RNP

RP4: Proposta de Fase 2

Grupo de Trabalho – Segunda Fase

GT-RAP: Serviço de Registro, Autenticação e Preservação de Documentos Digitais

Guido Lemos e Rostand Costa (LAVID/UFPB)

Março de 2018

1. Visão Geral

A validação da existência ou da posse de documentos formalmente assinados é fundamental em qualquer contexto legal. Normalmente, a certificação tradicional de documentos físicos se baseia em autoridades centrais, notariais ou não, para armazenar e aplicar os registros e mecanismos necessários para tal fim e também lidar com os aspectos e desafios da segurança. Desafios esses que se tornam cada vez mais difíceis à medida que os arquivos envelhecem.

Entretanto, a materialização e desmaterialização de documentos bem como o dinamismo e velocidade das relações digitais têm representado uma nova frente para entidades produtoras e/ou certificadoras de documentos. Principalmente quando começa a emergir a possibilidade de geração de documentos em papel a partir de documentos digitais e a geração de documentos digitais a partir de documentos em papel, demandando a garantia de que os termos estabelecidos no original sejam efetivamente conservados e recebam uma chancela de legitimação, independentemente da sua forma de representação.

De um ponto de vista prático, a certificação de documentos digitais apresenta três dimensões principais [Crosby 2016]: i) *Prova de Propriedade/Autoria* (quem é o detentor/autor do documento), ii) *Prova de Integridade* (o documento está íntegro e exatamente igual à quando foi criado) e iii) *Prova de Existência* (o documento foi criado e legitimado em um dado momento no tempo).

Neste sentido, a tecnologia de livros-razão distribuídos [Kakavand 2017] (ou DLTs, do inglês *Distributed Ledgers Technologies*), normalmente baseados em *blockchain*, se apresenta como um modelo alternativo para a certificação de documentos legais, sobretudo pela eliminação da necessidade de uma autoridade centralizada para verificar a autenticidade de um documento. Uma entidade emissora pode simplesmente armazenar a assinatura e a marcação de tempo associada com um documento legal na cadeia de blocos e validá-lo em qualquer tempo usando os mecanismos nativos da tecnologia [Wikipedia 2018].

Como é considerada à prova de fraudes e pode ser verificada por terceiros, de forma independente, este tipo de certificação provido por DLTs pode ser juridicamente relevante. Além disso, o registro da publicação usando *timestamps* e *hashs* criptográficos de arquivos em cadeia de blocos oferece um novo e irrefutável nível de certificação. Associadamente, o uso de *blockchain* para esse tipo de registro pode ainda permitir assegurar a privacidade do documento e dos autores envolvidos, se for o caso.

Esta proposta detalha a segunda fase de um projeto de pesquisa e desenvolvimento, chamado GT-RAP, cujo objetivo é investigar o potencial do uso combinado das tecnologias de *blockchain*, certificação digital e preservação digital para a criação de uma plataforma, escalável e agnóstica, especializada na autenticação e preservação de documentos digitais.

Como resultado da primeira etapa do projeto, foi feita a construção de um protótipo de serviço público para registro e verificação digital da autenticidade de documentos acadêmicos. O protótipo de serviço desenvolvido oferece uma interface para que instituições de ensino possam registrar documentos oficiais, como diplomas e certificados, usando *blockchain* e uma interface para que outras instituições e/ou pessoas interessadas possam verificar a legitimidade de um documento através do seu número de registro em uma DLT. Os documentos registrados no serviço são automaticamente inseridos em um repositório de preservação digital de longo termo.

1.1. Descrição do Produto/Serviço Resultante do Piloto

1.1.1 Contextualização e Motivação

1.1.1.1 Necessidade de Proteção de Documentos Acadêmicos

Os últimos dados[1] do Censo da Educação Superior realizado anualmente pelo INEP indicam que o Brasil teve em 2016 um total de um milhão e cem mil concluintes e um total de quase três milhões de ingressantes nas instituições públicas e privadas de ensino superior. Com isso, em 2016, o total de estudantes matriculados em cursos de ensino superior no país ultrapassa pela primeira vez os 8 milhões de alunos.

Os números[2] da CAPES sobre os programas de pós-graduação no Brasil indicam que em 2016 haviam 325.320 estudantes matriculados em cursos de pós-graduação *stricto sensu* no país, variando entre mestrado profissionalizante, mestrado acadêmico e doutorado. Neste mesmo ano foram titulados no Brasil 20.630 doutores e 59.349 mestres.

Em relação aos cursos de pós-graduação *lato sensu*, não há dados atualizados sobre a quantidade de cursos em funcionamento ou sobre a quantidade de alunos matriculados e titulados. São números bastante variáveis dada a natureza mais dinâmica desses cursos, sempre associados a necessidades do mercado, e também devido as baixas exigências regulamentares para sua abertura. Porém, é possível estimar, de forma bastante conservadora, que a pós-graduação *lato sensu* no Brasil seja, pelo menos, 10 vezes maior que a pós-graduação *stricto sensu*, o que nos levaria a diplomação de pelo menos 600.000 especialistas ao ano.

Com isso, podemos chegar a conclusão que no Brasil, apenas no ensino superior, são emitidos anualmente cerca de 1,8 milhão de diplomas. Se somarmos a este número a quantidade de diplomas emitidos no exterior e revalidados no país, é possível atingirmos a marca de 2 milhões de diplomas emitidos anualmente.

Apesar da emissão de tais diplomas ser controlada, exigindo-se o registro do documento por uma Universidade junto ao Ministério da Educação, as dimensões continentais de nosso país, aliadas à falta de suporte tecnológico, fazem com que a tarefa de verificar a autenticidade de um diploma emitido ou revalidado no país seja executada de maneira ineficiente.

Um exemplo dessa dificuldade envolveu o INEP, um órgão do próprio Ministério da Educação, responsável por diversas atividades relacionadas a avaliação do ensino no pais. Em 2011 o INEP foi obrigado a cancelar as avaliações de 4 cursos de graduação na área de Direito pelo fato de que um dos avaliadores *ad hoc* participantes do **Banco de Avaliadores do Sistema Nacional de Educação Superior** (BASIS) teria apresentado diplomas falsos de mestrado e doutorado [Folha 2011]. Tal fraude só foi descoberta por conta de uma denúncia anônima. Não fosse isso, possivelmente este avaliador teria continuado a representar o Ministério da Educação na avaliação do ensino superior no país.

Casos de uso de diplomas falsos para ingresso no ensino superior e no serviço público também não são raros. O Ministério Público do Paraná investigou o uso de mais de 500 diplomas falsos na cidade de Maringá que foram utilizados para ingressos em universidades e aprovação em concursos públicos [Gazeta 2013].

Há quadrilhas especializadas em vender diplomas falsos em nome de Instituições de Ensino Superior [Globo 2017]. No estado do Espírito Santo, mais de 100 professores estão sendo processados por usarem diplomas falsos [Gazeta 2017]. As fraudes também acontecem no processo de revalidação de diplomas estrangeiros. Um caso

1 http://portal.inep.gov.br
2 http://www.capes.gov.br/

emblemático, foi a quadrilha que revalidava de forma fraudulenta diplomas de medicina no estado do Mato Grosso [Globo 2013]. Além disso, há inúmeros relatos de casos de utilização de diplomas falsos para ludibriar clientes e, o que é mais grave, pacientes, no caso dos diplomas relacionados às áreas de saúde.

O processo de investigação, descoberta e tomada de providência em relação à falsificação de diplomas também envolve desafios específicos. Como os mecanismos de controles e verificação nem sempre são automatizados e o número de casos têm crescido nos últimos anos, é complicado para a justiça detectar e tomar as devidas providências frente aos prejuízos causados por essas quadrilhas e pessoas de má fé. A Secretaria de Estado da Educação do Espírito Santo (SEDU-ES), por exemplo, relata que as investigações referentes aos processos administrativos para apurar o uso de diplomas falsos nas escolas do estado podem durar até 180 dias, com possibilidade de prorrogação [Gazeta2017].

1.1.1.2 Gestão de Diplomas Acadêmicos

A *LDB - Lei de Diretrizes e Bases da Educação* (Lei 9394/1996) delega a responsabilidade pela emissão dos diplomas para as Instituições de Ensino Superior, além dos demais documentos acessórios como declaração de conclusão e certificados de conclusão de curso. Além disso, segundo a própria LDB, a responsabilidade pelo registro e manutenção de tais registros também é de responsabilidade da IES. Para o caso de instituições de ensino não-universitárias, tais registros são feitos por instituições indicadas pelo Conselho Nacional de Educação (CNE).

Quanto a revalidação de diplomas de universidades do exterior e emissão e registro de diplomas de pós-graduação, tais responsabilidades também são das instituições universitárias brasileiras e seguem as mesmas regras dos diplomas de graduação, observando a competência da universidade em relação àquela área.

Em relação à preservação dos registros, as universidades devem manter os registros e documentos emitidos por elas, relacionados à instituição em si e às faculdades e demais instituições de ensino que não possuem competência para registro.

A gestão de tais documentos está regulamentada pela Lei 8159/91. A referida lei cria o *Conselho Nacional de Arquivos* (CONARQ). O CONARQ estabelece recomendações e define a tabela de temporalidade de manutenção de arquivos públicos pelos órgãos responsáveis. Os diplomas universitários (código 135.421) possuem tempo de guarda recomendada de 5 anos com posterior eliminação. Já o registro do diploma possui tempo de guarda ativo de 5 anos, com posterior guarda permanente. No caso das instituições particulares o registro é efetuado por instituição credenciada e a documentação base é retornada para instituição não credenciada a fim de que proceda com a preservação.

Ainda sobre os diplomas de faculdades ofertantes não credenciadas, segundo a norma técnica 391/2013/MEC, cabe às universidades credenciadas apenas registrar o diploma, porém a emissão é de responsabilidade da instituição não credenciada. Neste sentido, cada instituição define seu fluxograma de emissão e registro de diplomas. Geralmente esse fluxo está descrito no regimento interno e nos documentos que definem os processos internos da instituição.

1.1.1.3 Uso de Diplomas Digitais

O uso de diplomas digitais apresenta uma série de vantagens quando comparado ao diploma tradicional: i) a eliminação, pelo emissor, do custo de impressão da versão em papel (normalmente especial e de alto custo); ii) a replicação e distribuição ilimitada e gratuita do documento pelo portador; e iii) a possibilidade de adoção, pelo destinatário, de mecanismos automatizados de verificação da autenticidade do documento. Tais características emprestam mais agilidade e segurança para que portadores de diplomas e interessados possam compartilhar e verificar a legitimidade de tais documentos de forma mais eficiente. Além disso, é possível padronizar e formalizar o processo de emissão e validação dos diplomas, dificultando tentativas de fraudes.

Embora o uso de diplomas digitais desponte como um caminho quase que natural para a gestão de documentos dessa natureza, ainda não existe uma legislação que trate diretamente do tema. A falta de uma regulação específica, assim como aspectos culturais, atrasam o avanço do processo de digitalização desses documentos e o seu uso em larga escala.

Um análise mais direta sobre isso está contido no parecer CNE/CES No. 226/2012, o qual faz algumas considerações sobre o uso de diplomas digitais a partir de uma consulta feita pela UNIVAP. Resumidamente, o parecer em questão indica que o uso desse tipo de documento não é proibido, porém a IES deve oferecer também a possibilidade de emissão de cópia física do documento, deixando a critério do aluno a escolha da melhor forma de acesso ao seu diploma.

Em uma iniciativa mais concreta, em 2013 a USP passou a oferecer a emissão de diplomas no formato digital [ITI 2013]. Um fato curioso ocorreu em 2016, quando a USP, mesmo após a adoção do diploma digital, ainda deixou de emitir mais de 4 mil diplomas por falta de papel [Estadao 2016], o que sugere que os dois tipos de diploma ainda conviviam na época. O Centro Universitário de Belas Artes foi outra instituição paulista de ensino que também adotou a emissão de diplomas digitais a partir de 2013 [Baguete 2013].

1.1.1.4 Desafios da Preservação Digital de Longo Termo

Na mesma proporção em que uma parte considerável dos artefatos relacionados à diversas atividades humanas está sendo criada em formatos digitais, é esperado que as práticas de preservação para essas informações também devam ser baseadas em técnicas e tecnologias adequadas e igualmente digitais.

Quando comparada com a preservação de coleções físicas, a preservação de conteúdo digital traz, em si, uma associação, quase paradoxal, de um grande potencial de risco e um grande potencial de proteção [Skinner 2010]. O potencial de risco é representado pela efemeridade do armazenamento digital que pode ser irremediavelmente perdido por causa de falhas técnicas ou humanas com muito mais facilidade e rapidez do que no caso de representações físicas de conteúdo. O potencial de proteção, por sua vez, é ancorado no fato de que coleções digitais podem ser indefinidamente reproduzidas e armazenadas com total fidelidade e integridade.

A área da preservação digital ainda está nos estágios iniciais de sua formação e o aparato tecnológico, metodológico e político para preservar a informação digital ainda está sendo construído. Boa parte do conhecimento acumulado na última década em preservação e acesso a recursos digitais está se consolidando em um conjunto de estratégias, abordagens tecnológicas e atividades que agora são coletivamente conhecidas como “curadoria digital”. Ainda um conceito em evolução, a curadoria digital envolve a gestão atuante e a preservação de recursos digitais durante todo o seu ciclo de interesse, tendo como perspectiva o desafio de longo prazo de atender a gerações atuais e futuras de usuários [Sayao 2012].

A perfeita continuidade de coleções digitais depende, em grande parte, de se buscar um equilíbrio da aplicação de medidas que aproveitem ao máximo o potencial de proteção ao ponto de neutralizar o seu inerente potencial de risco. Entretanto, o desafio pode representar muito mais um problema social e institucional do que uma questão meramente técnica, pois, em particular, para a preservação digital no meio acadêmico, depende-se de instituições que passam por mudanças de direção, missão, administração e fontes de financiamento [Sayao 2012].

Além disso, a preservação digital envolve desafios essencialmente diferentes dos encontrados na conservação de conteúdo em suportes mais tradicionais. De um ponto de vista mais tradicional, o ato de preservar traduz-se no ato de manter imutável e intacto. No ambiente digital, entretanto, a ação de preservar também pode se referir a mudar, recriar e renovar. Onde renovar pode significar mudar formatos, atualizar

mídias e/ou substituir *hardware* e *software*. Em suma: se, por um lado, queremos manter o conteúdo exatamente como foi criado, intacto; por outro lado, queremos continuar acessando-o em plataformas modernas. Este é o *Paradoxo da Preservação Digital*, conforme descrito por Sayão [Sayao 2012].

Um número crescente de organizações de memória cultural (incluindo as reunidas na iniciativa *MetaArchive* [Skinner 2009]) aposta que os esforços mais eficazes de preservação digital ocorrem na prática através de alguma estratégia para manter múltiplas cópias de conteúdo digital em locais distribuídos seguros [Ruusalepp 2012, Ferreira 2012]. Na era digital, esta estratégia requer investimentos numa matriz distribuída de servidores, capazes de armazenar coleções digitais em uma metodologia pré-coordenada.

A montagem de infraestruturas computacionais para preservação digital distribuída [Skinner2010] implica em adotar estratégias envolvendo a distribuição geográfica do armazenamento em vários locais e a implementação de segurança forte em caches individuais, uma combinação de abordagens que maximiza a sobrevivência de conteúdo, tanto em termos individuais quanto coletivos. Maximizar as medidas de segurança implementadas em caches individuais reduz a probabilidade de que qualquer cache individual seja comprometida. Por sua vez, a replicação reduz a probabilidade de que a perda de qualquer cache individual leve a uma perda do conteúdo preservado.

Entretanto, é pouco provável que uma única organização educacional tenha a capacidade de operar de forma adequada vários servidores distribuídos geograficamente. Neste sentido, a colaboração entre instituições é essencial, e tal colaboração exige investimentos técnicos e organizacionais [Costa2015, Costa2016]. Não é o caso de contar apenas com uma solução tecnológica adequada, mas também precisam ser estabelecidos acordos interinstitucionais robustos de longo prazo, ou não haverá compromisso suficiente para uma atuação sintonizada ao longo do tempo.

1.1.2 Serviço de Registro, Autenticação e Preservação de Documentos Digitais

É baseado neste cenário que propomos a construção de uma plataforma, escalável e agnóstica, para armazenamento e verificação digital da autenticidade de documentos digitais baseada no uso combinado das tecnologias de *blockchain*, certificação digital e preservação digital.

A estratégia utilizada como metodologia para o desenvolvimento do projeto prevê a divisão do esforço em três grupos de atividades, os quais estão relacionados ao levantamento do estado da arte e mapeamento de requisitos para certificação digital de documentos e preservação digital distribuída, definição de uma arquitetura genérica para autenticação e preservação de documentos digitais e a montagem de um protótipo para validação da abordagem proposta.

Acreditamos que com um serviço como o proposto aqui em funcionamento, a autenticidade de documentos (como diplomas ou certificados) emitidos ou revalidados por instituições acadêmicas brasileiras poderá ser mais facilmente verificada, tanto por órgãos públicos quanto por instituições privadas e pessoas físicas.

1.1. Identificação do Público Alvo

De forma geral, o público alvo do serviço proposto pode ser classificado em três categorias principais, todos relacionados com o ciclo de vida de um *documento digital assinado* (DDA): i) o **emissor** do DDA; ii) o **portador** (ou detentor/beneficiário do DDA e, iii) o **receptor** (ou destinatário) do DDA. O primeiro é o responsável por *emitir e assinar* um documento digital em nome ou benefício do segundo, o qual, por sua vez, o *guarda* e, eventualmente, o *distribui* no seu interesse ou sob demanda para um terceiro ator, o qual, dependendo da natureza e da dinâmica específica do documento, *verifica* a sua legitimidade e *aplica* o seu valor. Uma visão geral do contexto do serviço e

também o escopo do piloto e dos principais atores envolvidos está ilustrado na **Figura 1**.

Figura 1 – **Visão Geral do Serviço Proposto**

O serviço proposto não interfere no fluxo natural entre os três atores em pauta mas permite que tanto a atuação do **emissor** quanto do **receptor** do *documento digital assinado* seja facilitada, sobretudo na interação para a validação do mesmo. Sempre centrado no uso do DDA pelos atores, o serviço provê mecanismos para registrar e preservar o documento para o **emissor** e para autenticá-lo para o **receptor**, fazendo ainda a guarda de longa duração do mesmo, o que beneficia todos os atores.

No contexto do piloto, focado em diplomas acadêmicos, o **emissor** do diploma digital é a *IES de Origem*, o **portador** do diploma é o *aluno egresso* da *IES de Origem* e o papel do **receptor** é representado por outras *IES, órgãos públicos e empresas privadas* para as quais o portador do diploma está aplicando para uma posição que exige a apresentação do mesmo.

Participarão do piloto IES públicas e privadas de grande porte, além de uma primeira experiência de integração com uma emissora de certificados de cursos técnicos de curta duração, descritos na Seção 2.2. A Seção 3 traz alguns estudos preliminares de modelos de negócio aplicáveis ao contexto em pauta.

2. Definição do Piloto

O principal objetivo do GT-RAP, na sua primeira fase, foi investigar o potencial do uso combinado da tecnologia *blockchain* com repositórios ativos distribuídos para a criação de uma plataforma, escalável e agnóstica, especializada na autenticação e preservação de documentos digitais. Como prova de conceito da plataforma proposta, foi realizada a construção de um protótipo de serviço para registro e verificação digital da autenticidade de documentos acadêmicos.

A estratégia de modelagem do protótipo partiu da premissa de garantir uma integração pouco invasiva com os processos e sistemas em uso atualmente para emissão e registro de diplomas acadêmicos nas instituições de ensino. Considerando a necessidade de uma transição suave para permitir o aculturamento progressivo com as novas metáforas e tecnologias envolvidas, trabalhou-se com a possibilidade de uma possível convivência dos dois métodos de emissão.

Neste sentido, alguns requisitos básicos foram estabelecidos para a primeira etapa de operação do serviço:

- Tentar minimizar (ou eliminar) a necessidade de intervenção nos fluxos internos dos setores envolvidos na emissão e registro de diplomas das instituições;
- Considerar que o diploma tradicional, em papel, continuará sendo emitido normalmente e que o diploma digital será uma opção para o aluno;
- Identificar e aplicar os mesmos protocolos e níveis de alçada usados para a assinatura tradicional dos diplomas em cada instituição na assinatura digital da versão eletrônica;
- Garantir que o todo o controle e autonomia presentes hoje nas instituições de ensino permaneçam inalteradas para a assinatura digital da versão eletrônica. Não deve existir nenhuma transferência de responsabilidade para o serviço;
- As operações de registro e autenticação de documentos devem ser sempre lastreadas pela validação das assinaturas digitais dos documentos digitais envolvidos e não apenas baseadas na autenticação de usuários e sessões.

Para ilustrar melhor o contexto, a **Figura 2** traz o fluxo operacional atualmente praticado na UFPB[3] para a emissão de diplomas. Como pode ser visto, são feitas três assinaturas no diploma durante o processo de emissão, enquanto que na PUC-Rio são apenas duas, e por atores/setores diferentes.

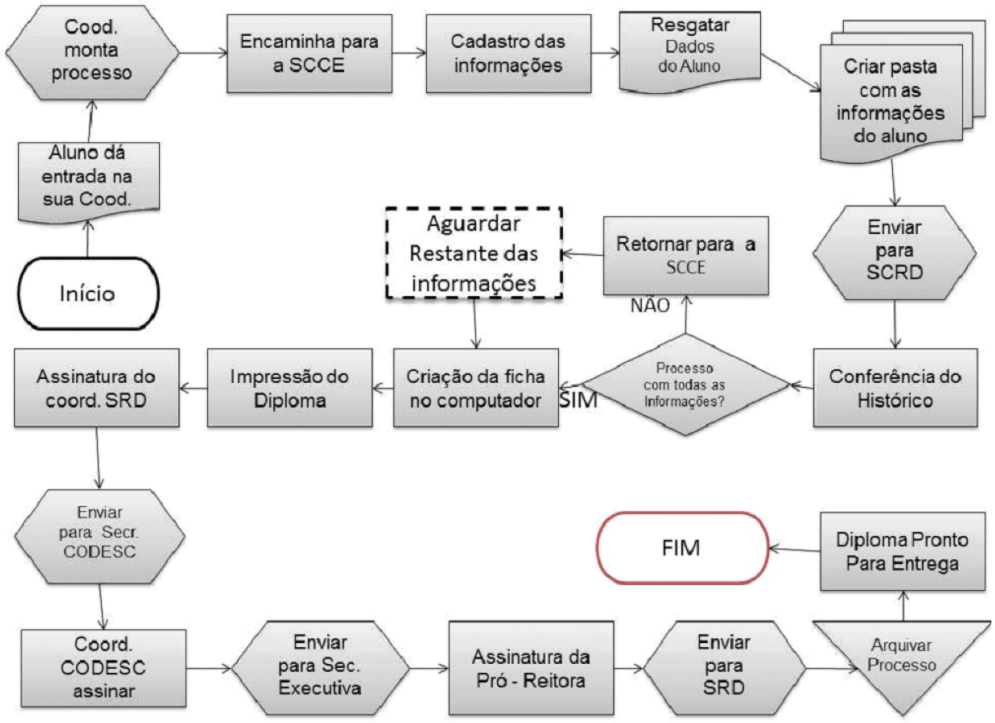

Figura 2 - **Fluxo Operacional para Emissão de Diplomas na UFPB**

Para permitir uma conciliação com tais fluxos internos, que variam de instituição para instituição, a integração com o serviço proposto pelo GT-RAP pode iniciar apenas a partir do momento em que a emissão do diploma tradicional em papel é concluída. Isso garante que todas as verificações do mérito e das exigências do título acadêmico já foram satisfeitas e concluídas (**Figura 3**).

A partir deste ponto e contando com o desejo e anuência expressa do interessado, o processo adicional de emissão e registro do diploma digital pode ser iniciado pela própria instituição. Esta fase possui cinco etapas lógicas bem definidas:

- Geração de uma versão eletrônica do diploma do aluno;

3 A UFPB e a PUC-RJ são instituições parceiras no desenvolvimento do projeto e, como potenciais usuários do serviço proposto, foram fundamentais no levantamento de requisitos e nos estudos preliminares de integração do protótipo com os seus respectivos sistemas de gestão acadêmica.

- Assinatura digital da versão eletrônica pelo(s) mesmo(s) responsável(eis) formal(is) na instituição que assinaram a versão impressa;
- Submissão da versão assinada para registro e preservação digital no serviço proposto;
- Recepção e arquivamento do recibo de registro na blockchain;
- Entrega ao aluno da versão eletrônica assinada do diploma e também do recibo do registro eletrônico.

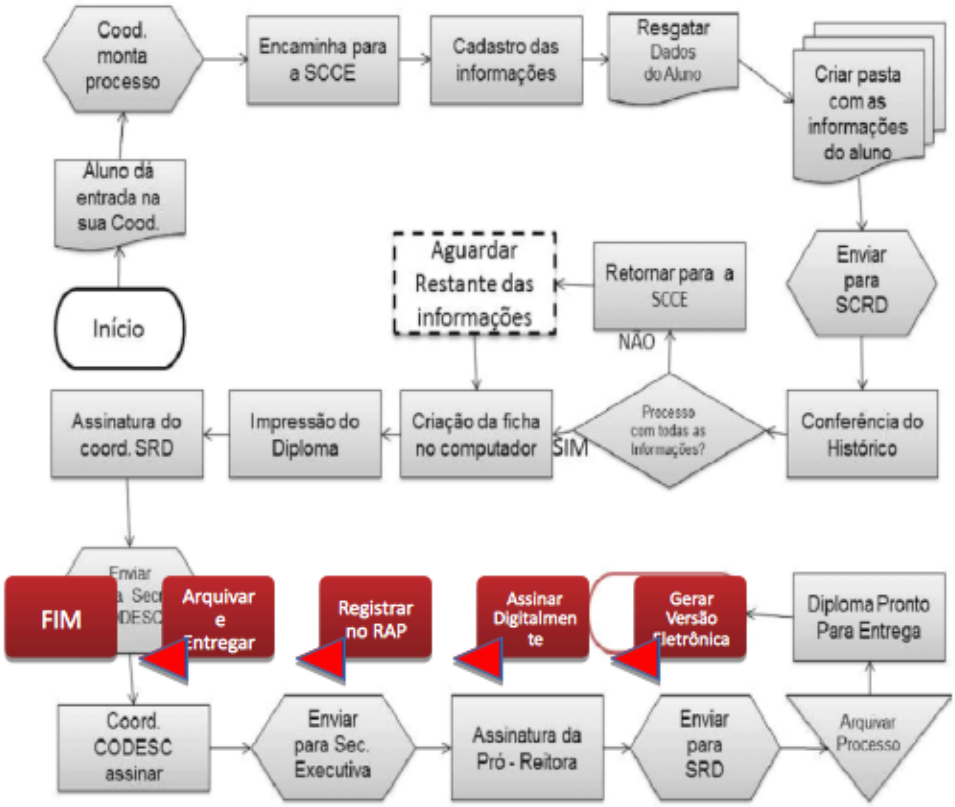

Figura 3 – **Possível Fluxo Operacional de Transição para Emissão de Diplomas**

Estas cinco etapas podem ser implementadas de diferentes formas em cada instituição. Dependendo da maturidade tecnológica e da disponibilidade de recursos, esses passos podem ser integrados ao sistema de controle acadêmico da instituição ou podem ser tratados em uma aplicação específica, por exemplo.

Para permitir a integração, o serviço oferece uma interface programável (API) para que instituições de ensino possam registrar diplomas acadêmicos na *blockchain* e uma interface interativa (Portal) para que os usuários possam verificar a autenticidade de um documento através do seu número de registro. Os documentos registrados no serviço são automaticamente inseridos no repositório de preservação digital de longo termo.

O modelo de implantação inicial previsto para desenvolvimento do protótipo está baseado em servidores dedicados e foi implantado na **Universidade Federal do Paraíba** (UFPB). Estes servidores formam a estrutura de desenvolvimento das interfaces e dos componentes de registro, autenticação e preservação. Para a fase do piloto, tal estrutura de desenvolvimento continuará sendo utilizada como tal, mas a versão de produção será implantada em recursos virtualizados disponibilizados pela RNP, conforme especificado na Seção 6.3.

2.1. Arquitetura do Piloto

O piloto do serviço de registro, autenticação e preservação de documentos acadêmicos utiliza-se de módulos clientes e módulos servidores. Os módulos clientes são utilizados pelos usuários para acessar o serviço. Os módulos servidores fornecem os serviços

demandados pelos módulos clientes através de APIs públicas. O protótipo permite o uso de diferentes formas de construção e uso de módulos clientes para acessar os serviços oferecidos.

Dessa forma, os módulos clientes usados para as operações de registro e preservação de diplomas podem ser *gateways* para o serviço proposto que operam de forma embutida e/ou integrada aos sistemas de gestão acadêmica das instituições (como o SIGAA, por exemplo) ou podem ser aplicações autônomas, construídas especificamente para esse fim. Os módulos clientes de registro e preservação são, prioritariamente, destinados para uso pelas instituições de ensino credenciadas para a utilização do serviço.

Os módulos clientes exclusivos para autenticação, por sua vez, podem ser portais interativos ou aplicações *desktop* ou *mobile*, e são destinados a usuários finais e instituições que precisam fazer, por razões variadas, a verificação da autenticidade e a prova da existência do registro de um determinado documento digital.

Os módulos clientes de registro e preservação além dos módulos clientes de autenticação tanto podem acessar a API do protótipo diretamente quanto podem fazer uso de componentes que tornam transparente essa integração, chamados aqui de agentes. São previstos dois agentes distintos: i) um que encapsula as operações de registro e preservação, e ii) outro que encapsula as operações de autenticação.

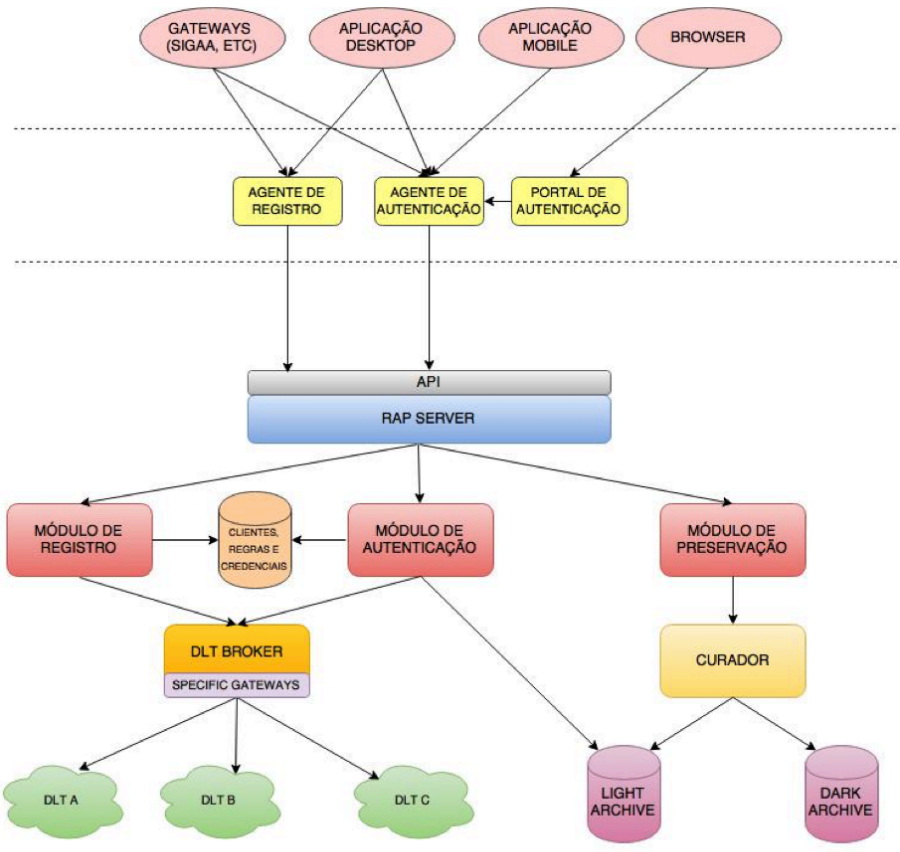

Figura 4 - **Arquitetura Geral do Protótipo**

O protótipo propriamente dito é composto por um conjunto de serviços dispostos em servidores. Conforme pode ser visto na **Figura 4**, estes serviços são: **Módulo de Registro**, **Módulo de Autenticação** e **Módulo de Preservação**. O acesso a tais serviços é intermediado por uma *API Backend*, chamada **RAP Server**. A API é consumida pelos programas clientes diretamente ou através do **Agente de Registro** e

do **Agente de Autenticação**. Há ainda um **Portal de Autenticação**, o qual permite o acesso interativo para as funcionalidades de autenticação através de um *browser*, e dois componentes internos: **DLT Broker** e **Curador**.

2.1.1 RAP Server (API Backend)

O RAP Server é o componente responsável por possibilitar e mediar a comunicação entre o meio externo, como o portal web e/ou sistemas que utilizam diretamente a API, e o meio interno que são os outros componentes da aplicação, como o módulo de preservação, módulo de autenticação e os demais.

Ele será utilizado por qualquer agente que necessite realizar operações de inserção, validação ou visualização de dados. Agindo como mediador este módulo irá tratar as requisições feitas verificando se os dados enviados condizem com o padrão adotado para a operação desejada, garantindo assim a correta execução destas operações.

Este módulo consiste de uma API que será utilizada como porta de entrada para novos arquivos na aplicação, por responder as requisições de verificação de autenticidade e visualização de dados e pelo envio dos arquivos para o módulo de preservação. Consiste de um banco de dados MongoDB e um servidor desenvolvido utilizando Node JS e Express.
A etapa de inserção se inicia com a recepção do arquivo que o utilizador da API deseja registrar. Em seguida o RAP Server utiliza o Módulo de Registro que por sua vez faz um pré-tratamento, valida o documento e o repassa para o DLT Broker que o insere na DLT requerida. Além disso o arquivo em si será salvo no módulo de preservação que é o responsável por manter os registros acessíveis e utilizáveis.

A etapa de verificação será feita através do fornecimento de um hash, ou do próprio arquivo a ser validado, e a partir dessa entrada será realizada uma busca utilizando o Módulo de Preservação que é o responsável pela manutenção dos arquivos e por fornecer operações de busca e recuperação. O módulo também é responsável por fornecer ao Portal Web dados de visualização referentes ao arquivo recuperado.

Tecnologias Adotadas:

- MongoDB
- Express
- Node JS

2.1.2 Portal de Autenticação

O portal consiste em um site web que será disponibilizado para facilitar a interação, através de uma interface gráfica, com o RAP Server (API Backend). Em outras palavras, o portal é uma forma de interação amigável e intuitiva com o sistema.

Este módulo permitirá a inserção, verificação de autenticidade ou visualização de um arquivo. No caso da inserção é feito o upload de um arquivo para o RAP Server que se responsabiliza pelo processo de inserção utilizando os módulos de registro e autenticação e delegando as ações para eles. Ao finalizar com sucesso a inserção o usuário receberá um hash, que deverá ser armazenado, para futuramente poder efetuar a validação ou visualização do documento inserido.

As funcionalidades de validação e visualização serão realizadas através do fornecimento do hash do arquivo, previamente inserido no sistema, e será informado ao usuário se o hash é válido ou não, ou seja, se o conteúdo do arquivo não foi modificado e está íntegro, e em caso positivo, será exibido na tela as informações do arquivo correspondente ao hash fornecido. Adicionalmente, será possível realizar a etapa de validação realizando o upload de um arquivo para o RAP Server, que por sua vez irá gerar o hash referente ao arquivo e fazer a consulta no módulo de verificação.

Tecnologias Adotadas:

- Angular 2

2.1.3 Módulo de Registro

O **Módulo de Registro** (MR) é o componente do protótipo responsável por providenciar que uma prova de existência do documento digital de entrada seja efetivamente registrada no(s) *ledger(s)* adequado(s).

O MR é ativado pelo *RAP Server* dentro do contexto de uma operação de registro de um novo documento digital e, após um pré-tratamento e validação da legitimidade do documento de entrada, faz a seleção do(s) *ledger(s)* adequado(s), obedecendo alguma heurística indicada pela instituição cliente, e, em seguida, faz o repasse do pedido de registro para o *DLT Broker,* o qual fará o depósito efetivo no(s) *ledger*(s) indicado(s).

No pré-tratamento do documento digital, além de outras ações, é feita a conferência da(s) assinatura(s) digital(is) aplicada(s) no documento a ser registrado. Além da corretude da(s) assinatura(s) digital(is) também será aferido se os certificado(s) utilizado(s) estão em conformidade, em quantidade e identidade, com o protocolo e certificado(s) fornecidos pela instituição cliente para registro do tipo de documento em pauta. Esse passo permite um controle *fim-a-fim* da legitimidade e integridade dos documentos digitais manuseados pelo serviço e será usado em vários pontos do protótipo.

Para a seleção de qual (ou quais, se o cliente optar por mais de um) *ledger* distribuído deve ser utilizado pelo registro, são usados parâmetros indicados na própria solicitação ou, na ausência destes, regras e heurísticas pré-definidas pelo cliente. Embora o escopo do protótipo contemplou apenas o registro nas cadeias *Bitcoin* e *Ethereum*, esta generalização considera um ciclo de vida de longa duração para o serviço, no qual novos *ledgers* concorrentes poderão emergir, oferecendo preços e condições diferenciadas. Neste sentido, é fundamental que o serviço ofereça flexibilidade de escolha para os clientes e suporte para o registro em *ledgers* diferentes, inclusive registrar um mesmo documento em mais de um deles.

Após as fases de validação do documento e seleção do(s) *ledger(s)*, o MR submete o pedido de registro devidamente instruído para o *DLT Broker.* Caso o registro seja bem sucedido, o *DLT Broker* devolve o(s) respectivo(s) recibo(s) para o MR, o qual por sua vez, os retorna para o *RAP Server*.

Qualquer erro ocorrido durante o processo, interrompe a operação e provoca a sinalização da condição para o *RAP Server*.

Tecnologias Adotadas:

- PKI.js para validação de assinatura digitais;
- Padrão *Chainpoint, versão 2.0,* para tratamento de lotes de documentos em único registro;
- MongoDB para armazenamento das credenciais, protocolos e regras para assinatura e seleção de *ledgers* de cada cliente.
- NodeJs
- Express

2.1.4 Módulo de Autenticação

O **Módulo de Autenticação** (MA) é responsável por verificar a autenticidade de diplomas digitais em função da consulta ao registo do referido documento em um dos ledgers distribuídos suportados pelo sistema, bem como por meio da recuperação do diploma no repositório de preservação.

Por meio do módulo de autenticação um usuário pode fazer uma consulta a um diploma digital. Essa consulta deverá suportar diferentes formas de recuperação da informação. Deverá ser possível acessar as informações sobre registro e o documento em si por meio do ID da transação registrada em um ledger. Deverá ser possível

também acessar as informações de registro e metadados em função do upload de uma cópia do diploma digital. Além disso, deverá ser possível recuperar as informações de diploma e registro por meio dos dados pessoais de um determinado ex-aluno que tenha perdido sua cópia do diploma digital ou do ID da transação de registro.

O processo de autenticação do MA é invocado a partir do módulo RAP-Server. O MA deverá oferecer um endpoint de acesso para consulta com opções diversificadas de busca ao diploma e/ou registro. Quando uma requisição de consulta chegar ao MA, são verificados os dados fornecidos e então o procedimento de recuperação das informações é executado. Dependendo do filtro de recuperação utilizado, a consulta será executada em uma ordem diferente.

Caso a consulta esteja sendo feita por meio da ID da transação de um *ledger*, inicialmente o MA irá se comunicar com o *DLT Broker* a fim de recuperar os dados de registro na respectiva blockchain. Uma vez retornado o registro, a busca pelo diploma digital será feito na base de repositório de preservação em função da *hash* que representa unicamente o diploma e que foi extraída do campo de dados do registro.

Caso a consulta esteja sendo feita com alguma informação diferente do ID da transação registrada em um ledger, a recuperação dos dados será iniciada por meio da comunicação entre o MA e o repositório de preservação. Nesse caso, algumas das chaves de busca que poderão ser utilizadas será o próprio diploma digital, um ID específico relacionado ao documento, algum dado pessoal do detentor do diploma como CPF ou algum mecanismo que gere a relação diplomado/instituição (a exemplo do mecanismo seu).

Tecnologias Adotadas:

- Node.js para implementação da lógica de negócios;
- Express para disponibilização da api de consulta e gerenciamento das requisições.

2.1.5 Módulo de Preservação

O **Módulo de Preservação** (MP) é o componente do serviço piloto que encaminha cada documento digital registrado no serviço para que este seja preservado e esteja continuamente acessível e utilizável por longo prazo, independentemente da continuidade do sistema (e da Instituição) que fez o seu registro.

A preservação consiste em adicionar documentos, operação conhecida como *ingest* e realizada por meio da criação submissão de um pacote SIP (Submission Information Package), e adicionalmente permite a pesquisa e recuperação destes documentos enquanto realiza um log de dados de cada operação realizada, seguindo as orientações internacionais da ISO 14721:2003, definida pela Open Archival Information System (OAIS).

O módulo serve como uma abstração para acesso ao sistema de curadoria digital que será utilizado, e é ativado toda vez que é necessária alguma operação de armazenamento ou recuperação de dados preservados pelo *RAP Server*.

As operações manipulam pacotes SIP, que contém, além do documento a ser preservado, metadados com informações extras como o EAD (Encoded Archival Description) que descreve o conteúdo do arquivo, junto com informações do autor, data de publicação, entre outras informações a respeito do conteúdo preservado. Outros metadados incluem a hash gerada do Blockchain e o PREMIS (Preservation Metadata Maintenance Activity), que armazena dados sobre o formato utilizado para possíveis transições de formato pelo módulo de curadoria.

Tecnologias Adotadas:

- Componente de criação de SIP do Archivematica;
- XML;
- PDF/A;

- EAD;
- PREMIS.
- NodeJS
- Express

2.1.6 Curador Digital

O componente de curadoria digital recebe o SIP do Módulo de Preservação através de uma interface HTTP REST e é responsável por converter este pacote em um AIP (Archival Information Package). Em seguida, o AIP é depositado em dois diferentes repositórios: um *light archive* e um *dark archive*. O *light archive* permite a recuperação dos objetos digitais, enquanto o *dark archive* serve como uma cópia segura e isolada para recuperação em casos de desastre. É possível ainda recuperar um documento e metadados relacionados. Para tanto o módulo de curadoria cria um pacote especial chamado DIP (*Description Information Package*) que poderá ser utilizado pelo Módulo de Preservação para fazer busca e obter acesso aos documentos e respectivos metadados preservados.

Adicionalmente, o Curador realiza de forma proativa uma averiguação dos arquivos preservados quanto aos seus formatos, atualizando os arquivos para formatos modernos caso seu formato atual se torne obsoleto. Ao detectar a obsolescência do formato de algum dos arquivos armazenados nos repositórios, este módulo realiza a conversão apropriada para um novo formato, utilizando os metadados de preservação PREMIS localizado no SIP.

O curador também serve como abstração de acesso aos repositórios de armazenamento dos objetos digitais. De forma análoga, enquanto o curador se responsabiliza por preservar o acesso ao arquivo quanto ao seu formato e codificação, os repositórios (*dark* e *light*) verificam constantemente a integridade dos arquivos quanto ao seu armazenamento físico nas mídias, armazenando réplicas dos arquivos em diferentes servidores e comparando as cópias entre si, realizando operações de *checksum* e verificação *bit* a *bit.*

Tecnologias Adotadas:
- **Archivematica** para curadoria digital;
- **OpenStack Swift** para gerenciamento dos repositórios (*light* e *dark archive*).

2.1.7 DLT Broker

O componente ***DLT Broker (DB)*** é responsável por abstrair a comunicação entre os módulos de Registro e Autenticação e os *ledgers* distribuídos. Basicamente, o módulo é responsável por executar operações de registro e consulta a registros em uma (ou em um conjunto de) *blockchain* a fim de retornar as informações necessárias à verificação de validade de um dado registro de diploma.

Em uma operação de registro, o módulo de Registro se comunica com o *DB* por meio de uma API. O módulo de Registro invoca uma chamada de registro de diploma em um *ledger*, passando as informações necessárias para que o processo de inclusão dos dados na *blockchain* específica possa ser concluído. Essa chamada deve ser feita por meio da passagem de uma estrutura de dados que descreve dentre outras características qual *ledger* será utilizado para a persistência dos dados, as informações de registro do documento e as configurações específicas de um dado *legder* necessárias para proceder com a operação. Após o registro ser feito, o DB retorna para o módulo de Registro o ID da transação que representa o registro na cadeia escolhida.

Na operação de consulta a registro, o DB se comunica com o módulo de Autenticação. A operação de consulta tem como objetivo validar um registro de diploma dentro de uma das cadeias gerenciadas pelo módulo *DLT Broker*. A validação do registro em si é feita pelo módulo Autenticador. Nesse caso, o módulo de Autenticação faz uma chamada ao DB passando os dados necessários para busca na(s) *blockchain(s)* específica(s) do registro do diploma. Dentre os dados que devem ser informados para consulta, são mandatórios a lista de transações contendo cada transação que identifica

unicamente um registro por *blockchain* e a lista de *ledgers* onde as consultas serão realizadas. Como resultado da consulta, o módulo *DB* retorna as informações de registro na *blockchain* (ou conjunto de *blockchains*) para o módulo de Autenticação que procederá com as verificações adicionais.

O DB deverá implementar as funcionalidades necessárias para se comunicar diretamente com os *ledgers* que serão suportados pelo sistema. Um conjunto de chamadas padrão deve ser definido de forma a abstrair essa comunicação. Afim de integrar um novo *ledger* ao sistema, esse conjunto de chamadas padrão deve ser implementada. Para tanto, as APIs e ferramentas específicas são utilizadas. Para os módulos usuários do DB essas diferenças técnicas entre *ledgers* devem ser transparentes. Quando um novo pedido de registro ou consulta chega ao DB verifica-se inicialmente o ID da cadeia em que o pedido deverá ser processado, após isso o registro ou consulta é realizado por meio de chamadas as implementações específicas de cada *ledger*. Caso ocorra algum erro no processo, o módulo gerador do pedido é notificado por meio de sinalização específica.

Tecnologias Adotadas:

- BitcoinJS - API que permite acesso à *blockchain*. Já implementa a interface base para registro e consulta de transações usando Bitcoin;
- Go-ethereum/Pyethereum - implementações do protocolo do ledger distribuído Ethereum em linguagens Go e Python, respectivamente;
- *Hyperledger Blockchain Explorer* - API com um conjunto de métodos para gestão de registros em blockchains do tipo *Hyperledger*.

2.2. Instituições Participantes

UFPB - Universidade Federal da Paraíba
CI - Centro de Informática
LAVID - Laboratório de Aplicações de Vídeo Digital (Coordenação)

Coordenador: **Prof. Dr. Guido Lemos**
CV Lattes: http://lattes.cnpq.br/6614550860293610
guido@lavid.ufpb.br

Coordenador Adjunto: **Prof. Dr. Rostand Edson Oliveira Costa**
CV Lattes: http://lattes.cnpq.br/3145331081780004
rostand@lavid.ufpb.br

Criado em 2003, o Laboratório de Aplicações de Vídeo Digital (LAVID) está integrado ao Centro de Informática (CI) da Universidade Federal da Paraíba (UFPB). O laboratório surgiu da proposta de desenvolver projetos de pesquisa em *hardware* e *software* voltados às áreas de Vídeo Digital, Redes de Computadores, TV Digital e Interativa e *Middlewares*. As pesquisas desenvolvidas são realizadas em parceria com outras universidades, institutos de pesquisa e empresas da iniciativa privada. Por ser um laboratório ativo na área de desenvolvimento, tem recebido financiamento de instituições parceiras como a Rede Nacional de Ensino e Pesquisa (RNP), Financiadora de Estudos e Projetos (FINEP) e Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq). Além do trabalho científico, os pesquisadores do LAVID estão envolvidos em atividades acadêmicas. No âmbito da UFPB, atividades ligadas aos cursos de graduação do CI e ao Programa de Pós-graduação em Informática. O resultado dessa sinergia entre pesquisadores e acadêmicos pode ser observado na forte participação do grupo em eventos, nacionais e internacionais, nas publicações e patentes que divulgam a produção técnico-científica do LAVID. Atualmente o LAVID é uma referência nacional e internacional em desenvolvimento de tecnologia para TV e Vídeo Digital e Accessibilidade.

Instituto de Tecnologia e Sociedade do Rio (ITS Rio)

Contato: **Prof. Dr. Fabro Boaz Steibel**
CV Lattes: http://lattes.cnpq.br/0433208213067580

O ITS Rio é um instituto de pesquisa independente e sem fins lucrativos. Formado por professores e pesquisadores de diversas instituições como UERJ, PUC-Rio, FGV, IBMEC, ESPM, MIT Media Lab, dentre outras, o ITS conta com uma rede de parceiros nacionais e internacionais e tem, dentre os seus focos de atividade, os debates sobre privacidade e dados pessoais, direitos humanos, governança da internet, novas mídias, comércio eletrônico, inclusão social, educação digital, cultura e tecnologia, propriedade intelectual, dentre outros temas. O ITS é um *hub* pluri-institucional, convergindo para suas atividades especialistas que possam, a partir de suas distintas formações e vínculos acadêmicos, refletir sobre o desenvolvimento das tecnologias da informação e da comunicação e seus impactos na sociedade.

Pontifícia Universidade Católica do Rio de Janeiro – PUC-RJ
Laboratório Telemídia

Contato: **Prof. Dr. Sérgio Colcher**
CV Lattes: http://lattes.cnpq.br/1104157433492666

O **Telemídia** é um laboratório do Departamento de Informática da PUC-Rio e oferece suporte à pesquisa e desenvolvimento de projetos nas áreas de Redes de Computadores, Sistemas Distribuídos, Sistemas Multimídia/Hipermídia e Comunicação de Dados Multimídia. Em particular, Sistemas de TV Digital, terrestres e IPTV têm sido foco de pesquisa e inovação do laboratório nos últimos anos. As pesquisas do Laboratório geraram tecnologias e protótipos de produtos que são aplicados em diversas áreas, tais como suporte ao desenvolvimento de programas de TV interativa, suporte à construção de aplicações que requerem qualidade de serviço, QoS, entretenimento, ensino a distância, comércio eletrônico e Internet das Coisas.

UFERSA – Universidade Federal Rural do Semi-Árido

Contato: **Prof. Dr. Daniel Faustino**
CV Lattes: **http://lattes.cnpq.br/7175882793842898**

A **Universidade Federal Rural do Semi-Árido** (UFERSA) é uma instituição pública federal de ensino superior brasileira, cuja reitoria está localizada em Mossoró, no estado do Rio Grande do Norte, e com campi nos municípios de Angicos, Caraúbas e Pau dos Ferros. A UFERSA oferece atualmente dez cursos: Agronomia, Medicina Veterinária, Zootecnia e Engenharia, Habilitação Agrícola, Engenharia de Pesca e Engenharia Ambiental. Oferece também cinco cursos de pós-graduação: Clínica e Cirurgia de Pequenos Animais, Bovinocultura, Agronégocio, Irrigação e Drenagem, e Carcinicultura. A UFERSA é a única instituição de ensino superior do semi-árido nordestino especializada no desenvolvimento da ciência e tecnologia e voltada para o agronegócio e para o fortalecimento da agricultura familiar. Atualmente, estão em andamento cerca de 70 projetos de pesquisas nas áreas de animais silvestre, carcinicultura, caprinocultura, agricultura irrigada, agricultura familiar, meio ambiente rural e urbano, e bovinocultura.

Escola Superior de Redes (ESR)

Contato: **Renato Duarte Rocha**
CV Lattes: **http://lattes.cnpq.br/4108530708376033**

A **Escola Superior de Redes** (ESR) é a unidade de serviço da Rede Nacional de Ensino e Pesquisa (RNP), criada para promover a capacitação, o desenvolvimento profissional e a disseminação de conhecimento em Tecnologias da Informação e Comunicação (TIC), em prol da evolução e da

permanente ampliação da rede de alta velocidade do país. Com uma experiência de mais de dez anos no mercado, a ESR já treinou mais de 20 mil profissionais em todo o Brasil, em suas oito unidades localizadas em diferentes capitais brasileiras. Em sua programação, constam mais de 50 cursos especializados em sete áreas temáticas: Administração e Projeto de Redes, Governança de TI, Segurança, Mídias de Suporte à Colaboração Digital, Administração de Sistemas, Gestão de Identidade e Desenvolvimento de sistemas.

2.3. Objetivos e Evoluções

São listadas a seguir um conjunto de ações relacionadas com a evolução e consolidação da versão desenvolvida na etapa de construção do protótipo. Para uma melhor contextualização das melhorias propostas, será referenciada a arquitetura apresentada na seção 2.1 de forma a posicionar cada ação prevista no respectivo módulo do serviço que será afetado.

2.3.1 Módulo de Autenticação

Um dos pontos de evolução necessários dentro do Módulo de Autenticação é a gestão de múltiplas assinaturas. Atualmente os serviço é capaz de lidar como uma assinatura por documento digital. Em muitos casos o processo de assinatura de um documento digital passa pelo crivo de mais de uma autoridade responsável. No caso de diplomas acadêmicos, a quantidade de pessoas que devem assinar um documento acadêmico por exemplo, varia de instituição para instituição. Desta forma, a possibilidade de inserção e validação de múltiplas assinaturas é um ponto de evolução do protótipo.

Um ponto importante de investigação está relacionado a prova de autoridade do ator que assina um documento digital. Basicamente é necessário responder as seguintes perguntas: um determinado ator tem alçada para assinar um determinado documento? Além disso, é possível verificar que o ator que assinou realmente tinha essa prerrogativa?
A fim de responder essa questão pretende-se investigar o uso de Certificado de Atributo (CA). Por meio de um certificado dessa natureza é possível qualificar um indivíduo. Em outras palavras, com o uso de CAs, é possível verificar se um determinado ator que está assinando um documento digital possui o título e consequentemente, a permissão, necessária para executar aquela tarefa. Por meio do uso desse mecanismo será possível verificar a alçada dos atores que assinaram um documento digital a ser preservado.

2.3.2 Módulo de Registro

O Módulo de Registro é responsável pela inclusão e verificação de existência de registros de documentos digitais em DLTs. Uma das ações objetivadas para esse módulo é a inclusão do suporte a uma terceira DLT. Pretende-se para tanto investigar DLTs que tenham sido concebidas com propósitos diferentes das já incorporadas ao serviço. Além disso, outro ponto que se pretende investigar de forma mais aprofundada é o uso de nós (cópias) locais das DLTs incorporadas como ponto de entrada para registro de transações. Atualmente, embora a arquitetura do Módulo de Registro permita a inclusão de APIs externas e nós como pontos de registro, apenas APIs externas foram utilizadas.
Um ponto chave que também pretende-se investigar é a possibilidade de realizar o registro de múltiplos documentos digitais por meio de uma única transação. Essa funcionalidade permite o barateamento no processo de inserção de transações em DLTs públicas, reduzindo os custos de operação do GT-RAP. Nesse sentido, uma das tecnologias candidatas é o *Chainpoint*[4], um protocolo que pode viabilizar a gestão de registro de múltiplos documentos em uma única transação.

4 https://chainpoint.org/

2.3.3 Módulo de Preservação

No contexto do Módulo de Preservação uma das funcionalidades que deve ser evoluída é a forma de gestão dos metadados relacionados ao documento preservado. Os aspectos da gestão dos metadados que devem evoluir são a sua representação, forma de verificação e recuperação. Pretende-se investigar o uso da tecnologia *OpenBages*[5] como mecanismo para gestão desses metadados. Ainda associado a gestão de metadados, espera-se investigar a melhor forma de preservar essas informações. Duas estratégias a serem investigadas são: armazená-las como um documento de metadados a parte ou embutí-las como metadados no próprio documento digital.

Outra funcionalidade a ser investigada no tocante ao Módulo de Preservação diz respeito à possibilidade de reconstrução da base de dados de acesso contínuo a partir da base de preservação de acesso restrito mantida pelo GT-RAP. Caso a base de acesso contínuo seja corrompida, deve ser possível reconstruí-la a partir dos metadados dos documentos preservados no serviço.

Por fim, outra funcionalidade que se deseja evoluir no contexto do Módulo de Preservação é a sua integração com o serviço de armazenamento da RNP, por meio da integração do serviço de curadoria do GT-RAP com o serviço de gestão de *Block Storage* construído com base na tecnologia *OpenStack Swift*. Ainda em relação ao armazenamento, será investigado o processo para construção de repositórios de preservação de longo termo que estejam de acordo com a norma ISO 16363 que descreve os procedimentos para construção e auditoria de repositórios digitais confiáveis, também conhecidos como TDRs (do inglês, *Trusted Digital Repositories*).

2.3.4 RAP Server

O RAP Server deve evoluir de forma a incorporar uma camada de segurança e autenticação para acesso por atores autorizados. Quanto a camada de segurança para comunicação com agentes externos e demais módulos, pretende-se evoluir a comunicação entre as partes utilizando mecanismos de assinatura de mensagens como o JWT[6] (do inglês, JSON Web Tokens). Quanto ao processo de autenticação e controle de acesso, será investigada a integração do GT-RAP com o sistema de gestão de identidades da RNP, o CAFe. Por fim, pretende-se incorporar mecanismos de balanceamento de carga que garantam acesso fluido ao RAP Server mesmo em cenários de alta demanda e avaliar a escalabilidade do serviço.

5 https://openbadges.org/
6 https://jwt.io/

3. Modelo de Negócios Proposto para o Piloto

De forma bem preliminar, é possível visualizar um modelo de negócios (**Figura 5**) para a oferta de um novo serviço para a RNP que tem bastante valor agregado para a sua carteira atual de clientes, formado, em sua maioria, por ministérios e instituições de ensino e pesquisa.

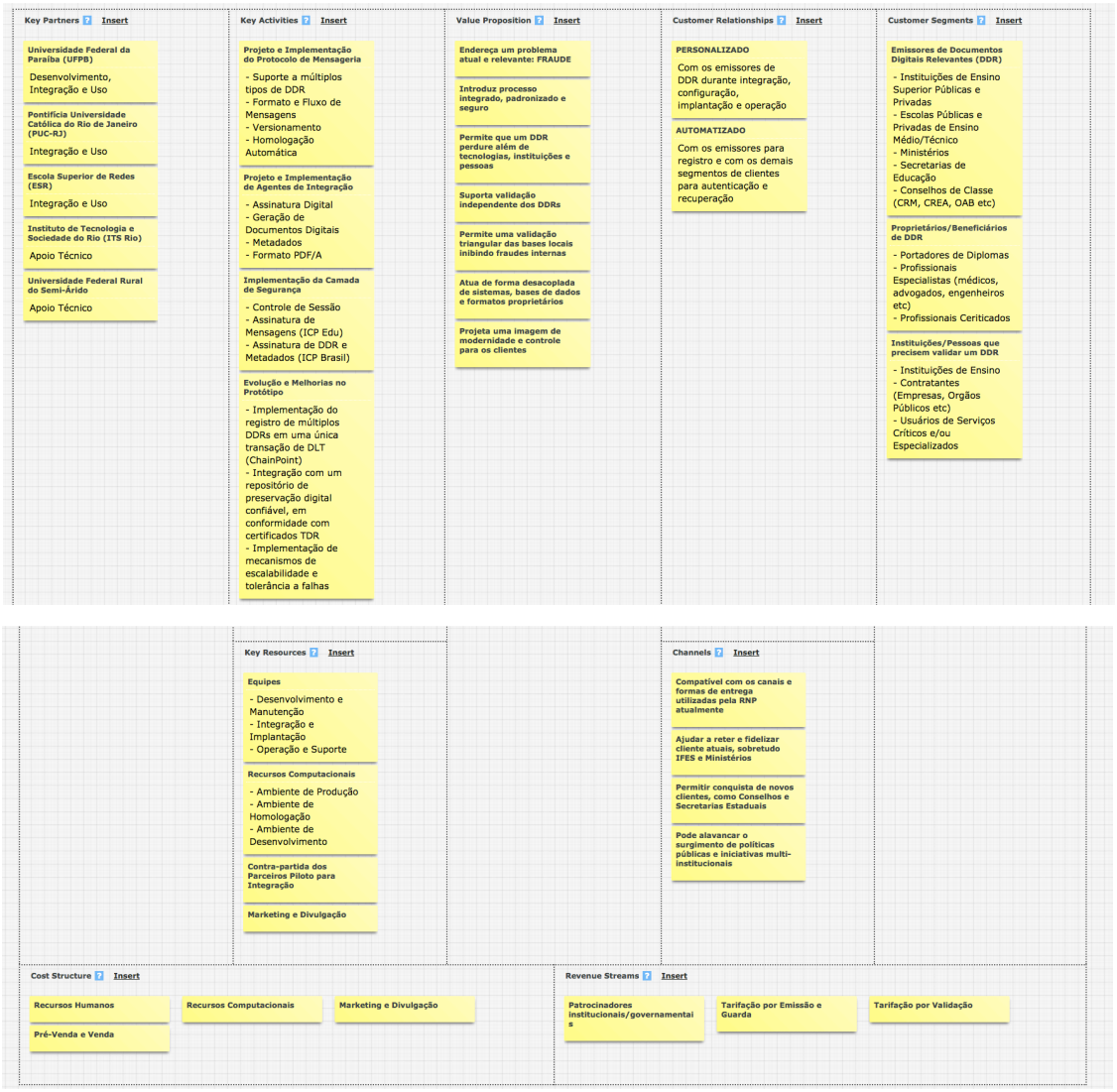

Figura 5 – ***Model Canvas* Preliminar**

De uma forma mais específica, o segmento de clientes (*Customer Segments*) vislumbrado é composto por três grupos: emissores de *Documentos Digitais Relevantes* (DDR); proprietários/beneficiários de DDRs e instituições/pessoas que precisem validar um DDR.

A proposta de valor (V*alue Proposition*) é baseada no apelo de que o serviço proposto endereça um problema atual e relevante: *combate a fraudes*, a partir da introdução de um processo integrado e padronizado que traz mais facilidade e segurança na emissão e validação dos DDRs. Por atuar de forma desacoplada de sistemas, bases de dados e formatos proprietários, o serviço permite a realização de uma validação triangular das bases locais dos clientes, inibindo fraudes internas e garantindo uma contínua sincronização na autenticação de DDRs legítimos. Além de permitir que um DDR perdure além de tecnologias, instituições e

pessoas e suportar a validação independente dos DDR, o serviço proposto projeta uma imagem de inovação, modernidade e controle para os clientes.

Do ponto de vista do relacionamento com clientes (*Customer Relationships*), os dois modelos clássicos estão presentes: tanto um relacionamento **personalizado**, com os emissores de DDR, durante as fases de integração, configuração, implantação e operação do serviço, quanto um relacionamento **automatizado**, com os emissores para registro e preservação e com os demais tipos de clientes para autenticação e recuperação.
Trata-se de um serviço compatível com os canais (*Channels*) e formas de entrega utilizadas pela RNP atualmente, mas pode ajudar a reter e fidelizar cliente atuais, sobretudo IFES e Ministérios, e também ajudar a conquistar novos clientes, como Conselhos e Secretarias Estaduais de Educação.

Outra motivação, talvez bem promissora, é que por endereçar um problema que ocorre em todo o país, a disponibilização de um serviço com tais características também pode alavancar o surgimento de políticas públicas e iniciativas multi-institucionais, que não só aportem os recursos necessários mas favoreçam uma implantação em escala regional ou nacional.

4. Aproveitamento dos Resultados do Piloto

A principal contribuição científica deste projeto é a investigação de uma nova abordagem baseada no uso de DLTs e repositórios ativos distribuídos para a autenticação e preservação de longo prazo de documentos digitais legais.

Do ponto de vista tecnológico, um dos principais resultados deste trabalho é a criação de um ambiente para dar suporte, inicialmente, a um **Serviço para Autenticação e Preservação de Documentos Digitais Acadêmicos**, com potencial para adoção por diversas organizações educacionais, sejam públicas ou privadas.

Este estudo de caso específico de autenticação digital apresenta um excelente potencial de aplicação real não financeira de DLTs e pode ser o embrião para a oferta futura de um serviço permanente de grande utilidade para as IES nacionais, parcela significativa da comunidade de usuários da RNP.

O serviço proposto oferece também mecanismos que possibilitam sua integração futura com diferentes plataformas que fazem uso deste tipo de documento, como a **Plataforma Lattes** do CNPQ, utilizada para o cadastro de pesquisadores no país, o **Sistema e-MEC**, utilizado pelo INEP nos processos de avaliação do ensino superior no Brasil, a **Plataforma Sucupira**, utilizada pela CAPES no processos de avaliação da pós-graduação no Brasil e o **SIGAA**, sistema de controle acadêmico desenvolvido pela UFRN e amplamente utilizado por Instituições Federais de Ensino Superior.

Uma eventual integração do serviço proposto com as plataformas mencionadas pode melhorar o processo de cadastramento de informações profissionais nestes sistemas, uma vez que permitirá a validação automática da autenticidade dos diplomas e certificados fornecidos, adicionando eficiência e economia ao processo e ajudando a impedir que situações como as apresentadas anteriormente voltem a acontecer.

Porém, cabe ressaltar que a infraestrutura a ser desenvolvida para dar suporte ao serviço proposto poderá apoiar também a criação de vários outros serviços para preservação e autenticação de documentos digitais e não apenas de diplomas.

Do ponto de vista da preservação digital e por conta das características de encapsulamento da replicação e do controle de falhas que pretendemos inserir na camada de armazenamento, tal abordagem pode trazer uma série de resultados complementares:

- Avançar na direção de uma integração transparente da funcionalidade de repositórios ativos com as outras camadas do modelo OAIS [Lavoie 2000];
- Habilitar a oferta de níveis distintos de capacidade de preservação, de acordo com a relevância do objeto digital;
- Possibilidade de operar em diferentes contextos de disponibilidade e capacidade de recursos computacionais.

5. Macro Cronograma de Desenvolvimento do Piloto

Listar e descrever todas as macro-atividades que permitirão o alcance dos objetivos indicados na seção 2.3, dando foco especificamente ao **desenvolvimento tecnológico** necessário para a evolução do produto e melhorias em processos de gestão e uso dos resultados relacionados ao protótipo existente. Destacar em quais trimestres serão realizadas.

Este cronograma deve atentar e estar alinhado as entregas pré-definidas, veja seção 6, em especial em conformidade e com nível de desenvolvimento compatível ao momento do projeto:

- Demonstração no Workshop da RNP (WRNP) – maio/2018
- Workshop de Disseminação dos Resultados para Instituições Clientes da RNP – novembro/2018
- Apresentação Final dos Resultados para o Comitê de Avaliação e RNP – fevereiro/2019

As macro-atividades descritas abaixo são necessárias ao alcance dos objetivos e evoluções indicados na seção 2.3. Estas ações contemplam em seu núcleo as atividades chaves (*Key Activities*) descritas no *Model Canvas* da seção 3, bem como atividades suplementares relacionadas ao processo de gestão, ambiente de produção e implantação do piloto. As macro-atividades pensadas foram:

1. **Planejamento do Processo de Implantação do Piloto** – Definição da estratégia de implantação do piloto nas instituições parceiras;
2. **Seleção e Nivelamento da Equipe de Implantação do Piloto** - Seleção de novos integrantes e eventual substituição de integrantes antigos que venham a ser desligados do projeto. Nivelamento dos novos membros da equipe, bem como nivelamento dos membros de equipe nas instituições parceiras onde os pilotos serão implantados a fim de viabilizar sua integração nos processos emissão e gestão de documentos acadêmicos;

3. **Definição e Preparação do Ambiente de Produção** – Definição das estruturas necessária para incorporação do piloto em um ambiente de produção a ser utilizado pelas instituições parceiras no processo de implantação e utilização do serviço piloto;
4. **Processo de Implantação e Acompanhamento do Piloto** – Implantação do serviço piloto e integração no fluxo de emissão e gestão de documentos acadêmicos nas instituições piloto. Acompanhamento contínuo do uso, avaliação de impacto, coleta de informações para melhoria e refinamento dos processos, serviços e ferramentas;
5. **Projeto e Implementação do Protocolo de Mensageria** – Definição do formato de fluxo de mensagens entre agentes de integração e o RAP Server, bem como entre os serviços internos do GT-RAP. Definição dos métodos de versionamento para os modelos de mensagens definidas e homologação automática. Generalização do modelo para suporte à inclusão e gestão de múltiplos DDRs.
6. **Projeto e Implementação de Agentes de Integração** – Concepção e construção de agentes de integração no formato de APIs que possam dar suporte a funções suplementares necessárias para o registro e autenticação de DDRs. Dentre essas funções suplementares destacam-se o suporte a geração destes DDRs, gestão de metadados desses documentos, exportação dos DDRs para o formato PDF/A e gestão de assinaturas digitais dos DDRs.
7. **Implementação da Camada de Segurança** – Incorporação de uma camada de segurança ao GT-RAP por meio da inclusão de mecanismos de controle de sessão e assinatura das mensagens que serão comunicadas entre os diversos serviços. Para tanto, uma alternativa será o uso de certificados ICP-Edu no processo de assinatura dessas mensagens. A assinatura dos DDRs e metadados será realizada com a utilização de certificados ICP-Brasil.
8. **Evolução e Melhorias no Protótipo** – Essa macro-atividade contempla ações necessárias a definição e implementação da funcionalidade de registros múltiplos DDRs em uma única transação. Bem como, a integração ao GT-RAP de um repositório de preservação digital em conformidade com requisitos de sistemas TDR. Além disso, a implementação de mecanismos de escalabilidade e tolerância a falhas.
9. **Avaliação e Refinamento do Processo de Implantação** – Análise do processo de implantação, dificuldades encontradas, refinamento do processo. Validação do serviço piloto, realização de refinamentos necessários na arquitetura e na solução. Avaliação e melhorias dos agentes de integração que dão suporte a implantação e uso do serviço por parte das instituições parcerias.

Macro atividades	1°. Trim.	2°. Trim.	3°. Trim.	4°. Trim.
1. Planejamento do Processo de Implantação do Piloto	X			
2. Seleção e Nivelamento da Equipe de Implantação do Piloto	X			
3. Definição e Preparação do Ambiente de Produção	X	X		
4. Processo de Implantação e Acompanhamento do Piloto		X	X	X
5. Projeto e Implementação do Protocolo de Mensageria	X	X		
6. Projeto e Implementação de Agentes de Integração	X	X	X	
7. Implementação da Camada de Segurança	X	X	X	
8. Evolução e Melhorias no Protótipo	X	X	X	X
9. Avaliação e Refinamento do Processo de Implantação	X	X	X	X

6. Recursos para o Desenvolvimento do Piloto

6.1. Aquisição de Equipamentos para o Desenvolvimento do Piloto

- Informar a quantidade e a descrição dos equipamentos e softwares necessários para o trabalho de **desenvolvimento do piloto**. No caso de computadores, devem ser utilizadas preferencialmente as configurações apresentadas no Anexo 2. No caso da proposta ser aprovada, a RNP solicitará o detalhamento das especificações dos equipamentos a serem adquiridos, seu objetivo de uso e custo estimado, para análise e aprovação. Caso o custo real no momento da aquisição dos equipamentos seja diferente do custo estimado, a quantidade ou a especificação de equipamentos a serem adquiridos poderá ser revista.

- Considerar o valor máximo de R$ 25.000,00 para custeio de equipamentos e softwares.

- Esses recursos de equipamentos poderão ser reavaliados com a RNP, na busca de soluções alternativas de sua implementação.

Descrição	Justificativa	Valor Unitário	Quantidade	Valor Total
Notebook 14” conforme descrição no Anexo 1	Uso para demonstração do GT-RAP em mostras, reuniões, workshops e demais eventos de exibição. A configuração justifica-se dada a necessidade de executar todos os serviços na própria máquina usada na demonstração quando necessário	R$ 4.087,00	1	R$ 4.087,00
Desktop s/ Monitor • Processador Intel Core i7 – • Memória RAM de 8GB • Armazenamento **HDD** 2TB	Experimentos relacionados a construção e uso de repositórios TDR em conformidade com a norma ISO 16363	R$ 2.100,00	4	R$ 8.400,00
Desktop s/ Monitor • Processador Intel Core i5 – • Memória RAM de 8GB • Armazenamento **SSD** 480 GB	Experimentos relacionados a construção e uso de repositórios TDR em conformidade com a norma ISO 16363	R$ 2.300,00	4	R$ 9.200,00
Total				R$ 21.687,00

6.2. Recursos Oferecidos pela RNP para Execução do Piloto

Recurso	Especificação	Justificativa	Quantidade
Licença de Software para Desenvolvedor	Biblioteca para geração e assinatura de arquivos no formato PDF/A	Para uso nos componentes de retaguarda do serviço e também nos clientes, através do Agente de Registro	1 (Runtime Free)
Certificados Digitais	Certificados Digitais ICP Brasil	Para geração dos diplomas assinados pelas instituições participantes do piloto	6

6.3. Recursos Virtualizados para o Desenvolvimento do Piloto

Listar todos os recursos que podem ser providos através de infraestruturas existentes na RNP que são necessários ao desenvolvimento do piloto.

Máquina Virtual	Quantidade de MVs	Memória	Processador	Disco	Outros Recursos
VM para Serviço de Autenticação	1	4G	2 núcleos	20Gb	[]
VM para Serviço de Registro	1	4G	2 núcleos	20Gb	
VM para Serviço de Preservação	1	4G	2 núcleos	1Tb	
VM para Serviço de Filas e Log	1	4G	2 núcleos	20Gb	
VM para Serviço RAPServer	1	4G	4 núcleos	20Gb	

6.4. Pessoal

Descrever o nome completo e a função de cada membro da equipe e respectivos valores em R$ (bruto)

Nome Completo	Função	Valor Mensal*	Data de Início	Data de Término	Valor Total
Guido Lemos	Coordenador Geral	R$ 1.700,00	01/05/2018	30/04/2019	R$ 20.400,00
Rostand Costa	Coordenador Adjunto	R$ 1.700,00	01/05/2018	30/04/2019	R$ 20.400,00
Daniel Faustino	Assistente 2 – 1	R$ 2.220,00	01/05/2018	30/04/2019	R$ 26.640,00
Felipe Alves	Assistente 3 – 1	R$ 1.300,00	01/05/2018	30/04/2019	R$ 15.600,00
Ademir Queiroga	Estagiário – 1	R$ 680,00	01/05/2018	30/04/2019	R$ 8.160,00
Claudio Djohnnatha	Estagiário – 2	R$ 680,00	01/05/2018	30/04/2019	R$ 8.160,00
Mateus Pires	Estagiário – 3	R$ 680,00	01/05/2018	30/04/2019	R$ 8.160,00
Thiago Nunes	Estagiário – 4	R$ 680,00	01/05/2018	30/04/2019	R$ 8.160,00
A definir	Estagiário – 5	R$ 680,00	01/05/2018	30/04/2019	R$ 8.160,00
A definir	Estagiário – 6	R$ 680,00	01/05/2018	30/04/2019	R$ 8.160,00
	Total	**R$ 11.000,00**			**R$ 132.000,00**

* O limite total mensal não deve ser superior a R$ 11.000,00 (valor bruto antes dos impostos)

7. Cronograma e Entregas Pré-Definidas

Os relatórios de planejamento, relatórios técnicos, relatórios de acompanhamento e demais entregas listadas a seguir são pré-definidas e fazem parte integrante desta proposta e devem ser entregues pela equipe deste Grupo de Trabalho à Gerência de Grupos de Trabalho, conforme cronograma indicado nesta seção. Também deverão ser realizadas entregas referentes a documentação, participação em eventos presenciais (WRNP, Workshop de Disseminação do GT e Workshop de Apresentação de Resultados) entre outros que compõem o desenvolvimento do projeto.

Os modelos destes relatórios e demais entregas serão compartilhados com o coordenador do GT na ocasião da reunião de boas vindas em data a ser agendada com os projetos selecionados para fase 2.

7.1. Relatórios

Os relatórios são entregas do projeto (Relatórios de Planejamento – RP e Relatórios Técnicos), na articulação com os grupos de outras organizações envolvidos no mesmo tema. O acompanhamento dos resultados parciais é realizado a partir dos relatórios trimestrais de acompanhamento (Relatório de Acompanhamento – RA) e na apresentação e discussão do tema no Workshop RNP (WRNP) e na transferência de conhecimento feita à RNP.

As responsabilidades da coordenação do projeto por parte dos contratados englobam a gestão do projeto do GT, incluindo a utilização da Wiki da RNP para disponibilização de informações sobre ações, atividades e tarefas, assim como de indicadores de progresso e status.

Além disso, todo o código fonte deve ser mantido atualizado pela equipe de desenvolvimento diretamente no ambiente de desenvolvimento colaborativo a ser indicado e disponibilizado pela RNP.

Os relatórios são agrupados em três tipos:

7.1.1. Relatórios de Planejamento (RPs)

RP5: Especificação de equipe, equipamentos e recursos virtualizados

Descrição do nome, telefone e email de cada pessoa da equipe, do seu grau de formação (graduando, mestrando, doutorando, professor/pesquisador), dos papéis a serem desempenhados pela equipe do projeto (desenvolvedor, analista, coordenador, coordenador adjunto, etc.) e seus respectivos valores de remuneração bruta atribuída, lembrando que a soma de todos da equipe deve se limitar ao total do edital.

Apresentar a estimativa de valores e a especificação detalhada de cada equipamento e software necessários ao desenvolvimento do protótipo, de acordo com o informado na proposta do GT.

Além disso, o GT pode apresentar demanda com especificação detalhada de máquinas virtuais necessárias ao desenvolvimento e implantação do piloto, com as respectivas justificativas de dimensionamento.

O modelo para este relatório será entregue aos coordenadores na ocasião da web conferência de boas vindas da fase 2.

RP6: Planejamento do Workshop RNP (WRNP)

Descrição da demonstração a ser realizada, equipamentos necessários, lista de integrantes do GT que irão participar, texto e demais documentos para divulgação no evento.

RP7: **Planejamento da estrutura de pacotes de trabalho de desenvolvimento tecnológico e do cronograma de entregas destes pacotes**

Estrutura de pacotes de trabalho a serem realizadas ao longo do GT que descrevem os principais grupos de atividades que são necessários para desenvolvimento deste projeto. Um pacote de trabalho é um grupo de atividades que não deve durar mais do que 3 meses de

execução. Cada pacote de trabalho deve ter uma data de entrega associada e o cronograma de marcos é a distribuição das datas de entrega de cada pacote de trabalho ao longo dos 12 meses de projeto.

RP8: Relatório de planejamento do Workshop de Disseminação do GT

Descrição das atividades previstas para a reunião de encerramento do projeto piloto. Este workshop pode ser apenas com os usuários participantes do piloto ou reunindo outros usuários interessantes para disseminação do resultado do projeto. Ex.: apresentações sobre o projeto e das experiências dos usuários do piloto, tutorial ministrado durante o workshop, além de documentação, manuais e códigos-fonte a serem disponibilizados.

RP9: Relatório de planejamento para inclusão no portfólio da RNP

Definição de como será a inclusão do produto no portfólio da RNP, detalhando onde será disponibilizado o produto ou o código, onde é possível encontrar mais informações sobre o produto online (página do produto na RNP ou em site do próprio), como será disseminado (por exemplo: via um curso na grade da ESR ou via manuais de usuário e tutoriais abertos) e seu modelo de sustentabilidade.

7.2. Relatórios Técnicos (RTs)

Os relatórios técnicos devem refletir os resultados das atividades realizadas pelo GT para alcançar o seu objetivo de implantação de um piloto.

RT4: Mapeamento de componentes e licenças de software

Descrição detalhada de cada componente (novo ou de reuso) que compõe a arquitetura do piloto, bem como sua respectiva licença de software. O entregável desse relatório deverá ser uma página na wiki onde as licenças e componentes podem ser incrementados ao longo do projeto.

RT5: Plano de testes do piloto

Descrição detalhada dos testes a serem realizados para a avaliação do piloto, indicando os procedimentos, resultados esperados e cronograma.

RT6: Avaliação dos resultados do piloto

Descrição dos resultados obtidos nos testes descritos no RT4, contendo avaliação, relato dos problemas encontrados e das soluções implementadas.

RT7: Recomendações para a implantação

Descrição da proposta de implantação, identificando o público alvo; descrição e dimensionamento da infraestrutura necessária para a implantação dos resultados; arquitetura proposta; definição dos processos de monitoração e gerenciamento do serviço; estimativa e perfil dos recursos humanos para a gerência e operação dos resultados.

7.2.1. Relatórios de Acompanhamento (RA)

RA5 a RA9: Relatórios de acompanhamento

Relato do progresso das atividades que foram planejadas no período.

RWRNP: Relatório de participação no WRNP

Relato da experiência da participação no WRNP, como sugestões e considerações dos visitantes ao trabalho do GT.

7.3. Site de divulgação do Grupo de Trabalho

7.3.1. Atualização do site do GT

Deverá ser atualizado o site do GT com as informações relevantes do projeto na fase piloto, para disseminação do trabalho. O site do projeto deverá citar o apoio da RNP, com referência ao site da RNP. Deve-se disponibilizar o site do projeto também em inglês.

7.4. Participação no Workshop da RNP (WRNP)

7.4.1. Apresentação em Sessão Técnica e Demonstração do Protótipo

A discrição da RNP, deverá ser realizada uma apresentação e uma demonstração técnica da proposta do GT durante o Workshop da RNP (WRNP), que acontece em conjunto com o Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC).

7.5. Workshop de Disseminação do GT

7.5.1. Realização do Workshop de Disseminação do GT

O GT deve organizar um workshop para a disseminação dos resultados do GT para potenciais interessados em absorver os produtos/serviços desenvolvidos durante o piloto, focando nos aspectos técnicos explorados durante o piloto e nos diferentes casos de uso da solução desenvolvida.

7.6. Entrega dos Produtos Desenvolvidos Durante o Piloto

7.6.1. Piloto Desenvolvido

Fontes, executáveis, scripts, arquivos de configuração etc.

7.6.2. Documentação do Piloto

Documentação técnica, manuais de instalação, manuais do usuário etc.

7.7. Avaliação do Piloto

7.7.1. Apresentação dos Resultados do GT

Deverá ser realizada uma apresentação para um comitê de avaliação dos GTs, com ênfase no piloto desenvolvido e no produto/serviço a ser disponibilizado para os usuários da RNP. A partir dessa avaliação, serão selecionados os GTs que poderão ser recomendados para possível modelagem de serviço/produto para oferta da RNP.

Cronograma de Entregas Pré-Definidas

03/05/2018

- RP5: Especificação de equipe, equipamentos e recursos virtualizados
- RP6: Planejamento do Workshop RNP (demonstração, material e viagens)

07/05/2018 a 08/05/2018

- WRNP: Apresentação em sessão técnica e demonstração dos resultados da fase protótipo e proposta de piloto.

25/05/2018

- RP7: Planejamento da estrutura de pacotes de trabalho de desenvolvimento tecnológico e do cronograma de entregas destes pacotes
- RWRNP: Relatório de participação no WRNP

29/06/2018

- RT4: Relatório de mapeamento de componentes e licenças de software
- RT5: Plano de testes do piloto

27/07/2018

- Site do GT atualizado
- Iniciar a implantação do piloto[7]
- RA5: Relatório de acompanhamento trimestral

31/08/2018

- Entrega do **código-fonte** da versão implantada no piloto (códigos-fonte, executáveis, *scripts*, arquivos de configuração etc.), incluindo o sistema e as ferramentas de suporte à operação;
- Entrega de **documentação** (manuais de instalação e administração, manuais de usuário etc.).

28/09/2018

- RP7: Relatório de planejamento do Workshop de Disseminação do GT

26/10/2018

- RA6: Relatório de acompanhamento trimestral

Entre 01/11/2018 a 30/11/2018 (data a definir)

- Realização do Workshop de Disseminação do GT (data a definir)

25/01/2019

- RA7: Relatório de acompanhamento trimestral
- RT6: Avaliação dos Resultados do Piloto
- RT7: Recomendações para a implantação do serviço/produto

Entre 01/02/2019 a 28/02/2019 (data a definir)

- Apresentação Final dos Resultados para o comitê de avaliação

7 Início das atividades planejadas no RP6.

29/03/2019

- RP8: Relatório de planejamento para inclusão no portfólio da RNP
- Atualização do RT4: Relatório de mapeamento de componentes e licenças de software
- Entrega final do **código-fonte** e **documentação**

12/04/2019

- RA8: Relatório de acompanhamento trimestral

8. Referências

[Baguete 2013] Baguete. Certisign oferece diploma digital. http://www.baguete.com.br/noticias/22/02/2013/certisign-oferece-diploma-digital, 2013. [Online; accessed 21-March-2018].

[Costa 2015] R. Costa, G. Lemos, V. Becker, and A. Malaguti. Estratégias para criacão de uma rede nacional para preservação digital de acervos audivisual brasileiros. Reflexões sobre Preservação Audiovisual/10 anos da CineOP – Mostra de Cinema de Ouro Preto, 2015.

[Costa 2016] R. Costa, G. Lemos, V. Becker, and A. Malaguti. We need to talk about digital preservation of audiovisual collections: Strategies for building national networks. jAUTI 2016: V Iberoamerican Conference on Applications and Usability of Interactive TV / 18 Con-vencion Cientıfica de Ingineria Y Arquitectura, 2016.

[Crosby 2016] Michael Crosby, Pradan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman. Blockchain technology: Beyond bitcoin. Applied Innovation, 2:6–10, 2016.

[Gazeta 2013] Gazeta do Povo. MP investiga o uso de mais de 500 diplomas falsos em Maringá. http://www.gazetadopovo.com.br/vidaecidadania/conteudo.phtml?id=1363754tit=MP-investiga-o-uso-de-mais-de-500-diplomas-falsos-em-Maringa, 2013. [Online; accessed 21-March-2018].

[Estadao 2016] Estadao. Sem papel, USO atrasa impressão de diplomas por quatro meses.http://educacao.estadao.com.br/noticias/geral,sem-papel-usp-atrasa-diplomas-por-quatro-meses, 10000064951, 2016. [Online; accessed 21-March-2018].

[Ferreira 2012] M. Ferreira, R. Saraiva, and E. Rodrigues. Estado da arte em preservação digital. 2012.

[Folha 2011] FOLHA. INEP cancela avaliação de quatro cursos por suspeita de fraude. http://www1.folha.uol.com.br/saber/941107-inep-cancela-avaliacao-de-quatro-cursos-por-suspeita-de-fraude.shtml, 2011. [Online; accessed 21-March-2018].

[Globo 2013] GLOBO. Esquema de revalidação de diploma de medicina é desarticulado pela PF. http://g1.globo.com/mato-grosso/noticia/2013/10/pf-deflagra-operacao-contra-esquema-revalidacao-de-diplomas-de-medicina.html, 2013. [Online; accessed 21-March-2018].

[Globo 2017] GLOBO. Dono de universidade denuncia esquema de venda de diplomas falsos por R$ 550,00 em MT. http://g1.globo.com/mato-grosso/noticia/dono-de-universidade-denuncia-esquema-de-venda-de-diplomas-falsos-por-r-550-em-mt.ghtml, 2017. [On-line; accessed 21-March-2018].

[ITI 2013] ITI. USP adota diploma com certificação digital. http://www.iti.gov.br /noticias/indice-de-noticias/4230-usp-adota-diploma-com-certificacao-digital, 2013. [Online; accessed 21-March-2018].

[Kakavand 2017] H. Kakavand, N. Kost De Sevres, and B. Chilton. The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies. 2017.

[Lavoie 2000] Brian Lavoie. Meeting the challenges of digital preservation: The OAIS reference model. OCIC Newsletter, 243:26–30, 2000.

[Gazeta 2017] Gazeta Online. Sedu pode levar até 180 dias para investigar diplomas falsos - mais de 100 professores processados por usarem diplomas falsos no ES. http://www.gazetaonline.com.br/noticias/cidades/2017/05/sedu-pode-levar-ate-180-dias-para-investigar-diplomas-falsos.html, 2017. [Online; accessed March-2018].

[Ruusalepp 2012] Raivo Ruusalepp and Milena Dobreva. Digital preservation services: state of the art analysis. Technical Report, dc-net. 2012.

[Sayão 2012] Luis Fernando Sayão and Luana Farias Sales. Curadoria digital: um novo patamar para preservação de dados digitais de pesquisa. Informação & Sociedade, 22(3), 2012.

[Skinner 2010] K. Skinner and M. Schultz. A guide to distributed digital preservation. Lulu. Com, 2010.

[Skinner 2009] Katherine Skinner and Martin Halbert. The metaarchive cooperative: a collaborative approach to distributed digital preservation. Library Trends , 57(3):371–392, 2009.

[Wikipedia 2018] Wikipedia. Proof of existence. https://en.wikipedia.org/wiki/Proof of Existence, 2018. [Online; accessed 21-March-2018].

Anexo 1 – Tabela de Equipamentos - Configuração Padrão

Notebook 14" (Core i7 - 8GB - 500GB) - R$ 4.087,00
Especificação:

- Sistema Operacional: Ubuntu 12.04 SP1 com Suporte de longo prazo (LTS)
- Memória DDR3L de 8 GB (2x4 GB) e 1600 MHz, BCC
- Vídeo: Intel® HD 4400 Graphics integrado
- Disco rígido de 500 GB (5.400 RPM)
- Sem modem
- Rede Sem FIO: Intel® Centrino® Advanced -N + WiMAX 7260 802.11ac/a/b/g/n 2x2 + Bluetooth 4.0 LE Half Mini Card, Brasil
- Leitor de impressões digitais e apoio para as mãos do leitor de Smart Card (com ou sem contato)
- Bateria de íon de lítio de 4 células (45 Wh)
- Bateria Adicional de 4 Células (45Whr)
- Processador da 4ª geração Intel (R) Core (TM) i7-4600U (2,1 GHz, cache de 4 M), com Smart Card, BCC
- Tela WLED antirreflexo com alta definição (1920 x 1080), iluminação traseira e visualização ampla de 14"
- Adaptador Mini DisplayPort para VGA
- 3 anos de Suporte, Serviço no local e Proteção contra Danos Acidentais

Desktop s/ monitor (Core i7 - 8GB - 500GB) - R$ 3.600,00
Especificação:

- Sistema Operacional Windows® 7 Professional Original 64-Bit em Português
- Processador Intel® Core™ I7-4770S Processor (Quad Core HT, 3.10GHz Turbo, 8MB, w/ HD Graphics 4600)
- Memória 8GB (2X4GB) 1600MHz DDR3 Non-ECC
- Placa Gráfica Integrada Intel® Graphics
- HD 500GB 2.5 inch SATA (5.400 RPM) Opal Sed with Fips Hard Drive
- Unidade de DVD+/-RW SATA 8x com leitor de cartão
- Rede Sem Fio 802.11a/b/g/n PCIe Card
- Teclado com entrada USB
- Mouse óptico
- 3 anos de Suporte, Serviço no local e Proteção contra Danos Acidentais

Monitor LED 23.8" - R$ 800,00

Servidor s/ monitor (rack) – R$ 6.500,00
Especificação:

- Servidor rack 1U
- Processador Intel® Pentium® 1403 2.60GHz, 5M Cache, 2C, 80W, Max Mem 1066MHz
- Memória 4GB RDIMM, 1600 MT/s
- 2 slots PCIe
- Placa de vídeo Matrox® com 16MB de memória
- Placa de rede on-board Dual Port GbE
- DVD-ROM
- Fonte Hot-plug de 550W
- HD SATA de 500GB, 7.2k RPM
- Sem sistema operacional
- 5 anos de garantia com atendimento no próximo dia útil

Anexo 2 – Tabela de Pessoal

Referência (Função)	Horas/mês (Sugeridas)	Valor Mensal/R$ (bruto*)
Coordenador geral	20	2100,00
Coordenador adjunto	20	1500,00
Assistente 1	160	4900,00
Assistente 2	160	2450,00
Assistente 3	80	1300,00
Estagiário**	80	680,00

* Os valores mensais são referentes ao valor bruto sobre o qual podem incidir os recolhimentos de acordo com a legislação vigente (INSS e IRPF) dependendo da forma de contrato estabelecida.

** No caso de estagiários, os contratos são realizados através do CIEE.