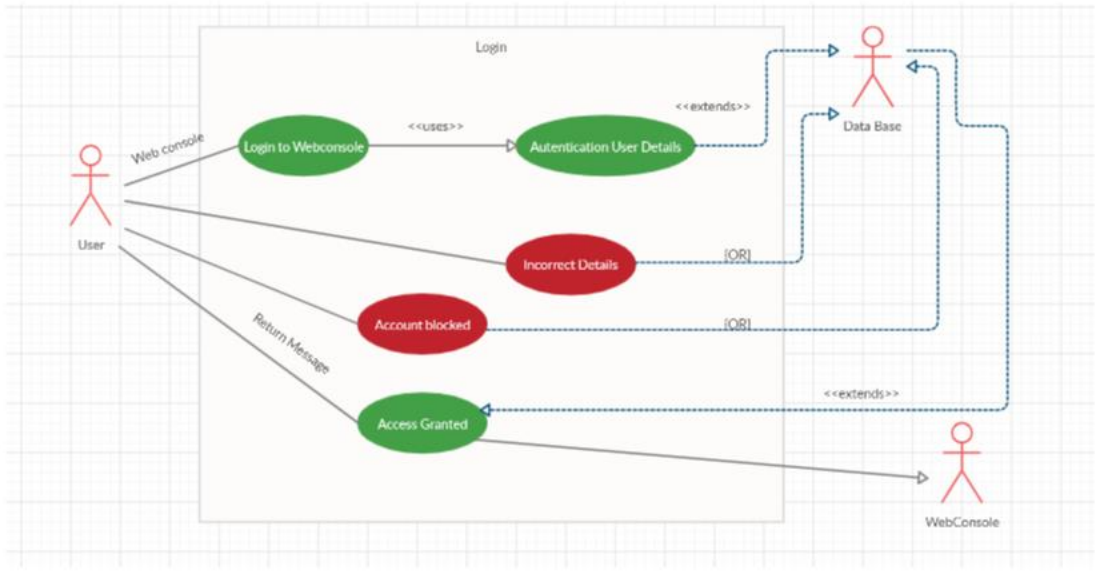

Figura 33 Login

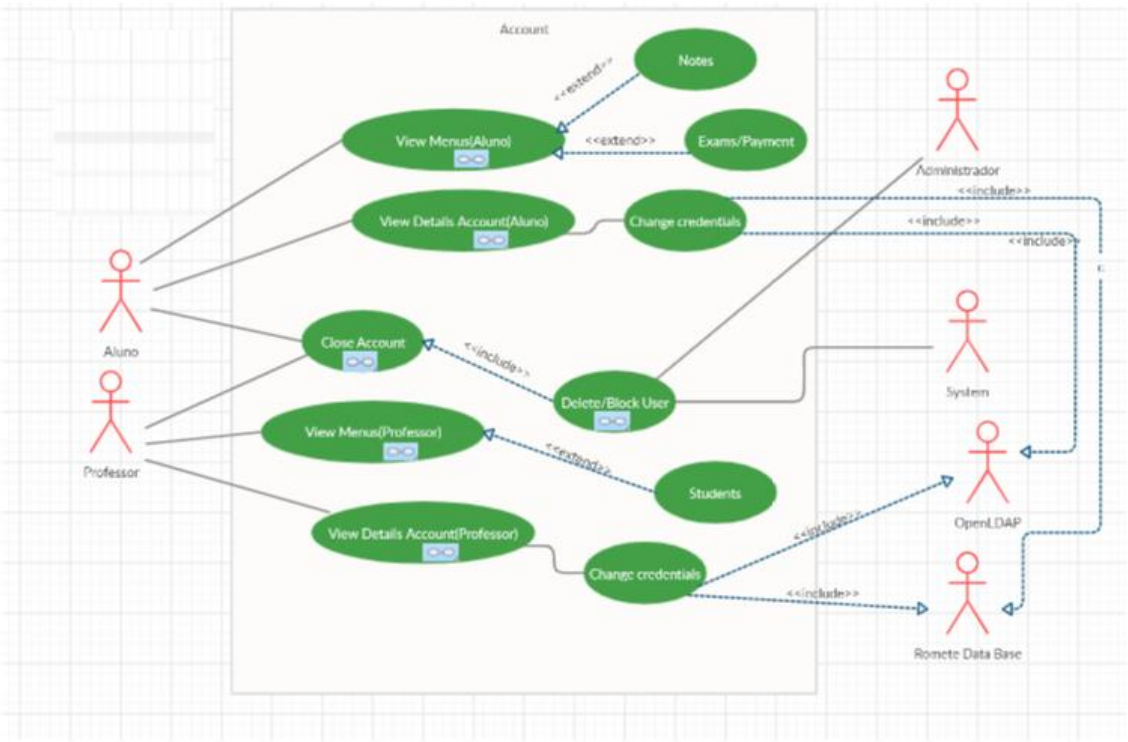

Figura 34 Account

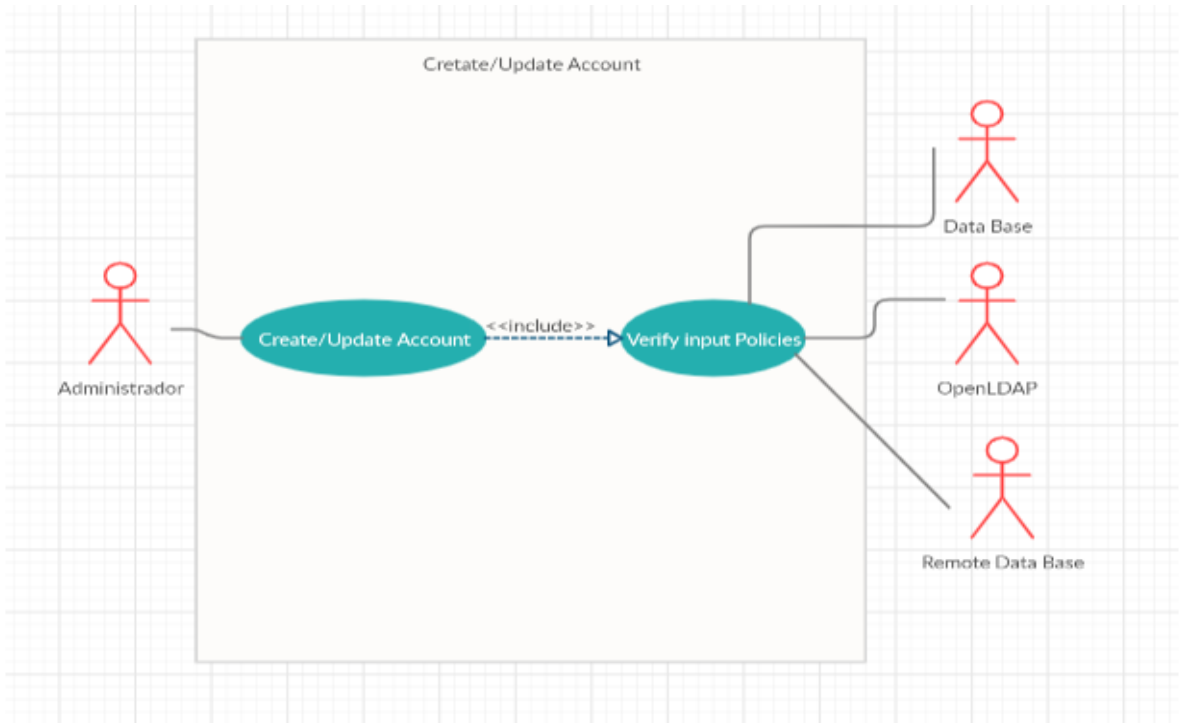

Figura 35 Create/Update Account

Glossário de Acrónimos

TFC- Trabalho de final de curso

IAM- Identity and Access Management

HIPAA- Health Insurance Portability and Accountability Act

TI- Tecnologia da Informação

IDM-Identity Management

PKI- public key infrastructure

NIST- National Institute of Standards and Technology

SSO- Single sign-on

HR- Human Resources

SSH- Secure Socket Shell

API- Application Programming Interface~

REST- Representational State Transfer

SDK- Software development kit

RDBMS- Relational Database Management System

LDAP- Lightweight Directory Access Protocol

CRM- Customer relationship management

IoT- Internet of Things

URI- Uniform Resource Identifier

SAML- Security Assertion Markup Language

SOAP- Simple Object Access Protocol

IP- Internet Protocol

JDBC- Java Database Connectivity

LDIF- LDAP Data Interchange Format