Universidade Fernando Pessoa

Gestão de Diplomas Online
Geração, Distribuição e Autenticação Online de Diplomas Académicos

Rúben Pereira Relvas

Faculdade de Ciência e Tecnologia

Universidade Fernando Pessoa

Dissertação apresentada á Universidade Fernando Pessoa como parte dos Requisitos para obtenção do grau de Mestrado em Engenharia Informática no ramo de Computação Móvel

Orientador: Prof. Doutor Luis Borges Gouveia

Julho 2020

Rúben Pereira Relvas

Gestão de Diplomas Online

Geração, Distribuição e Autenticação Online de Diplomas Académicos

Gestão de Diplomas Online

Geração, Distribuição e Autenticação Online de Diplomas Académicos

Por:

Rúben Pereira Relvas

Orientador:
Professor Doutor Luis Borges Gouveia

Dissertação apresentada á Universidade Fernando Pessoa como parte dos Requisitos para obtenção do grau de Mestrado em Engenharia Informática no ramo de Computação Móvel.

Universidade Fernando Pessoa – Porto, 2020

Resumo

Nesta dissertação pretende-se implementar um sistema de informação com o propósito de aumentar a eficiência nas emissões de diplomas digitais, também a distribuição, autentificação e acessibilidade aos diplomas universitários em formato digital, permitindo assim um sistema de informação *open source* dinâmico para permitir interligar universidades, alunos e outras instituições académicas, mesmo com as respetivas diferenças em termos de privacidade e políticas na gestão de documentos. Já existem atualmente métodos comprovados para a emissão de diplomas digitais, quer teóricos quer práticos. Contudo, há ainda muito espaço por explorar, nomeadamente quando se pretende tirar partido das melhores funções que as tecnologias disponibilizam para assegurar a integridade, flexibilidade e segurança no processo de emissão dos diplomas digitais.

Para garantir a eficiência na emissão e distribuição torna-se necessário desenvolver e disponibilizar uma interface Web ligada a um servidor online com o propósito de facilitar a gestão em sistemas de informação dos diplomas universitários.

Um sistema de informação com interface Web permite ao utilizador autenticar-se, gerir o seu perfil, fazer pedidos para emissão de diplomas digitais e partilhar um código de *hashcode* permitindo a outras pessoas validar o diploma digital na mesma interface Web.

A autenticação requer a validação em sistemas de informação e os diplomas digitais podem recorrer ao uso de *Blockchain*, Selos, Certificados, Assinaturas Digitais, assegurando a confiança em todos os documentos geridos pelo sistema de informação.

Palavras-chave

Diploma Digital Universitário, Interface Web, Hashcode, Blockchain, Certificados Digitais, Distribuição Online

Abstract

This dissertation intends to implement an information system with the purpose of increasing the efficiency in digital diploma emissions, the distribution, authentication and accessibility of university diplomas in digital format, thus allowing a dynamic open source information system to interconnect universities, students and other academic institutions, even with their differences in privacy and policy in document management. There are already proven methods for the issue of digital diplomas, both theoretical and practical. However, there is still work to be done and areas to be explored, especially when emergent or new technology offers are available to support integrity, flexibility and security in the process of issuing digital diplomas.

To guarantee the efficiency in the issuance and distribution it is necessary to develop and make available a Web interface connected to an online server for the purpose of facilitating the management of information systems to produce university diplomas.

An information system with Web interface allows the user to authenticate himself, manage his profile, make requests for the issuance of digital diplomas and share a hashcode code allowing other people to validate the digital diploma.

Authentication requires validation in information systems and digital diplomas can use, as Blockchain, Stamps, Certificates, Digital Signatures, ensuring the trust in all documents withim the proposed information system.

Keywords

University Digital Diplomas, Web Interface, Hashcode, Blockchain, Digital Certificates, Online Distribution

Agradecimentos

Quero agradecer ao meu orientador, Professor doutor Luis Borges Gouveia, pela disponibilidade que ofereceu durante o processo de desenvolvimento da minha dissertação.

Também agradeço aos professores e colegas da Universidade Fernando Pessoa que me ouviram e ofereceram opiniões para sobres as ideias iniciais da dissertação, obtendo os objetivos que pretendo concluir no final da dissertação.

Por último agradeço aos meus pais por me terem oferecido a oportunidade de concluir mais um ciclo de estudos universitários.

A todos, um grande obrigado.

Tabela de Conteúdos

Índice de Figuras

Índice de Tabelas

Acrónimos

Um relato estruturado de siglas relacionadas com o trabalho, de acordo com a sua sequência de apresentação.

EU, (*European Union*), em Português, União Europeia (EU) é uma união económica e política de estados, certas políticas económicas envolvem diplomas universitários, mas não tem métodos automáticos para reconhecer os mesmos diplomas universitários conforme referido em documentos oficiais (Your Europe, 2018).

SI, Sistema de Informação é um sistema automático de informação, permitindo gerar, organizar e distribuir informação para utilizadores local ou global (s/d, *An Introduction to Information Retrieval*).

BC, *BlockChain* é uma tecnologia que regista a distribuição de dados de forma descentralizada como método de segurança (Yli-Huumo *et al.*, 2016).

BD, Base de dados é um sistema de ficheiros relacionados entre si e que também pode referir o seu conteúdo (s/d, *Best Relational Databases Software in 2018*). As bases de dados permitem o armazenamento e recuperação eficiente de dados.

ES, Ensino Superior é o nível mais elevado do sistema educativo, referindo-se normalmente a uma educação realizada em universidades, faculdades ou instituições que conferem graus académicos ou diplomas profissionais (como o caso em Portugal dos Institutos Politécnicos e os Institutos Universitários).

DD, Diploma Digital é um documento universitário comprovando que um universitário concluiu um curso, em formato digital (s/d, *Digital Diploma Mills: The Automation of Higher Education*).

DU, Diploma Universitário é um documento universitário comprovando que um universitário concluiu um curso, em formato papel.

IW, Interface Web (*Web Interface*) é um espaço onde ocorre interação entre homem e máquina, com o objetivo de controlar a máquina e receber as suas respostas (s/d, *Interaction design: Beyond human computer interaction*).

EU, Equivalência Universitária é um comprovativo de uma universidade que emite para provar que um universitário com um diploma no estrangeiro tem um reconhecimento universitário no estado da universidade.

RA, Reconhecimento Universitário é um reconhecimento da conclusão de cursos ou normas de cursos universitários por parte das universidades noutros estados.

AU, Aluno Universitário é um individuo que recebe formação e instrução para adquirir ou ampliar os seus conhecimentos, num dado contexto, que deve ser explicito, em uma data instituição de ensino superior.

IU, Instituição Universitária é uma instituição de ensino superior pluridisciplinar e formação de quadros profissionais de nível superior e domínio do saber humano. Em contexto universitário, além da formação, existe também uma componente associada com a criação e desenvolvimento de conhecimento.

CU, Curso Universitário é um nível elevado dos sistemas educativos e uma educação realizada em universidades.

IA, Inteligência Artificial é a inteligência similar á humana exibida por mecanismos ou software (s/d, *Artificial Intelligence: A Modern Approach*).

FFP, Fundação Ensino e Cultura Fernando Pessoa tem por finalidade o desenvolvimento de atividades de promoção da educação, do ensino, da cultura e da investigação científica, da formação profissional e corporativa, da saúde pública.

UFP, Universidade Fernando Pessoa instituída pela FFP e reconhecida de interesse público pelo Decreto-Lei nº 107/96, de 31 de Julho, é o resultado de um projeto inovador de ensino superior, iniciado nos anos de 1980, através do Instituto Superior de Ciências da Informação e da Empresa, e do Instituto Erasmus de Ensino Superior, que lhe serviram de base estruturante e cuja antiguidade de graus e diplomas herdou.

UO, Universidade Online é uma universidade em acesso aberto na Internet, e de certas formas inteiramente gratuita, contem temas e recursos para uma experiência de aprendizagem *online*.

APOI, Apache POI é uma *framework* na plataforma Java que possibilita a leitura e a escrita de dados em um documento do Microsoft Office.

MD5, Algoritmo de Mensagem Direta 5 é uma função *Hash* criptográfico cujo desempenho é uma série de dados com entrada aleatória, com um tamanho fixo no valor de *Hash* para o resultado.

SHA-2, Secure *Hash Algorithm* 2 é um conjunto de funções *Hash* criptográficas projetadas pela Agência Nacional de Segurança dos Estados Unidos ou NSA.

QR Code, *Quick Response Code* é um código de barras bidimensional que pode ser facilmente passado por um digitalizador usando a maioria dos telefones móveis equipados com câmara (*smartphones*).

URL, *Uniform Resource Locator*, é um termo técnico como localizador uniforme de recursos, refere-se ao endereço de rede no qual se encontra algum recurso informático, como por exemplo um arquivo de computador ou um dispositivo periférico como impressora, equipamento multifuncional ou unidade de rede.

Ether, *Ethereum* é uma plataforma de computação distribuída baseada na tecnologia BC, é um sistema operacional que apresenta funcionalidade de contrato inteligente ou *scripting*.

1 Introdução

1.1. Descrição do Problema

A aquisição do diploma universitário para um aluno universitário que concluiu o seu curso é um momento que acontece uma vez por cada curso concluído. Contudo, o processo de emissão tem custos, riscos de garantias, questões de autenticidade e burocracias elevadas. Tudo isto envolve tempo e recursos, envolvendo um conjunto de problemas que podem vir a piorar ano após ano, principalmente quando o número para processos de emissões aumenta (Brandão, 2018). Processos estes que podem aumentar em escola, mas essencialmente em complexidade, por via de um previsível aumento na diversidade de diplomas e perfis a certificar.

No século XXI há uma expansão no mercado educativo com o surgimento das Universidades Online, o que implica uma automação e incorporação de práticas de base digital, muitas vezes em alternativa ao presencial, também para a realização de muitas das interações administrativas. Esta automação no mercado educativo implica 3 problemas em Instituições Universitárias: liberdade académica, direitos de propriedade intelectuais e rendimento. Estes problemas podem ser resolvidos de acordo com duas práticas:

- A primeira prática é a exploração da comercialização cooperativa de pesquisa, licenciamento e reatribuição dos direitos das propriedades intelectuais;
- A segunda prática é a comercialização através da automação do currículo académico e direitos das propriedades intelectuais (Petrina, 2005).

Os problemas envolvem principalmente as emissões e distribuição de diplomas académicos por rácios associados com as seguintes questões:

- Custos na própria emissão do diploma como o papel e impressão deve respeitar um perfil de qualidade definido pela instituição emissora;
- Falta de Estabilidade na própria mobilidade em que uma pessoa pode levar o diploma para onde quiser, mas a validação do diploma leva o seu tempo a

comprovar – potenciando dificuldades de diversa ordem na compreensão, validação e verificação do diploma e do seu significado;

- Verificação de Autenticidade, que envolve a validação da própria informação no diploma. Esta ação é ainda mais comum ser realizada por comunicação individual, não automática e personalizada, com a universidade que emitiu o diploma;

- Burocracias que envolvem o enquadramento legal de origem do diploma, a acrescentar às normas e preferências próprias, definidas pelas universidades que geram os diplomas e as suas equivalências.

Curiosamente, o processo de emissão de diplomas universitários não tem sido alterado nas últimas décadas. Podemos assim, considerar que as emissões de diplomas em:

- Universidades Privadas possuem controlo completo das emissões e números de vagas das candidaturas ano após ano levando a poucas burocracias nas emissões. Todos os recursos para emissões de diplomas são propriedade da universidade privada e não usam recursos exteriores diminuindo assim os seus custos. As validações são feitas tradicionalmente por um pedido ao gestor de diplomas na universidade por um meio de comunicação e leva algum tempo a validar a informação pedida na sua base de dados e depois envias a resposta a que fez o pedido de validação, dando um número de pedidos pode levar a uma falta de estabilidade com o tempo necessário para fazer autenticação em questão – estes processos são no entanto muito sensíveis a escala e complexidade e, em função disso, tem associados custos e tempos de espera, com impacto para a qualidade de serviço, bem como o aumento de custos de funcionamento da instituição em causa;

- Universidades Públicas tem de cumprir exigências anuais e procedimentos administrativos que lhes são normalmente impostos por um quadro legal, maior que a própria instituição. Tal pode aumentar a falta de estabilidade com o número de processos em questão, introduzindo alterações promovidas exteriormente à instituição. Todos os recursos para emissões de diplomas podem ou não ser propriedade da universidade pública. Com o uso de recursos

exteriores, podem aumentar os problemas em questão da necessidade de integração e de interação com terceiros, aumentando o tempo de resposta (com menos controlo);

- Universidades Online contém mais problemas do que outras universidades. As Universidades Online pode ser um sistema completamente automático, sem presença física, ou seja, pode ter apenas uma representação digital. Assim, toda a interação é normalmente canalizada para um servidor da Internet e as interações com a universidade *online*, realizadas por meio de uma interface Web. Por esta razão, qualquer recurso na emissão de diplomas encontra-se no exterior da universidade *online* e o número de emissões de diplomas é definido pelo número de cursos concluídos. Dependendo do contexto, os limites de vagas anuais nos cursos *online* mão são tão estáveis, o que leva a custos não só elevados, mas também sem conhecimento prévio do número de emissões por ano. Estes diplomas devem alicerçar nas burocracias, também as respostas à credibilidade dos diplomas emitidos para os cursos das universidades *online*: se estes comprem todas os requisitos de ensino académico.

1.2. Soluções Possíveis

A solução mais óbvia passa pela emissão dos diplomas universitários em formato digital, aumentando a eficiência da produção nas emissões. Tal pode permitir reduzir os problemas nas instituições académicas para melhorar a distribuição e validações dos seus certificados, através de uma interface Web (Petrina, 2005).

Um Sistema de informação baseado na Web proporciona acesso fácil a documentos e outros recursos digitais, bem como facilita a sua gestão. Os documentos são importantes como recursos de informação, mas a sua busca é ainda pouco suportada por motores de pesquisa.

Vários cientistas estão a tentar explorar e propor tecnologias para representar estruturas de modo a melhorar a descoberta de informação, criando assim um sistema que oferece uma melhor busca de informação e validação da informação (MABEE, 1993).

Nesta dissertação pretende-se propor e implementar um sistema de informação para garantir a eficiência e reduzir os problemas, envolvendo uma interface Web ligada a um servidor online com portefólios universitários digitais, opções para processos de emissões, equivalências e autenticidade de documentos universitários com os seus certificados. Aumentando assim a sua eficiência e integrando os diplomas com o próprio processo de ensino e aprendizagem, além de permitir a distribuição de diplomas globalmente (Stumpe and Katina, 2017).

A implementação de métodos com o propósito de aumentar a distribuição e validação do diploma universitários envolve a emissão do diploma em formato digital, de que atualmente, já existem alguns exemplos, mas pouco implementados e distribuídos. A União Europeia mencionado em Your Euroe (2018), alerta que não há métodos automáticos para fazer validações de diplomas académicos, entre os seus estados membros. Por isso todas as instituições universitárias geram os seus diplomas e equivalências universitárias como bem entenderem. Existem apenas simples validações de diplomas digitais em certas entidades certificadoras, normalmente promovidas por instituições de maior dimensão e/ou prestígio (Universidade do Porto, 2018; Valid, 2019).

Existem assim poucas universidades e empresas que atuam como entidades certificadoras, propondo os seus métodos digitais para o propósito da distribuição e validação dos seus documentos. Devido às suas preferências e privacidade, só os documentos públicos implementam uma boa distribuição e validação, para o utilizador em geral. Para documentos com alguma informação considerada privada está bastante limitada a métodos que envolve autentificação do utilizador ou do validador que pretende fazer a validação de informação ou mesmo a pedir uma equivalência entre países, como mostram, por exemplos, os serviços online disponíveis de Universidade do Porto, 2018 e Valid, (2019). O mesmo se passa na UFP, onde existe um serviço especializado associado com as relações internacionais; porem, neste caso, sem dimensão digital.

Dois casos digitais são o “e-Diploma” (Valid, 2019) e o “Digitary” (Universidade do Porto, 2018). São duas interfaces Web privadas para suportar uma entidade certificadora e utilizadores, mas ao serviço das suas respetivas comunidades. Cada utilizador tem o seu diploma em formato digital e quando alguém quiser validar o seu

diploma o próprio utilizador envia de forma eletrónica um código num endereço à outra pessoa e essa pessoa pode validar o diploma na mesma interface Web.

A implementação de métodos para validação de diplomas requer a introdução da informação para identificar o aluno diplomado e o seu diploma universitário. Estes métodos envolvem uma busca com a introdução de informação que está disponível no documento em questão. Já foram implementados serviços de busca como o mencionado. Estes serviços servem como fontes de boas práticas, tais como os casos de buscas de documentos legais e outros que envolvem informação privada (Brandão, 2018). Um outro exemplo são os serviços de consulta de patentes. Um dos aspetos comuns destes serviços é o custo baixo dos recursos nas bases de dados, com uma boa proteção de dados – o maior custo está quase sempre associado na gestão da informação para alimentar a base de dados (o que não se coloca no nosso contexto, pois essa informação existe por se tratar de informação administrativa e operacional que é mantida pelas instituições de ensino superior).

Um exemplo de busca envolvendo só a identificação do documento leva à busca que compara a identificação introduzida à lista de identificações existentes, na base de dados. Esta implementação pode estar a comprometer uma lista com diversas identificações de documentos. Um exemplo de dois campos de informação introduzida, como nome ou número de cliente e a identificação do documento, constitui a forma mais comum de acesso. Assim, a lista na base de dados em questão pode ser filtrada com a informação adicional, podendo inclusive oferecer mais informação de contexto, como listas de identificadores correlacionados ou próximos dos introduzidos (caso haja cobertura legal no que respeita à privacidade). Podemos assim conseguir um serviço mais conveniente e rápido obter uma resposta e a base de dados usou poucos recursos.

Mais um exemplo de buscas a documentos digitais e que pode ser mais conhecido, é o das Consultas de Faturas e Recibos Verdes no Portal das Finanças do governo de Portugal. Mencionado na reportagem (TVI24, 2018), qualquer cidadão português tem acesso à interface Web. Neste serviço é possível fazer uma consulta a qualquer um dos documentos existentes, basta ter o NIF do Adquirente e o número do documento e introduzir esses dados na busca disponível.

1.3. Outras Possibilidades

Um diploma universitário em formato digital não serve só para validar a conclusão do curso, mas também para explorar métodos que ainda não tem qualquer implementação automática, ao prover em base digital, o acesso a esta informação. Uma exploração seria um sistema de informação para obter equivalência universitária noutro país. A implementação de equivalências pode envolver um sistema de informação automático com os registos de realizações académicas dos alunos diplomados, aumentando à eficiência e benefícios das comparações de equivalências universitárias noutros estados. Em complemento, para empresas de recursos humanos ou para contratantes, pode ser forma de validar e comparar perfis, numa escala e com uma profundidade não possível sem a existência de funcionalidades e base digital. Por último, para instituições oficiais e de regulação poderia facilitar a obtenção de estatísticas, com mais velocidade e de maior qualidade.

No século XXI o processo de equivalência universitária é o mesmo nas últimas décadas como mencionado em Your Europe (2018), envolvendo um gestor de equivalências universitárias, por cada instituição universitária. O gestor verifica o diploma do cada aluno (independentemente da sua origem) que pode vir do estrangeiro, mais uma lista de cursos e disciplinas, em questão a instituição universitária de origem. Faz a comparação com os requisitos da sua instituição universitária e competente enquadramento legal e produz uma conclusão para mostra se o aluno do estrangeiro tem equivalência ou se a esta, faltam requisitos e quais. Este procedimento administrativo envolve uma quantidade razoável de trabalho, toma tempo e exige uma comparação individual por cada aluno do estrangeiro.

Nesta dissertação pretende-se propor um sistema de informação automático para as instituições universitárias para a emissão e validação de diplomas universitários próprios e assim oferecer aos seus antigos alunos, um processo expedito de verificação dos seus diplomas, com o propósito de aumentar a eficiência de emissões de diplomas digitais e a sua distribuição. A proposta envolvendo uma ligação às bases de dados entre o sistema de informação proposto e as instituições universitárias com informação dos seus cursos e dos alunos que os concluíram, utilizando o acesso aos sistemas de informação das várias universidades inscritas para obter informação sobre os respetivos diplomas académicos.

A informação encontrada nos diplomas ou requisitos de cursos universitários é considerada informação pública já que um aluno universitário pode apresentar o seu diploma a quem quiser e os requisitos de cursos está presente na Internet por cada instituição universitária. Assim os gestores de equivalências universitárias podem fazer uma comparação e um mapeamento dos requisitos de outras instituições universitárias e obter um relatório de síntese da comparação para servir de guia em automação das emissões de equivalência entre instituição universitárias.

Uma simples automação de equivalências universitárias pode ajudar vários alunos e as suas instituições universitárias, mas não basta para ter uma boa eficiência. Considerando o número de instituições universitárias na União Europeia vezes uma média de requisitos por curso, existe uma enorme quantidade de informação para o gestor de equivalências comparar, com a informação da sua instituição universitária. E a uma escala mundial, ainda mais complexo se torna. Uma implementação envolvendo inteligência artificial como menciona (Ligeza, 1995) pode revelar-se necessária. Se considerarmos um exemplo no sistema de informação proposto para processar os dados de comparação e produzir um resumo de equivalências dos cursos entre duas instituições universitárias, tomando também trabalho anterior já realizado. O gestor de equivalências universitárias pode aceitar e publicar o mesmo resumo no sistema de informação proposta, reutilizando trabalho já realizado e aumentando assim a sua eficiência.

1.4. Autenticação e Validação

O sistema de autenticação na era moderna envolve requisitos funcionais e legais que tem de ser compridos. Entre estes, estão a garantia de segurança dos sistemas de informação e dos certificados dos documentos. Existem várias tecnologias que asseguram a autenticação. Uma delas é a tecnologia Blockchain que proporciona graus elevados de confiança nos seus serviços mesmo que com elevados processos na transação e transparência de dados. As funções de Blockchain são utilizados em contextos mais críticos como o das cripto moedas, como por exemplo no funcionamento de transação e autenticação da Bitcoin, à escala global (Swan, 2015).

O sistema proposto tem de oferecer uma boa autenticação e segurança de dados. Por isso, implementações de funções e métodos da tecnologia Blockchain podem ser uma mais-valia. Como o sistema proposto envolve documentos e certificados legais, todas as transações de dados tem de ter comprovação que os dados vieram mesmo das instituições universitárias ou entidades certificadoras e não houve qualquer alteração, corrupção ou falsificação nas suas transações de dados, por mais que os mesmos dados fossem transmitidos ou retransmitidos por várias entidades na Internet. Um contexto que torna ideal a sua resolução por recurso ao Blockchain.

1.5. Entidades Certificadoras

Nesta dissertação é analisado o acesso a um Sistema de Informação como a Base de Dados de diplomas de Universidades pode se inscrever num sistema de validação de diplomas universitários. Com o propósito de utilizar e aceder aos sistemas de informação das várias universidades inscritas para obter informação sobre os respetivos diplomas académicos, criando assim um espaço comum de partilha de informação.

O diploma académico digital vai ser validado pelo sistema, e essa validação vai depender das ligações aos sistemas de informação das várias universidades para permitir emitir e validar os diplomas académicos. Assim, para permitir testar os parâmetros dos diplomas na versão experimental deste trabalho, seria também interesse uma ligação à base de dados da Universidade Fernando Pessoa e aos respetivos recursos porque é essencial dispor desta informação para obter dados realistas para os testes conducentes a efetuar para emitir e validar diplomas digitais, em contexto real.

O trabalho envolve o desenvolvimento de uma base de dados para integração do sistema de informação da Universidade Fernando Pessoa. A sua implementação requer:

- Dados Públicos como graus, cursos e atividade académica da Universidade Fernando Pessoa (aulas e outros dados adicionais para a produção do complemento de diplomas);

- Dados Privados como informação de diplomas académicos da Universidade Fernando Pessoa (nomeadamente os dados sensíveis e pessoais associados com cada um dos alunos associado ao diplome emitido – e em respeito do RGPD, regulamento geral de proteção de dados).

Nesta dissertação foi solicitado à Universidade Fernando Pessoa a autorização a um acesso temporário e restrito a uma pequena área da base de dados dos diplomas académicos da Universidade, sem ser necessário ter conhecimento ou comprometer os dados reais e privados dos alunos da Universidade, com o propósito de gerar diplomas fictícios e temporários apenas para efeitos de realização de testes. Por isso, apenas é necessário conhecer os parâmetros das ligações à base de dados da Universidade Fernando Pessoa e os parâmetros de segurança, e não os dados concretos – esse mesmo processo pode ser replicado para outras instituições e proporcionar um espaço de testes de introdução do serviço de validação.

Caso a política de privacidade de dados da Universidade Fernando Pessoa não permita ter acesso à base de dados dos diplomas, pode-se criar, em alternativa, uma base de dados fictícia dentro do sistema de informação da Universidade que permita garantir a mesma validade nos testes necessários realizar, bastando-me apenas conhecer quais são os parâmetros semelhantes aos da base de dados real da Universidade e autorização para criar a mencionada base de dados fictícia dentro do sistema de informação da universidade (o que acabou por ser realizado).

No sistema proposto, a base de dados tem à informação pública que já está disponível no local Web institucional da Universidade Fernando Pessoa. Desta forma, não se compromete a informação considerado privada ou confidencial pela Universidade. A informação de dados privados sobre os diplomas dos alunos que concluíram o seu curso é gerada automaticamente pelo sistema de informação da Universidade na base de dados, após a conclusão do curso. Como a informação nos diplomas é considerada privada para propósitos do mercado de certificados académicos, só é considerada pública e distribuível após o pagamento e emissão do 1º diploma.

Para o sistema de informação da Universidade Fernando Pessoa poder controlar a informação dos diplomas e garantir o seu mercado de certificados, o próprio sistema de informação da Universidade pode disponibilizar a informação de diplomas sobre

cursos concluídos na base de dados, para propósitos de validação das emissões disponíveis e controla a distribuição dos diplomas digitais.

O sistema de informação da Universidade Fernando Pessoa tem métodos para controlar a distribuição como:

- “Não Válida”, não houve nenhuma emissão ou pagamento do 1º diploma, por isso, mesmo que a informação do diploma digital, esta disponível com os seus certificados, não tem distribuição ou validação fora da UFP;
- “Válida”, houve uma emissão e um pagamento do 1º diploma, por isso, a informação do diploma digital que esta disponível com os seus certificados, e é permitido distribuir as suas validações online e um ficheiro digital.
- “Revogado”, houve algum problema na segurança ou limite de distribuição, por isso um diploma é revogado e proibido distribuir, ao mesmo tempo uma 2º versão do diploma é emitida e o diplomado é informado sobre o processo de revogação.

1.6. Assinaturas Digitais

A assinatura digital é uma tecnologia essencial para documentos digitais e pode ser gerada com vários métodos e parâmetros, envolvendo tecnologias, como o “Adobe Reader” (Adobe, 2017), “Microsoft Office” (Suporte do Office, 2018) e “Autenticacao.gov” (.GOV, 2018).

O programa “Adobe Reader” e “Microsoft Office” utiliza parâmetros personalizáveis envolvendo informação do indivíduo ou indivíduos que assina o documento como:

- Nome;
- Empresa;
- Identificação da sua posição de trabalho;
- Informação de contacto;
- Imagem da Digitalização de uma assinatura tradicional em papel;

- Assinatura Digital do Autenticacao.gov
- Assinatura Digital Móvel do Autenticacao.gov

O Diploma Digital tem um formato final para distribuição e validação do Adobe “PDF” para garantir que o ficheiro não se pode alterar ou falsificar.

O Diploma Digital tem uma aparência que mostra à estrutura e às preferências da Universidade que deve corresponder ao Diploma Académico tradicional emitido em papel. Estes aspetos gráficos podem ser implementados no Microsoft Office da mesma maneira que à estrutura do Diploma tradicional foi implementada.

Logo que um aluno tenha o seu curso concluído, deve estar identificado no ficheiro do diploma reservado para o aluno. A informação do ficheiro é utilizado para gerar um “Hashcode” (Deepakumara, Heys and Venkatesan, 2001) e depois introduzir no mesmo diploma como identificação do diploma.

Entre os serviços e tecnologias atualmente disponíveis para documentos digitais e distribuição global, destacam-se os seguintes:

- Selos Temporais

Os selos temporais passam prova da data e hora de criação, envio ou receção de um documento ou a transação eletrónica do seu processo. Esta validação cronológica é um requisito legal em muitos contextos, como no âmbito da Contratação Pública. As vantagens dos selos temporais são:

  - Certificam a existência de um documento ligado a um horário com data e hora;
  - Provam que um documento não foi alterado;
  - Garantem transparência e segurança na contratação pública;
  - Garantem que a abertura dos documentos é efetuada na hora definida.

- Certificados qualificados de assinatura digital

O Certificado de autenticação Web é um demostrador de que é possível autenticar uma página Web e associar ao mesmo uma pessoa individual ou várias pessoas à

qual o certificado tenha sido emitido. Os certificados podem ser em dois formatos Validação da Organização e Validação da Extensão:

- Validação da Organização

  Os certificados Validação da Organização ativam o HTTPS no navegador.

  Deste modo, asseguram que a Entidade possui uma identidade corporativa, bem como legitimidade e credibilidade online.

- Validação da Extensão

  O Certificado SSL com Validação da Extensão é automaticamente diferenciado da Validação da Organização, uma vez que visualiza o endereço do site, o SSL fica a verde.

  Este Certificado é um dos mais populares e utilizados no mundo, por empresas que queiram garantir o mais alto nível de segurança, confiança e legitimidade aos que visitam e utilizam a sua página Web. Muito comum em contexto do comércio eletrónico e dos negócios digitais.

- Certificados qualificados de Selos Eletrónicos

O Certificado Qualificado Selos Eletrónicos é utilizado exclusivamente por uma pessoa ou várias e garante a sua representação legal. São dados em formato eletrónico associado a outros dados em formato eletrónico para garantir a origem e a integridade. Os Selos Eletrónicos podem ser usados em:

- Faturas eletrónicas;
- Extratos de conta eletrónicas;
- Declarações eletrónicas;
- Outros documentos digitais com certidões e documentos emitidos em formato digital.

- Certificados de Autenticação de sítios web.

Hoje em dia, grande parte dos documentos como faturas, declarações, ofícios, certidões e outros documentos emitidos em papel são transacionados por via

eletrónica num formato digital. Em formato digital, é possível que todas as aprovações de documentos possam ser realizadas eletronicamente, bastando que se utilizem assinaturas digitais geradas a partir dos Certificados Digitais Qualificados ou Avançados.

Dado que existem mais do que um serviço das tecnologias digitais associadas com assinaturas digitais, são considerados métodos dinâmicos e opções mais personalizadas para as entidades certificadoras registadas no sistema proposto neste trabalho, permitindo assim uma boa interação entre o Sistemas de Gestor de Diplomas Online e Entidades Certificadoras sem ter conflito com as preferências e políticas da Universidade que use o sistema (e da possibilidade de esta evoluir no seu sistema de assinatura digital).

1.7. Razões da escolha

Todos os AU que concluírem um CU vão sempre pedir a emissão do DU no seu CU. Contudo, o processo de emissão dos DU tem os seus problemas que leva a um consumo de tempo elevado que pode ainda aumentar ano após ano. Soluções envolvendo DD e SI com BD pode diminuir os problemas e aumentar a validação com a sua distribuição, proporcionado assim grande vantagem para várias IU (Brandão, 2018).

Figura 1 Diploma Universitário

Um DU tem o seu valor no estado de origem, mas não tem valor internacional (Your Europe, 2018). Para obter valor internacional é preciso um AU apresentar o seu DU, mais uns documentos numa IU noutro estado e pedir EU, este processo tem que ser repetido por cada estado que o AU pretende ter RA. Este processo de EU tem um consumo elevado de tempo devido aos problemas das emissões DU, e pode ser melhorado consideravelmente com métodos e tecnologias modernas mencionado em (MABEE, 1993).

Métodos de emissões e distribuição são os mesmos nas últimas décadas, possuem custos, versatilidades, autenticidades, burocracias elevadas envolvendo tempo e recursos, por isso são considerados poucos eficientes, métodos digitais já foram considerados, mas pouco implementação. Métodos digitais não foram bem explorados e ainda podem ser considerados para obter maior eficiência nas emissões e distribuição globalmente (Guimbretière, 2003).

1.8. Objetivos do trabalho

Nesta dissertação o objetivo principal é o propor e desenvolver um protótipo de um SI com o propósito diminuir os problemas de DU, passando pela emissão dos DU em formato DD. Este esforço tem como finalidade o de contribuir para a eliminação de fraude no processo de expedição de diplomas e promover uma maior transparência, agilidade e aumentar a eficiência de emissões, a distribuição, autentificação e acessibilidade aos DU.

O SI proposto para emissões dos DU no ES garante a autenticidade, integridade, confiabilidade, disponibilidade, rastreabilidade e validade jurídica dos documentos emitidos, com recurso a soluções *open source* para interligar universidades, alunos e outras IU, mesmo com as respetivas diferenças em termos de privacidade e políticas na gestão de documentos.

O SI proposto considera métodos atualmente utilizados e comprovados para a emissão a DD. Adicionalmente, vai também implementar métodos e tecnologias ainda não explorados, nomeadamente quando se pretende tirar partido de melhores opções para assegurar a integridade, flexibilidade e segurança no processo de emissão e distribuição de DD.

Figura 2 Diploma na Interface Web

1.9. Estrutura do trabalho

Este relatório possui cinco capítulos que reportam o esforço realizado no projeto de dissertação. A primeira parte apresenta os objetivos do trabalho e o seu enquadramento, introduzindo as questões e problemas associados com a validação de diplomas. Descreve igualmente algumas das alternativas para o uso e exploração de assinaturas digitais. Conclui este capítulo a apresentação da motivação, dos seus objetivos e estrutura do documento.

O segundo capítulo apresenta as questões e as tecnologias associadas com o reconhecimento dos diplomas e as alternativas digitais para estes. Introduz também um conjunto de tecnologias que asseguram a validação e segurança de diplomas digitais e dos seus benefícios em contexto *online*.

O terceiro capítulo apresenta o sistema proposto, discutindo as tecnologias utilizadas, tomando como ponto de partida, a oferta de sistemas de terceiros, estudados. O quarto capítulo descreve o trabalho realizado no desenvolvimento do protótipo apresentando a sua arquitetura e opções tomadas para as estruturas de suporte à gestão da informação. Por último, o capítulo 5 fecha o trabalho, reportando a sua conclusão e informando do trabalho futuro.

2 Reconhecimento universitário e os diplomas *online*

2.1. Reconhecimento Universitário

A EU tem normas para reconhecer DU entre os seus membros de estados, certas normas envolve as IU de cada estado membro definir as suas regras de CU e os seus DU, que requer a um AU organizar o seu DU, mais um certificado de conclusão de CU e pedir uma EU noutros estados para ter RA, mais para estes casos não há nenhum método automático para reconhecer DU.

Casos normais para obter RA noutros estados envolve um AU com um DU pedir um processo de RA e acaba por não cumprir os requisitos, porque a IU no estrangeiro tem regras muito diferentes e requer que o AU cumpra os requisitos em falta para obter a sua EU.

Um processo de EU requer uma comparação do DU do estado de origem com o DU do estado estrangeiro, este processo requer que um AU tenha conhecimento do processo de EU e ter conhecimento das diferenças entre IU estrangeiras para ter um processo sem atrasos ou falta de requisitos. (Your Europe, 2018).

No século XXI há uma expansão no mercado educativo com a aparência das UO que implica uma automação e incorporação do mesmo mercado. Esta automação no mercado educativo implica 3 problemas em IU: liberdade académica, direitos de propriedade intelectuais e rendimento. Estes problemas podem ser resolvidos de acordo com duas práticas (Petrina, 2009):

- A exploração da comercialização cooperativa de pesquisa, licenciação e reatribuição dos direitos das propriedades intelectuais;
- A comercialização através da automação do currículo académico e direitos das propriedades intelectuais.

Nas últimas décadas não houve praticamente alterações na emissão do DU. Com a tecnologia houve melhoramentos na segurança, diminuição dos custos e gestão da

informação. Com o DD a maior parte dos custos podem ser eliminados, mas tem uma grande eficiência na sua distribuição e autenticação por um sistema automatizado. Após emitir um DU pode-se proceder a um serviço online e publico para que qualquer pessoa possa validar a autenticação do mesmo DU, isto é um serviço online que traz maior segurança e agilidade nos processos de autenticação do DU (José Luiz Brandão, 2018).

Com menciona Noble (1998), IU estão a entrar numa nova era de educação superior, que esta a esforçar IU a seguir direção para a era da automação, por meios de CU online sem requerer a participação de Educadores Universitários. A nova era esta a ser imposta de maneira a corresponder á demanda na qualidade de ensino na sociedade, mas a nova era tem de ser desenvolvida por métodos apropriados sem houver conflitos com os métodos tradicionais.

Hoje em dia o DD já existe com normas de implementação, mencionado na Administracao Digital (2018), o DD no âmbito das IU, públicas e privadas, pertencentes a sistema de ensino deve ser assinado por um certificado digital ICP-Brasil, a norma também abrange outros documentos acadêmicos como o registro e o histórico escolar dos AU. O uso do certificado ICP-Brasil garantirá a autenticidade, integridade, confiabilidade, disponibilidade, rastreabilidade e validade jurídica dos documentos emitidos.

O propósito da implementação do DD é de contribuir para a eliminação de fraude no processo de expedição de diplomas e promover maior transparência e celeridade nos procedimentos de emissão dos DU.

Também mencionado em Cryptoid (2018), DD será obrigatório por lei no território nacional e as IU terão dois anos para implementar o processo de DD nos seus sistemas, estando assim disponíveis sistemas com o ICP-Brasil obrigatórios no ano de 2020.

2.2. Sistema de Informação e Interface Web

Um SI baseado na Web proporciona acesso fácil a documentos e outros recursos digitais bem como a sua gestão. Os documentos são importantes como recursos de informação, mas a sua busca e pouco suportada por motores de pesquisa.

Figura 3 Sistema de Informação & Interface Web

Existem diversos esforços para explorar e representar estruturas para melhorar as buscas de informação, criando assim um sistema que oferece uma melhor busca de informação (MABEE, 1993).

Uma interface Web é uma das melhores formas de mostrar as opções possíveis, com o propósito de ajudar os utilizadores a entender as suas opções e proporcionar melhores serviços na Web sem comprometer dados do utilizador. Tal pode ser uma grande ajuda para vários utilizadores já que melhora a experiencia de cada utilizador com dados relacionados com as suas preferências individuais (Kurniawan, 2004; Untergasser *et al.*, 2007).

Tomando o princípio de que grandes bases de dados devem ser protegidas de maneira a não saber como os dados são organizados, para um serviço que fornece a informação da organização de dados não é a opção mais desejável.

Por via de métodos de buscas, atualizações ou do crescimento no tráfego de dados, as estruturas de informação estão em constante mutação. Para lidar com os requisitos de flexibilidade para adaptar a estas constantes alterações nas estruturas de dados, as bases de dados constituem uma ferramenta essencial, proporcionando uma gestão da informação mais facilitada (Codd, 1970).

2.3. A tecnologia Blockchain

De acordo com Yli-Huumo et al., (2016) a tecnologia BC é uma transação de dados descentralizados e gestão de dados, implementada inicialmente na cripto moeda Bitcoin. O interesse na tecnologia BC tem aumentado por causa da sua segurança, anonimidade e integridade dos dados, sem participação de organizações indesejadas ou um ator central, possuindo assim um caráter distribuído. Estas caraterísticas tem fomentado o interesse de investigadores de várias áreas.

Figura 4 Blockchain Ethereum

Áreas na pesquisa de BC envolvem transações e mapeamentos de dados com o objetivo de resolver as limitações da privacidade e segurança, mas ainda não tem avaliações concretas para aumentar a sua eficiência (Yli-Huumo *et al.*, 2016).

Mencionado em Swan (2015), o BC é muito mais significativo que a Bitcoin, porque está em posição de se tornar o quinto paradigma de computação disruptiva após *mainframes*, computadores pessoais (PC), Internet e as redes móveis.

Com o potencial de registo mundial descentralizado para o registo, inventário e transferência de todos os ativos, não apenas finanças, mas propriedades e bens intangíveis podem ser considerados. Assim, ativos como votos, software, dados de saúde e até ideias podem ser objeto de registo sujeito a validação – o mesmo acontece com os DU.

2.4. Hash code e QR Code

Mencionado por Notions (2011), há um interesse de pesquisa excecional em funções Hash criptográficas, especialmente após os ataques populares contra o MD5 e o SHA-1, para propósitos de garantir segurança criptográfica no mundo Web.

Referido por Deepakumara, Heys and Venkatesan (2001), a segurança da informação, a autenticação de mensagens é uma técnica essencial para verificar se as mensagens recebidas vêm da fonte original e não foram alteradas. O *Message Digest* 5 (MD5) é um dos algoritmos especificados para uso no IPSEC (*Internet Protocol Security*), como base num HMAC, uma técnica para produzir MAC baseada no uso de uma função Hash, tem um interesse crescente em aceleradores criptográficos de alta velocidade para aplicativos IPSEC, como Redes Privadas Virtuais.

Outra referência por Kim *(*2006), o HMAC é um código de autenticação de mensagens amplamente usado por um gerador de função pseudoaleatório baseado em funções Hash criptográficas, como MD5 e SHA-1, é provado seguro desde que a função de compressão da função Hash utilizada, seja uma função pseudoaleatória.

Mencionado por Kieseberg *(*2011) e Kucirkova, Audain and Chamberlain (2018), o código QR (*Quick Response Code*) é a marca comercial de um tipo de código de barras matricial (ou código de barras bidimensional) desenvolvido inicialmente para a indústria automóvel, a informação codificada por um código QR pode ser composta de quatro tipos padronizados ou modos de dados (numéricos, alfanuméricos, byte)

ou, através de extensões suportadas, virtualmente qualquer tipo de dados. A segurança examina os QR Codes e como eles podem ser usados tanto em contexto humano como automático – uma das grandes vantagens deste tipo de codificação.

Como afirmam Liu, Yang and Liu (2008), o código de resposta rápida tem sido amplamente utilizado nos campos de identificação automática, com uma implementação do reconhecimento do código de resposta rápida em tempo real usando dispositivos móveis, que é uma tecnologia eficiente usada para transferência de dados. Tal constitui um excelente meio de ligação entre o analógico e o digital e entre o humano e o automático.

2.5. Inteligência Artificial

A Inteligência Artificial é um campo alargado de estudo, que inclui áreas como agentes que recebem informação do seu ambiente e executam ações com autonomia, enquanto programas de computador. Estes agentes implementam funções de mapeamento de sequências para ações e definem vários métodos diferentes para representação das funções, proporcionando soluções flexíveis e com capacidade de decisão e resolução de problemas, sem intervenção humana.

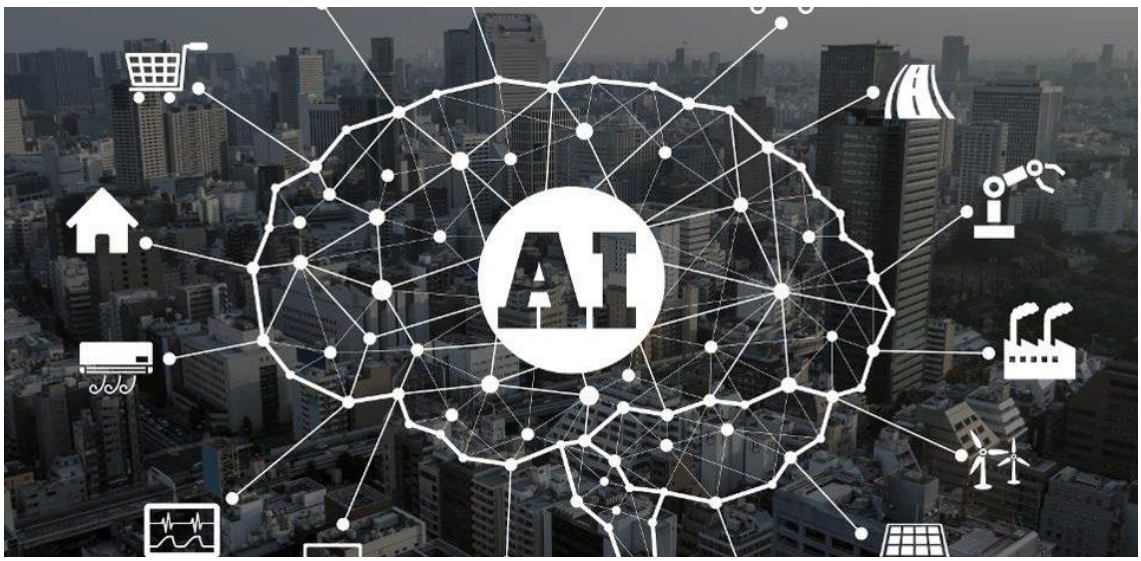

Figura 5 Inteligência Artificial

Por cada situação envolvendo um agente de IA e um ambiente de estudo o agente tem que ser o apropriado para interagir com o ambiente de maneira a poder gerar mapeamentos de funções para obter os resultados mais eficientes (Ligeza, 1995).

2.6. *Diplomas Online*

A Universidade do Porto licenciou a plataforma Web Digitary e ligou-a ao sistema de informação SIGARRA (Universidade do Porto, 2018), permitindo aos seus alunos graduados, dispor dos respetivos diplomas e correspondentes suplementos ao diploma em formato digital. No sistema, os estudantes que pretende dispor os seus documentos, devem solicitá-los através da opção Certificados associada à sua página pessoal. Os documentos estão disponíveis para ciclos de estudo ou cursos da Universidade do Porto, todos estudantes podem gerir o acesso aos seus próprios documentos *online*.

Figura 6 Digitary

Os utilizadores na “Digitary” têm opções através da criação de DAT ou *Document Access Tickets* que enviam a terceiros, para empregadores ou outras instituições de ensino superior. Os *tickets* enviados a terceiros são usados para aceder e visualizar os documentos, confirmando a autenticidade dos mesmos através da plataforma Web seguro alojado na Universidade do Porto.

Todos os estudantes da Universidade do Porto têm acesso à plataforma Digitary, depois de entrarem na página inicial da plataforma Web, acessível também através do endereço *https://diplomas.up.pt*. Caso um estudante não tenha os documentos na plataforma Digitary, por motivo de estes ainda não terem sido gerados pelos serviços académicos ou o estudante ainda não concluiu um curso académico, mostra um aviso de acesso não concedido.

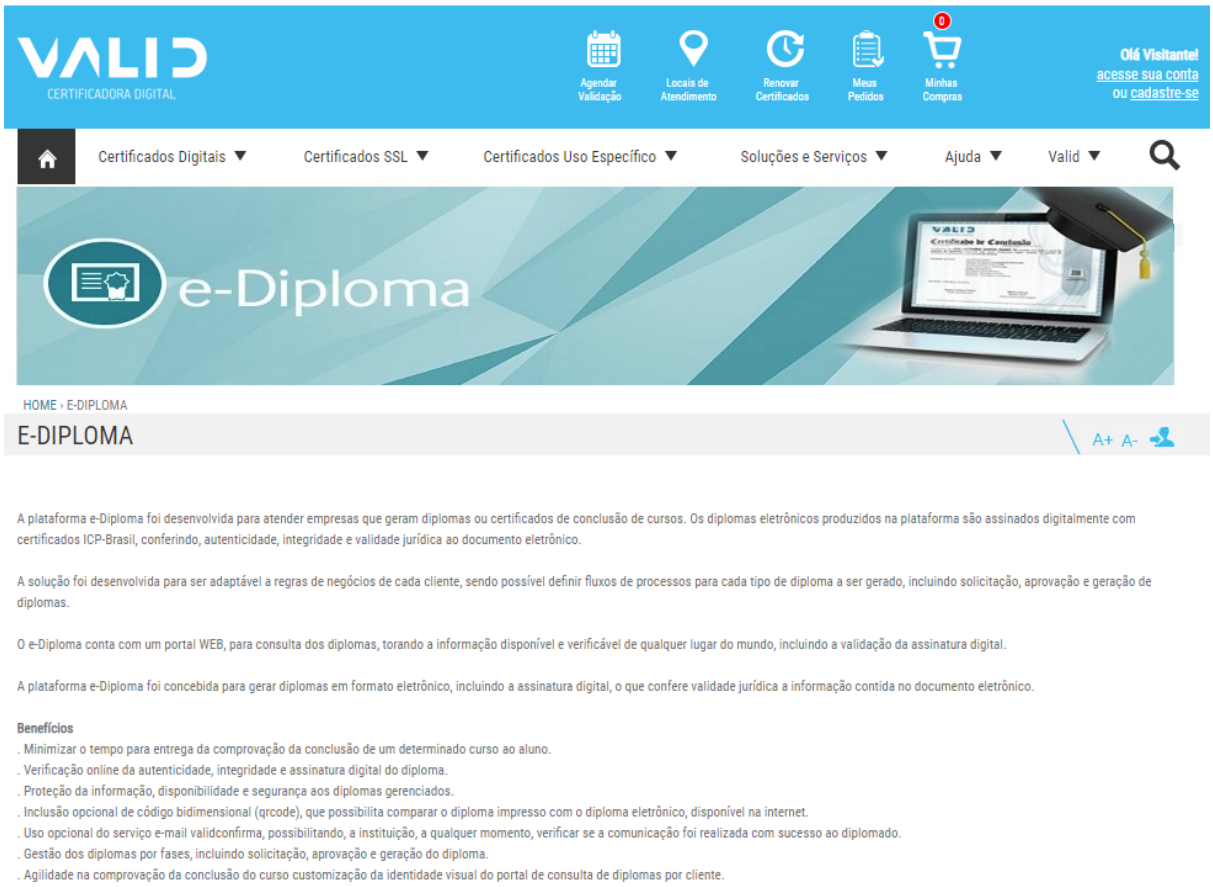

Figura 7 e-Diploma

A plataforma Web “e-Diploma” é um sistema foi desenvolvida para universidades que geram diplomas ou certificados de conclusão de cursos (Valid, 2019). Todos os diplomas eletrónicos gerados ou registados no e-Diploma são assinados digitalmente com certificados ICP-Brasil (Administracao Digital, 2018b), conferindo assim autenticidade, integridade e validade jurídica ao documento eletrónico. O sistema e-Diploma é uma solução empresarial que foi desenvolvida para ser adaptável às regras das universidades registados, enquanto clientes, sendo possível definir processos para cada tipo de diploma a ser gerado ou registado, incluindo a sua solicitação e aprovação.

O sistema e-Diploma é uma plataforma Web de consulta dos diplomas, permitindo disponibilizar e validar informação em qualquer lugar, por via digital, incluindo a validação das assinaturas digitais usadas nos documentos. O sistema foi criado para gerar e registar diplomas em formato digital com assinatura digital, o que confere validade jurídica à informação contida no documento digital. O sistema e-Diploma pode ser aplicada a qualquer entidade certificadora registada como qualidade de empresa, permitindo a gestão de certificados de conclusão e respetivos documentos (além dos diplomas, documentos como suplementos, atestados de capacidade, declaração de formação ou certificados provisórios).

Os benefícios no sistema e-Diploma, extensíveis a sistemas deste tipo, foram enumerados como:

- Minimizar o tempo para entrega, comprovação, conclusão dos documentos;
- Validação *online* da autenticidade, integridade e assinatura digital do documento;
- Proteção da informação, disponibilidade e segurança dos documentos gerados;
- Opões disponíveis de código bidimensional QR Code, permitindo comparar o diploma impresso com o diploma digital, disponível na Internet;
- Opões disponíveis do serviço e-mail para validação, possibilitando, à instituição, a verificação a qualquer momento, da comunicação realizada;

- Gestão dos documentos por fases, incluindo solicitação, aprovação e geração do documento;
- Agilidade na comprovação da conclusão do curso, com personalização da identidade visual do portal de consulta de documentos por cliente ou emissor de diplomas.

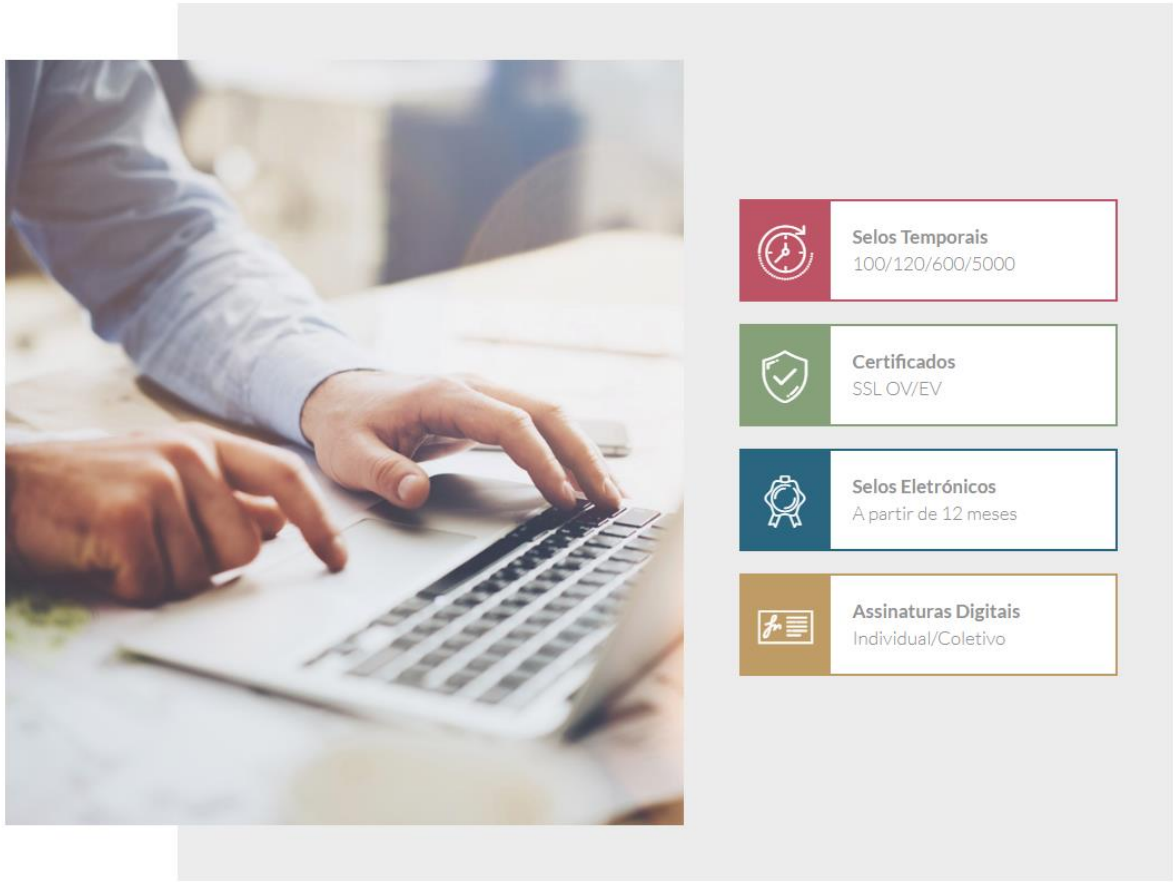

Figura 8 Global Trusted Sign

Empresas como a *Global Trusted Sign* (Global Trusted Sign, 2019) ou *Digital Sign* (Digital Sign, 2019) oferecem serviços com o propósito de digitalizar documentos tradicionais impressos em papel, para clientes que paguem os seus serviços.

A *Global Trusted Sign* e *Digital Sign* são empresas com serviços, credenciadas em Portugal para operar no quadro do Regulamento EU N.º 910/2014. Estas oferecem quatro serviços relevantes no nosso contexto:

- Selos Temporais

Figura 9 Selos Temporais

Os selos temporais passam prova a data e hora de criação, envio ou receção de um documento ou transação eletrónica do seu processo. Esta validação cronológica é um requisito legal no âmbito da Contratação Pública. As vantagens dos selos temporais são:

- Certificam a existência de um documento ligado a um horário com data e hora;
- Provam que um documento não foi alterado;
- Garantem transparência e segurança na contratação pública;
- Garantem que a abertura dos documentos é efetuada na hora definida.

- Certificados qualificados de Assinatura Digital

Figura 10 Certificados qualificados de Assinatura Digital

O Certificado de autenticação Web é um demostra que é possível autenticar uma página Web e associar ao mesmo uma pessoa individual ou várias pessoas à qual o certificado tenha sido emitido. Os certificados podem ser em dois formatos Validação da Organização e Validação da Extensão:

- Validação da Organização

Os certificados Validação da Organização ativam o HTTPS no navegador.

Deste modo, assegurar que a Entidade possui uma identidade corporativa, bem como legitimidade e credibilidade *online*.

- Validação da Extensão

  O Certificado SSL com Validação da Extensão é automaticamente diferenciado da Validação da Organização, uma vez que visualizam o endereço do *site* (local de presença Web), o SSL fica a verde.

  Este Certificado é um dos mais prestigiados e utilizados no mundo, por empresas que queiram garantir o mais alto nível de segurança, confiança e legitimidade aos que visitam e utilizam a sua página Web.

- Certificados qualificados de Selos Eletrónicos

Figura 11 Certificados qualificados de Selos Eletrónicos

O Certificado Qualificado Selos Eletrónicos é utilizado exclusivamente por uma pessoa ou várias e garante a sua representação legal. São dados em formato eletrónico, associados a outros dados também em formato eletrónico para garantir a origem e a integridade dos primeiros. Pode ser entendido como o equivalente digital ao tradicional carimbo. Os Selos Eletrónicos podem ser usados em:

- Faturas eletrónicas;

- Extratos de conta eletrónicas;
- Declarações eletrónicas;
- Outros documentos digitais com certidões e documentos emitidos em formato digital.

- Certificados de Autenticação de sítios web

Figura 12 Certificados de Autenticação de sítios web

Hoje em dia, grande parte dos documentos como faturas, declarações, ofícios, certidões e outros documentos emitidos em papel são transacionados por via eletrónica num formato digital. Em formato digital, é possível que todas as aprovações de documentos possam ser realizadas eletronicamente, bastando que se utilizem assinaturas digitais geradas a partir dos Certificados Digitais Qualificados ou Avançados.

2.7. Comparação de técnicas para diplomas digitais

Os sistemas de Digitary (Universidade do Porto, 2018) e E-Diploma (Valid, 2019) foram desenvolvidos para o propósito de gerar DD para EC. Nestas propostas foi realizada uma escolha da tecnologia que proporcione uma melhor distribuição com as preferências de um sistema privado ou público.

O sistema *Global Trusted Sign* (Global Trusted Sign, 2019) não foi desenvolvido para EC, mas para todos os propósitos de documentos digitais, oferecendo opções que pode satisfazer as preferências e requisitos dos clientes quer comerciantes ou empresariais.

A tabela seguinte resume as tecnologias enumeradas e mapeia com os sistemas existentes, de forma a comparar com o protótipo proposto a desenvolvimento.

Sistema	Tecnologias para Diplomas em Formato Digital			
	Selos Temporais	Certificados	Selos Eletrónicos	Assinatura Qualificadas
Digitary	X		X	
E-Diploma		X		
Global Trusted Sign	X	X	X	X
Projeto da Dissertação	X	X	X	X

Tabela 1 Tecnologias de Diplomas Digitais

O sistema da dissertação tem o propósito de garantir várias opções com tecnologias existentes, para permitir as EC e AU satisfazer os seus requisitos e preferências, com duas ou mais tenologias disponíveis.

Figura 13 ICP-Brasil

Uma norma recente de diplomas digitais é ICP-Brasil (José Luiz Brandão; Santo Contrato, 2018) ou Infraestrutura de Chaves Públicas Brasileira que é uma cadeia

hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão.

A norma ICP-Brasil foi proposta em 2018. Nos DD será obrigatório implementar a norma em todo o território Brasileiro, dando às Instituições de Ensino Superior dois anos para implementar um processo coma norma em vigor – processo que tem por limite o corrente ano. "*A Portaria nº 330, publicada em 6 de abril de 2018, estabelece a obrigatoriedade do uso do certificado digital no padrão da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil para assinatura dos diplomas digitais*" (Cryptoid, 2018).

3 Sistema proposto e tecnologias associadas

3.1 Proposta e comparação do sistema

No projeto da dissertação pretende-se implementar um sistema de informação com o propósito de utilizar métodos e tecnologias digitais para validar, autenticar e distribuir diplomas eletrónicos, semelhantes aos métodos e tecnologias existentes em contexto de mercado.

É pretendido implementar um sistema de informação para garantir a eficiência de distribuição, envolvendo uma interface Web com portefólios universitários digitais, opções para processos de emissões, equivalências e autenticidade de documentos universitários com os seus certificados. Acredita-se que uma proposta destas aumenta a eficiência do trato administrativo e proporciona uma distribuição de dados global (Stumpe and Katina, 2017).

Para tal procede-se à implementação de métodos para expandir validações de documentos com a introdução da informação que identifica o aluno e o seu diploma universitário. Estes métodos envolvem uma busca com a introdução de informação que esta disponível no documento em questão. Já foram implementados serviços de busca como descrito nos sistemas reportados.

Um diploma universitário em formato digital não serve só para validar a conclusão do curso, mas também para explorar métodos que ainda não tem qualquer implementação automática, tais como sistemas de equivalência, quer nacionais, quer internacionais, sendo estes últimos de maior complexidade e custos administrativos associados. A implementação de equivalências pode envolver um sistema de informação automático com os registos de realizações académicas dos alunos, aumentando à eficiência e benefícios das comparações de equivalências universitárias, independentemente dos contextos de validação, quer da origem, quer do local de aplicação do DD.

No projeto da dissertação pretende-se adicionar um sistema de informação automático para as instituições universitárias, com o propósito de aumentar a eficiência de emissões de diplomas digitais e a sua distribuição. Envolvendo uma

ligação às bases de dados entre o sistema de informação proposto e as instituições universitárias com informação dos seus cursos e dos alunos que os concluíram, utilizando o acesso aos sistemas de informação das várias universidades inscritas para obter informação sobre os respetivos diplomas académicos.

3.2 Restrições do trabalho desenvolvido

As restrições neste problema são encontradas nos testes, com a conclusão do desenvolvimento da IW e as suas funcionalidades concluídas, inicia-se os testes de funcionamentos, para obter dados reais e concretos são necessários ligações a BD de uma IU para fazer testes envolvendo informação de DU fictícios, outra ligação é ao sistema de informação bancário para poder testar processos com pagamento multibanco ou eletrónicos.

Estes níveis de integração não foram implementados, tendo apenas sido realizada a sua menção e criados as estruturas de dados associas, que carecem de teste e afinação. Deste modo, o sistema desenvolvido constitui um protótipo inicial. Estas duas restrições impedem os testes de funcionamento associados com o impacto e funcionalidade do sistema como serviço autónomo. Nesse contexto, um esforço adicional ao realizado terá de ser realizado.

3.3 Tecnologias utilizadas

Para o desenvolvimento do protótipo foram utilizadas um conjunto de tecnologias. O critério principal para a sua escolha foi, além de poderem responder aos requisitos estabelecidos, serem tecnologias de domínio aberto (*open source*). Nesta seção é dada conta dos diferentes recursos tecnológicos considerados.

Base de Dados PostgreSQL

O PostgreSQL é sistema de gestão de base de dados objeto-relacional. É um software *open source* com mais de 30 anos de desenvolvimento ativo que lhe garantiu uma forte reputação de confiabilidade, robustez de recursos e desempenho (PostgreSQL, 2019).

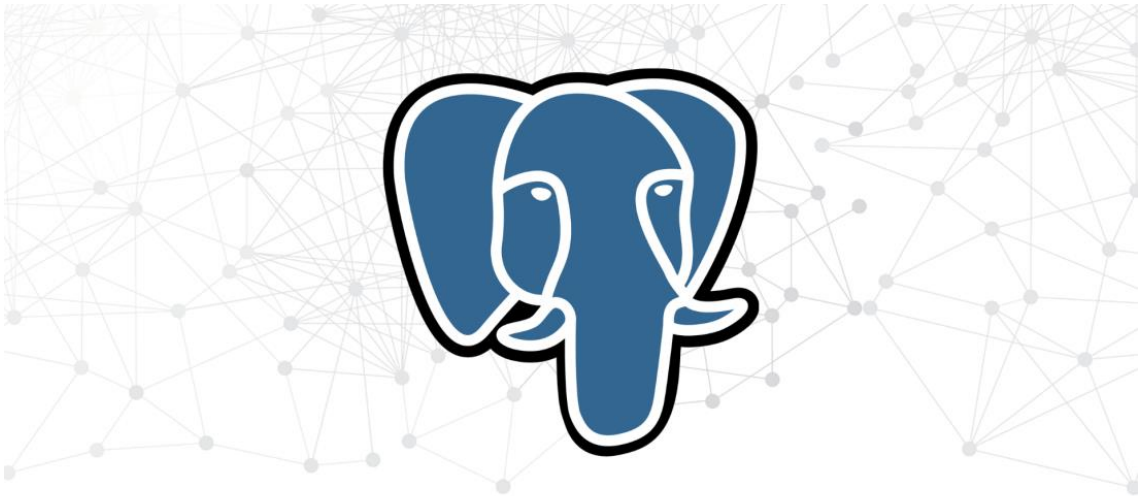

Figura 14 PostgreSQL Logo

As características do PostgreSQL levaram a que este software a ser reconhecido como um dos Sistemas de Gestão de Bases de Dados mais avançados contando recursos como:

- Consultas complexas;
- Chaves estrangeiras;
- Integridade transacional;
- Controle de concorrência e de gestão de versões de dados;
- Suporte ao modelo híbrido relacional objetos;
- Funcionalidade no acesso a dados;
- Mecanismo de Gatilhos;

- Suporte de vistas;
- Integração com linguagens de procedimentos como PL/pgSQL, PL/Python, PL/Java, PL/Perl para integração de operação;
- Mecanismos de indexação por texto;
- Estrutura para guardar dados Georreferenciados PostGIS.

O SQL no PostgreSQL é a linguagem de pesquisa padrão para base de dados relacional-objetos. A linguagem SQL é uma das normas e o padrão para consulta e criação de bases de dados, especialmente em bases de dados relacionais. O SQL é uma linguagem de quarta geração de consulta a base de dados em que uma consulta SQL especifica a forma do resultado e não o caminho para chegar a ele.

Servidor API para Cliente Diplomados e Entidades Certificadoras

O *Spring Boot* é um projeto da Spring que facilita o processo de configuração e publicação de aplicações. A intenção da Spring é possibilitar a programadores a criação de projetos e as suas implementações de forma rápido e fácil. O *Spring Boot* favorece a convenção sobre a configuração, utilizando padrões de configuração da aplicação pré-definidos como: WEB, *Template*, Persistência, Segurança e entre outras alternativas.

Figura 15 Spring Boot Logo

O projeto *String Boot* permite a programados agrupar várias dependências e modelos para desenvolver um projeto Web para interação homem-máquina entre os clientes Web e os servidores Web, com as bases de dados e processos de informação.

Uma simples interação homem-máquina pode funcionar com pedidos GET e POST (HTTP) ao Servidor, resultando uma resposta para o utilizador.

Hibernate ORM

O Hibernate ORM é uma *framework open source* para o mapeamento objeto-relacional para a linguagem de programação Java, fornecendo uma estrutura para mapear um modelo de domínio orientado aos objetos, para uma base de dados relacional.

Figura 16 Hibernate ORM Logo

O Hibernate manipula problemas de incompatibilidade na relação objeto-relacional, substituindo acessos de base de dados diretos e persistentes a funções de manipulação de objetos de alto nível.

O principal recurso do Hibernate é o mapeamento de classes Java para tabelas de base de dados e mapeamento de tipos de dados Java para tipos de dados SQL. Também fornece recursos de consulta e recuperação de dados e gera as chamadas SQL.

Interface Web / Interface Homem-Máquina

A relação entre o utilizador e a aplicação de computador constitui o interface homem-máquina e é a parte de um programa em computador que se comunica com o utilizador para fornecer informação e controle necessários para que o utilizador realize uma determinada tarefa. No contexto atual, mantendo o utilizador informado e permitindo que essa interação seja amigável e fácil de entender. A interface de utilizador ou interface homem-máquina é o ponto de ação no qual o ser humano está em contato com a máquina – no nosso contexto, com recurso a uma interface Web.

Figura 17 Interface Homem-Máquina

Para que uma interface homem-máquina seja utilizável e faça sentido para os utilizadores, deve ser adaptada às necessidades e competências dos utilizadores. Deste modo, devem ser tomados em consideração também um conjunto de requisitos não funcionais, em complemento com os requisitos funcionais que estabeleçam a operação do sistema, mas também o seu ambiente de operação, considerando o uso das seguintes tecnologias:

- Thymeleaf;
- Bootstrap;
- Javascript.

Thymeleaf

Thymeleaf é um mecanismo de modelo Java XML / XHTML / HTML5 open source que funciona em ambientes baseados na Interface Web. É adequado para servir XHTML / HTML5 na camada de visualização da interface Web. Pode ainda processar um qualquer arquivo XML, mesmo em ambientes offline ou localhost, fornecendo uma integração completa no Spring Framework.

Figura 18 Thymeleaf Logo

Nas aplicações de Interface Web, o Thymeleaf pretende ser um substituto completo para as *JavaServer Pages* ou JSP, implementam o conceito de modelos naturais (arquivos de modelo que podem ser abertos diretamente em navegadores e também são exibidos corretamente como páginas da Interface Web).

Bootstrap

O Bootstrap é uma framework Web em open source, para o desenvolvimento componentes de Interface Web interativo, responsivo e móvel. Contém CSS e opcionalmente modelos de design baseados em JavaScript para tipos de letra, formulários, botões, navegação e outros componentes de interface, melhorando a experiência do utilizador, proporcionando um site amigável e responsivo.

Figura 19 Bootstrap Logo

JavaScript

O JavaScript referido como JS, é uma linguagem de programação interpretada de alto nível que está em conformidade com a especificação ECMAScript. O JavaScript possui orientação a objeto baseada em protótipo e funções de primeira classe.

Juntamente com HTML e CSS em interfaces Web, o JavaScript é uma das principais tecnologias em operação na World Wide Web.

O JavaScript permite páginas de Interface Web. A grande maioria dos sites usa esta tecnologia e os principais navegadores da Web possui um mecanismo JavaScript dedicado para a sua execução.

Apache POI

O APOI é uma framework na plataforma Java que possibilita a leitura e a escrita de dados em um documento do Microsoft Office. É possível ler e escrever dados em arquivos como o Excel, o Word e o PowerPoint. O APOI é bastante utilizado em outras frameworks conhecidas. Tem funcionalidades como exportar dados de uma BD diretamente para um arquivo Excel e preencher dados num documento Word.

Figura 20Apache POI Logo

No exemplo de documentos Word pode-se criar um projeto simples que abre, escreve e altera um arquivo de DU, com os campos Diplomado, Data, Título, Valor, Assinado e Aprovado. A partir desses campos serão calculados diversos dados para o DU, como a conclusão do CU.

Código QR

O código QR pode ser convertido em texto interativo, endereço URI, número de telefone, localização georreferenciada, e-mail, contato ou um SMS. Foi criado intencionalmente para catalogar peças na produção de veículos, mas hoje o QR é usado na gestão de inventário e controle de existências (stocks) nas indústrias e no comércio.

Figura 21 Código QR 0000-0000-0000-0000

Foram desenvolvidas aplicações que ajudam utilizadores a inserir dados em telemóveis usando a própria câmara. Atualmente, os QRCode são comuns também em revistas e na publicidade, para registar endereços e URL, bem como informações pessoais detalhadas.

Código Hash

Uma função Hash criptográfica é uma função Hash considerada praticamente impossível de inverter, as funções Hash unidirecionais são considerados os operários da criptografia moderna.

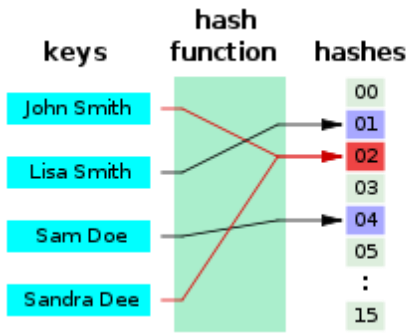

Figura 22 Código Hash

Os dados de entrada são considerados “mensagem”, e o valor do resultado da mensagem é considerado “resumo”. Uma função de dispersão criptográfica deve possuir quatro propriedades principais:

- ser fácil computar o valor de resultado para qualquer mensagem;
- ser difícil gerar uma mensagem a partir de seu resumo;
- ser difícil modificar a mensagem sem modificar o seu resumo;
- ser difícil encontrar duas mensagens diferentes com o mesmo resumo.

As funções Hash criptográficas possuem várias aplicações em segurança da informação, principalmente em assinatura digital, código de autenticação de mensagem, e outras formas de autenticação.

Podem ser utilizadas como funções Hash, para indexar dados em tabelas Hash, para impressão digital, para detetar dados duplicados ou identificar arquivos únicos, e como *Checksum* para detetar corrupção de dados acidental, contexto da segurança da informação, valores do resultado criptográficos são às vezes conhecidos como impressão digital, *Checksums*, ou apenas valores de resultado.

O MD5 (Algoritmo de Mensagem Direta 5) é uma função Hash criptográfico cujo desempenho é a tomada de uma série de dados de entrada de aleatória de tamanho e um valor de saída de tamanho fixo o valor de Hash. Não importa o tamanho ou comprimento da entrada. O que é sempre fixo é o tamanho de saída. Neste caso, de 128 bits (16 bytes ou uma sequência de 32 caracteres hexadecimais).

MD5

O algoritmo MD5 é uma função Hash amplamente utilizada que produz um valor de Hash com 128 bits, tem sido projetado inicialmente para usar como uma função Hash criptográfica, infelizmente contem vulnerabilidades extensas, mas ainda pode ser usado como uma soma de verificação para verificar a integridade dos dados, mas somente contra corrupção não intencional. O MD5 mantem processos adequados para finalidades não criptográficas, por exemplo, para determinar a partição de uma chave específica num banco de dados.

Figura 23 MD5 Logo

SHA-2

Os SHA-2 são construídos usando a estrutura Merkle-Damgård, a partir de uma função de compressão unidirecional construída usando a estrutura de Davies-Meyer a partir de uma cifra de bloco especializada ou classificada.

Figura 24 SHA-256

O SHA-2 inclui mudanças significativas de seu antecessor, o SHA-1. A família SHA-2 consiste em seis funções Hash com valores de Hash que são 224, 256, 384 ou 512 bits conhecidos como SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA -512/256.

Os SHA-256 e SHA-512 são funções Hash novas geradas com palavras de 32 e 64 bits. Ambas usam diferentes quantidades de deslocamento e constantes de adição, mas as suas estruturas são praticamente idênticas, com a diferença no número de iterações ou processos de funcionamento.

Os SHA-224 e SHA-384 são versões cortadas dos SHA-256 e SHA-512, respetivamente, geradas com diferentes valores iniciais e os SHA-512/224 e o SHA-512/256 também são versões cortadas do SHA-512.

Blockchain

Ethereum é uma plataforma de computação distribuída baseada na tecnologia BC, é um sistema operativo *open source*, que apresenta funcionalidade de contrato inteligente ou *scripting*.

Figura 25 Blockchain Ethereum

Ether é um Token ou chave eletrónica, que tem um BC que é gerado na plataforma Ethereum. Este pode ser transferido entre contas e usado para compensar os nós de mineração do participante para cálculos realizados.

A Ethereum fornece uma máquina virtual descentralizada, a Máquina Virtual Ethereum ou EVM, que pode executar scripts usando uma rede internacional de nós públicos. O conjunto de instruções da máquina virtual, em contraste com outras como o Bitcoin Script, é considerado Turing-completo.

3.4 Abordagem metodológica

Identificação problema

A emissão de um DU para um AU que concluiu o seu CU é um processo de emissão com custo elevados envolvendo tempo e recursos, tais custos ficam cada vez mais elevados (José Luiz Brandão, 2018).

De acordo com Your Europe, (2018) o DU não tem valor internacional, por isso é preciso um AU apresentar o seu DU mais uns documentos numa IU noutro estado e pedir EU.

Métodos de emissões e distribuição são os mesmos nas últimas décadas e considerados poucos eficientes, métodos digitais já foram pouco implementação e não foram bem explorados para obter maior eficiência.

Revisão da literatura dos métodos existentes

Poucas universidades e empresas fizeram os seus métodos digitais de distribuição e validação dos seus DU, mas é tudo privado e só fazem validações dos seus DD.

Implementações existentes para tirar proveito do DU digital ainda não foram exploradas em todos os seus benefícios, como a automação da EU.

Conceção e desenvolvimento de um sistema de informação para resolver o problema

Pretende-se propor um sistema de informação para garantir a eficiência, envolvendo uma interface Web para processos de emissões e autenticidade de DD (Thornley, 2012). Nesta dissertação é pretendido implementar métodos para aumentar a distribuição e validação do DU, envolvendo o uso do diploma em formato digital para potencial uso internacional e entre IU.

Em complemento é proposta solução automática para EU, mas não basta para ter uma boa eficiência, por isso implementações envolvendo IA (Ligeza, 1995) constitui

um requisito. Ainda como complemento, o sistema proposto tem que oferecer uma boa autenticação e segurança de dados, por isso implementações de funções e métodos da tecnologia BC são essenciais.

Realização de um estudo empírico

A realização de testes ao sistema proposto, verificando as funções especificas do SI em contexto real ou simulado para integração da BD da Universidade Fernando Pessoa poderá permitir recolher dados mais concretos e avaliar o valor oferecido aos utilizadores de modo a permitir verificar se as funcionalidades concebidas se justificam e estão adequadas aos prepósitos considerados.

Resultado

A objetivo último do projeto é obter um SI para IU poderem emitir, distribuir e validar os seus DU por todos os seus AU e poder interagir mais com outras IU para melhorar as EU entre estados na EU.

4 A proposta do protótipo de gestão de diplomas *online*

4.1 Requisitos do Gestão de Diplomas Online

Listagem dos requisitos funcionais

Serviços:

- Comunicação por Internet
- Segurança de Dados
- Gestão de Informação
- Validação de Documentos
- Distribuição de Documentos
- Web Servidor

Utilizadores:

- Comunicação por Internet
- Interface Web
- Sessão de Clientes
- Registos de Dados
- Ligação as Entidades Certificadoras
- Dispositivo Web

Gestores de Entidades Certificados ou Provadores:

- Comunicação por Internet
- Interface Web
- Sessão de Administrador

- Autorização de Administrador
- Registo e Alteração de Dados
- Dispositivo Web

Listagem dos requisitos não funcionais

Serviços:

- Comunicação por Email
- Segurança de Documentos
- Gestão de Perfil
- Opções de Conta
- Registo e Recuperação de Contas
- Distribuição de Dados
- Equivalências de Diplomas
- Funções Hashcode
- Funções Blockchain
- Preços dos Serviços
- Resposta e Soluções as Falhas nos Serviços

Utilizadores:

- Interface Móvel
- Gestão do Perfil de Clientes
- Registos de Informação Opcional
- Pedido de Emissão

- Pedidos de Validação
- Pedidos de Distribuição
- Pedidos de Pesquisa

Gestores de Entidades Certificados ou Provadores:

- Interface Web
- Sessão de Administrador
- Autorização de Administrador
- Registo e Alteração de Dados
- Gerar ou Alterar de Emissão
- Gerar ou Alterar de Validação
- Gerar ou Alterar de Distribuição
- Gerar ou Alterar de Pesquisa

Requisitos do sistema (software e hardware)

Hardware:

- Dispositivo Computacional PC ou Móvel
- Rede de Internet
- Servidor

Software:

- Sistema Operativo no Servidor
- Sistema Operativo na Entidade Certificadora
- Sistema Operativo no Dispositivo do Cliente
- Browser Web no Cliente e Entidade Certificadora

- Base de Dados PostgreSQL
- Plataforma Springboot
- Bibliotecas Bootstrap
- Bibliotecas JavaScript

4.2 Arquitetura geral da aplicação de Gestão de Diplomas Online

A arquitetura do sistema de alto nível segue um modelo genérico de cliente-servidor (Figura 26). À esquerda, temos os clientes em dois grupos, utilizadores diplomados e validadores, no meio temos o servidor Web que disponibiliza os serviços *online* e na direita temos os administradores das entidades certificadoras e do Servidor Web que geram informação e documentos para disponibilizar no sistema.

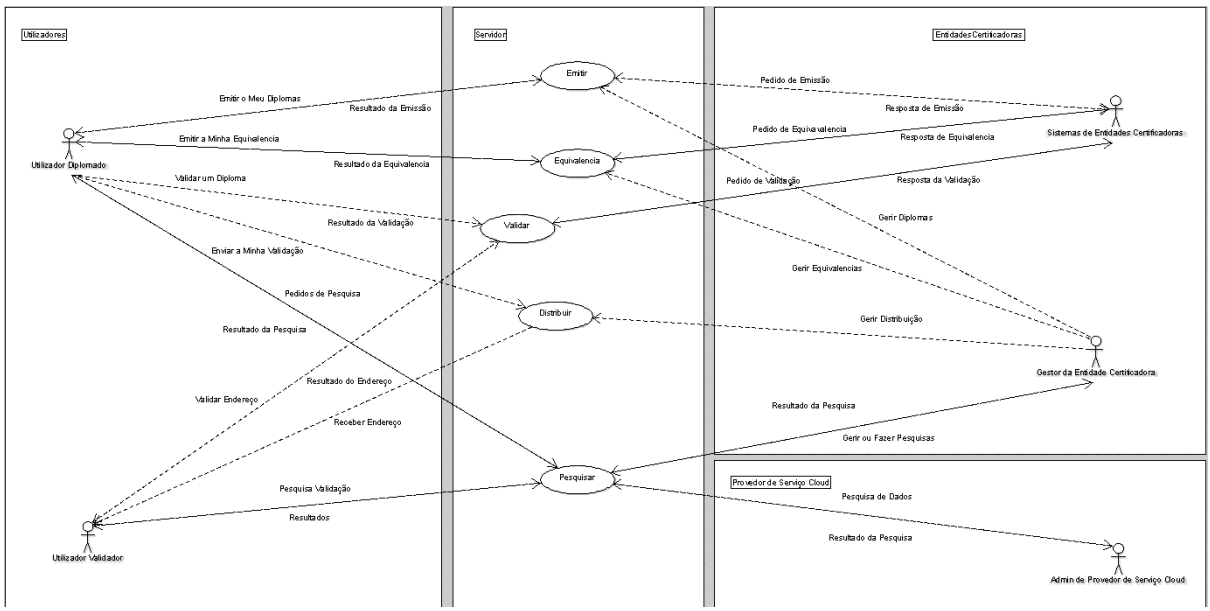

Figura 26 Arquitetura genérica de visualização de alto nível cliente-servidor do Gestão de Diplomas Online

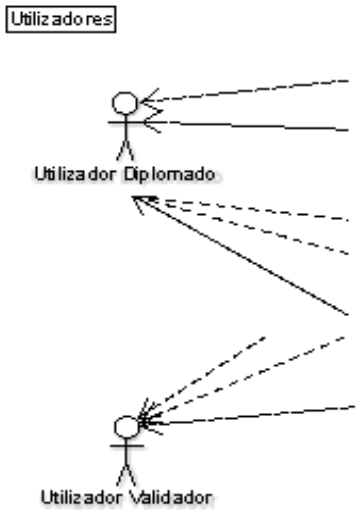

Figura 27 Utilizadores

Os Utilizadores sejam Utilizadores Diplomados ou Validadores tem acessos a funções disponíveis, permitindo utilizar as Emissões, Equivalências, Validações, Distribuição e Pesquisa.

Utilizadores Diplomas tem uma conta registada, podendo tirar partido de todas funções para emitir os seus diplomas, pedir as suas equivalências, fazer validações de diplomas em questão, distribuir os seus diplomas e validações com terceiros e fazer pesquisas de informações públicas.

Utilizadores Validadores não tem uma conta registada, mas podem utilizar funções limitadas, permitindo fazer validações de diplomas enviados por Utilizadores Diplomados em endereços eletrónicos e também podem fazer pesquisas de informações públicas.

O Servidor disponibiliza as suas funções de 5 diferentes maneiras Emissão, Equivalência, Validações, Distribuição e Pesquisa.

Emissão permite gerar diplomas automaticamente nas Universidades inscritas como qualidade de empresa no Sistema.

Equivalência permite gerar equivalências automaticamente entre uma ou duas universidades do sistema.

Validação permite validar documentos registados no sistema para garantir a valides dos documentos distribuídos.

Distribuição permite distribuir documentos registados no sistema, mesmo para entidades de terceiros ou não registados no sistema.

Pesquisa permite buscas de informação ou documentos públicos gerados pelas entidades certificadores ou utilizadores.

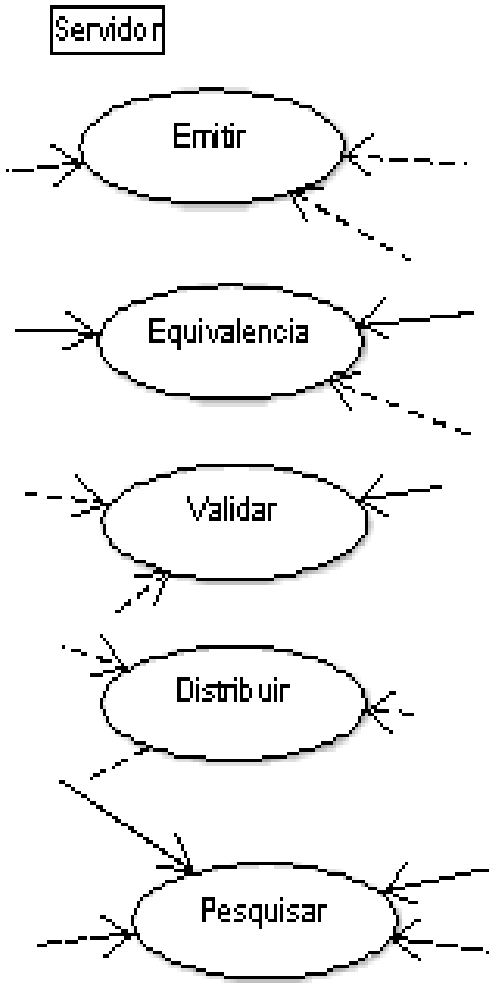

Figura 28 Serviços

AS Entidades Certificadores são em geral os administradores de dados ou os sistemas de dados automáticos, que produzem, gerem e disponibilizam dados no sistema de Gestão de Diplomas Online.

O Sistema de Entidades é um sistema automático das Universidades inscritas como qualidade de empresa, que geram documentos e validações para o sistema Gestão de Diplomas Online.

O Gestor de Entidades é um administrados por parte das Universidades inscritas como qualidade de empresa, com o propósito de organizar, alterar e distribuir a informação gerada pela sua própria Universidade no sistema Gestão de Diplomas Online. O Administrado Provador é o gestor de toda a informação que passa pelo sistema Gestão de Diplomas Online, mais organiza, atualiza os dados dos serviços disponíveis.

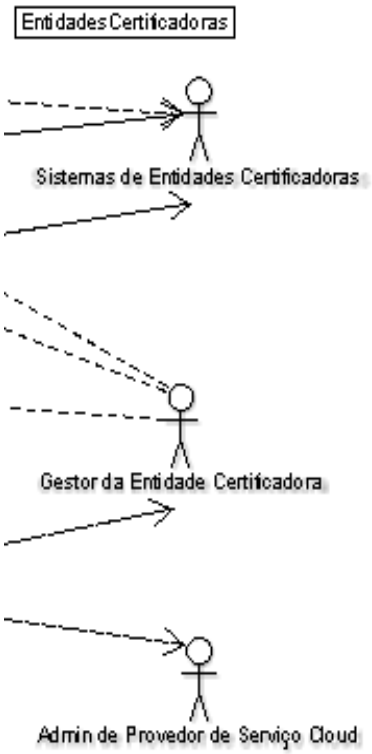

Figura 29 Gestores das Entidades

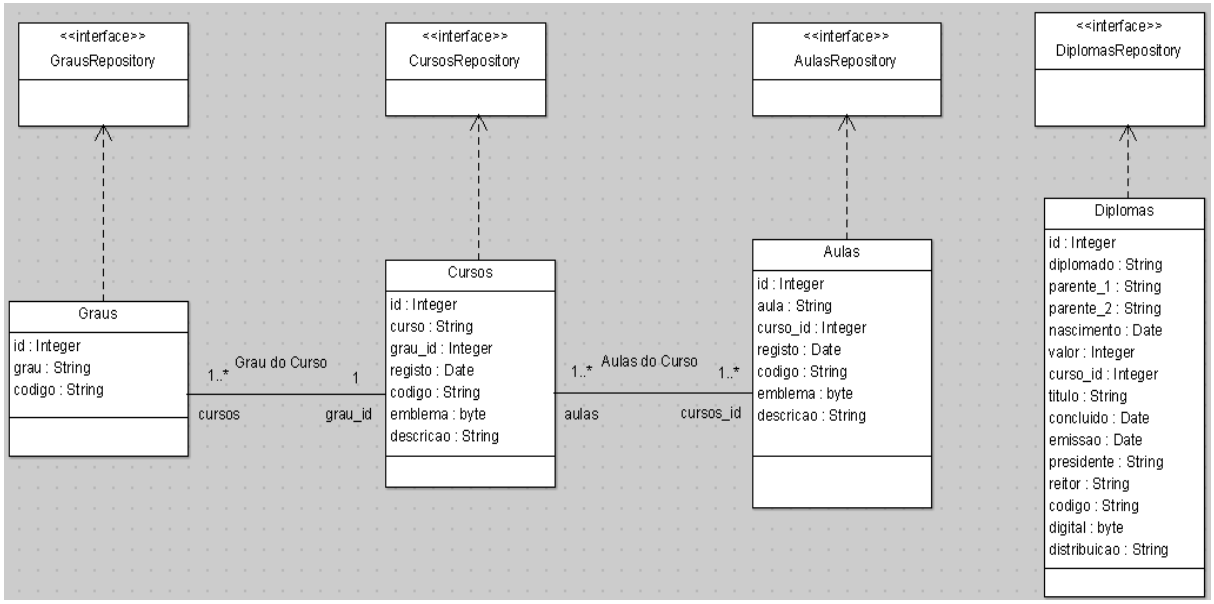

Figura 30 Diagrama de Classes para Base de Dados das Entidades Certificadoras

O sistema Gestão de Diplomas Online precisa de uma ligação à base de dados por cada Entidade Certificadora registada no sistema com qualidade de Empresa como mostra a Figura 30.

A ligação as Entidades Certificadoras permitem obter documentos dos Diplomas e Equivalências, fazer validações dos mesmos documentos.

A informação disponibilizada no Sistema pode ser identificada como pública e privada.

- Informação Pública:

  Graus académicos disponíveis na Entidade Certificadora.

  Cursos académicos disponíveis por Grau académico.

  Aulas académicas disponíveis pelos Cursos académicos.

- Informação Privada:

  Diplomas de alunos com cursos concluídos por parte da Entidade Certificadora.

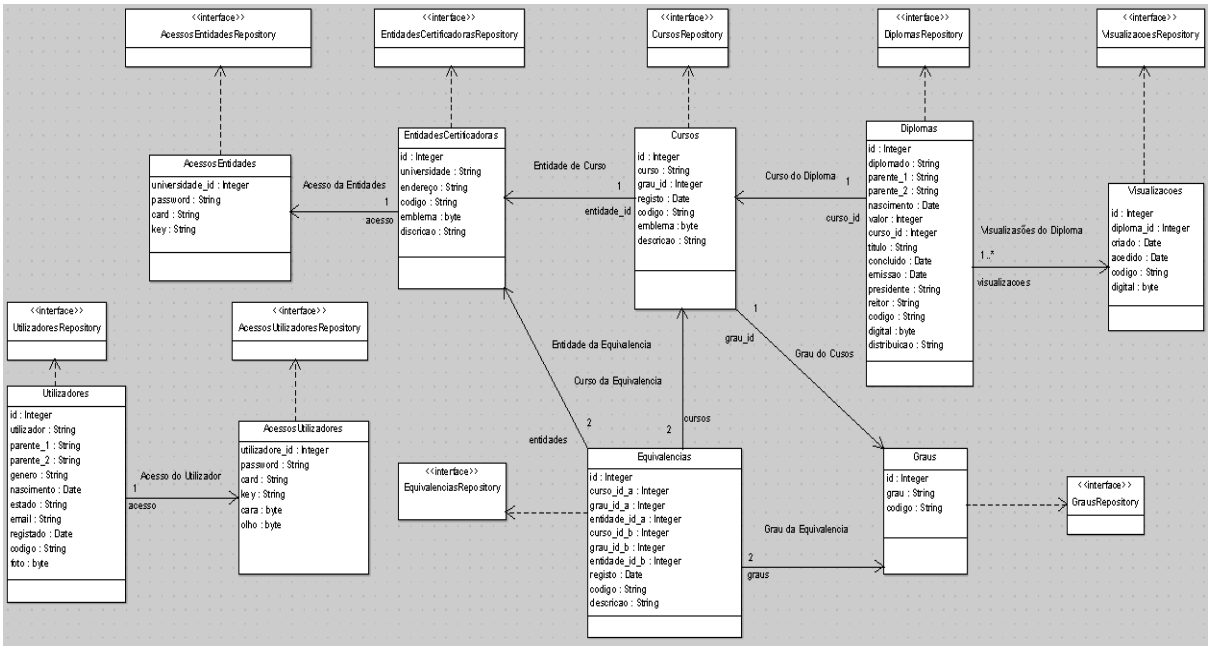

Figura 31 Diagrama de Classes para Base de Dados do Gestão de Diplomas Online

O Servidor do Gestão de Diplomas Online tem vários tipos de informação na sua base de dados como mostra na Figura 31, para garantir a sua organização de dados, a informação envolve Utilizadores, Acesso dos Utilizadores, Entidades Certificadoras, Acesso das Entidades Certificadoras, Graus Académicos, Cursos Académicos, Equivalências Académicas, Diplomas e Visualização de Diplomas.

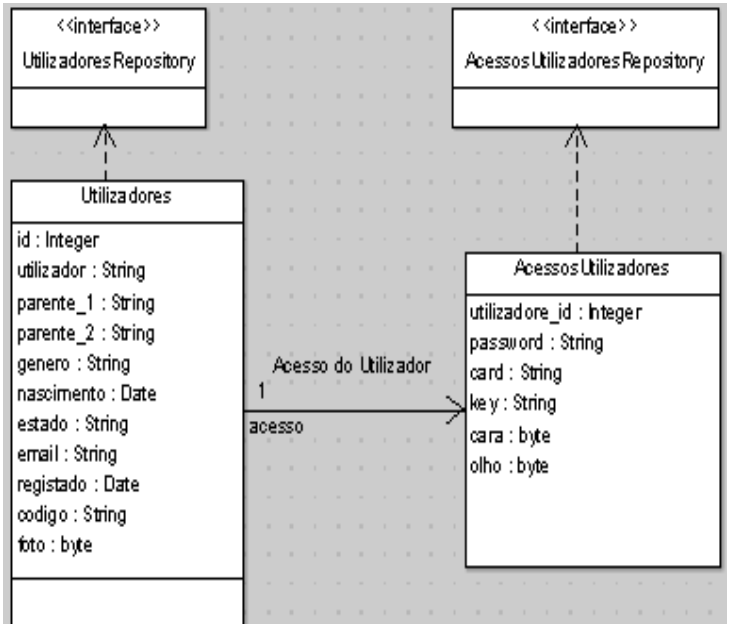

Figura 32 Utilizadores & Acessos

Os Utilizadores identificam os clientes registados no sistema e permite criar o seu perfil digital.

Os Acessos dos Utilizadores geram os acessos dos clientes nas suas contas, permitindo ao cliente aceder a sua conta de várias maneiras, como palavra passe, cartão de identificação ou Cartão do Cidadão, chave, identificação facial ou ocular.

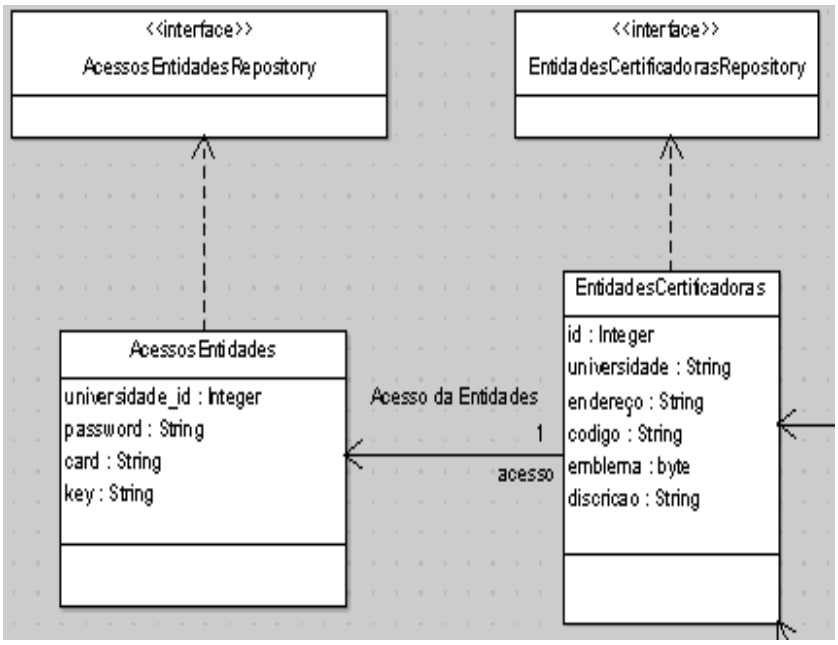

Figura 33 Entidades Certificadoras e Acessos

As Entidades Certificadores identificam as Universidades registadas no sistema como qualidade de empresa e permite criar o seu perfil digital.

Os Acessos das Entidades Certificadores geram os acessos das Universidades nas suas contas, permitindo ao Universidade aceder a sua conta de várias maneiras, como palavra passe, cartão de identificação ou chave.

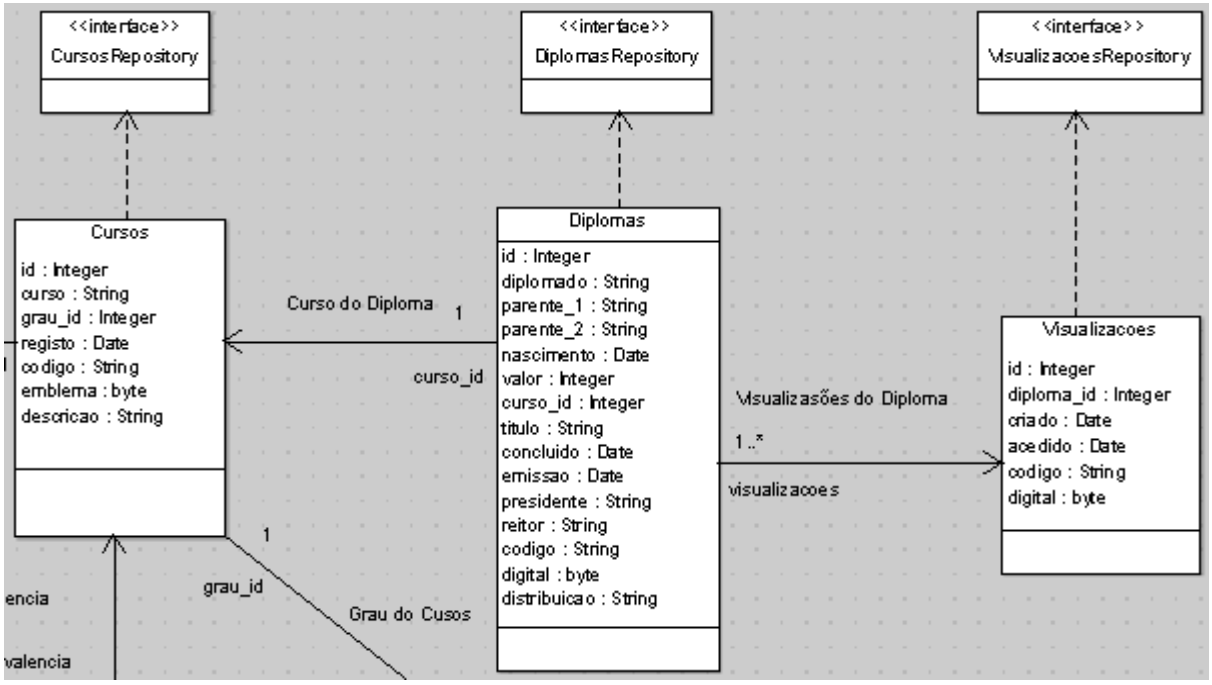

Figura 34 Cursos, Diplomas, Visualizações

Os Cursos identificam os estudos académicos registados no sistema Gestor de Diplomas Online por parte das Entidades Certificadoras.

Os Diplomas identificam todos os diplomas registados para distribuição e validação por parte dos Utilizadores Diplomados e das Entidades Certificadoras.

As visualizações identificam uma lista de registos para visualizações dos diplomas digitais disponíveis no sistema Gestor de Diplomas Online.

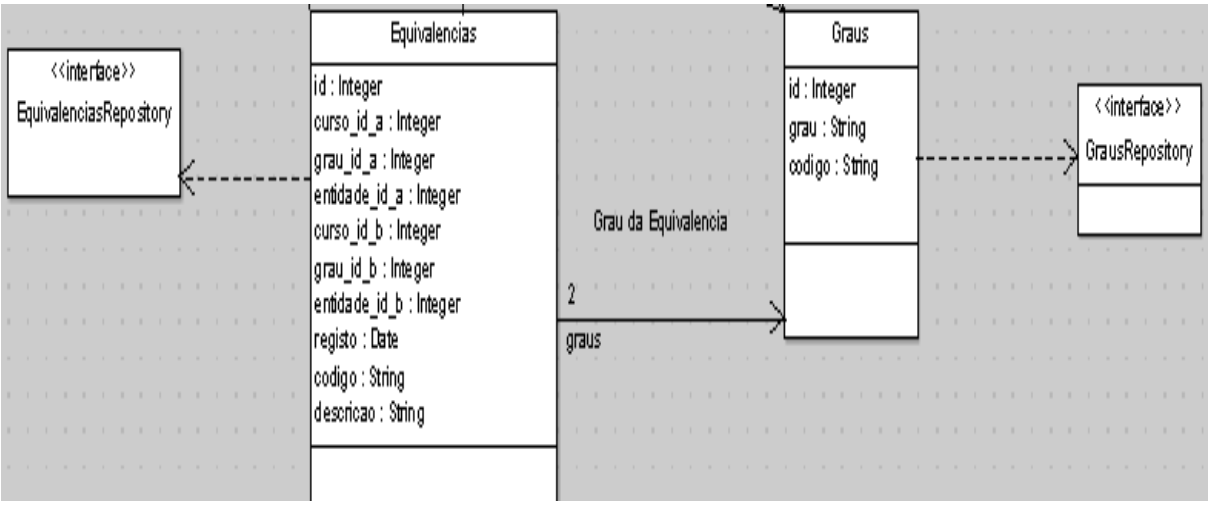

Figura 35 Equivalências & Graus

As Equivalências identificam diplomas registados com equivalências para distribuição e validação por parte dos Utilizadores Diplomados e Entidades Certificadores entre dois estados.

Os Graus identificam os níveis académicos dos cursos registados no sistema Gestor de Diplomas Online, como Licenciatura, Mestrado e Doutoramento.

4.3 Arquitetura da Gestão de Diplomas Online

Diagramas de Atividade

O Gestão de Diplomas Online tem 5 diferentes serviços Emitir, Equivalência, Validar, Distribuir e Pesquisa, os serviços podem ser acedidos por várias entidades com acessos diferentes por meios de pedidos ao sistema como mostra nas Figuras 36, 37, 38, 39, 40 e 41.

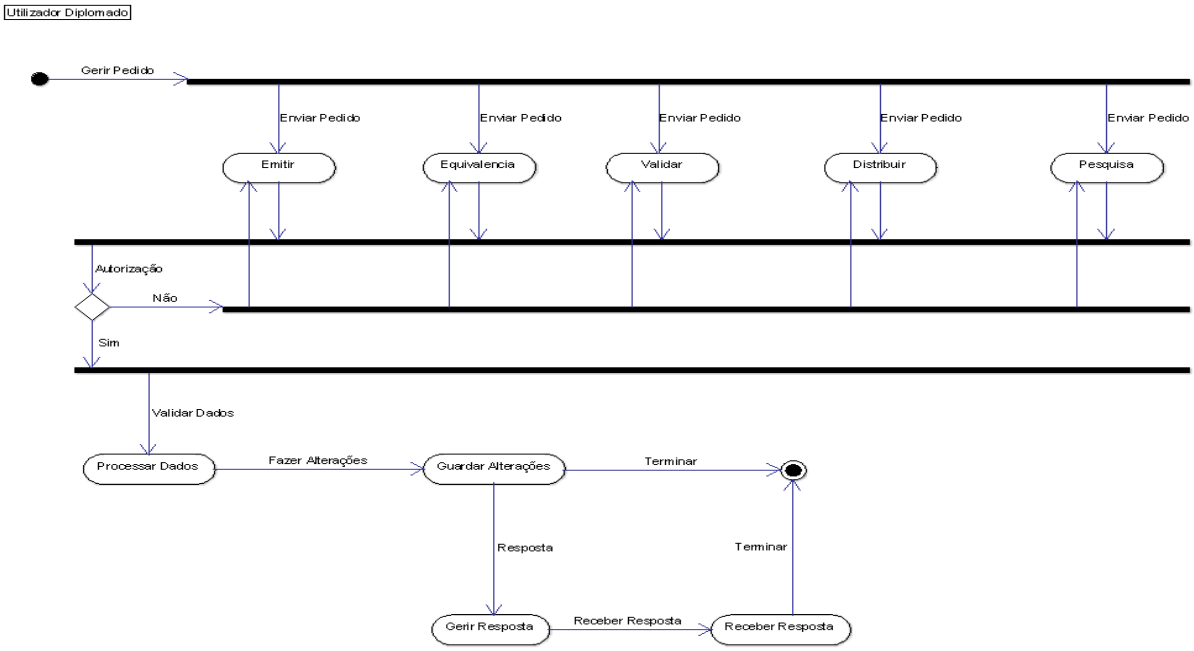

Figura 36 Atividades por parte do Utilizador Diplomado no Gestão de Diplomas Online

O utilizador diplomado na Figura 36 é um cliente registado no sistema Gestor de Diplomas Online, que pode utilizar os serviços:

- Emitir, para obter diplomas e equivalências dos seus cursos concluídos;
- Equivalências para pedir uma equivalência de um diploma dos seus cursos concluídos;
- Validar, para validar diplomas atualmente em distribuição no sistema;
- Distribuir, para partilhar os diplomas com traseiros por endereço;
- Pesquisa, para fazer buscas de documentos e informação pública no sistema.

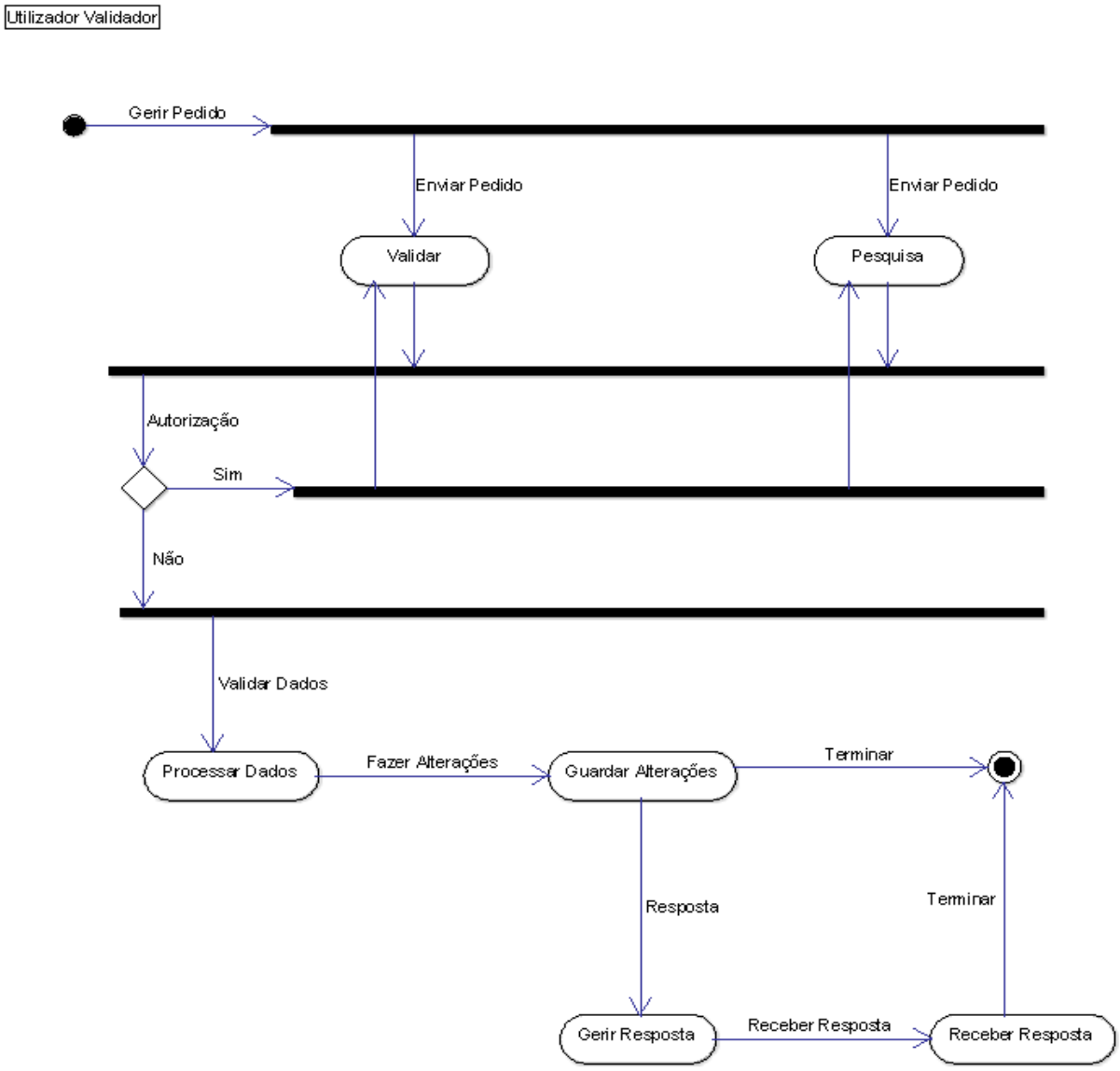

Figura 37 Atividades por parte do Utilizador Validados no Gestão de Diplomas Online

O utilizador validador na Figura 37 é um cliente não registado no sistema Gestor de Diplomas Online, que pode utilizar os serviços:

- Validar, para validar diplomas atualmente em distribuição no sistema e enviados por o utilizador diplomado num endereço;
- Pesquisa, para fazer buscas de documentos e informação pública no sistema.

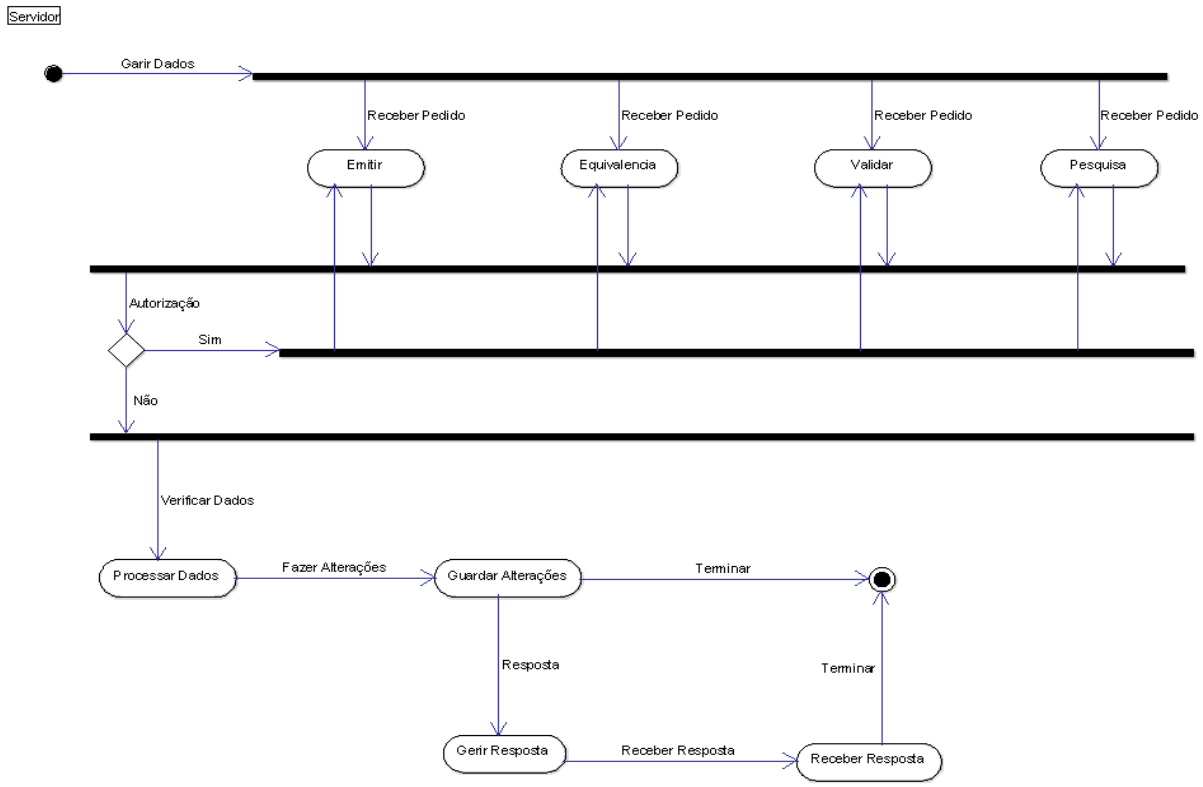

Figura 38 Atividades por parte do Servidor no Gestão de Diplomas Online

O servidor do Gestor de Diplomas Online na Figura 38 é um sistema automático que pode utilizar os serviços:

- Emitir, para pedir e receber diplomas ou equivalências dos utilizadores diplomados e entidades certificadores registadas como qualidade de empresa;
- Equivalências para pedir e receber equivalência de um diploma e fazer comparações com outros diplomas de estados diferentes;
- Validar, para pedir e receber autenticação para diplomas atualmente em distribuição no sistema;
- Pesquisa, para pedir e receber pedidos de buscas de documentos e informação pública no sistema.

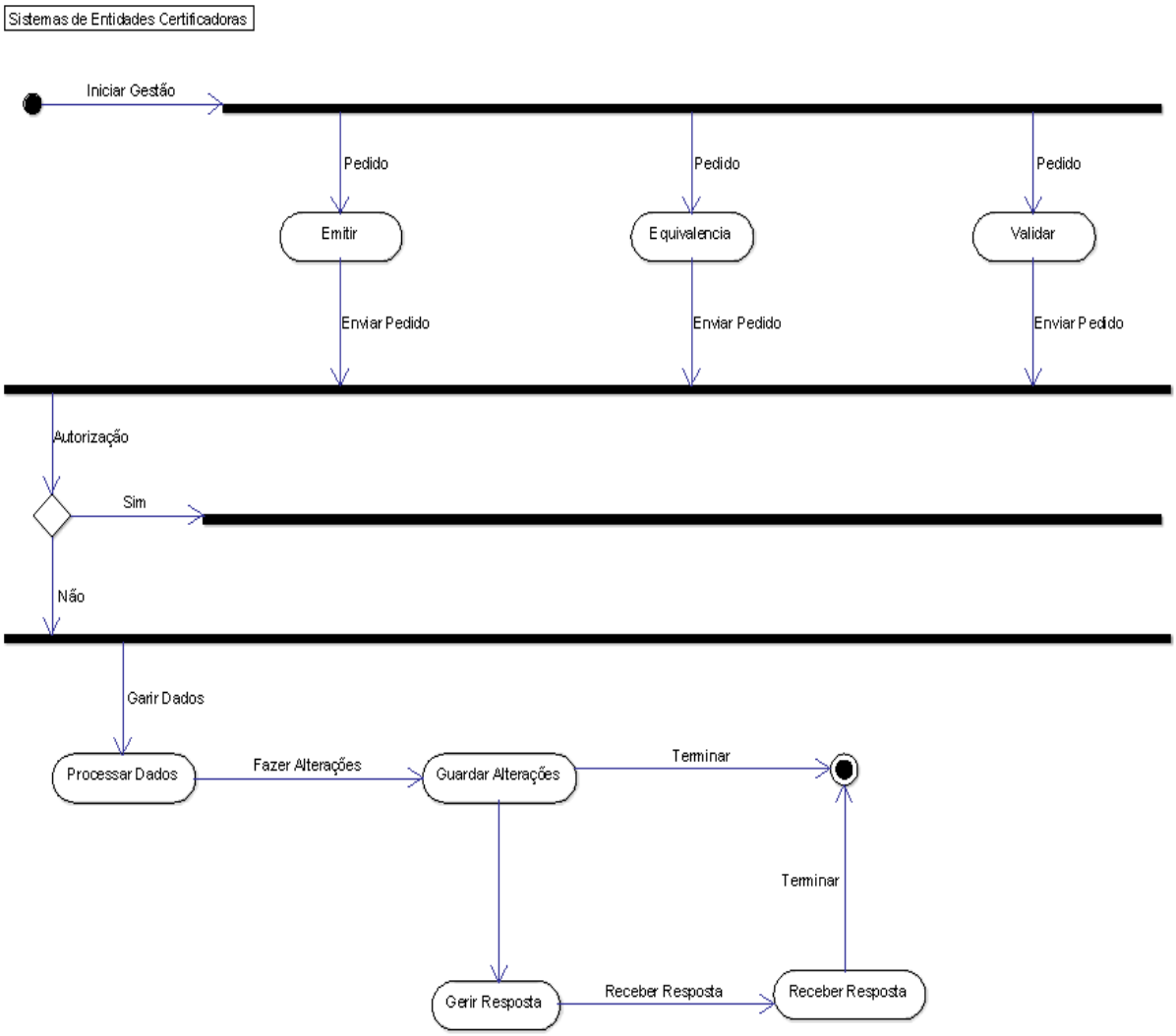

Figura 39 Atividades por parte do Entidades Certificadores no Gestão de Diplomas Online

O sistema da entidade certificadora na Figura 39 é um sistema automático nas entidades certificadoras que pode utilizar os serviços:

- Emitir, para gerar diplomas e equivalências dos utilizadores diplomados na sua entidade certificadora e distribuir os mesmos diplomas e equivalências no sistema;
- Equivalências para gerar equivalência dos seus diplomas e comparações com outros diplomas de estados diferentes;
- Validar, para garantir autenticação para todos os seus diplomas atualmente em distribuição gerados pela sua entidade certificadora.

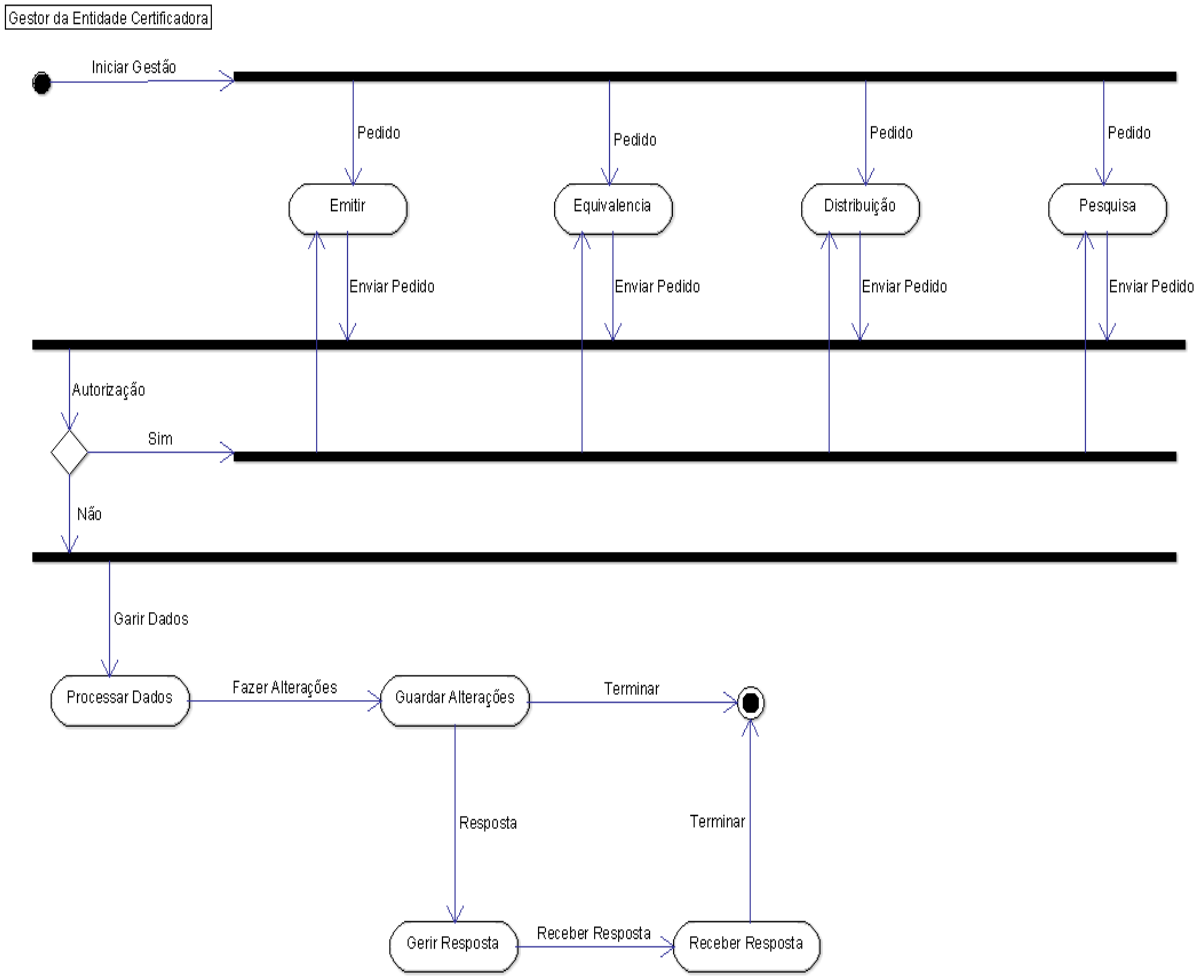

Figura 40 Atividades por parte do Gestor de Entidades no Gestão de Diplomas Online

O gestor no sistema de entidades certificadoras na Figura 40 é um dos administradores nas entidades certificadoras que pode utilizar os serviços:

- Emitir, para alterar ou controlar diplomas e equivalências gerados pela sua entidade certificadora;
- Equivalências para alterar ou controlar equivalência dos seus diplomas e comparações com outros diplomas de estados diferentes;
- Validar, para alterar ou controlar autenticação de diplomas atualmente em distribuição gerados na sua entidade certificadora;
- Pesquisa, para adicionar, altera ou remover informação de buscas de documentos e informação pública no sistema.

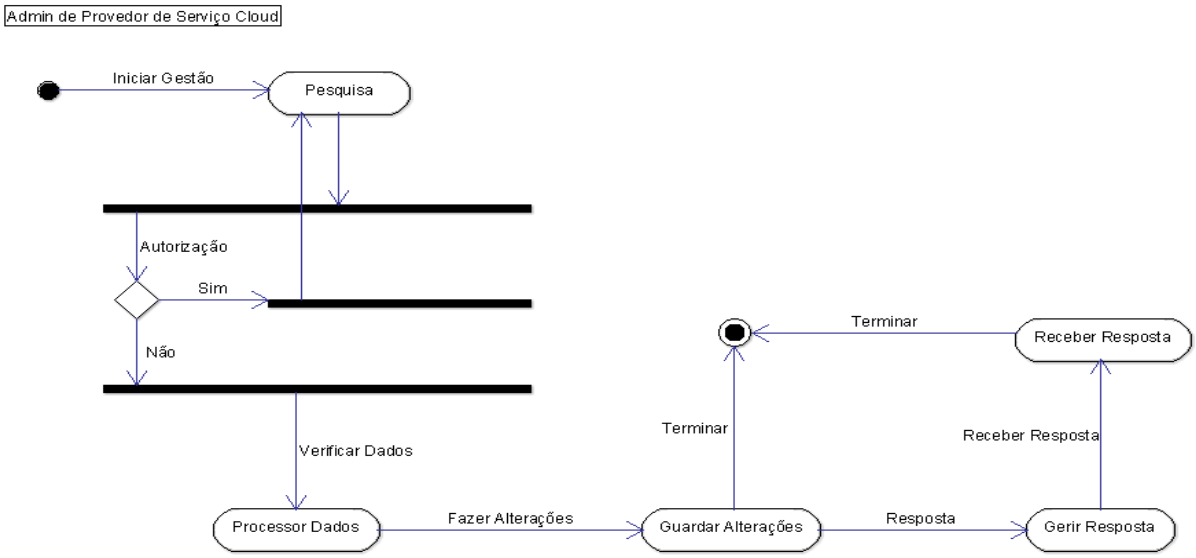

Figura 41 Atividades por parte do Administrador do Provedor do Serviço

O administrador aprovador do serviço no sistema Gestão de Diplomas Online da Figura 41 é um administrado de distribuição para informação que pode utilizar os serviços:

- Pesquisa para adicionar, alterar ou remover informação de buscas dos documentos e informação pública no sistema.

Diagramas de Sequência

Todos os serviços disponíveis aos utilizadores têm pedidos que são encaminhamentos pelo Servidor que vai da origem até ao destino e quando forem concluídos é enviado um resultado.

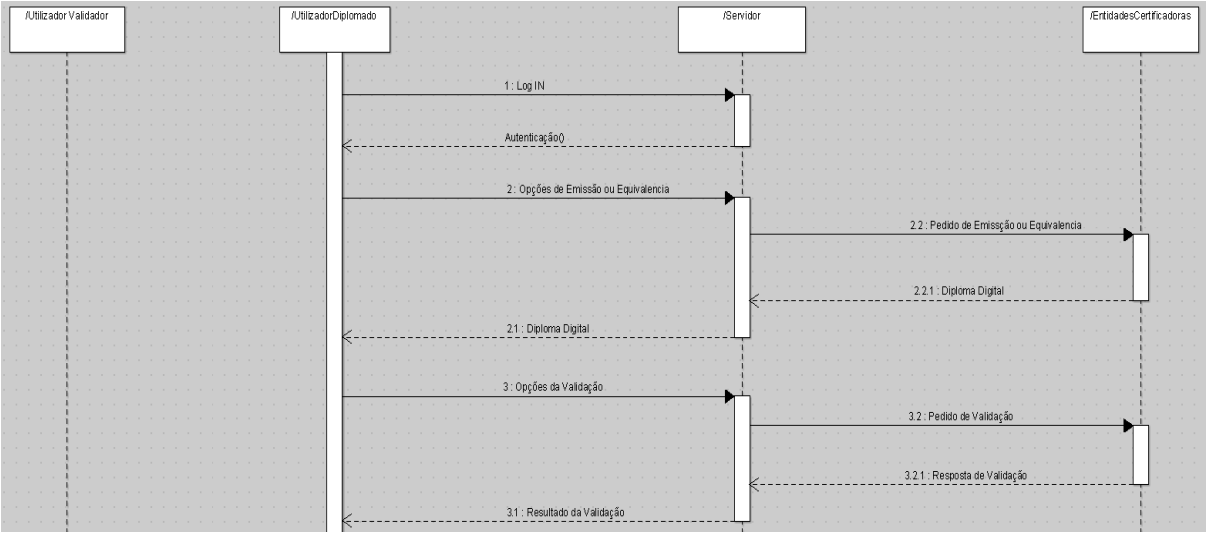

Figura 42 Sequencias da Autenticação, Emissões e Validações para Utilizadores Diplomados

Um Utilizador Diplomado como mostra na Figura 42 pode Autenticar-se mandando um pedido de autenticação ao servidor, pedidos de Emissão ou Validação passam pelo servidor e são reencaminhados para a Entidade Certificadora que gerou o Diploma em questão.

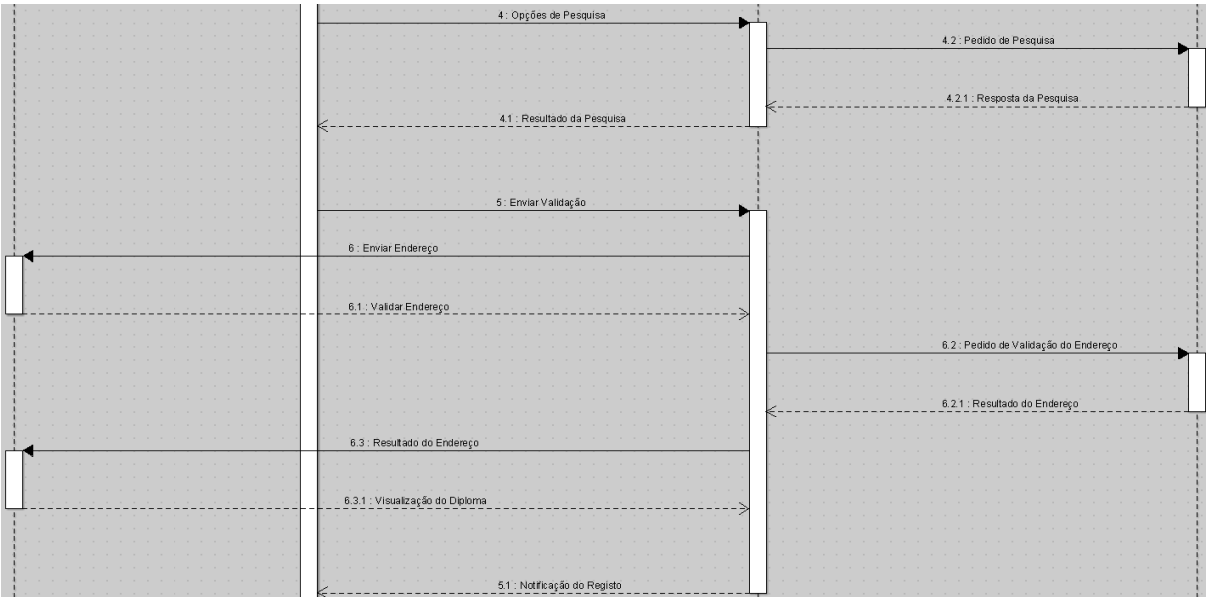

Figura 43 Sequencias da Pesquisa, Enviar Validações para Utilizadores Diplomados

Os pedidos de pesquisas como mostra a Figura 43 podem ou não ser reencaminhados para as Entidades Certificadoras, porque envolve apenas informação pública no servidor, os pedidos de Enviar Validações vão ser reencaminhados primeiro para o Utilizador Validador e depois enviados para a Entidade Certificadora que gerou o diploma em questão.

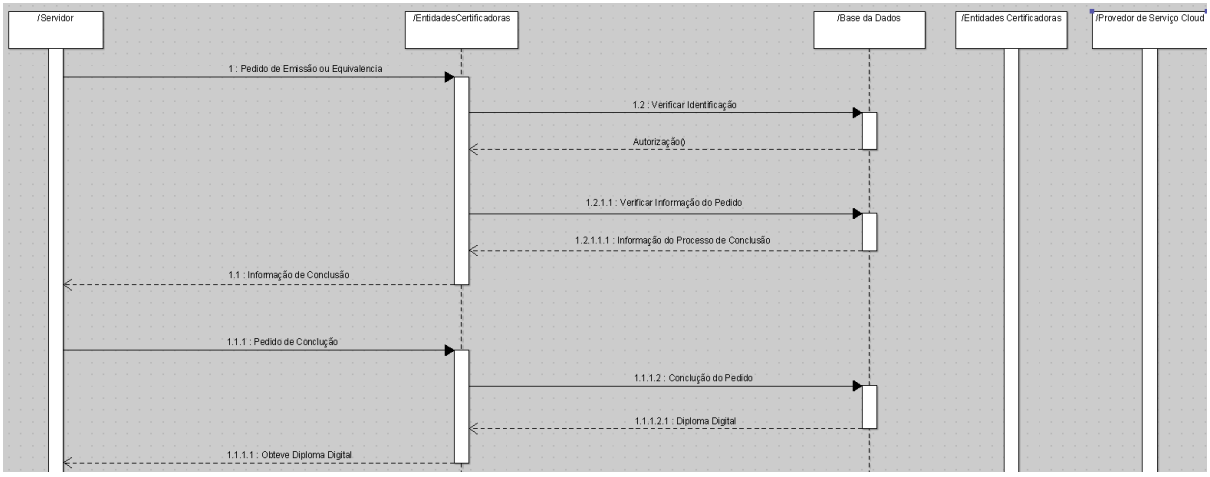

Figura 44 Sequencias da Emissões ou Equivalências para o Servidor

Os processos para Emissões ou Equivalências de Diplomas como mostra a Figura 44 é enviado para a Entidade Certificadora em 3 passos diferente autenticação de utilizador diplomado, validar a informação do pedido e conclusão do pedido.

Os 3 passos envolvem confirmar e alterar dados na Base de Dados na Entidade Certificadora.

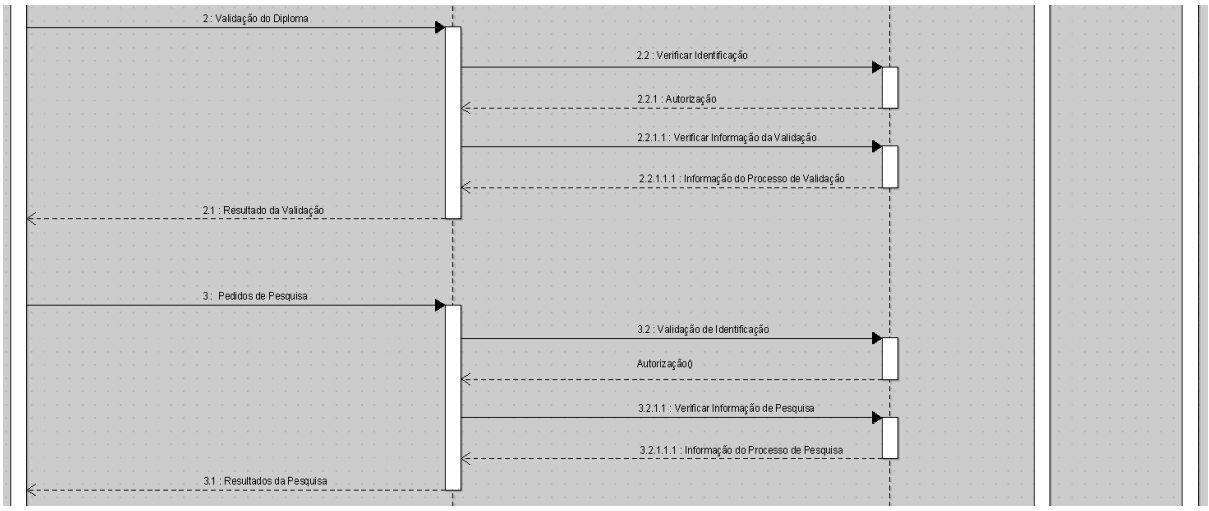

Figura 45 Sequencias da Validações e Pesquisa para o Servidor

Todos os processos de Validações ou Pesquisa como mostra a Figura 45 tem de passar por uma autenticação na Base de Dados na Entidade Certificadora ou falha sem processar os dados.

Todos os pedidos que passa nas Entidades Certificadoras tem de ter um acesso de Aluno registado na sua Base de Dados.

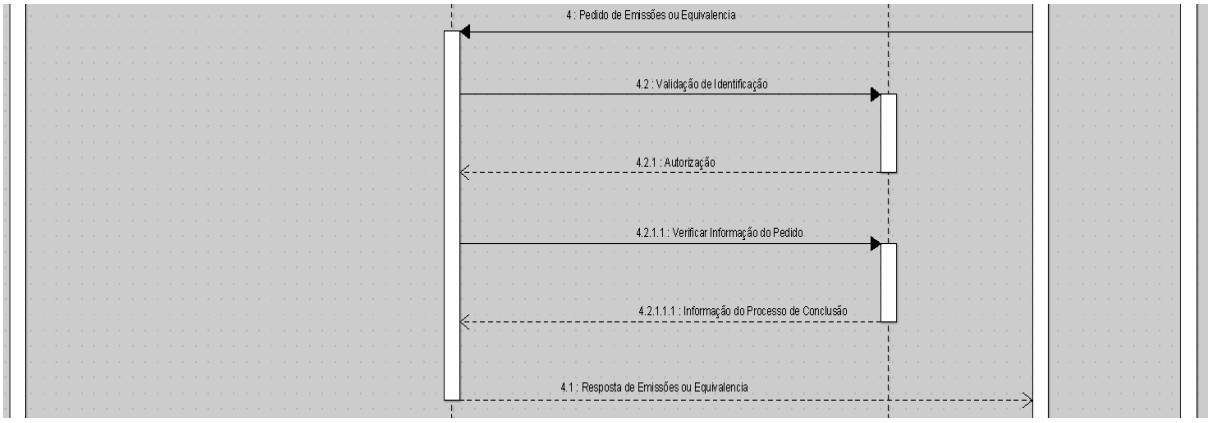

Figura 46 Sequencias das Emissões ou Equivalências para o Gestor de Entidades Certificadora

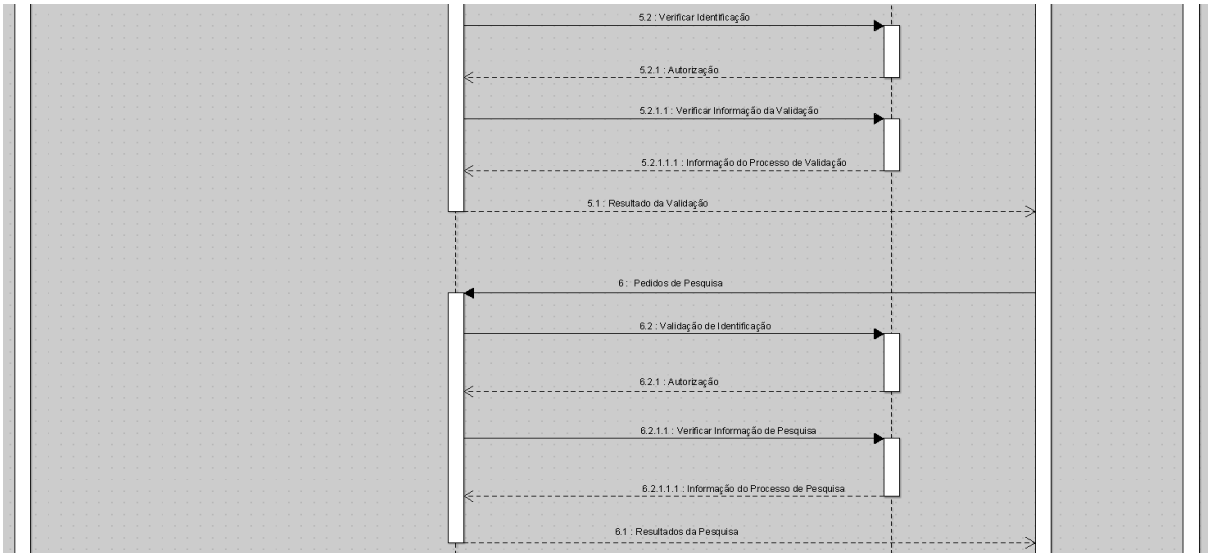

Figura 47 Sequencias das Validações e Pesquisa para o Gestor de Entidades Certificadora

Todos os pedidos de Emissões, Equivalências, Validações e Pesquisa nas Entidades Certificadoras como mostra as Figuras 46 e 47, são geridos por um Gestor com acesso administrativo nas Entidades Certificadoras. O propósito dos Gestor de Entidades Certificadoras é garantir que os sistemas da Entidade Certificadora interagem com o sistema do Gestor de Diplomas Online.

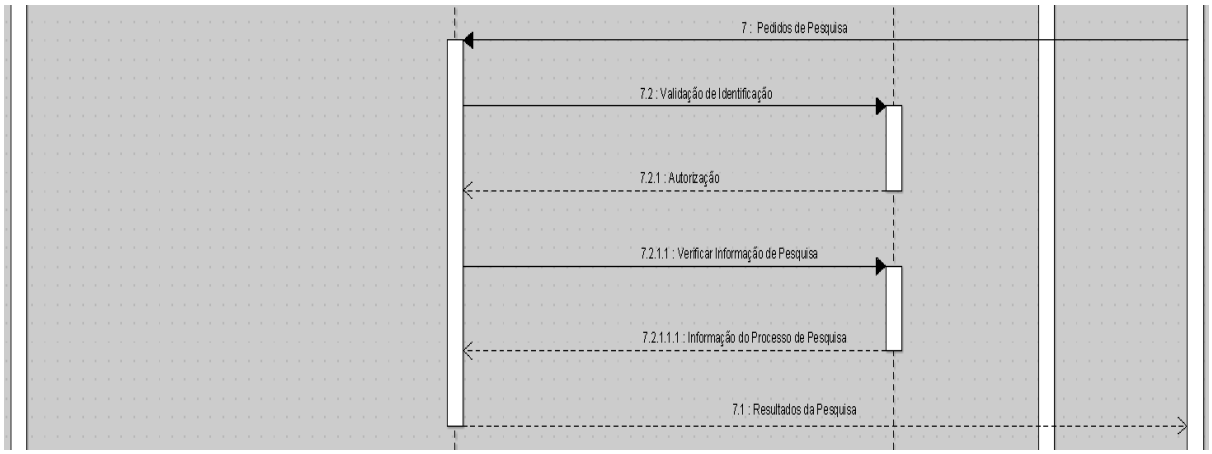

Figura 48 Sequencias das Pesquisas para o Administrador Provador de Serviços

Todos os pedidos de pesquisa no Sistema de Gestão de Diplomas Online na Figura 48 são geridos por um Provador de Serviços para garantir os Serviços de pesquisa interagem com os sistemas de Entidades Certificadoras.

Diagramas de Máquina de Estados

A distribuição de um diploma em questão como mostra a Figura 49 é controla pela Entidade Certificadora que gerou o próprio diploma, para este propósito um diploma na distribuição tem 3 estados de distribuição “Não Válido”, “Válido” e “Revogado”.

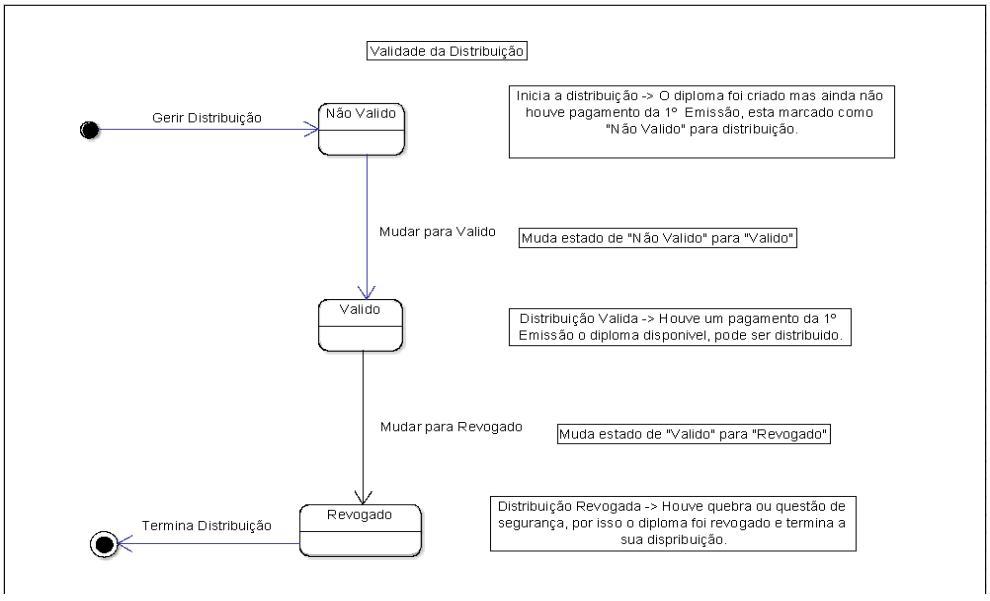

Figura 49 Diagrama de Máquina de Estados para distribuição de Diplomas

O servidor no Gestão de Diplomas Online tem um funcionamento de estado em todas as suas funções como mostra a figura 50 identificando todas as etapas dos pedidos.

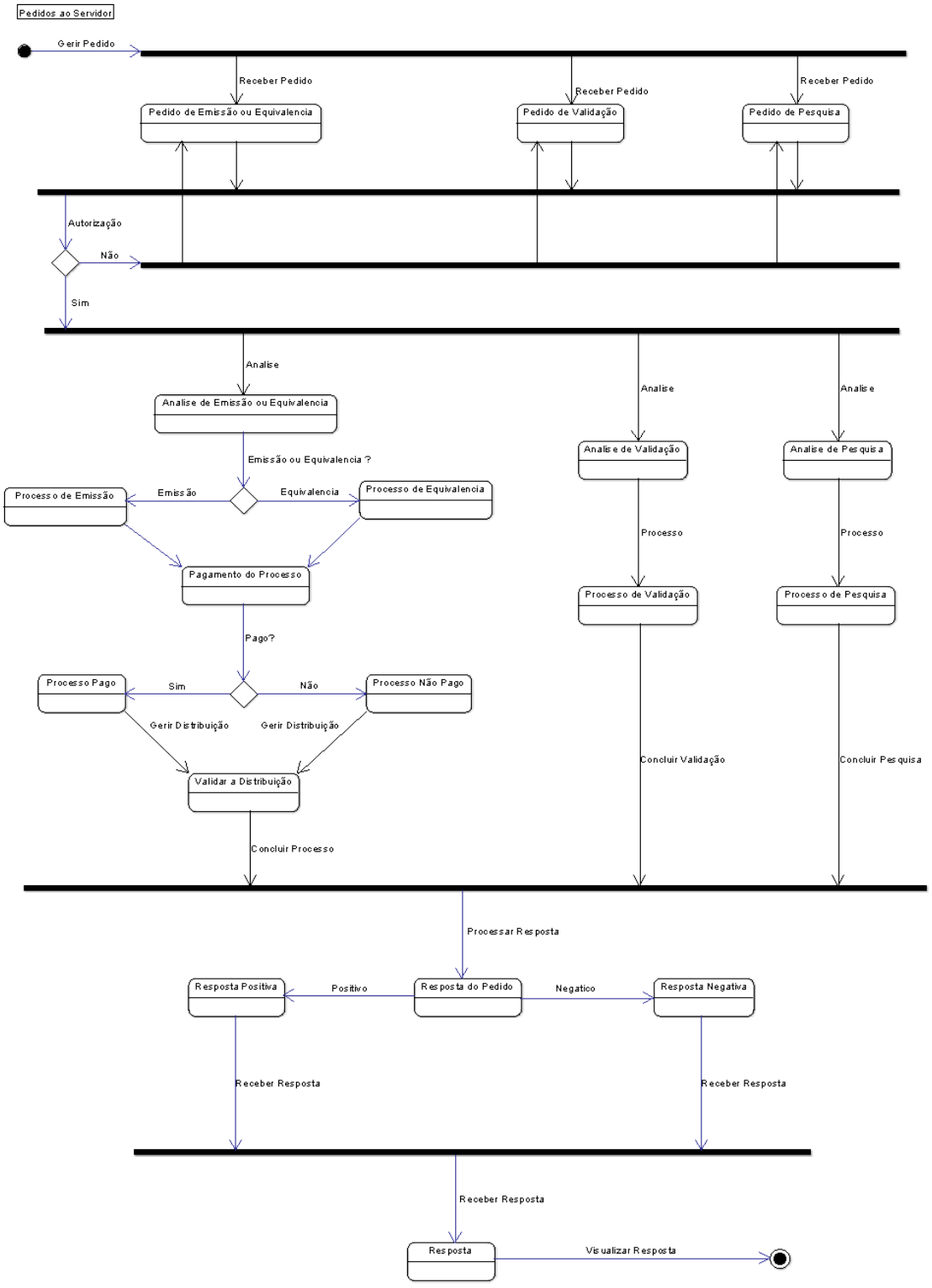

Figura 50 Diagrama de Máquina de Estados para o Servidor do Gestão de Diplomas Online

4.4 Componentes da Gestão de Diplomas Online

No presente protótipo são considerados os seguintes componentes, em fase de implementação:

- Componentes de *Bootstrap*

  As ferramentas do *Bootstrap* proporciona uma interface Web dinâmica e funcional em vários dispositivos como sistemas operativos ou *browser* diferente, essas ferramentas ajudam o sistema do Gestor de Diplomas Online a ter uma boa relação homem-máquina com os seus clientes.

- Componentes de Configuração e Gestão

  Configuração e Gestão é o registo e atualização detalhada de informação que descreve o *hardware* e software de uma empresa ou serviço. É um processo para estabelecer e manter á consistência no desempenho de um sistema, atributos funcionais e físicos com os seus requisitos, *design* e informação operacional ao longo de sua utilização.

  A gestão e configurações de informação disponível no sistema do Gestor de Diplomas Online é essencial para garantir as funções dos dados na autenticação, distribuição, validação e pesquisa.

- Componentes de Comunicação

  Comunicação é um processo que envolve a troca de informação entre dois ou mais participantes por meio de dados e regras mutuamente entendíveis. É um processo que acontece na tecnologia de comunicação, que permite criar e interpretar mensagens que provocam uma resposta.

  O sistema do Gestor de Diplomas Online envolve comunicações com os cientes e sejam utilizadores ou entidades certificadoras, como as entidades certificadoras podem exigir uma comunicação com preferências o sistema tem de proporcionar opções de comunicação.

- Componentes de Segurança de Informação

  Segurança de Informação está relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. A Segurança de Informação não está restrita somente a sistemas de computadores, informação eletrónicas ou sistemas de armazenamento, aplica-se a todos os aspetos de proteção de dados e informação.

  No sistema do Gestor de Diplomas Online a segurança de informação é importante para garantir que todos os dados de perfil, documentos e transmissões para garantir a integridade nos serviços disponíveis no sistema.

- Componentes de Perfis de Utilizadores

  Perfis de Utilizadores em redes sociais, *sites* de relacionamento, blogues pessoais, ou comunidades virtuais, refere-se a um cadastro de dados pessoais, com contato e preferenciais de um determinado utilizador. Parte destes dados podem ser públicos, para compartilhar com os outros utilizadores, ou privados, dependendo do tipo de perfil, tipo de comunidade ou configurações de privacidade definidas pelo utilizador.

  O perfil do utilizador permiti identificar melhor um cliente para poder interagir com outros clientes ou entidades certificadoras para tirar melhor partido na comunicação social.

- Componentes de Bases de Dados PostgreSQL

  Bases de Dados são conjuntos de arquivos relacionados entre si com registos sobre pessoas, empresas ou documentos. São coleções de dados organizados que se relacionam de forma a criar alguma informação e obter mais eficiência durante uma pesquisa

  O servidor no sistema do Gestor de Diplomas Online mantem toda a informação numa base de dados PostgreSQL, permitindo organizar e distribuir informação disponível do sistema.

- Componentes de *SpringBoot*

  SpringBoot framework oferece diversos módulos que podem ser utilizados de acordo com as necessidades do um projeto, para desenvolvimento Web, persistência, acesso remoto e programação orientada a objetos.

  O sistema do Gestor de Diplomas Online é uma ferramenta que oferece vários modelos e ferramentas que pode desenvolver um projeto das várias tecnologias para funcionalidades de um servidor.

- Componentes de *Blockchain*

  Funciona de forma pública, partilhada e universal, que cria consenso e confiança na comunicação direta entre duas partes, ou seja, sem o intermédio de terceiros.

  A tecnologia *Blockchain* proporciona no sistema do Gestor de Diplomas Online um registo de distribuição que garante toda a informação na distribuição e comunicação, permitindo uma segurança e autenticação nos serviços.

- Componentes de *Hashcode*

  Um uso é uma estrutura de dados designada por tabela Hash, amplamente usada em computadores para consulta de dados rápida. As funções Hash aceleram consultas a tabelas ou bases de dados por deteção de registos duplicados em um arquivo grande.

  No sistema do Gestor de Diplomas Online funções de Hashcode permite gerar uma identificação única para cada documento, proporcionando maior eficiência e segurança nas pesquisas.

- Componentes de HTML

  HTML é uma linguagem de marcação utilizada na construção de páginas Web. Documentos HTML podem ser interpretados por navegadores.

Na interface homem-máquina do sistema do Gestor de Diplomas Online vai utilizar a programação em HMTL como código base nas suas páginas Web.

- Componentes de JavaScript

  JavaScript é uma linguagem de programação interpretada, originalmente implementada nos navegadores Web para que scripts pudessem ser executados do lado do cliente e interagissem com o utilizador sem a necessidade deste script passar pelo servidor, realizando comunicação assíncrona e alterando o conteúdo de um documento exibido.

  Nas páginas Web do sistema do Gestor de Diplomas Online as funções é modelos no HTML vão tirar maiores benefícios na interação homem-máquina, visualizações e animação.

4.5 Design do Projeto

Base de Dados PostgreSQL Entidade Certificador

Conforme mencionado na introdução, o projeto precisa de ter interação com as entidades certificadoras para disponibilizar diplomas online e otimizar processos de Equivalências Académicas.

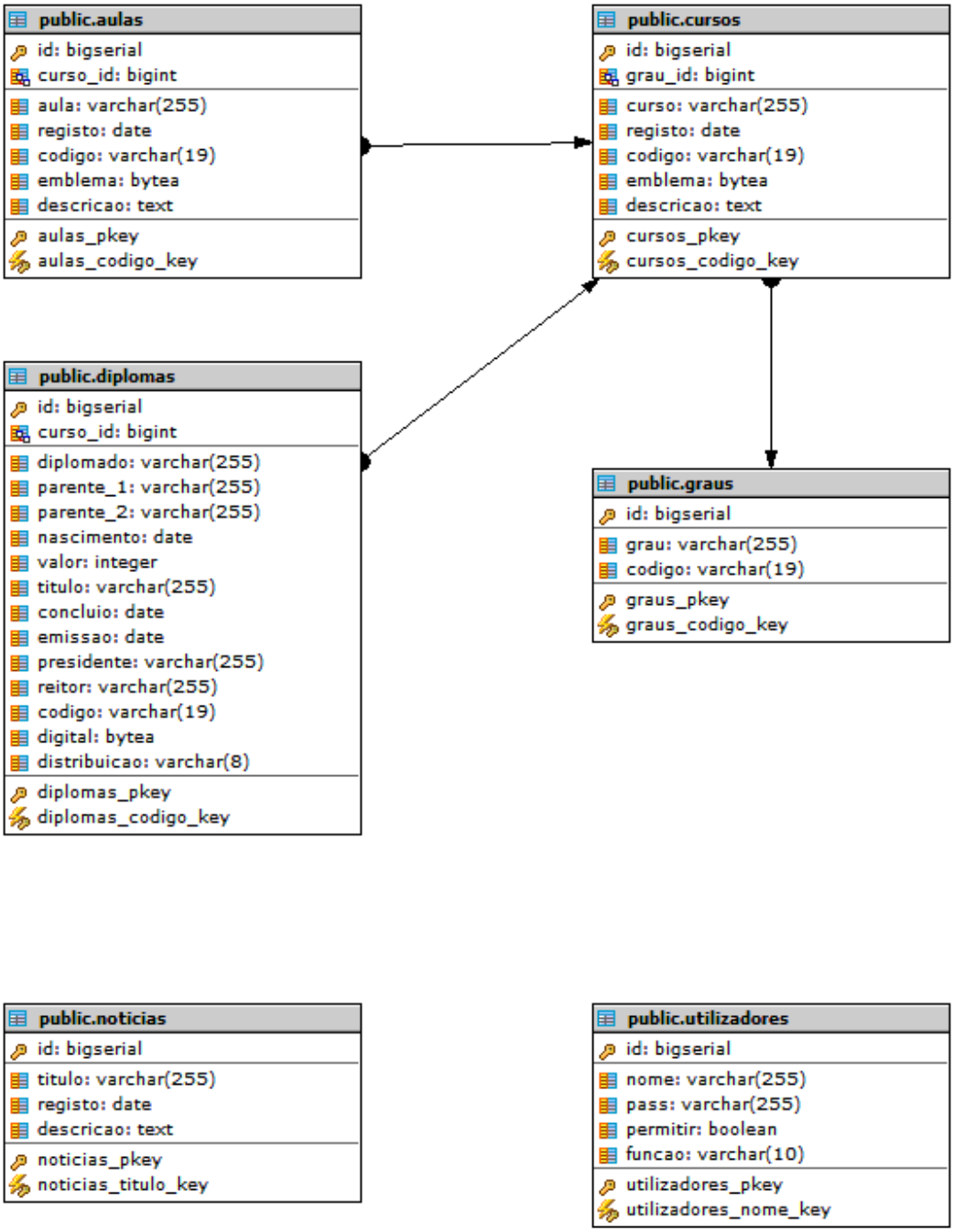

Figura 51 Base de Dados PostgreSQL Entidade Certificador

A proposta de base de dados da entidade certificadora, envolve 6 tabelas simples:

- Utilizadores:

  Guarda registos de utilizadores ou sistemas com acesso a Entidade Certificadora seus bancos de dados.

- Notícias:

  Publica notícias envolvendo o sistema na Entidade Certificadora para informar administradores de sistemas sobre alterações ou atualizações.

- Graus:

  Graus académicos disponíveis na Entidades Certificadoras.

- Cursos:

  Cursos de graus académicos disponíveis na Entidades Certificadoras.

- Aulas:

  Aulas por cursos académicos disponíveis na Entidades Certificadoras.

- Diplomas:

  Diplomas de alunos que concluíram um curso académico e são considerados diplomados.

Base de Dados PostgreSQL Servidor

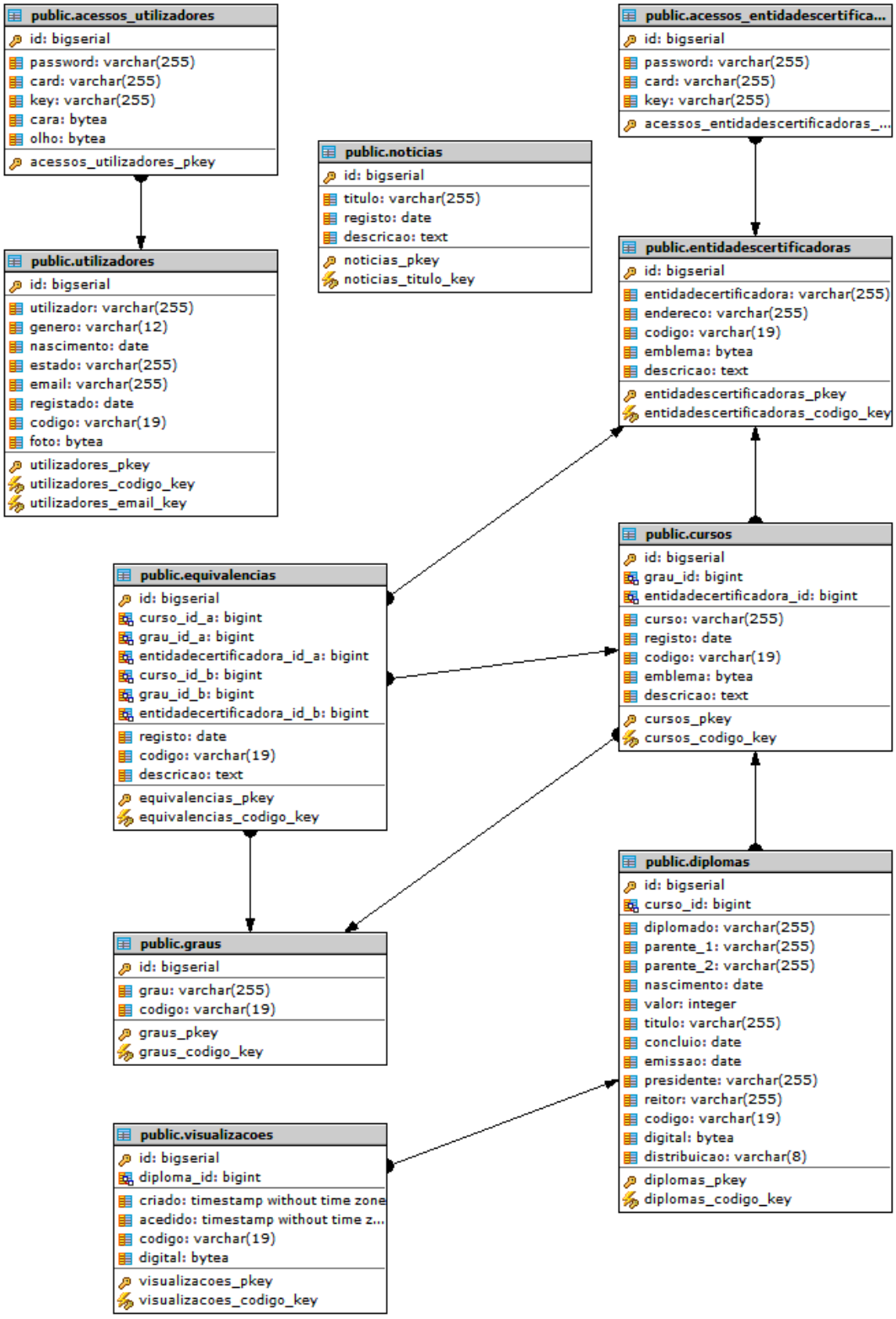

Figura 52 Base de Dados PostgreSQL Servidor

A base de dados para disponibilizar os serviços online e otimizar processos de distribuição e autenticação exige uma estrutura de dados própria.

Uma proposta para esta estrutura de base de dados no Gestor de Diplomas Online envolve 10 tabelas simples:

- Utilizadores:

  Guarda registos de utilizadores ou sistemas com acesso ao Gestor de Diplomas Online e os seus bancos de dados.

- Acessos do Utilizador:

  Guarda registo de acessos dos utilizadores para poder autenticar a sessão de cliente.

- Entidades Certificadoras:

  Guarda registos de Entidades Certificadoras com acesso ao Gestor de Diplomas Online

- Acessos da Entidade Certificadora:

  Guarda registo de acessos das entidades certificadoras para poder autenticar a sessão de entidade.

- Notícias:

  Publica notícias envolvendo o sistema na Entidade Certificadora para informar administradores de sistemas sobre alterações ou atualizações.

- Graus:

  Graus académicos disponíveis na Entidades Certificadoras.

- Cursos:

  Cursos dos graus académicos disponíveis na Entidades Certificadoras.

- Aulas:

  Aulas por cursos académicos disponíveis na Entidades Certificadoras.

- Diplomas:

  Diplomas de alunos que concluíram um curso académico e são considerados diplomados.

- Equivalências:

  Equivalências entre diplomas que são considerados por uma entidade certificadora.

- Visualizações:

  Registos de visualizações dos diplomas online.

Todas as interações entre os Serviços API e Base de Dados são geridas pelo Hibernate ORM com adicionar, alterar, remover e buscas de dados.

O Serviço no *Spring Boot* API envolve buscas do índice como número e código de identificação, outras buscas envolvem comparação dinâmica de texto alfabético, para proporcionar opções alternativas de pesquisa.

4.6 Interface e layouts do protótipo

A interface desenvolvida recorre ao uso do *browser* para acesso aos diferentes serviços do protótipo, a seguir apresentados.

Servidor API para Entidades Certificadoras

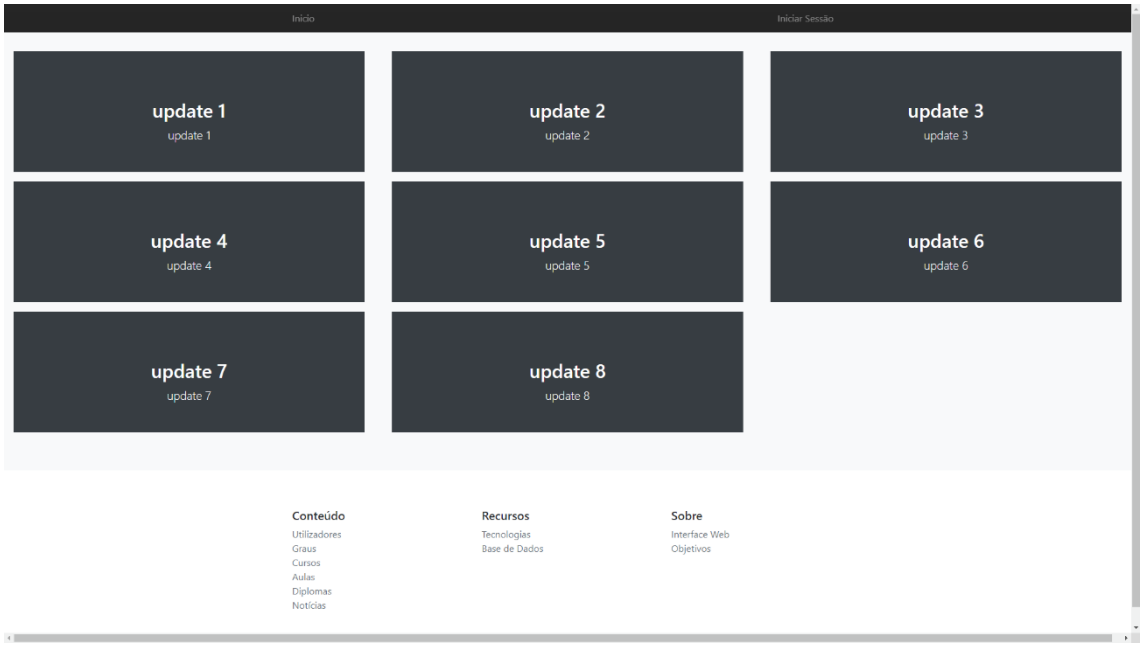

Figura 53 Universidade API Inicio

Um serviço para as Universidade seria uma Interface Web API que de maneira simples permitindo opções adicionar, alterar, remover ou busca de informação para fornecer informação utilizável para os serviços do Gestor de Diplomas Online.

O serviço para a universidade envolve autenticação de utilizadores como alunos diplomados e administradores como professores que geram os diplomas ou a informação de graus, cursos, aulas, diplomas e notícias.

Figura 54 Gerar Diplomas Universitários

Os utilizadores podem tem opões de inícios de sessão, registo e recuperação e conta.

- Opções de Inicio de Sessão:

Figura 55 UFP Inicio de Sessão

- Opções de Registo de Sessão:

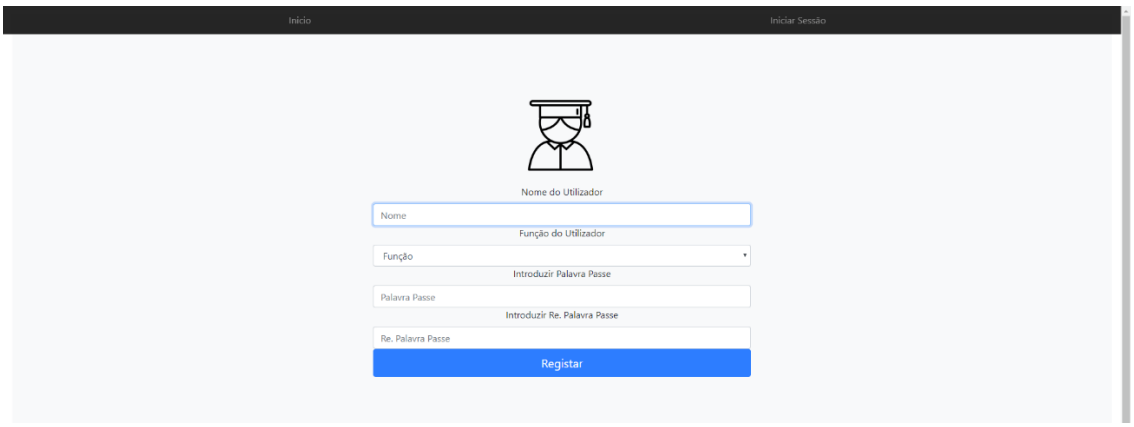

Figura 56 UFP Registo de Sessão

- Opções de Recuperação de Sessão:

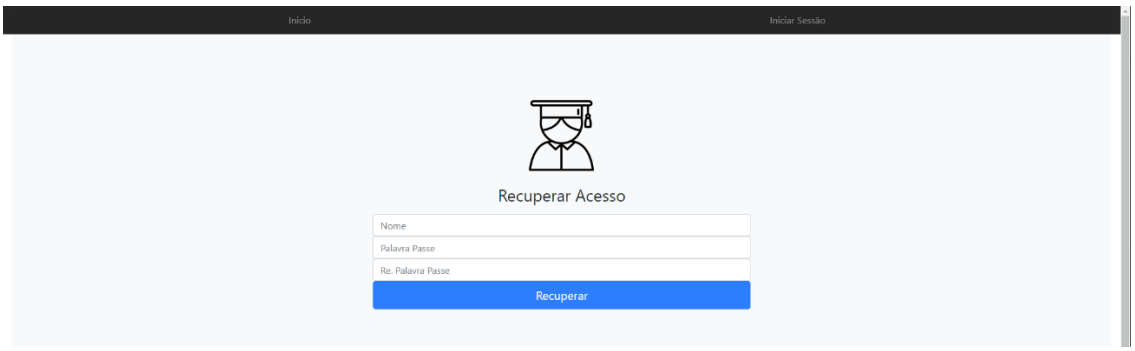

Figura 57 UFP Recuperação de Sessão

Servidor API para Entidades Certificadoras

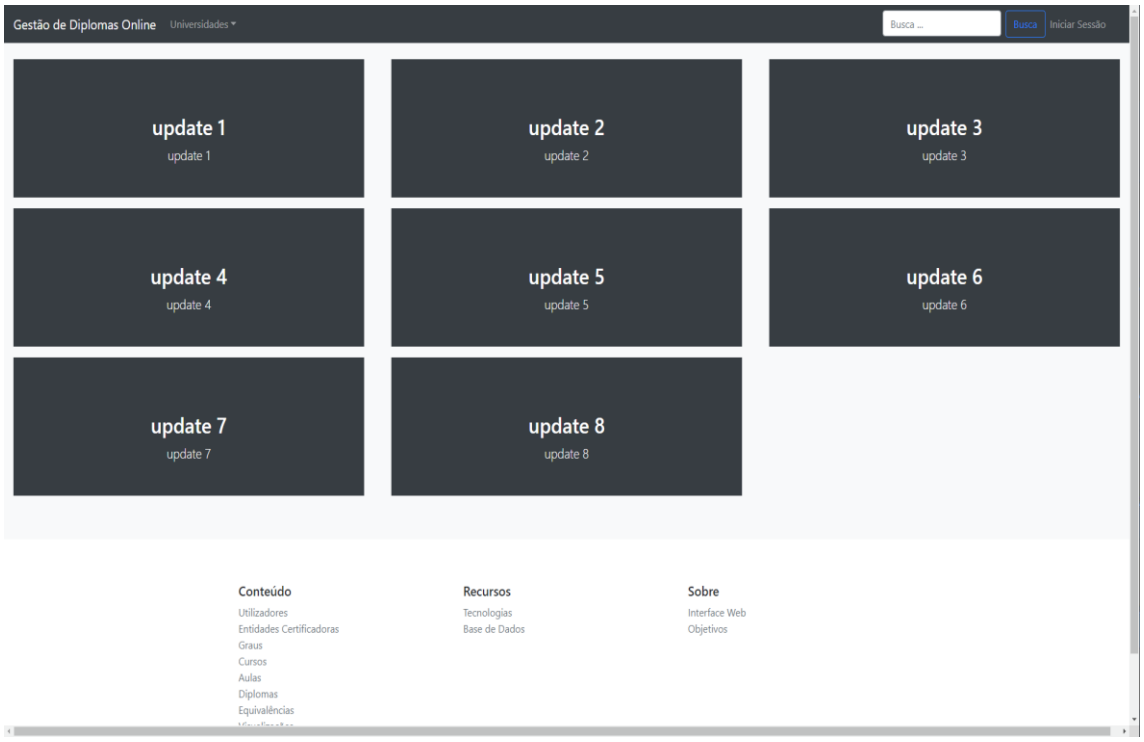

Figura 58 Gestor de Diplomas Online API Inicio

- Opções de Inicio de Sessão:

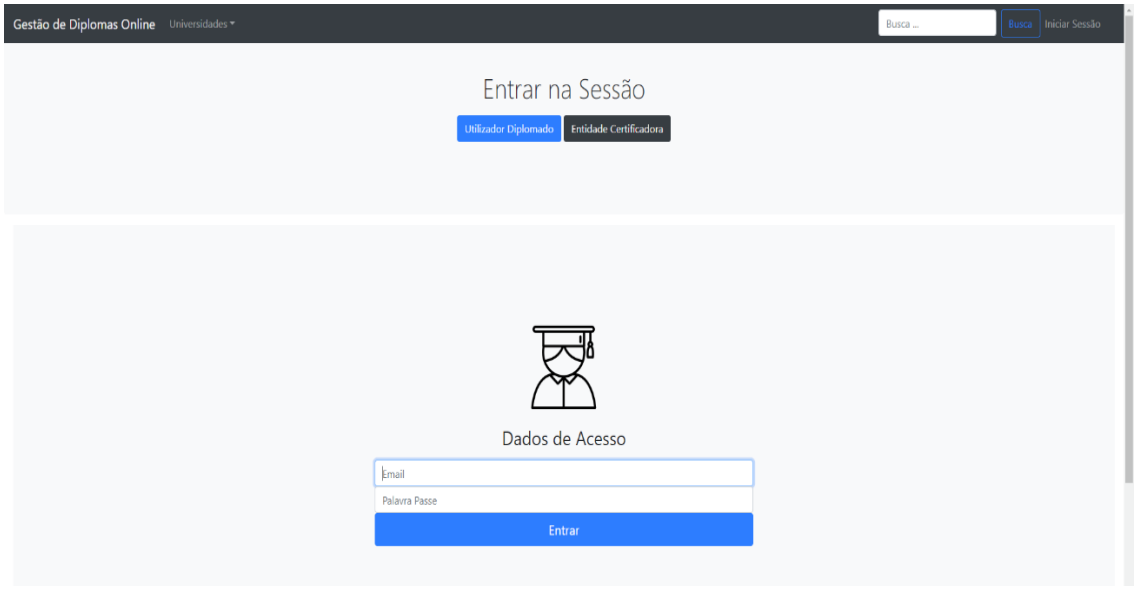

Figura 59 Gestor de Diplomas Online Inicio de Sessão

- Opções de Registo de Sessão:

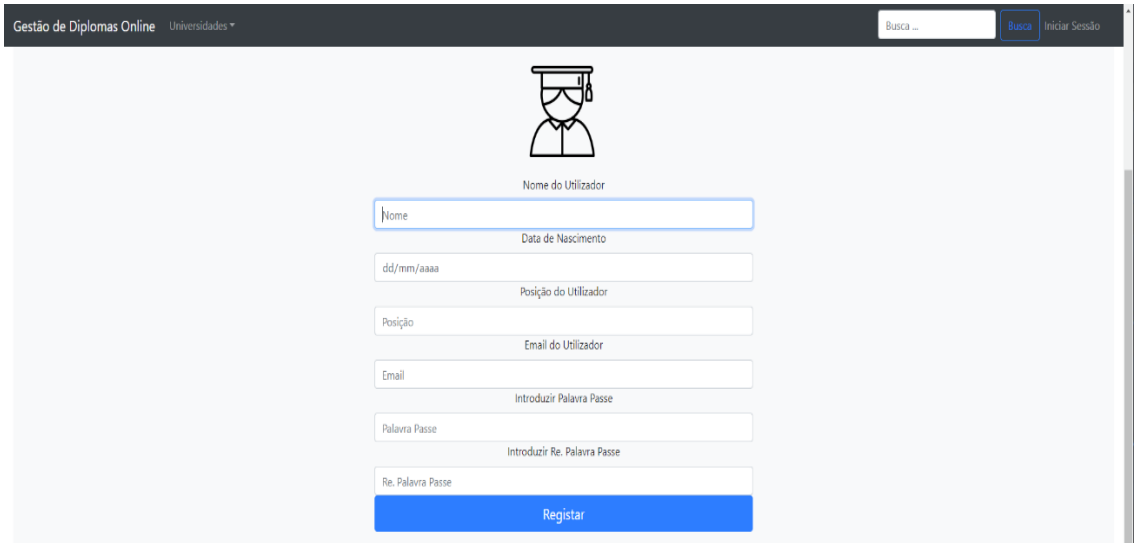

Figura 60 Gestor de Diplomas Online Registo de Sessão

- Opções de Recuperação de Sessão:

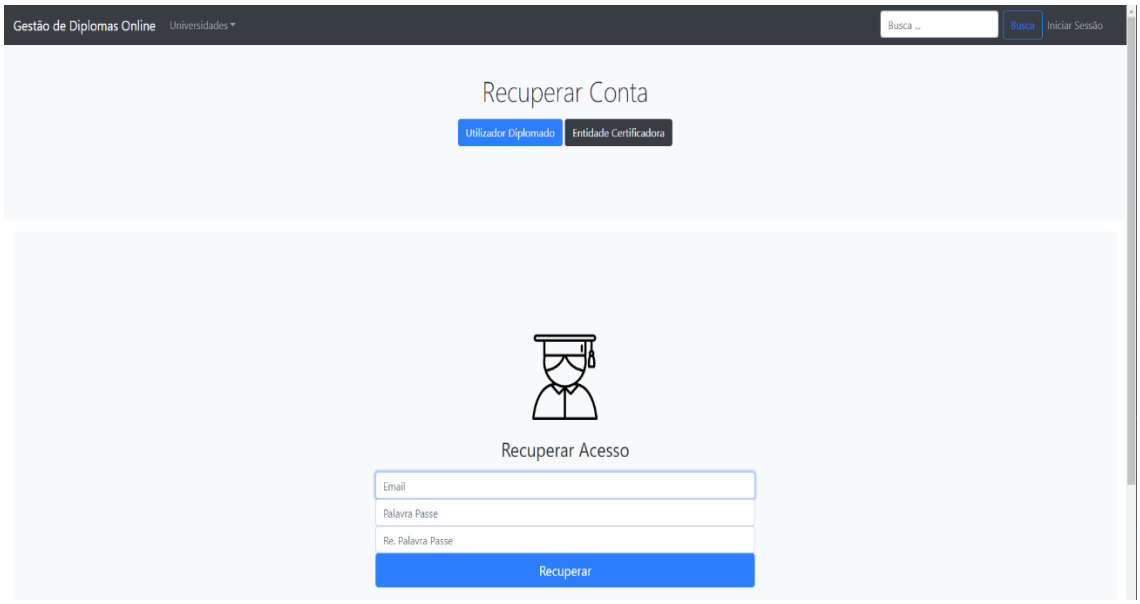

Figura 61 Gestor de Diplomas Online Recuperação de Sessão

5 Conclusão e trabalho futuro

5.1 Conclusão

O trabalho realizado teve por objetivo propor um protótipo funcional para desenvolver um Gestor de Diplomas Online com a implementação de várias tecnologias na área de validação e distribuição dos documentos *online*, permitindo opções para cumprir os requisitos das EC e dos AU da EU.

Para o efeito foram avaliadas aplicações e tecnologias existentes no mercado e as opções para o desenvolvimento deste tipo de sistemas. Foram ainda considerados os requisitos funcionais e não funcionais que um sistema deste tipo deve obedecer.

No projeto Gestor de Diplomas Online implementado foi considerada a intenção de criar um demonstrado de que a distribuição, autenticação, e produtividade dos diplomas académicos pode ser melhorado em formato digital através de uma RESTfull API.

5.2 Trabalho Futuro

Em trabalho futuro espero pode continuar com desenvolvimentos nas áreas relacionadas com o projeto apresentado, explorando APIs, Base de Dados e Sistemas de Informação de modo a criar plataformas digitais para dar resposta a contextos específicos de trabalho, em função de avaliação de tecnologia e escolha de alternativas para a criação de um protótipo ou aplicação funcional.

Em complemento e na consequência dos esforços realizados foi obtido um sistema que pode ser objeto de testes e desenvolvimento em ambiente real no contexto de uma IU.

Referências

.GOV (2018) *CMD Assinatura Digital - AUTENTICAÇÃO.GOV*, *.GOV*. Available at: https://www.autenticacao.gov.pt/cmd-assinatura (Accessed: 5 December 2018).

Administracao Digital (2018a) *Diploma Digital de ensino superior será assinado com certificado ICP-Brasil | Administração Digital*, *Administracao Digital*. Available at: https://administracaodigital.wordpress.com/2018/04/18/diploma-digital-de-ensino-superior-sera-assinado-com-certificado-icp-brasil/ (Accessed: 4 March 2019).

Administracao Digital (2018b) *Diploma Digital de ensino superior será assinado com certificado ICP-Brasil | Administração Digital*, *Administracao Digital*. Available at: https://administracaodigital.wordpress.com/2018/04/18/diploma-digital-de-ensino-superior-sera-assinado-com-certificado-icp-brasil/ (Accessed: 25 February 2019).

Adobe (2017) *Assinatura de PDFs no Adobe Acrobat Reader.*, *Adobe*. Available at: https://helpx.adobe.com/pt/reader/using/sign-pdfs.html (Accessed: 5 December 2018).

Brandão, J. L. (2018) *Diploma Digital é a onda do momento*, *Crypto Id*. Available at: https://cryptoid.com.br/colunistas/jose-luiz-brandao/diploma-digital-e-onda-do-momento/ (Accessed: 29 October 2018).

Codd, E. F. (1970) 'A relational model of data for large shared data banks', *Communications of the ACM*. doi: 10.1145/362384.362685.

Cryptoid (2018) *O diploma digital será obrigatório em todo o território nacional e as Instituições de Ensino Superior terão dois anos para implementar o processo | CRYPTOID*, *Cryptoid*. Available at: https://cryptoid.com.br/banco-de-noticias/32742-diploma-digital-sera-obrigatorio-em-todo-o-brasil/ (Accessed: 4 March 2019).

Deepakumara, J., Heys, H. M. and Venkatesan, R. (2001) 'FPGA implementation of MD5 hash algorithm', *Canadian Conference on Electrical and*

Computer Engineering 2001. Conference Proceedings (Cat. No.01TH8555). doi: 10.1109/CCECE.2001.933564.

Digital Sign (2019) *DigitalSign | Apresentação DigitalSign - Quem Somos*, *Digital Sign*. Available at: https://www.digitalsign.pt/pt/institucional/quem-somos (Accessed: 5 March 2019).

Global Trusted Sign (2019) *GTS - Global Trusted Sign*, *Global Trusted Sign*. Available at: https://www.globaltrustedsign.com/public_c (Accessed: 5 March 2019).

Guimbretière, F. (2003) 'Paper augmented digital documents', in *Proceedings of the 16th annual ACM symposium on User interface software and technology - UIST '03*. doi: 10.1145/964696.964702.

Kieseberg, P. *et al.* (2011) 'QR code security', in. doi: 10.1145/1971519.1971593.

Kim, J. *et al.* (2006) 'On the security of HMAC and NMAC based HAVAL, MD4, MD5, SHA-0 and SHA-1', *Security and Cryptography for Networks. 5th International Conference, SCN 2006. Proceedings (Lecture Notes in Computer Science Vol. 4116)*. doi: 10.1007/11832072_17.

Kucirkova, N., Audain, J. and Chamberlain, L. (2018) 'QR codes', in *Jumpstart! Apps*. doi: 10.4324/9781315674452-5.

Kurniawan, S. (2004) 'Interaction design: Beyond human computer interaction', *Springer*. doi: 10.1007/s10209-004-0102-1.

Ligeza, A. (1995) 'Artificial Intelligence: A Modern Approach', *Neurocomputing*. doi: 10.1016/0925-2312(95)90020-9.

Liu, Y., Yang, J. and Liu, M. (2008) 'Recognition of QR Code with mobile phones', in *Chinese Control and Decision Conference, 2008, CCDC 2008*. doi: 10.1109/CCDC.2008.4597299.

MABEE, P. M. (1993) 'Phylogenetic interpretation of ontogenetic change: sorting out the actual and artefactual in an empirical case study of centrarchid

fishes', *Zoological Journal of the Linnean Society*, 107(3), pp. 175–291. doi: 10.1111/j.1096-3642.1993.tb00289.x.

Noble, D. (1998) 'Digital Diploma Mills: The Automation of Higher Education', *Monthly Review*, 49(9), p. 38. doi: 10.14452/mr-049-09-1998-02_4.

Notions, S. *et al.* (2011) 'Cryptographic Hash Functions : Recent Design Trends and', *eprint.iacr.org*, pp. 1–36. Available at: http://eprint.iacr.org/2011/565.pdf.

Petrina, S. (2005) 'How (and why) Digital Diploma Mills (don't) Work: Academic Freedom, Intellectual Property Rights, Automation and UBC's Master of Educational Technology Program', *Workplace: A Journal for Academic Labor*, pp. 38–59.

PostgreSQL (2019) *PostgreSQL*, *PostgreSQL*. Available at: https://www.postgresql.org/about/ (Accessed: 23 April 2019).

Santo Contrato (2018) *O que é ICP Brasil e como funciona?*, *Santo Contrato*. Available at: https://www.santocontrato.com.br/o-que-e-icp-brasil/ (Accessed: 17 March 2019).

Stumpe, F. and Katina, P. F. (2017) 'A cybernetic ontology for project management', *International Journal of System of Systems Engineering*, 8(1), p. 42. doi: 10.1504/ijsse.2017.083937.

Suporte do Office (2018) *Adicionar ou remover uma assinatura digital nos ficheiros do Office*, *Microsoft*. Available at: https://support.office.com/pt-pt/article/adicionar-ou-remover-uma-assinatura-digital-nos-ficheiros-do-office-70d26dc9-be10-46f1-8efa-719c8b3f1a2d (Accessed: 5 December 2018).

Swan, M. (2015) *Blockchain Blueprint for a New Economy*, *Geriatric Nursing*. doi: 10.1017/CBO9781107415324.004.

TVI24 (2018) *Recibos verdes e faturas.*, *TVI24*. Available at: https://tvi24.iol.pt/economia/irs/recibos-verdes-e-faturas-comece-a-juntar-as-suas (Accessed: 27 November 2018).

Universidade do Porto (2018) *DIGITARY - Certificados online*, *Universidade do*

Porto. Available at: https://sigarra.up.pt/up/pt/web_base.gera_pagina?p_pagina=página estática genérica 1596 (Accessed: 3 November 2018).

Untergasser, A. *et al.* (2007) 'Primer3Plus, an enhanced web interface to Primer3', *Nucleic Acids Research*. doi: 10.1093/nar/gkm306.

Valid (2019) *e-Diploma*, *VALID*. Available at: http://www.validcertificadora.com.br/ediploma (Accessed: 18 January 2019).

Yli-Huumo, J. *et al.* (2016) 'Where is current research on Blockchain technology? - A systematic review', *PLoS ONE*. doi: 10.1371/journal.pone.0163477.

Your Europe (2018) *No automatic EU-wide recognition of academic diplomas*, *European Union*. Available at: https://europa.eu/youreurope/citizens/education/university/recognition/index_en.htm (Accessed: 23 November 2018).

Apêndice: recursos utilizados

Tecnologias e recursos usados para o desenvolvimento do protótipo.

Emulador Intellij IDEA

- Java
- Hibernate ORM
- Maven

Base de Dados PostgreSQL

- SQL
- Diagramas

Sistemas de Informação

- SpringBoot API
- Interface Web
- Bootstrap
- Thymeleaf

Algoritmos de Segurança de Informação e Transações

- Blockchain
- Ethereum
- Código Hash: MD5 e SHA-2
- Código QR
- Apache POI