

Relatório Técnico Final

Preservação digital e gestão arquivística
apoiada no aprimoramento da
implantação do modelo RDC-Arq

Julho de 2023

PRESIDÊNCIA DA REPÚBLICA

Luiz Inácio Lula da Silva
Presidente da República

Geraldo José Rodrigues Alckmin Filho
Vice-Presidente da República

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO

Luciana Santos
Ministra da Ciência, Tecnologia e Inovação

INSTITUTO BRASILEIRO DE INFORMAÇÃO EM CIÊNCIA E TECNOLOGIA

Tiago Emmanuel Nunes Braga
Diretoria

Reginaldo de Araújo Silva
Coordenação de Administração - COADM

Gustavo Saldanha
Coordenação de Ensino e Pesquisa em Informação para a Ciência e Tecnologia - COEPI

José Luis dos Santos Nascimento
Coordenação de Planejamento, Acompanhamento e Avaliação - COPAV

Marcel Garcia de Souza
Coordenação-Geral de Informação Tecnológica e Informação para a Sociedade - CGIT

Bianca Amaro de Melo
Coordenação-Geral de Informação Científica e Técnica - CGIC

Alexandre Faria de Oliveira (Substituto)
Coordenação-Geral de Tecnologias de Informação e Informática - CGTI

Milton Shintaku
Coordenação de Tecnologias para Informação - COTEC

Benício Mendes Teixeira Júnior (Substituto)
Coordenação de Governança em Tecnologias para Informação e Comunicação - COTIC

©2023 INSTITUTO BRASILEIRO DE INFORMAÇÃO EM CIÊNCIA E TECNOLOGIA

Este Relatório é licenciado sob uma licença [Creative Commons Attribution 4.0](https://creativecommons.org/licenses/by/4.0/), sendo permitida a reprodução parcial ou total desde que mencionada a fonte.

EQUIPE TÉCNICA

Diretor do Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict)
Tiago Emmanuel Nunes Braga

Coordenador-Geral Substituto de Tecnologias de Informação e Informática (CGTI)
Alexandre Faria de Oliveira

Coordenador do Projeto
Alexandre Faria de Oliveira

Autores

Alexandre Faria de Oliveira
Daniel Monteiro
Tatiana Canelhas Pignataro
Marcello Silva Coutinho
Marcos Sigismundo da Silva
Maxwell Borges Bezerra
Henrique Oliveira Costa
Lara Luiza da Silva Aquino
Raul Neres Carlos
Claudio Gonçalves Silva Gama

Marília Cristina Silva
Juliana Colem Rodrigues
Sérgio Augusto Coelho Diniz Nogueira
Júnior
Marilete da Silva Pereira
Alex Pereira de Holanda
Jady Pamella Barbacena da Silva
Adriano Pellizzaro da Motta
Gláide Elisa Silva Menezes

Normalização

Denise Oliveira Araújo
Marilete da Silva Pereira

Diagramação

Alisson Eugênio Costa

Este Relatório Técnico é um produto do projeto Este Relatório de Técnico é um produto do projeto Preservação digital e gestão arquivística apoiada no aprimoramento da implantação do modelo RDCArq.

Ref. TJDFT - Processo SEI no 01302.000067/2021-45 e 01302.000389/2020-11 Ref. FUNDEP 28209

As opiniões emitidas nesta publicação são de exclusiva e inteira responsabilidade dos autores, não exprimindo, necessariamente, o ponto de vista do Instituto Brasileiro de Informação em Ciência e Tecnologia ou do Ministério da Ciência, Tecnologia e Inovações.

É permitida a reprodução deste texto e dos dados nele contidos, desde que citada a fonte. Reproduções para fins comerciais são proibidas.

Sumário

1 INTRODUÇÃO.....	5
2 OBJETIVOS.....	7
2.1 Objetivo Geral.....	7
2.2 Objetivos Específicos.....	7
3 CONTEXTUALIZAÇÃO E RESULTADOS.....	8
3.1 Relatórios e interação das equipes.....	8
3.1.1 Reuniões técnicas.....	8
3.1.2 Reuniões de alinhamento.....	10
3.2 Meta 1: Estudos de infraestrutura para solução RDC-Arq.....	11
3.2.1 Estudos de infraestrutura para solução RDC Arq.....	12
3.2.2 Processo de implantação do sistema no Openshift do TJDF.....	15
3.2.2.1 Criação dos volumes (PVC).....	17
3.2.2.2 Criação e deployment dos serviços e aplicações.....	17
3.2.2.3 MySQL.....	18
3.2.2.3 Elasticsearch.....	18
3.2.2.4 Gearmand.....	19
3.2.2.5 Fits.....	19
3.2.2.6 Clamav.....	19
3.2.2.7 MCPServer.....	20
3.2.2.8 MCPClient.....	21
3.2.2.9 Dashboard.....	21
3.2.2.10 Storage service.....	22
3.2.2.11 Inicialização e preparação dos serviços.....	22
3.2.2.12 Criação dos bancos de dados.....	22
3.2.2.13 Criação das tabelas.....	23
3.2.2.14 Criação das rotas.....	24
3.2.2.15 Testes de Escalabilidade.....	26
3.2.2.16 Estudo para dois fluxos (pipelines) de preservação em openshift.....	30
3.3 Definições para alinhamento com as políticas de Segurança da Informação do Tribunal.....	38
3.4 Meta 2: Análise de padrão de design de código para solução RDC-Arq.....	40
3.4.1 Análise de padrão de design de código para solução RDCArq.....	41
3.4.2 Tipos de design patterns.....	41
3.5 Meta 3: Estudo para implantação de barramento RDC-Arq.....	49

3.5.1 Estudo para implantação de barramento RDC-Arq orientado a eventos.....	50
3.5.1.1 Estudo para integração com o serviço de mensageria Kafka.....	53
3.5.1.1.1 Integração com o Hipátia.....	53
3.5.2 Estudos para implantação de banco de dados no barramento Hipátia para gerenciamento dos dados de acesso aos sistemas.....	55
3.5.2.1 Definição das tabelas do Hipátia (MySQL versão 5.7 com SSL).....	55
3.5.3 Desenvolvimento do “Barrapres Gestão”	58
3.5.4 Estudos dos metadados RDC-Arq do PJE.....	61
3.5.5 Tipos de metadados.....	61
3.6 Meta 4: Estudos para extração de conteúdos AtoM >> Sistema de Gestão Documental.....	63
3.7 Meta 5: Prova de Modelos.....	63
3.7.1 Diagnóstico de compliance da solução RDC Arq PJE com as normas arquivísticas, inclusive modelo OAIS.....	63
3.8 META 6: Transferência do Conhecimento.....	69
3.8.1 Website.....	69
3.8.2 Fórum de discussão.....	72
3.8.3 Workshop de repasse tecnológico.....	73
3.8.4 Publicações.....	73
4 CONSIDERAÇÕES FINAIS.....	74
BIBLIOGRAFIA CONSULTADA.....	76
APÊNDICES.....	78
APÊNDICE A - Metadados de Gestão PJe (MoReq-Jus, e-Arq e Resolução n° 24 do conarq).....	78
APÊNDICE B - Metadados Descritivos Dublin Core.....	102
APÊNDICE C - Metadados Descritivos ISAD(G).....	106
APÊNDICE D - Outros Metadados ISAD(G).....	110
Apêndice E - Metadados PJe.....	115
Apêndice F - Avaliação das políticas de segurança da informação do Tribunal e o modelo Hipátia.....	136
Apêndice G - Resultados do Diagnóstico de Maturidade.....	147

1 INTRODUÇÃO

O Tribunal de Justiça do Distrito Federal e Territórios (TJDFT) estabeleceu diretrizes internas para orientar a gestão documental. Assim, o órgão avançou ao estabelecer diretrizes internas capazes de orientar a gestão e preservação de documentos no formato digital em consonância com as tendências nacionais e internacionais da área. A resolução 16, de 25 de agosto de 2016, permitiu a gestão documental dos processos em meio analógico.

O sucesso desta resolução demanda avanços no processo de modernização da gestão documental já regulamentado no âmbito da política de gestão documental. Nesse contexto, documentos em formato digital são incorporados ao processo e ampliam o alcance da gestão documental. O tema está no âmbito da política de gestão documental do Poder Judiciário, fruto de discussões ocorridas em meio ao Programa Nacional de Gestão Documental e Memória do Poder Judiciário (PRONAME). Ao reconhecer esses procedimentos técnicos preconizados pela Ciência da Arquivologia, o Conselho Nacional de Justiça (CNJ) editou a Recomendação 37/2011 veiculando os requisitos e instrumentos necessários à gestão documental, independente do suporte em que se encontre a informação.

A parceria do Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict) e TJDFT promove soluções viáveis de implantação de um Repositório Arquivístico Digital Confiável (RDC-Arq) e identifica a necessidade de aprimoramento do modelo de RDC-Arq com a incorporação de outros sistemas. Esse projeto ainda está em curso e incorpora diversos avanços. Todavia, dada a natureza da pesquisa e o ineditismo desse projeto, novas ações foram identificadas durante a evolução da pesquisa. Essas necessidades estão expressas neste projeto de pesquisa que aborda a Preservação digital e gestão arquivística apoiada no aprimoramento da implantação do modelo RDC-Arq.

Este relatório tem o objetivo de apresentar os principais resultados e entregas de 2021 do projeto de pesquisa

para a implantação do RDC-Arq no contexto de preservação de processos judiciais eletrônicos.

Este relatório está estruturado em 5 partes. Um breve histórico da necessidade e consequente definição da elaboração do projeto está descrito na **Introdução**. Os objetivos geral e específicos são abordados em **Objetivos**. **Contextualização e Resultados** mostra as tratativas entre equipes técnicas em **Relatórios e interação das equipes**. Nesta mesma seção, os estudos que fundamentam a escolha de ferramentas e de procedimentos metodológicos estão em Metas 1, 2, 3, 4, 5 e 6. Por fim, a avaliação da condução do projeto destacando as entregas e apontando os próximos passos estão em **Considerações Finais**.

2 OBJETIVOS

2.1 Objetivo Geral

Aprimorar a implementação do modelo RDC-Arq na estrutura do TJDFT.

2.2 Objetivos Específicos

- Melhorar o desempenho e infraestrutura do barramento RDC-Arq;
- Disponibilizar novas formas de acesso ao RDC-Arq;
- Possibilitar integração com o Processo Judicial Eletrônico - PJe;
- Desenvolver módulo de interface para o AtoM;
- Provar modelos propostos; e
- Disseminar conhecimento.

3 CONTEXTUALIZAÇÃO E RESULTADOS

3.1 Relatórios e interação das equipes

3.1.1 Reuniões técnicas

A importância das reuniões técnicas para resolver problemas arquivísticos e de TI dentro dos projetos de preservação digital para o Tribunal de Justiça do Distrito Federal e dos Territórios (TJDFT), em colaboração com as equipes do Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT), foi evidenciada. Essas reuniões desempenharam um papel crucial no desenvolvimento dos projetos, permitindo a discussão e a resolução de desafios técnicos complexos de forma eficaz.

No contexto dos projetos de preservação digital, as reuniões técnicas proporcionaram um ambiente propício para alinhar conhecimentos e perspectivas. As equipes arquivísticas, com sua experiência em princípios arquivísticos, requisitos legais e diretrizes específicas, compartilharam suas percepções com as equipes de TI, que contribuíram com seus conhecimentos especializados em sistemas, infraestrutura e segurança da informação. A colaboração dos profissionais do IBICT enriqueceu ainda mais essa troca de informações, proporcionando uma visão especializada em preservação digital. Essa sinergia permitiu encontrar soluções integradas que atenderam aos requisitos tanto arquivísticos quanto técnicos.

As reuniões técnicas também desempenharam um papel crucial na identificação e resolução ágil de problemas. Durante o desenvolvimento do projeto de preservação digital, diversos desafios técnicos surgiram e precisaram ser enfrentados. A colaboração permitiu identificar gargalos e obstáculos, bem como encontrar soluções eficientes e eficazes, evitando atrasos significativos e interrupções no andamento dos projetos.

Outro aspecto importante das reuniões técnicas foi a oportunidade de compartilhar melhores práticas e experiências. Cada equipe trouxe seu conjunto único de habilidades, conhecimentos e experiências adquiridas ao longo do tempo.

Durante as reuniões técnicas, essas experiências foram compartilhadas, permitindo que lições aprendidas e casos de sucesso fossem discutidos e aplicados em projetos semelhantes. Essa troca de informações contribuiu para uma abordagem mais eficiente e de maior qualidade nos projetos de preservação digital.

Além disso, as reuniões técnicas proporcionaram atualização e aprendizado contínuo. Na área de preservação digital, novas tecnologias, padrões e melhores práticas surgem constantemente. Ao reunir as equipes regularmente, foi possível manter todos atualizados sobre as últimas tendências e avanços nesse campo. Isso permitiu que os projetos de preservação digital do TJDFT fossem conduzidos com base em conhecimentos atualizados e em conformidade com os padrões e diretrizes mais recentes.

O compartilhamento de informações, a discussão aberta de desafios e a busca por soluções conjuntas promoveram uma cultura de colaboração e cooperação entre as equipes envolvidas. Esse ambiente de trabalho em equipe foi essencial para enfrentar com sucesso os desafios complexos da preservação digital e alcançar os objetivos estabelecidos pelo TJDFT.

Principais tópicos abordados nas reuniões:

- Definições em relação à infraestrutura tecnológica do RDC-Arq;
- Definição dos processos a serem preservados;
- Revisão de metadados;
- Arquitetura de integração dos sistemas do RDC-Arq;
- Integração PJE;
- Estudos guarda longa e guarda permanente;
- Alinhamento para testes de ambiente;
- Estudos para segurança do ambiente tecnológico de acesso às informações preservadas;
- Estudos de formatos de preservação;
- Estudos para conformidade do ambiente de preservação com normas internacionais.

3.1.2 Reuniões de alinhamento

Em fevereiro de 2021, foi realizado um workshop colaborativo previsto na fase de planejamento inicial do Processo Ágil de Desenvolvimento de Software (PADS) do TJDF, por meio do *Lean Inception* de Paulo Caroli, adaptada no TJDF e incorporada ao PADS, para alinhar as partes interessadas em relação a melhor solução para o problema de preservação digital no Tribunal. Ao final do workshop foi possível estruturar a solução em Produtos Mínimos Viáveis (MVPs)¹. Posteriormente, esses MVPs foram decompostos em uma lista de atividades (backlog). Utilizando conceitos da metodologia Ágil, a dinâmica de interação e atualização das informações do projeto entre as equipes se deu em reuniões de ponto de controle, que possibilitaram o acompanhamento do projeto por meio de artefato conhecido como *roadmap*, que também faz parte do PADS e do GPPTI do TJDF. Essa ferramenta permite monitorar os MVPs ou etapas do projeto e é revisada periodicamente para adequação às necessidades do projeto. A execução, cadência, priorização, organização e transparência das atividades são gerenciadas pelo sistema/conceito chamado Kanban².

As reuniões de ponto de controle de acompanhamento das atividades do projeto de pesquisa ocorreram **a cada 15 dias** com a participação das equipes técnicas e de negócio do TJDF e IBICT e facilitação do Escritório de Projetos do TJDF. As reuniões quinzenais de alinhamento desempenharam um papel fundamental na gestão de projetos de preservação digital realizados pelo TJDF. Essas reuniões permitiram que a equipe envolvida revisasse o progresso alcançado, discutisse desafios e definisse as próximas etapas do projeto. Com a natureza complexa e em constante evolução desses projetos, as reuniões de alinhamento garantiram a constância das revisões e mantiveram o projeto alinhado aos objetivos estabelecidos. Além disso, o uso do Kanban como uma ferramenta visual de gestão

¹ Disponível em: <https://caroli.org/mvp-produto-minimo-viavel/>.

² Importante salientar que a proposta de uso do Kanban vem do Processo de Gestão Ágil de Portfólio e de Projetos de TI do TJDF - GPPTI. Disponível em: <https://www.google.com/url?q=https://www.tjdft.jus.br/transparencia/governanca-de-tic/pads-gppti/gppti.pdf&sa=D&source=docs&ust=1691694288899532&usq=AOvVaw39iSvvopUXFP839vDvaKJS>.

permitiu acompanhar o fluxo de trabalho e identificar possíveis gargalos ou atrasos, contribuindo para o sucesso da gestão de projetos de preservação digital no TJDFT.

Durante as reuniões quinzenais, a equipe discutia o progresso das atividades realizadas, compartilhava informações sobre possíveis obstáculos encontrados e colaborava na definição das próximas etapas do projeto. Essas reuniões eram essenciais para manter a constância das revisões e garantir que o projeto estivesse alinhado com os objetivos estabelecidos. Através dessas reuniões, a equipe conseguiu identificar e resolver problemas rapidamente, permitindo ajustes no planejamento, se necessário.

Além das reuniões quinzenais de alinhamento, outra abordagem que contribuiu para o sucesso da gestão de projetos foi o uso do Kanban. Com o uso da ferramenta, foi possível criar um quadro que representava as etapas do projeto, desde a concepção até a entrega final. Cada etapa era representada por um cartão que continha informações sobre as atividades a serem realizadas e as pessoas responsáveis por elas. Esse quadro era atualizado durante as reuniões quinzenais de alinhamento, permitindo que a equipe acompanhasse o progresso do projeto e identificasse possíveis obstáculos.

As reuniões quinzenais de alinhamento e o uso do Kanban foram ferramentas essenciais para garantir a eficácia da gestão de projetos de preservação digital no TJDFT. Essas práticas permitiram que a equipe mantivesse a atualização das revisões, reavaliasse o progresso do projeto e tomasse decisões para garantir o sucesso do empreendimento.

3.2 Meta 1: Estudos de infraestrutura para solução RDC-Arq

A meta 1 é dedicada ao levantamento bibliográfico de propostas de modelos de infraestruturas associados a projetos similares, bem como o estudo de infraestruturas implementadas em instituições públicas nacionais e internacionais. Além disso, é destinada à análise de requisitos de desempenho e confiabilidade necessários ao ambiente para guarda de informações relacionadas a processos

judiciais e ao estudo para estabelecer a infraestrutura de preservação, regras e políticas de gerenciamento do acervo para a preservação em fase de guarda intermediária, como continuidade do tratamento arquivístico dos processos judiciais eletrônicos. Todo esse processo investigativo resulta na proposição do modelo de arquitetura computacional ideal para projetos de barramento RDC-Arq que considera aspectos de segregação de ambientes.

3.2.1 Estudos de infraestrutura para solução RDC Arq

O ambiente computacional do TJDFT utiliza a abordagem de DevOps (junção das palavras *development* e *operations*), que encurta o ciclo de vida de desenvolvimento de sistemas e fornece a entrega contínua com alta qualidade de software. Facilita a integração entre os times de desenvolvimento e infraestrutura, a gestão de ambientes e sistemas, além de promover maior aderência ao ambiente de execução das aplicações desde o início do desenvolvimento.

O TJDFT utiliza primariamente duas ferramentas para implementação do modelo DevOps: *Openshift*, *GitLab* e *SonarQube*, que, por sua vez, empregam *Kubernetes*, *Docker*, *melhoria* e *avaliações de segurança do código*. Os relacionamentos entre as ferramentas utilizadas nesse modelo DevOps seguem as seguintes etapas:

1. Desenvolvedor realiza um push no repositório no *GitLab* do TJDFT;
2. O pipeline de CI/CD é ativado no *GitLab*;
3. A leitura das diferentes aplicações descritas nos *DockerFiles* é realizada;
4. As imagens *Dockers* são construídas;
5. As imagens são enviadas para o *Registry* do TJDFT;
6. As imagens são submetidas para o *SonarQube* que realiza as verificações dos parâmetros mínimos aceitáveis de um código-fonte;

7. O *Openshift* busca as imagens no *Registry* e as utiliza no Kubernetes para criar as aplicações.

Quadro 1 - Descrição das ferramentas utilizadas.

GITLAB
O <i>GitLab</i> é um gerenciador de repositório de software baseado em git, que permite o versionamento de código, com suporte a Wiki, gerenciamento de tarefas e <i>Continuous Integration</i> (CI) / <i>Continuous Delivery</i> (CD), muito comumente chamadas apenas de CI/CD, que são ferramentas de integração e entrega contínua, essenciais ao modelo DevOps. No TJDF, o <i>Openshift</i> não faz o build (geração do código executável das aplicações) de projetos por questões de segurança, repassando esse trabalho para a ferramenta de entrega contínua do <i>GitLab</i>, a partir do código dos projetos versionados na plataforma.
SONARQUBE
O SonarQube é uma plataforma <i>open source</i> capaz de fazer inspeções contínuas da qualidade de um software com revisões automáticas e análise estática de código, a fim de detectar <i>bugs</i> e código mal escrito ou fora do padrão em várias linguagens de código de programação. Essa solução oferece ainda relatórios sobre códigos duplicados, padrões de codificação, testes de unidade, complexidade de códigos e recomendações de segurança.
DOCKER
O Docker é uma plataforma <i>open source</i> que facilita a criação e administração de ambientes isolados. Com ele, é possível empacotar uma aplicação ou ambiente dentro de um container, como se fossem máquinas virtuais modulares e extremamente leves. Em conjunto com o Kubernetes, o Docker ainda realiza as mesmas tarefas do seu objetivo original, a diferença é que o sistema automatizado solicita que o Docker realize essas tarefas, em vez do administrador fazer essas solicitações manualmente.
KUBERNETES
O Kubernetes é uma plataforma <i>open source</i> que automatiza as operações dos containers Linux. Ele possibilita a criação e gerenciamento de um cluster de containers em clouds privadas ou públicas, eliminando grande parte dos processos manuais necessários para implantar e escalar as aplicações em containers. Dessa forma, o gerenciamento dos clusters é feito com facilidade e efetividade.
OPENSIFT
O <i>Openshift</i> é uma plataforma de containers Kubernetes para empresas com operações automatizadas em todo o conjunto de sistemas. Com ele é possível criar, desenvolver e implantar aplicações de forma simples e rápida, em qualquer infraestrutura. A plataforma inclui um sistema operacional Linux para empresas, ambiente de execução de container, rede, monitoramento, registro e soluções de autorização e autenticação. Assim, a integração de arquitetura, processos, plataformas e serviços necessários para impulsionar o trabalho das equipes de desenvolvimento e de operações é feita de forma aliada e harmoniosa.
O SOFTWARE ARCHIVEMATICA

O Archivematica é um sistema para a preservação digital gratuito e de código aberto. Ele foi projetado para manter os dados baseados em padrões de preservação digital e o acesso a longo prazo para coleções de objetos digitais.

O software fornece um conjunto integrado de ferramentas livres que permite aos usuários processar objetos digitais para o armazenamento de arquivos em conformidade com o modelo funcional ISO-OAIS. O código do Archivematica é liberado sob a licença GNU Affero General Public License e sua documentação é liberada sob uma licença Creative Commons.

Fonte: Elaborado pelos autores (2023).

O software *Archivematica* consiste na implantação de diversas aplicações que trabalham em conjunto na preservação dos arquivos. São eles:

- **Archivematica MCPServer (servidor):** é um gerenciador de tarefas que utiliza o software gearman para enfileirar tarefas a serem executadas.
-
- **Archivematica MCPClient (cliente):** é uma ferramenta cliente do archivematica que executa as tarefas registradas no gearman pelo Archivematica MCPServer, dentre essas tarefas podemos destacar a execução de scripts, envio de e-mails, utilização de outros softwares para identificação e conversão de arquivos, análise de anti-vírus, dentre outras..
- **Archivematica Dashboard (GUI):** é uma interface gráfica web voltada para o usuário acompanhar a execução de microsserviços e tarefas. Desenvolvida na linguagem de programação python com o framework Django. Esse serviço lida com sistemas externos e configurações de fluxo de trabalho, status e decisões de processos de transferência e SIP e dá acesso ao backlog e armazenamento de arquivos.
- **Storage Service (armazenamento):** serviço responsável por gerenciar os repositórios, tais como a movimentação de arquivos entre os diretórios do Archivematica e disponibilização dos espaços (Spaces) às suas devidas finalidades, tais como arquivamentos de AIPs, DIPs, Backlog e disponibilização de diretórios para os usuários..
- **Clamavd:** é um kit de ferramentas de software antivírus gratuito, de plataforma cruzada e de código aberto, capaz de detectar muitos tipos de

software malicioso, incluindo vírus. Um de seus principais usos é em servidores de e-mail como verificador de vírus de e-mail no servidor.

- **Gearmand**: é uma estrutura de aplicativo de código aberto projetada para distribuir para outras máquinas ou processos que são mais adequados para fazer o trabalho. Ele permite que você trabalhe em paralelo, para balancear a carga de processamento e para chamar funções entre linguagens. (gearman.org).
- **MySQL**: é um sistema de gerenciamento de banco de dados relacional de código aberto.
- **Redis**: é um armazenamento de estrutura de dados na memória, usado como um banco de dados de chave-valor distribuído na memória, cache e agente de mensagens, com durabilidade opcional.
- **Nginx**: é um servidor web que também pode ser usado como proxy reverso, balanceador de carga, proxy de e-mail e cache HTTP. Gratuito e de código aberto, lançado sob os termos da licença BSD de 2 cláusulas, uma grande fração dos servidores web o usa frequentemente como um balanceador de carga.
- **Elasticsearch**: serviço que fornece um mecanismo de pesquisa de texto completo distribuído e com capacidade para vários locatários, com uma interface da web HTTP e documentos JSON sem esquema.
- **Fits**: é usado para caracterizar arquivos que não têm um formato de arquivo reconhecido.

Archivematica é um projeto ativo e dinâmico de código aberto com uma grande comunidade de usuários. Os desenvolvedores estão em constante atividade na melhora do sistema. Atualmente o software se encontra na versão v1.14.1.

Neste projeto foi utilizado a versão v1.13.2 por se tratar de uma versão mais estável e amplamente utilizada pelas principais organizações.

3.2.2 Processo de implantação do sistema no Openshift do TJDF

A implementação do *software Archivematica* em ambiente de contêineres começa com a criação de um repositório de versionamento de código no *GitLab*. Em seguida, é necessário a elaboração de imagens *docker para todos os containers que serão criados*, representada por um arquivo de configuração chamado *DockerFile*. Nesses arquivos são definidas as especificações da imagem, isto é, como ela deverá ser construída e comandos necessários para sua correta configuração.

Este projeto foi desenvolvido inicialmente com 12 arquivos do tipo *Dockerfile*:

- *Dockerfile-archivematica-dashboard*
- *Dockerfile-archivematica-mcp-client*
- *Dockerfile-archivematica-mcp-server*
- *Dockerfile-archivematica-storage*
- *Dockerfile-archivematica-storage-inicial*
- *Dockerfile-fits-ngserver*
- *Dockerfile-gearmand*
- *Dockerfile-hipatia-dje*
- *Dockerfile-hipatia-dje-cron*
- *Dockerfile-kibana*
- *Dockerfile-mysql*
- *Dockerfile-openssh*

O arquivo de configuração define as regras de implementação que o *Openshift* envia para o *Kubernetes*, que implementa a instância, denominada de *POD*, que executará o sistema em container. Um *POD* é a menor unidade de aplicação *Kubernetes*, podendo ser composto por um ou mais containers fortemente acoplados, de forma a compartilhar acessos.

A partir da implementação em *Docker Compose* descrita no *Github* oficial do *software Archivematica*, foi desenvolvida a containerização para o ambiente do *TJDFT* seguindo as orientações pré-definidas pelo Tribunal.

As etapas da implementação consistem na criação de volumes (*Persistent Volume Claim - PVC*) no *Openshift*, na criação dos arquivos necessários para integração contínua dos serviços utilizados pelo *Archivematica*, no *deployment* de

cada serviço no *Openshift*, na inicialização e preparação dos serviços e, por fim, na criação das rotas no *Openshift*.

Todo o projeto encontra-se no repositório de códigos do Tribunal, acessível pela rede interna, disponível no endereço: <https://gitlab.tjdft.jus.br/externos/ibict/archivematica-ibict-pje>. A seguir descrevem-se as etapas da implementação em detalhes.

3.2.2.1 Criação dos volumes (PVC)

A primeira etapa a ser realizada para implementação do Archivematica é a criação de cinco volumes (PVC) no *Openshift* que são utilizados pelas aplicações: *Storage Service*, *Elasticsearch*, *Fits*, *Clamav*, *MCPServer*, *MCPClient*, *Dashboard* e *MySQL*. O Quadro 2 apresenta os volumes criados no projeto *Archivematica - Stage* no *Openshift* com seus respectivos nomes, capacidades e aplicações associadas.

Quadro 2 - Listagem dos volumes.

NOME DO PVC	CAPACIDADE	APLICAÇÃO ASSOCIADA
<code>am-storage</code>	200GB	<i>Storage Service</i> (AIPs e DIPs)
<code>am-transfer</code>	50GB	<i>Storage Service</i> e <i>Hipátia PJe</i> (Transfer Source)
<code>am-storage-service-staging-data-pje</code>	200GB	<i>Storage Service</i> (Pilha de Processamento)
<code>elasticsearch-data</code>	1GB	<i>Elasticsearch</i>
<code>am-pipeline-data</code>	200GB	<i>Fits</i> , <i>Clamav</i> , <i>MCPServer</i> , <i>MCPClient</i> , <i>Dashboard</i> e <i>Storage Service</i>
<code>hipatia-pje-logs</code>	10GB	<i>Hipátia PJe</i> (logs)

Fonte: Elaborado pelos autores (2021).

As classes de serviço utilizadas para os volumes foram a **production-iscsi**, por orientação da equipe de infraestrutura do TJDF.

3.2.2.2 Criação e deployment dos serviços e aplicações

Esta etapa consiste na criação dos conjuntos de dados necessários para integração contínua no *GitLab* que são:

- (i) *DockerFile* e respectivos arquivos da imagem; e
- (ii) a descrição da imagem no arquivo **gitlab-ci.yml**. As subseções a seguir retratam os serviços e aplicações utilizadas.

3.2.2.3 MySQL

Os arquivos dessa aplicação estão disponíveis no endereço: <https://gitlab.tjdft.jus.br/externos/ibict/archivematica-ibict-pje/-/blob/master/Dockerfile-mysql>. A descrição da imagem no **gitlab-ci.yml** foi a seguinte:

Figura 1 - Descrição da imagem dos arquivos MySQL.

```
deploy_mysql_prod:
  <<: *template_deploy
  only:
    - tag
  variables:
    IMAGE_TAG: prod
    IMAGE_NAME: "archivematica-production/mysql-am"
    DOCKERFILE_PROJ: "Dockerfile-mysql"
  before_script:
    - SA_USER_TOKEN=$SA_USER_TOKEN_PROD
```

Fonte: Da pesquisa (2023).

Em seguida, foi realizado o *deployment* da imagem no *Openshift* com o nome “**am-mysql-pje**” e associado a seu respectivo PVC.

3.2.2.3 Elasticsearch

O *deployment* dessa aplicação foi realizado a partir da imagem no *DockerHub*, sem necessitar do registro de uma nova imagem no *Registry* do TJDF. Dessa forma, a imagem utilizada foi: **Elasticsearch 6.5.4:docker.elastic.co/elasticsearch/elasticsearch:6.5.4**.

Também foi necessária a configuração de limites de memória para essa aplicação. Na edição de limites de recurso da aplicação no *Openshift*, foi definido o mínimo garantido de 1Gb e um máximo de 2Gb.

Por fim, foi realizado o *deployment* da imagem no *Openshift* com o nome “**am-elasticsearch-pje**” e associado a seu respectivo PVC.

3.2.2.4 Gearmand

Os arquivos dessa aplicação estão disponíveis no endereço: <https://GitLab.tjdft.jus.br/docker-images/archivematica-ibict/-/tree/master/gearmand-a>.

A descrição da imagem no **Gitlab-ci.yml** foi a seguinte:

Quadro 3 - Descrição das informações dos arquivos Gearmand.

```
deploy_gearmand_prod:
  <<: *template_deploy
  only:
    - tag
  variables:
    IMAGE_TAG: prod
    IMAGE_NAME: "archivematica-production/gearmand-am"
    DOCKERFILE_PROJ: "Dockerfile-gearmand"
  before_script:
    - SA_USER_TOKEN=$SA_USER_TOKEN_PROD
```

Fonte: Da pesquisa (2023).

Em seguida, foi realizado o *deployment* da imagem no *Openshift* com o nome “**am-gearmand-pje**”. Nenhuma configuração adicional foi necessária.

3.2.2.5 Fits

O **deployment** dessa aplicação foi realizado a partir da imagem no *DockerHub*, sem necessitar do registro de uma nova imagem no *Registry* do TJDF. Dessa forma, a imagem utilizada foi a **Fits 0.8.4** da **Artefactual: artefactual/ fits-ngserver:0.8.4**.

Foi realizado o **deployment** da imagem no *Openshift* com o nome “**am-fits-ngserver-pje**” e associado a seu respectivo PVC.

3.2.2.6 Clamav

O **deployment** dessa aplicação foi realizado a partir da imagem no *DockerHub*, sem necessitar do registro de uma nova imagem no *Registry* do TJDF. Dessa forma,

a imagem utilizada foi *Clamav* mais atual da **Artefactual**: **artefactual/clamav:latest**. Ademais, foram definidas algumas variáveis de ambiente descritas no Quadro 3.

Quadro 3 - Variáveis de ambiente do Clamav

NOME DA VARIÁVEL DE AMBIENTE	VALOR
CLAMAVA_MAX_FILE_SIZE	200
CLAMAV_MAX_SCAN_SIZE	200
CLAMAV_MAX_STREAM_LENGTH	300

Fonte: Elaborado pelos autores (2021).

Por fim, foi realizado o *deployment* da imagem no *Openshift* com o nome “clamav-am-pje” e associado a seu respectivo PVC.

3.2.2.7 MCPServer

Os arquivos dessa aplicação estão disponíveis no endereço: <https://gitlab.tjdft.jus.br/externos/ibict/archivematica-ibict-pje/-/blob/master/Dockerrfile-archivematica-mcp-server>.

A descrição da imagem no **Gitlab-ci.yml** foi a seguinte:

Figura 4 - Descrição da imagem dos arquivos MCPServer.

```
deploy_archivematica-mcp-server_prod:
  <<: *template_deploy
  only:
    - tags
  variables:
    IMAGE_TAG: prod
    IMAGE_NAME: "archivematica-production/archivematica-mcp-server"
    DOCKERFILE_PROJ: "Dockerfile-archivematica-mcp-server"
  before_script:
    - SA_USER_TOKEN=$SA_USER_TOKEN_PROD
```

Fonte: Da pesquisa (2023).

Em seguida, foi realizado o *deployment* da imagem no *Openshift* com o nome “am-mcp-server-pje” e associado a seu respectivo PVC.

Atenção: as variáveis de ambiente dessa aplicação foram definidas no *DockerFile*.

3.2.2.8 MCPClient

Os arquivos dessa aplicação estão disponíveis no endereço: <https://GitLab.tjdft.jus.br/docker-images/archivematica-ibict/-/tree/master/archive-matic-a-mcp-client>. A descrição da imagem no **gitlab-ci.yml** foi a seguinte:

Figura 5 - Descrição da imagem dos arquivos *MCPClient*.

```
deploy_archivematica-mcp-client_prod:
  <<: *template_deploy
  only:
    - tags
  variables:
    IMAGE_TAG: prod
    IMAGE_NAME: "archivematica-production/archivematica-mcp-client"
    DOCKERFILE_PROJ: "Dockerfile-archivematica-mcp-client"
  before_script:
    - SA_USER_TOKEN=$SA_USER_TOKEN_PROD
```

Fonte: Da pesquisa (2023).

Em seguida, foi realizado o *deployment* da imagem no *Openshift* com o nome “**am-mcp-client-pje**” e associado a seu respectivo PVC.

Atenção: as variáveis de ambiente dessa aplicação foram definidas no *DockerFile*.

3.2.2.9 Dashboard

Os arquivos dessa aplicação estão disponíveis no endereço: <https://GitLab.tjdft.jus.br/docker-images/archivematica-ibict/-/tree/master/archivematic-a-Dashboard>. A descrição da imagem no **gitlab-ci.yml** foi a seguinte:

Figura 6 - Descrição da imagem dos arquivos *Dashboard*.

```
deploy_archivematica-dashboard_prod:
  <<: *template_deploy
  only:
    - tags
  variables:
    IMAGE_TAG: prod
    IMAGE_NAME: "archivematica-production/archivematica-dashboard"
    DOCKERFILE_PROJ: "Dockerfile-archivematica-dashboard"
  before_script:
    - SA_USER_TOKEN=$SA_USER_TOKEN_PROD
```

Fonte: Da pesquisa (2023).

Em seguida, foi realizado o **deployment** da imagem no *Openshift* com o nome “**archivematica-dash-am**” e associado a seu respectivo PVC.

Atenção: as variáveis de ambiente dessa aplicação foram definidas no *DockerFile*.

3.2.2.10 Storage service

Os arquivos dessa aplicação estão disponíveis no endereço: <https://gitlab.tjdft.jus.br/externos/ibict/archivematica-ibict-pje/-/blob/master/Dockerfile-archivematica-storage>.

A descrição da imagem no **gitlab-ci.yml** foi a seguinte:

Figura 7 - Descrição da imagem dos arquivos *Storage Service*.

```
deploy_archivematica-storage-service_prod:
  <<: *template_deploy
  only:
    - tags
  variables:
    IMAGE_TAG: prod
    IMAGE_NAME: "archivematica-production/archivematica-storage"
    DOCKERFILE_PROJ: "Dockerfile-archivematica-storage"
  before_script:
    - SA_USER_TOKEN=$SA_USER_TOKEN_PROD
```

Fonte: Da pesquisa (2023).

Em seguida, foi realizado o *deployment* da imagem no *Openshift* com o nome “**am-storage-pje**” e associado aos seus respectivos PVCs.

Atenção: as variáveis de ambiente dessa aplicação foram definidas no *DockerFile*.

3.2.2.11 Inicialização e preparação dos serviços

Nessa etapa foi realizada a criação do banco de dados (*database*) e a criação das tabelas na aplicação *MySQL*. Em seguida, deve-se reinicializar as aplicações *MCPServer*, *MCPClient*, *Dashboard* e *Storage Service*.

3.2.2.12 Criação dos bancos de dados

Para criar os bancos de dados, deve-se entrar na aplicação MySQL e executar os seguintes comandos:

Figura 8 - Comandos para criação de bancos de dados na aplicação MySQL.

```
sh-4.2$ bash
bash-4.2$ mysql -u root -p12345

mysql> DROP DATABASE IF EXISTS SS;
mysql> CREATE DATABASE SS;
mysql> GRANT ALL ON SS.* TO 'archivematica'@'%' IDENTIFIED BY 'demo';"

mysql> DROP DATABASE IF EXISTS MCP;
mysql> CREATE DATABASE MCP;
mysql> GRANT ALL ON MCP.* TO 'archivematica'@'%' IDENTIFIED BY 'demo';"
```

Fonte: Da pesquisa (2023).

3.2.2.13 Criação das tabelas

Para criar as tabelas nos respectivos bancos de dados, deve-se entrar nas aplicações *Dashboard* e *Storage Service* (armazenamento) e executar um *script python*.

Figura 9 - *Script python* para criação de tabelas nas aplicações *Dashboard* e *Storage Service*.

```
CMD ["tail", "-f", "/dev/null"]
```

Fonte: Da pesquisa (2023).

Contudo, para executar o *script python*, foi necessário modificar o *entrypoint* de cada um dos serviços (*Dashboard* e *Storage Service*) para que o POD inicie sem erros no *Openshift*. Dessa forma, o *entrypoint* padrão foi comentado no *DockerFile* e em seu lugar, foi usado o seguinte *entrypoint*:

Uma vez modificados os *entrypoints* e feito o *redploy* das aplicações, é possível acessar cada aplicação e executar os *scripts python* necessários para a criação das tabelas nos respectivos bancos de dados.

Para a aplicação do *Storage Service*, são executados os seguintes comandos:

Figura 10 - Comandos para a aplicação do *Storage Service*.

```
$ /src/storage_service/manage.py migrate --noinput
$ /src/storage_service/manage.py create_user --username="test"
--password="test" --email="test@test.com" --api-key="test" --superuser
```

Fonte: Da pesquisa (2023).

Para a aplicação do *Dashboard*, são executados os seguintes comandos:

Figura 11 - Comandos para a aplicação do *Dashboard*.

```
$ /src/storage_service/manage.py migrate --noinput
$ /src/dashboard/src/manage.py install --username="test"
--password="test" --email="test@test.com" --org-name="test"
--org-id="test" --api-key="test"
--ss-url="http://archivematica-storage-se:8000" --ss-user="test"
--ss-api-key="test" --site-url="http://archivematica-dash-am:8000"
$ cd /src/dashboard/frontend
$ npm install --unsafe-perm
```

Fonte: Da pesquisa (2023).

Após a execução dos comandos, redefine-se cada *endpoint* para o original e é realizado o *redploy* da aplicação.

Neste momento, o *software* do *Archivematica* e todos seus serviços estão operando como o esperado.

3.2.2.14 Criação das rotas

Para disponibilizar o sistema na rede interna do TJDF, é necessário configurar as rotas dentro do *Openshift*.

As orientações da equipe de infraestrutura do Tribunal estão no seguinte endereço: <https://gitlab.tjdft.jus.br/infraestrutura/openshift/integracao/dns>.

Deve-se criar uma rota segura para a aplicação, que usa TLS/HTTPS. Uma rota é uma referência ao serviço do POD, que deve expor uma determinada porta. Nas configurações do *Openshift* os tipos de *Termination* de uma rota atualmente são: *Edge*, *Reencrypt* ou *Passthrough*. A recomendação da equipe de infraestrutura do Tribunal foi para usar a terminação *Edge*.

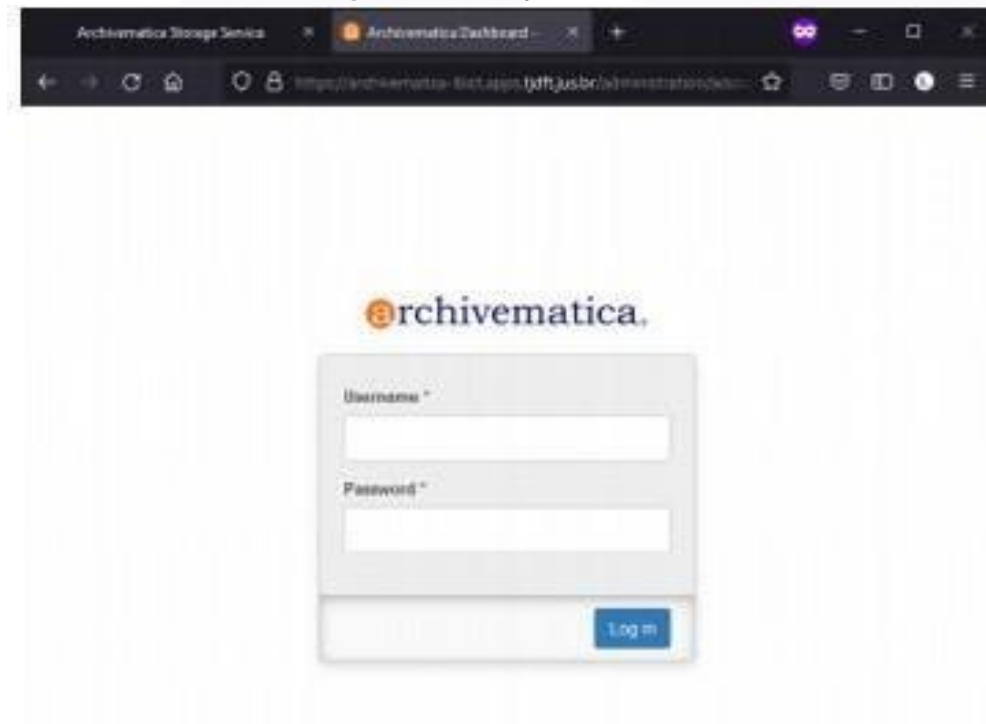
Uma rota segura é publicada com HTTPS (porta 443) ou possui redirecionamento das requisições de HTTP (porta 80) para HTTPS (porta 443), como mostra o vídeo no endereço (acessado na rede interna): <https://drive.tjdft.jus.br/index.php/s/D7dYX65pNi3ggAs>.

Dessa forma, foram criadas duas rotas para os serviços:

- *Dashboard*: <https://archivematica-ibict.apps.tjdft.jus.br>
- *Storage*: <https://archivematica-storage-ibict.apps.tjdft.jus.br>

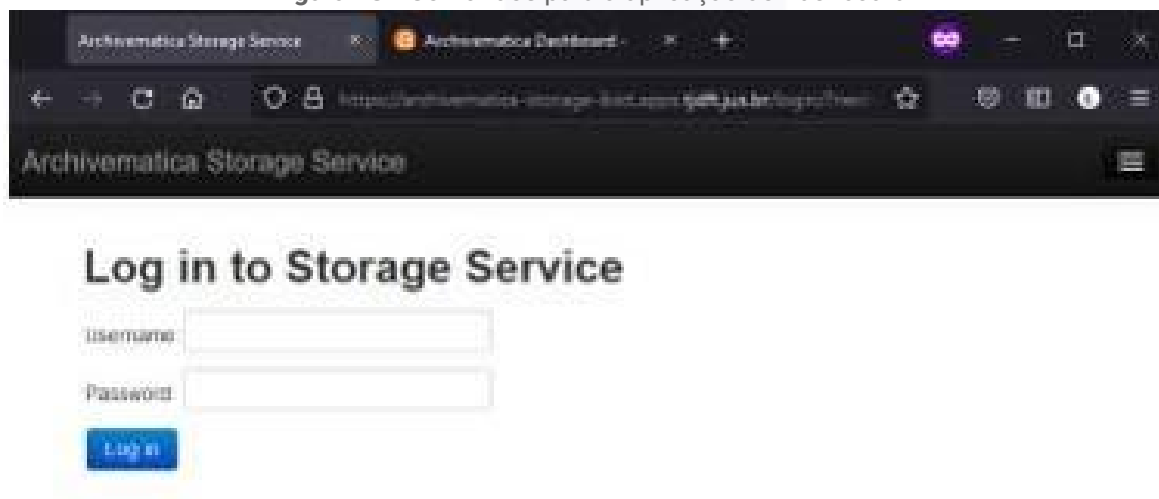
As Figuras 12 e 13 apresentam respectivamente os serviços do *Dashboard* e do *Storage* sendo executados com sucesso.

Figura 12 - Serviço de *Dashboard*.



Fonte: Captura de tela da página web do Archivematica (2021).

Figura 13 - Comandos para a aplicação do *Dashboard*.



Fonte: Captura de tela da página web do Archivematica (2021).

3.2.2.15 Testes de Escalabilidade

→ Estudos para criar mecanismo de escalabilidade dos serviços à medida do crescimento da demanda

Descrição de um teste completo de escalabilidade para um ambiente de preservação de processos digitais no *OpenShift* envolvendo *Archivematica* e *AtoM*:

1. **Instalação e configuração:** O primeiro passo é instalar e configurar o ambiente. Isso inclui instalar o *OpenShift*, o *Archivematica* e o *AtoM*. O *OpenShift* é uma plataforma de nuvem para hospedar aplicativos Docker. O *Archivematica* é uma ferramenta de preservação digital que pode ser usada para preservar arquivos digitais. O *AtoM* é um sistema de gerenciamento de conteúdo (CMS) que pode ser usado para armazenar e exibir arquivos digitais.
2. **Carregamento de dados:** O próximo passo é carregar os dados no ambiente. Isso pode ser feito carregando os dados diretamente no *Archivematica* ou usando o *AtoM* como um intermediário. Se o *AtoM* for usado como um intermediário, os dados devem ser carregados no *AtoM* e, em seguida, exportados para o *Archivematica*.
3. **Teste de escalabilidade:** O último passo é testar a escalabilidade do ambiente. Isso pode ser feito executando um teste de carga no ambiente. Um teste de carga é um teste que simula o uso do ambiente por muitos usuários. O teste de carga pode ser usado para medir o desempenho do ambiente e identificar quaisquer gargalos.

Para executar um teste de escalabilidade bem-sucedido:

- Use uma ferramenta de teste de carga para executar o teste;
- Defina o tamanho da carga do teste de acordo com as necessidades do ambiente;
- Monitore o desempenho do ambiente durante o teste de carga; e
- Documente os resultados do teste de carga.

Alguns dos resultados que podem ser esperados de um teste de escalabilidade bem-sucedido:

- O ambiente deve ser capaz de lidar com a carga de teste sem problemas;
- O desempenho do ambiente deve ser consistente ao longo do tempo; e
- O ambiente não deve apresentar nenhum gargalo.

Se os resultados do teste de escalabilidade não forem satisfatórios, pode ser necessário fazer alterações no ambiente. Essas alterações podem incluir:

- Adicionar mais nós ao ambiente;
- Atualizar o *hardware* do ambiente; e
- Melhorar o desempenho do *Archivematica* ou do *AtoM*.

Ações adicionais para melhorar a escalabilidade do ambiente de preservação de processos digitais:

- Usar um sistema de armazenamento escalável.
- Usar um sistema de cache.
- Usar um sistema de distribuição de carga.
- Usar um sistema de monitoramento.

→ **Detalhamento das ações envolvidas no teste de escalabilidade para o ambiente de preservação de processos digitais no *OpenShift* envolvendo *Archivematica* e *AtoM***

1. Instalação e configuração: O primeiro passo é instalar e configurar o ambiente. Isso inclui instalar o *OpenShift*, o *Archivematica* e o *AtoM*.
 - **Instalação do *OpenShift*:** O *OpenShift* pode ser instalado em um hardware local ou em uma nuvem pública. Para instalar o *OpenShift* em um hardware local, você precisará baixar o instalador do

OpenShift e executá-lo. Para instalar o *OpenShift* em uma nuvem pública, você precisará criar um cluster *OpenShift*.

- **Instalação do Archivematica:** O *Archivematica* pode ser instalado como um aplicativo Docker no *OpenShift*. Para instalar o *Archivematica*, você precisará criar um novo projeto no *OpenShift* e, em seguida, implantar o aplicativo *Archivematica* no projeto.
- **Instalação do AtoM:** O *AtoM* pode ser instalado como um aplicativo Docker no *OpenShift*. Para instalar o *AtoM*, você precisará criar um novo projeto no *OpenShift* e, em seguida, implantar o aplicativo *AtoM* no projeto.

2. **Carregamento de dados:** O próximo passo é carregar os dados no ambiente.

Isso pode ser feito carregando os dados diretamente no *Archivematica*.

- **Carregamento de dados diretamente no Archivematica:** Para carregar os dados diretamente no *Archivematica*, você precisará usar o aplicativo *Archivematica* para importar os dados. O aplicativo *Archivematica* pode importar dados de uma variedade de fontes, incluindo arquivos locais, pastas remotas e serviços de armazenamento em nuvem.
- **Carregamento de dados usando o AtoM:** O aplicativo *AtoM* pode importar dados de uma variedade de fontes, incluindo arquivos locais, pastas remotas e serviços de armazenamento em nuvem.

3. **Teste de escalabilidade:** O último passo é testar a escalabilidade do ambiente. Isso pode ser feito executando um teste de carga no ambiente.

- **Teste de carga:** Um teste de carga é um teste que simula o uso do ambiente por muitos usuários. O teste de carga pode ser usado para medir o desempenho do ambiente e identificar quaisquer gargalos. Para executar um teste de carga, você precisará usar uma ferramenta de teste de carga. Existem muitas ferramentas de teste de carga disponíveis, incluindo *JMeter*, *Gatling* e *LoadRunner*. Ao executar um teste de carga, você precisará definir o tamanho da carga do teste conforme as necessidades do ambiente. Por

exemplo, se o ambiente for projetado para lidar com 1000 usuários simultâneos, você precisará definir o tamanho da carga do teste para 1000 usuários. Você também precisará monitorar o desempenho do ambiente durante o teste de carga. Isso pode ser feito usando uma ferramenta de monitoramento de desempenho. Existem muitas ferramentas de monitoramento de desempenho disponíveis, incluindo *Nagios*, *Zabbix* e *Prometheus*. Após a conclusão do teste de carga, você precisará documentar os resultados do teste. Isso incluirá o desempenho do ambiente, quaisquer gargalos identificados e quaisquer recomendações para melhorar o desempenho do ambiente.

Aqui estão alguns resultados que podem ser esperados de um teste de escalabilidade bem-sucedido:

- O ambiente deve ser capaz de lidar com a carga de teste sem problemas.
- O desempenho do ambiente deve ser consistente ao longo do tempo.
- O ambiente não deve apresentar nenhum gargalo.

Se os resultados do teste de escalabilidade não forem satisfatórios, pode ser necessário fazer alterações no ambiente. Essas alterações podem incluir:

- Adicionar mais nós ao ambiente.
- Atualizar o hardware do ambiente.
- Melhorar o desempenho do Archivematica ou do AtoM.

→ **Alterações de ambiente que podem ser feitas para melhorar a escalabilidade:**

- **Adicionar mais nós ao ambiente:** Adicionar mais nós ao ambiente aumentará a capacidade do ambiente de lidar com a carga de trabalho.

Para adicionar mais nós ao ambiente, você precisará criar novos nós no OpenShift.

- **Atualizar o *hardware* do ambiente:** Atualizar o *hardware* do ambiente melhorará o desempenho do ambiente. Para atualizar o *hardware* do ambiente, você precisará comprar novos nós com hardware mais poderoso.
- **Melhorar o desempenho do Archivematica ou do AtoM:** Melhorar o desempenho do Archivematica ou do AtoM melhorará o desempenho do ambiente. Para melhorar o desempenho do Archivematica ou do AtoM, você pode fazer algumas coisas, como:
 - Atualizar o Archivematica ou o AtoM para uma versão mais recente;
 - Usar um sistema de armazenamento mais rápido;
 - Usar um cache; e
 - Usar um sistema de distribuição de carga.

3.2.2.16 Estudo para dois fluxos (pipelines) de preservação em openshift

Diante da necessidade TJDFT em utilizar dois Archivematica com regras de preservação distintas para preservar os documentos de guarda permanente e os documentos de guarda longa, foi realizado um estudo que analisou a possibilidade de se operar múltiplos pipelines ao invés de múltiplos Archivematica no ambiente tecnológico.

Em um primeiro momento, após analisar casos aplicados em outros países, alguns problemas de atualização de versões, falta de documentação e de assistência da Artefactual, empresa responsável pelo software, foram identificados. Contudo, posteriormente, foi realizado um diálogo mais aprofundado com a comunidade no exterior, mostrando que existe a possibilidade desta configuração em ambiente de produção. As discussões foram apresentadas em uma reunião para a equipe do TJDFT.

Destaca-se assim que o Archivematica é composto por duas interfaces que são instaladas e interoperam concomitantemente. A interface Dashboard é a interface de gestão documental onde os pacotes de preservação são submetidos e processados. Já a interface *Storage Service* fica sob a responsabilidade dos gestores de preservação e de Tecnologia da Informação, por ser um local de acesso direto aos pacotes preservados e também sob a responsabilidade do profissional de tecnologia da informação, já que o *Storage Service* apresenta as configurações técnicas do sistema do Archivematica.

No *storage service* encontram-se as configurações dos *spaces*, que são os protocolos de conexão que serão usados entre o *dashboard* e um *storage*. Cada pipeline representa uma interface *dashboard*, que um *Storage Service* pode trabalhar e operar com múltiplos pipelines que vão ter protocolos específicos conforme sua funcionalidade.

De maneira geral, os múltiplos pipelines podem ser utilizados para restringir o acesso a dados sigilosos por pessoas que estariam utilizando o Dashboard, mas não tem permissão para visualizar tal conteúdo conforme seja necessário. Os múltiplos pipelines também podem ser utilizados quando há planos de preservação diferenciados para documentos que possuem destinações finais diferentes, por exemplo, como no caso do TJDFT.

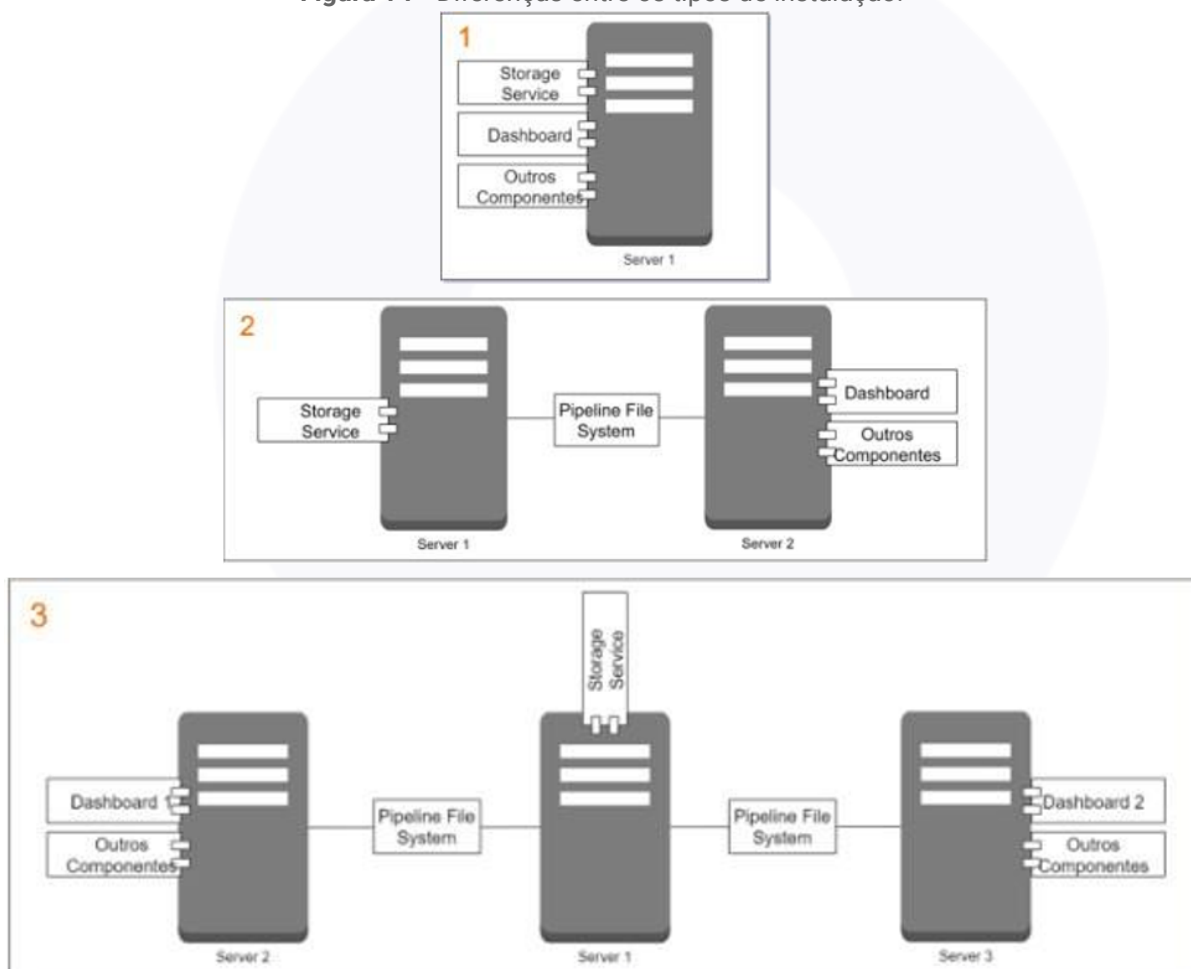
Desse modo, o acesso a um único *Storage Service* por administrador independentemente da quantidade de dashboards, e a possibilidade de ter uma única interface de configuração do *Storage Service*, facilitando o acesso e a administração do sistema são algumas das vantagens da utilização de múltiplos pipelines. Através dessa configuração, também é possível restringir acessos a dados sigilosos, mover os pacotes entre os diferentes pipelines sem a perda da rastreabilidade e operar tendo diferentes configurações de regras e comandos do plano de preservação.

Por conseguinte, a desvantagem a princípio envolveria apenas os estudos, as implicações e a aplicabilidade dos múltiplos pipelines em ambiente de *Docker*, já que é o tipo de sistema computacional utilizado pelo TJDFT. Na instalação em *Virtual Machine*, foi necessário separar o componente *Storage Service* dos demais

componentes do Archivematica e de maneira prática, o *Storage Service* por SSH captura os documentos do dashboard e salva nos respectivos locais do *Storage Service*. Diferentemente da instalação comum, para conseguir operar o Archivematica com diferentes pipelines é necessário criar um protocolo de acesso no *Storage Service* chamado de “*Pipeline Local File System*” que vai realizar a comunicação entre o *storage Service* e seus respectivos pipelines.

A figura abaixo demonstra as diferenças entre os diferentes tipos de instalação. A primeira imagem representa uma instalação comum na qual o *Storage Service*, o *Dashboard* e os outros componentes ficam na mesma máquina. A segunda imagem demonstra um primeiro teste realizado, onde o dashboard e os outros componentes foram separados do *Storage Service* e conectados através do protocolo *Pipeline File System*. Já a terceira imagem representa a aplicação de múltiplos dashboards geridos por apenas um *Storage Service*.

Figura 14 - Diferenças entre os tipos de instalação.



Fonte: Da pesquisa (2023).

O estudo está na fase final das análises, sendo a integração com o Openshift, o principal foco das atenções, pois todos os parâmetros antes estudados, mudam com essa nova abordagem da solução tecnológica. O uso de multi-pipelines vem para ajudar nos seguintes pontos:

- Restringir acesso (*dashboard*) a documentos a serem preservados de origens distintas;
- Processamento pode ser escalado;
- Trabalhar com documentos no corrente/intermediário e de preservação definitiva em pipelines distintos;
- Trabalhar com documentos de múltiplos sistemas de forma isolada;
- Storage único para gerenciamento dos pacotes;

No entanto, elenco possíveis casos que dificultem a configuração, manutenção e usabilidade e devem ser analisados e testados:

- Dificuldade da integração e configuração;
- Possibilidade de separar as pipelines em SS distintos posteriormente;
- Pelo fato que cada pipeline estar ligada a repositórios distintos, podemos mover os pacotes entre pipelines;
- Caso ocorra um problema no storage, afetará todas as pipelines;
- Pipelines distintas, no entanto, locais (locations) padrões únicos; e
- Banco de dados único, sem possibilidade de multi-tenant;

Segue abaixo o passo-a-passo realizado desde a instalação, configuração, integração e teste de usabilidade e de API:

1. Instalação do Archivematica P1 (pipeline 1);
2. Instalação do Archivematica P2 (pipeline 2);
3. Instalação do Archivematica SS;
4. Integração dos Archivematicas com SS por meio do Pipeline Local Filesystem;
5. Integração com AtoM, 2.6 para o P1 e 2.7 para o P2;
6. Testes:
 - a. preservação;
 - b. preservação e acesso;
 - c. Indexação via linha de comando.

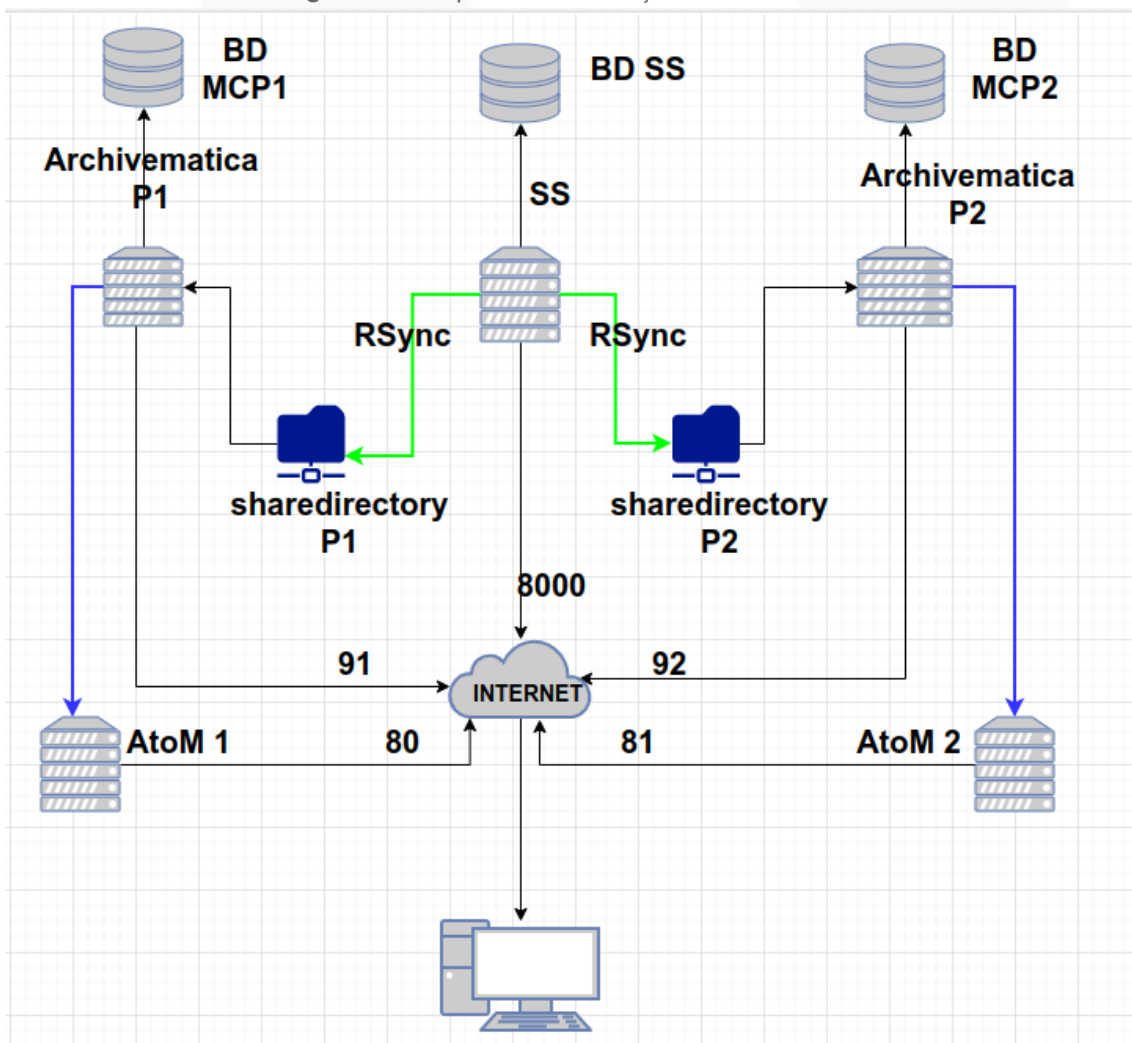
→ Instalação

Os parâmetros abaixo são referentes aos ambientes do Ibict em container, e uso do recurso de volumes para persistência e compartilhamento de informações entre containers. Dessa forma instalamos um Archivematica *Storage Service* (SS) e dois Archivematica (*Dashboard*, *Server* e *Client*). Também aproveitamos as

instalações existentes de dois AtoMs nas versões 2.6.4 e 2.7.1 para integrar com os Archivematica e enviar os pacotes DIP.

Segue desenho ilustrativo como seria a arquitetura da solução:

Figura 15 - Arquitetura instalação Archivematica.



Fonte: Da pesquisa (2023).

Na instalação, cada aplicação teve seus bancos e volumes/storages separados e integrados quando foi necessário. As portas também foram ajustadas para não dar conflitos nas aplicações.

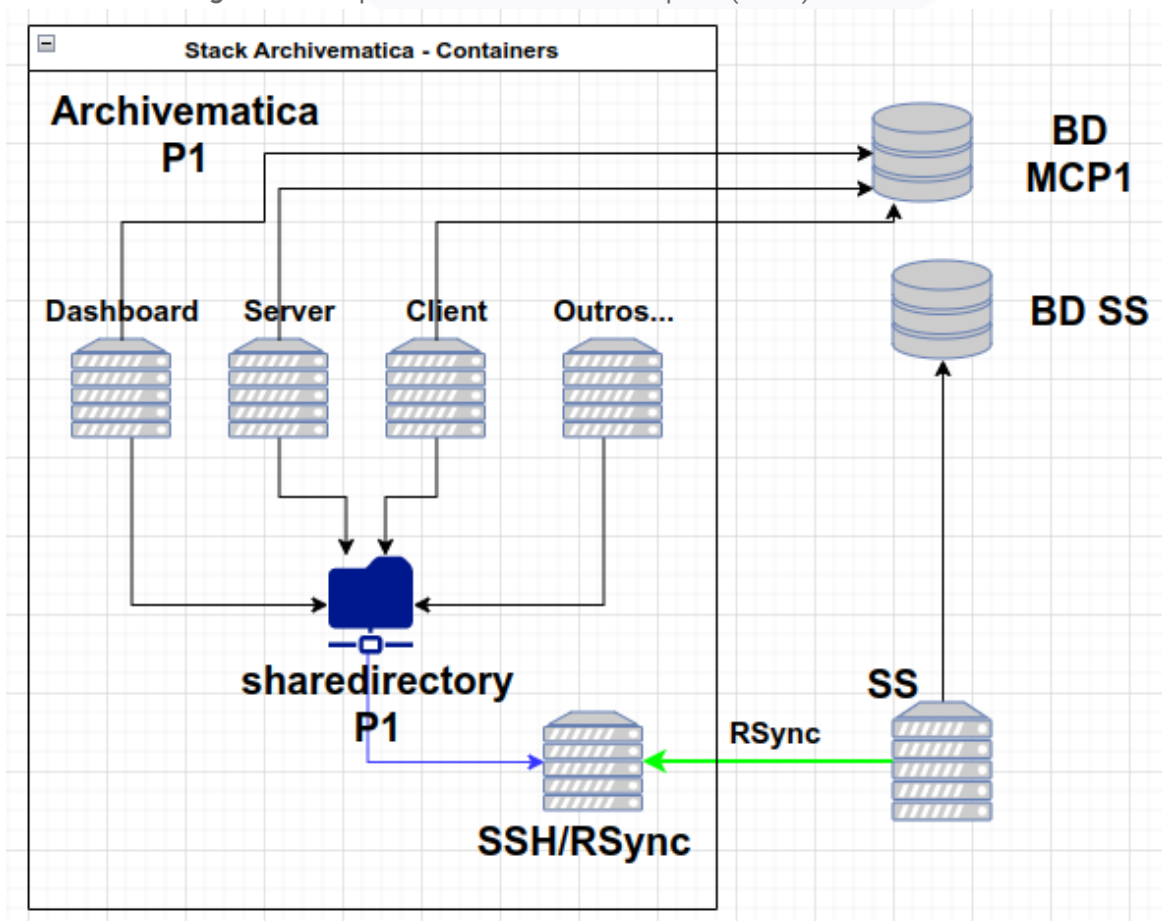
Logo, cada aplicação Archivematica ficou isolada, com seu *sharedirectory* único e distinto para persistência das informações. A integração com o SS ocorre em dois momentos.

O primeiro é a integração via Pipeline onde se dá o credenciamento dos dados de integração (*host*, *usuário*, *token API*), mais o identificador UUID do Archivematica. O segundo momento, é a configuração dos espaços (*spaces*) e locais (*locations*) que se dá por meio de um protocolo de acesso (em *spaces*) chamado *Pipeline Local Filesystem*.

Essa integração, usando o protocolo do Pipeline Local Filesystem realiza chamadas via *SSH/RSync* para o *host* do Archivematica, acessando o *sharedDirectory* para que selecionando os diretórios para configurar os locais (*locations*) de um espaço e atribuídos a uma pipeline.

Veja abaixo uma imagem ilustrativa apresentando uma arquitetura de containers da pilha (*stack*) Archivematica:

Figura 16 - Arquitetura de containers da pilha (*stack*) Archivematica.



Fonte: Da pesquisa (2023).

Na imagem, podemos observar os containers (*dashboard*, *server*, *client* e outros) referentes a aplicação Archivematica, no entanto, adicionamos um novo container com recurso e acesso via *SSH* e *RSync* e adicionamos o volume do *sharedDirectory* do Archivematica. Dessa forma, deixando somente o acesso a essa parte da aplicação acessível à aplicação *SS*.

O acesso via *SSH* e *RSync* deve ocorrer sem a necessidade de senha, para isso é recomendado a criação e compartilhamento de chaves públicas e privadas.

Com essa configuração funcional, ao acessar o *SS*, no menu de espaços e selecionar o espaço que foi configurado o Protocolo de Acesso, o *Pipeline Local Filesystem* e ao configurar um novo ou existente local (*location*) ao selecionar um Path para um local (*location*), o *SS* por meio do *RSync* vai até o *sharedDirectory* do Archivematica e lista os diretórios disponíveis para seleção.

→ Teste de Preservação e Preservação com Acesso (AtoM)

Esse teste é avaliar o funcionamento das aplicações de forma separada. No primeiro teste avaliamos o funcionamento do Archivematica 1 interoperando com AtoM 2.7. No segundo momento, avaliamos o Archivematica 2 interoperando com AtoM 2.6.4. Para ambas as aplicações, realizamos testes de preservação e após realizamos testes de preservação com acesso na plataforma de acesso AtoM.

→ Indexação via linha de comando

Este processo visa indexar os pacotes preservados, no entanto estamos atuando no mesmo storage *SS* em duas pipelines distintas para duas aplicações Archivematica. O objetivo desta análise é verificar a persistência dos pacotes após serem preservados em cada aplicação, ou seja, os pacotes preservados e executados na aplicação de origem não se misturam entre pipelines de outra aplicação.

Segue abaixo o comando executado:

```
python manage.py rebuild_elasticsearch_aip_index_from_files  
/var/archivematica/sharedDirectory/www/AIPsStore --delete-all
```

OBS: O *path* do *AIPsStore* dependendo da sua configuração pode ser outro

A integração entre o Archivematica e o Archivematica *Storage Service* (SS) no ambiente *OpenShift*, juntamente com a utilização de múltiplas pipelines, proporciona uma solução robusta e escalável para a preservação digital. Através da configuração adequada dos espaços (*spaces*) e locais (*locations*) utilizando o protocolo *Pipeline Local Filesystem*, é possível estabelecer conexões remotas entre o SS e os Archivematica, permitindo a consulta e ação direta nos diretórios e subdiretórios do Archivematica.

Ao utilizar o ambiente de contêiner, é possível isolar as aplicações do Archivematica e do SS, garantindo a separação dos bancos de dados e dos volumes persistentes. Além disso, o compartilhamento de chaves públicas e privadas para acesso via *SSH* e *RSync* permite uma integração segura e simplificada entre os componentes.

Através dos testes realizados, verificou-se que a preservação com acesso e indexação via linha de comando podem ser executadas com sucesso em ambientes com múltiplas pipelines. Cada aplicação do Archivematica, juntamente com sua respectiva versão do AtoM, pôde operar de forma independente, preservando e disponibilizando o acesso aos documentos de forma isolada entre as pipelines.

No entanto, é importante considerar que a configuração, manutenção e usabilidade de múltiplas pipelines requerem análise e testes cuidadosos. Questões como a dificuldade de integração e configuração inicial, a possibilidade de separar pipelines em instâncias distintas do SS e os possíveis impactos de problemas no *storage* devem ser considerados durante o planejamento e implementação do ambiente.

3.3 Definições para alinhamento com as políticas de Segurança da Informação do Tribunal

Foi realizado estudo visando avaliar o atual estágio de desenvolvimento do barramento tecnológico, integrante do modelo Hipátia de preservação digital, frente ao Guia de Boas Práticas de Desenvolvimento, Infraestrutura e Segurança das Aplicações do TJDFT e a Política Corporativa de Segurança da Informação baseada na RESOLUÇÃO 21 DE 8 DE NOVEMBRO DE 2016. O estudo completo foi anexado no Apêndice F deste relatório.

A premissa é seguir as recomendações e melhores práticas definidas pelo Guia em relação aos requisitos de segurança da informação, arquitetura, experiência dos usuários, ferramentas, infraestrutura e operação, obedecendo as melhores práticas de mercado, antes e durante a implantação, o desenvolvimento e a manutenção das aplicações.

O Ibict considera de extrema importância padronizar os procedimentos de desenvolvimento da ferramenta em relação às recomendações e boas práticas do TJDFT para implantação, manutenção, sustentação e eventual desligamento, para garantir isonomia nos princípios de segurança de sistemas durante todo o ciclo de vida da aplicação.

Pretende-se, dessa forma, que o PPD-PJe seja o documento de referência na resolução de questões e promoções de melhorias/atualizações das práticas e tecnologias que visam a implementação da Política de Preservação Digital do TJDFT no âmbito do sistema PJe.

Avaliação de segurança do barramento Barrapres

No processo de avaliação do barramento de preservação digital para o Tribunal de Justiça do Distrito Federal e dos Territórios (TJDFT) foi utilizado o software SONARQUBE. Foi constatado que o Barrapres passou nos testes com êxito geral. No entanto, foram identificadas algumas ressalvas não críticas relacionadas à segurança.

A avaliação permitiu uma análise aprofundada do código-fonte do barramento de preservação digital, fornecendo percepções valiosas sobre sua qualidade e segurança. A plataforma identificou áreas em que o código

poderia ser otimizado, como duplicações, complexidade excessiva e violações de regras de codificação.

No que diz respeito à segurança, embora o barramento tenha sido considerado globalmente seguro, algumas ressalvas não críticas foram identificadas. Com base nos resultados da avaliação, a equipe do Ibict pôde priorizar as ações corretivas necessárias. As ressalvas não críticas de segurança foram analisadas e levadas em consideração para a implementação de melhorias no código. A equipe trabalhou para abordar as áreas destacadas e tomar medidas para fortalecer ainda mais a segurança do barramento.

É importante ressaltar que a identificação dessas ressalvas é uma prática recomendada no processo de avaliação de segurança e qualidade do código. Elas fornecem oportunidades de aprimoramento contínuo e garantem que o barramento de preservação digital esteja alinhado com as melhores práticas de segurança.

Em resumo, a avaliação no SONARQUBE indicou que o barramento de preservação digital do TJDFT passou nos testes com sucesso. Embora algumas ressalvas não críticas relacionadas à segurança tenham sido identificadas, a equipe responsável pela implementação do barramento agiu prontamente para abordar essas questões e aprimorar a segurança do sistema. Essa abordagem garantiu que o barramento de preservação digital esteja alinhado com as melhores práticas de desenvolvimento e segurança de software.

O documento completo está no Apêndice E deste relatório.

3.4 Meta 2: Análise de padrão de design de código para solução RDC-Arq

Aqui são realizados os levantamentos de padrões de design de código e análise da aplicação dos padrões abordados na estrutura do barramento RDC-Arq. Por consequência, a partir da relação de requisitos de negócio e aplicação das

validações automatizadas nos códigos, elabora-se o modelo para estruturação de códigos para barramento RDC-Arq e o aplica à estrutura do TJDFT. Essa meta se finaliza com a apresentação em reunião presencial/virtual e entrega de relatório com detalhamento da etapa.

3.4.1 Análise de padrão de design de código para solução RDCArq

O desenvolvimento de softwares deve seguir padrões modernos de codificação. Ele deve ser pensado para a solução de problemas de forma específica, mas também ser flexível o suficiente ser reutilizável e atender novos requisitos.

Para Gamma (2000), os padrões de projeto (*Design Patterns*) permitem melhor reutilizar projetos e arquiteturas, fornecendo alternativas que deixam mais claras a documentação e manutenção de sistemas. Padrões de projeto visam a criação de projetos de software flexíveis e extensíveis.

3.4.2 Tipos de design patterns

Os criadores do conceito de *design patterns* propuseram 23 padrões, divididos em três categorias

- **Criacionais:** padrões que propõem soluções flexíveis para criação de objetos.
 - *Abstract Factory;*
 - *Factory Method;*
 - *Singleton;*
 - *Builder;*
 - *Prototype;*
- **Estruturais:** padrões que propõem soluções flexíveis para composição de classes e objetos.
 - *Proxy;*
 - *Adapter;*

- *Facade;*
- *Decorator;*
- *Bridge;*
- *Composite;*
- *Flyweight.*
- **Comportamentais:** padrões que propõem soluções flexíveis para interação e divisão de responsabilidades entre classes e objetos.
 - *Strategy;*
 - *Observer;*
 - *Template Method;*
 - *Visitor;*
 - *Chain of Responsibility;*
 - *Command;*
 - *Interpreter;*
 - *Iterator;*
 - *Mediator;*
 - *Memento;*
 - *State.*

A pesquisa com *design patterns* está compatibilizando os estudos com o método de programação orientada a eventos adotada no TJDF. A programação orientada a eventos é um conceito que difere como as rotinas são executadas. Nesse contexto, as rotinas são acionadas por indicações de um serviço de mensagens (ou eventos) que indica aos sistemas as funções e respostas de acordo com os acontecimentos de cada um, tornando todas as comunicações entre sistemas bastante flexível e assíncronas.

O desenvolvimento de software precisa de padronização para garantir a qualidade, eficiência e consistência do processo de desenvolvimento. A padronização pode ajudar a melhorar a comunicação entre membros da equipe, facilitar a manutenção do código, permitir a reutilização de componentes, reduzir erros e aumentar a eficiência no desenvolvimento de software.

Existem várias áreas no qual a padronização é importante no desenvolvimento de software, como a nomenclatura de variáveis, a arquitetura do sistema, o controle de versão, o processo de testes e a documentação. Alguns exemplos de padrões incluem a utilização de metodologias de desenvolvimento ágil, padrões de codificação como o PEP8 para Python, padrões de nomenclatura de variáveis, padrões de arquitetura de software como o MVC (*Model-View-Controller*) e o uso de ferramentas de integração contínua.

Nesse contexto é necessário também ter adotado a prática de testes automatizados. Os testes automatizados são essenciais no desenvolvimento de software, eles reduzem erros, aceleram o processo de desenvolvimento, aumentam a qualidade do código, facilitam os testes de regressão e economizam tempo e recursos.

Quando executados de forma sistemática e consistente, os testes automatizados permitem que a equipe de desenvolvimento detecte erros de forma rápida e eficiente, possibilitando que sejam corrigidos antes que se tornem problemas maiores e mais difíceis de solucionar. Além disso, a execução de forma automatizada acelera o desenvolvimento e aumenta a qualidade do código, já que garante que ele seja testado de forma mais completa e consistente.

Os testes automatizados também facilitam a execução de testes de regressão, que verificam se as alterações realizadas no código afetaram outras partes do software. Dessa forma, é possível evitar problemas decorrentes de mudanças não intencionais, aumentando a confiabilidade do software.

→ Padrões de desenvolvimento

A importância na adoção dos padrões de desenvolvimento de software, se dá no fato das equipes poderem garantir que seus projetos sejam desenvolvidos de maneira consistente, eficiente e de alta qualidade.

Devido ao modelo de desenvolvimento adotado no projeto, é importante utilizar a prática da integração contínua. Ela garante a integração frequente de alterações de código em um repositório central, seguida de compilação automatizada, testes automatizados e análise de código para detectar problemas o

mais cedo possível no processo de desenvolvimento. Por isso o projeto passou a adotar algumas práticas:

1. **Utilização de repositório de código compartilhado:** Uma das práticas mais importantes para a integração contínua é o uso de um repositório de código compartilhado, como o GIT, que permita a integração frequente de alterações de código.
2. **Criação de *pipeline* de integração contínua:** Um pipeline de integração contínua é uma série de etapas automatizadas que executam tarefas como compilação, testes e análise de código. Essas etapas devem ser executadas automaticamente após cada integração de código no repositório.
3. **Início dos estudos para testes automatizados:** Testes automatizados são essenciais para a integração contínua, por ajudarem a detectar problemas o mais cedo possível no processo de desenvolvimento. Utilize ferramentas de teste automatizado para executar testes de unidade, testes de integração e testes de aceitação.
4. **Início dos estudos para análise do código de forma automática:** Estudos de ferramentas de análise estática de código e detecção de problemas de qualidade no desenvolvimento, como violações de padrões de codificação, vulnerabilidades de segurança e potenciais bugs.
5. **Implementação da cultura *DevOps*:** A integração contínua é uma prática fundamental da cultura DevOps, que visa promover a colaboração entre equipes de desenvolvimento e operações para garantir uma entrega de software rápida e confiável. O projeto possibilita que as equipes de desenvolvimento e operações trabalhem em conjunto para implementar uma estratégia de integração contínua eficaz.

→ MVC (Model, View e Controller)

O projeto incorporou também o padrão MVC para desenvolvimento do *Barrapress*. Essa arquitetura de *software* que divide uma aplicação em três

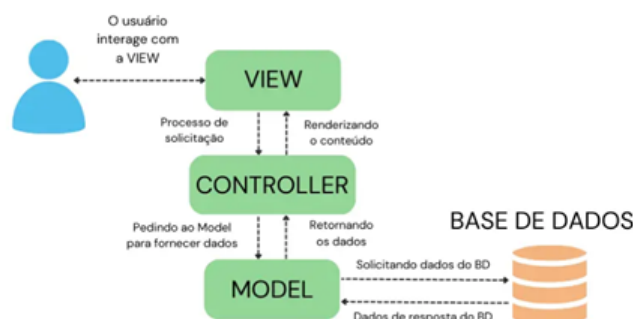
componentes principais: *Model* (Modelo), *View* (Visualização) e *Controller* (Controlador). O objetivo do padrão MVC é separar as preocupações de apresentação, processamento e armazenamento de dados em módulos independentes, facilitando a manutenção e evolução do *software*.

- O Modelo (*Model*) representa os dados e a lógica de negócio da aplicação. Ele é responsável por acessar e manipular os dados armazenados, além de fornecer métodos para que a camada de controle possa acessar e modificar esses dados. Em geral, o Modelo é representado por classes que encapsulam a lógica de negócio da aplicação.
- A Visualização (*View*) é responsável pela apresentação dos dados ao usuário. Ela é composta por uma interface gráfica que exibe os dados do Modelo e permite que o usuário interaja com a aplicação. A camada de Visualização não deve ter acesso direto ao Modelo, e sim através do Controlador.
- O Controlador (*Controller*) atua como um intermediário entre a camada de Modelo e de Visualização. Ele recebe as entradas do usuário pela camada de Visualização, e as usa para atualizar o Modelo e alterar a aparência da Visualização. Ele é responsável por coordenar as ações da aplicação e garantir que a lógica de negócio seja respeitada.

O padrão MVC permite que a camada de Visualização seja alterada sem afetar o Modelo, pois a comunicação entre eles é realizada através do Controlador. Da mesma forma, é possível modificar a lógica de negócio da aplicação sem afetar a interface gráfica, pois a comunicação entre o Modelo e o Controlador é realizada por meio de interfaces bem definidas. Isso torna a aplicação mais modular e flexível, facilitando a manutenção e evolução do *software*.

Figura 17 - Organização do modelo MVC.

Organização: Modelo MVC (Model-View-Controller)



Fonte: Da pesquisa (2023).

→ Padrão de Projeto: *Adapter*

As classes e métodos, em sua maioria, são desenvolvidas para poderem ser utilizadas mais de uma vez, onde é feito o reaproveitamento do código e a sua adaptação para diferentes funcionalidades.

Figura 18 - Reaproveitamento de código para diferentes funcionalidades.

```

if (tipo=='verificaAIP'):
    params['url']=f'{url}:{p.port}/api/transfer/status/{parametros}'
    r = requests.get(**params)

elif (tipo=='verificaDIP'):
    params['url']=f'{url}:{p.port}/api/ingest/status/{parametros}/'
    r = requests.get(**params)

elif (tipo=='Envio'):
    params['url']=f'{url}:{p.port}/api/v2beta/package/'
    params['data']=parametros
    r = requests.post(**params)
    return r.json()
  
```

Fonte: Da pesquisa (2023).

→ ORM (*Object-Relational Mappers*)

O Hipátia trabalha com o modelo ORM, onde existe um mapeamento das tabelas e colunas do banco de dados relacional para o *python*, através do *framework* *Peewee*.

Figura 19 - Mapeamento de tabelas e colunas através do *framework* *Peewee*.

```
1 from __init__ import *
2 from MySQLModel import baseSQL
3 from Sistemas import Sistemas
4
5 class Archivematica(baseSQL):
6     class Meta:
7         db_table='archivematica'
8         identificador=pw.IntegerField(primary_key=True,db_column='id')
9         id_sistemas = pw.ForeignKeyField(Sistemas,to_field='identificador',backref='id_sistema_archivematica',db_column='id_sistema')
10        server = pw.CharField()
11        port = pw.CharField()
12        user_db = pw.CharField()
13        api_key = pw.CharField()
14        folder_uuid = pw.CharField()
15        package_type = pw.CharField()
16        auto_approve = pw.CharField()
```

Fonte: Da pesquisa (2023).

→ Variáveis de ambiente

Para maior segurança, os dados sensíveis foram inseridos diretamente no banco de dados para acesso através do ORM ou em arquivo oculto “.env”, o qual está relacionado às variáveis de ambiente.

Figura 20 - Inserção de dados sensíveis através de arquivo “.env”.

```
barramento >  .env
1 DB_HOST='192.168.100.112'
2 DB_PORT='3306'
3 DB_USER='usuario'
4 DB_PASSWORD='123456'
5 DB_NAME='hipatia'
6 SISTEMA='1'
7 DIR_BASE='/workspaces/bar/barramento'
8 DIR_BAGIT='/workspaces/bar/barramento/documentos'
```

Fonte: Da pesquisa (2023).

→ Definição para testes automatizados

A equipe de desenvolvimento tem analisado diversas soluções para aplicação de testes automatizados, uma delas é o *Pytest*. Ele é uma estrutura de ações que suporta testes unitários, de integração e de sistema em Python. Ele tem se mostrado fácil de usar e tem sintaxe simples e intuitiva. O *Pytest* também possui vários recursos avançados, como cobertura de código, parametrização, testes paralelos, entre outros.

A equipe está estudando a implantação dessa estrutura no orquestrador *Openshift* seguindo alguns passos básicos. Primeiramente, deve-se criar um novo projeto *OpenShift* para o aplicativo desejado, e em seguida, criar um novo aplicativo *Python* dentro do projeto *OpenShift*. Adicionar o *Pytest* como uma dependência do aplicativo e criar um arquivo *pytest.ini* para configurar as opções do *Pytest* também são passos necessários.

O próximo passo é criar um arquivo *Dockerfile* na raiz do repositório Git que contém o código-fonte do aplicativo. Este arquivo é usado para construir uma imagem *Docker* do aplicativo que inclua o *Pytest* e outras dependências necessárias. Deve-se fazer o push do código-fonte e do *Dockerfile* para o repositório Git, e então criar uma nova imagem Docker do aplicativo usando o comando “*oc new-build*”.

O aplicativo deve ser implantado no OpenShift usando o comando “*oc new-app*”, e então deve-se configurar o OpenShift para executar os testes automaticamente sempre que houver uma alteração no código-fonte. Para fazer isso, deve-se criar um novo objeto *CronJob* no OpenShift usando o comando “*oc create cronjob*”.

Dessa forma, sempre que houver uma alteração no código-fonte do aplicativo, o *OpenShift* irá construir automaticamente uma nova imagem *Docker*, implantar o aplicativo e executar os testes do *Pytest* para garantir que tudo esteja funcionando corretamente. Caso haja algum problema, o *OpenShift* irá notificar o responsável por e-mail ou *Slack* para poder corrigi-lo rapidamente.

Em resumo, a proposta de testes automatizados está estruturada da seguinte forma:

1. Criar um novo projeto *OpenShift* para o aplicativo desejado;
2. Criar um novo aplicativo *Python* no projeto *OpenShift*;
3. Adicionar o *Pytest* como uma dependência do aplicativo;
4. Criar um arquivo *pytest.ini* para configurar as opções do *Pytest*;
5. Criar um arquivo *Dockerfile* na raiz do repositório Git que contém o código-fonte do aplicativo;
6. Fazer o push do código-fonte e do *Dockerfile* para o repositório Git;
7. Criar uma nova imagem Docker do aplicativo usando o comando `oc new-build`;
8. Implantar o aplicativo no *OpenShift* usando o comando `oc new-app`;
9. Configurar o *OpenShift* para executar os testes automaticamente sempre que houver uma alteração no código-fonte;
10. Criar um novo objeto *CronJob* no *OpenShift* usando o comando `oc create cronjob`.

A pesquisa para atualização do Hipátia está mesclando esses conceitos para aprimorar sua flexibilidade na comunicação com os sistemas geradores, permitindo a reutilização do código conforme a demanda e necessidade das instituições.

3.5 Meta 3: Estudo para implantação de barramento RDC-Arq

Inicialmente essa etapa previa o levantamento de requisitos informacionais para implantação do modelo *OnDemand*, propondo uma arquitetura informacional para suporte a chamadas *OnDemand*. Previa também o estudo e implementação da descrição da tipologia documental a partir de códigos disponibilizados pelo MNI, ou outro serviço de fornecimento de dados, aplicada ao PJe para endereçamento dos pacotes na árvore de arranjo do ambiente de acesso AtoM.

O Termo Aditivo 02 do TED 001/2020 formalizou a alteração de escopo da meta 3 com o objetivo de tornar as aplicações da solução RDC-Arq desacopladas,

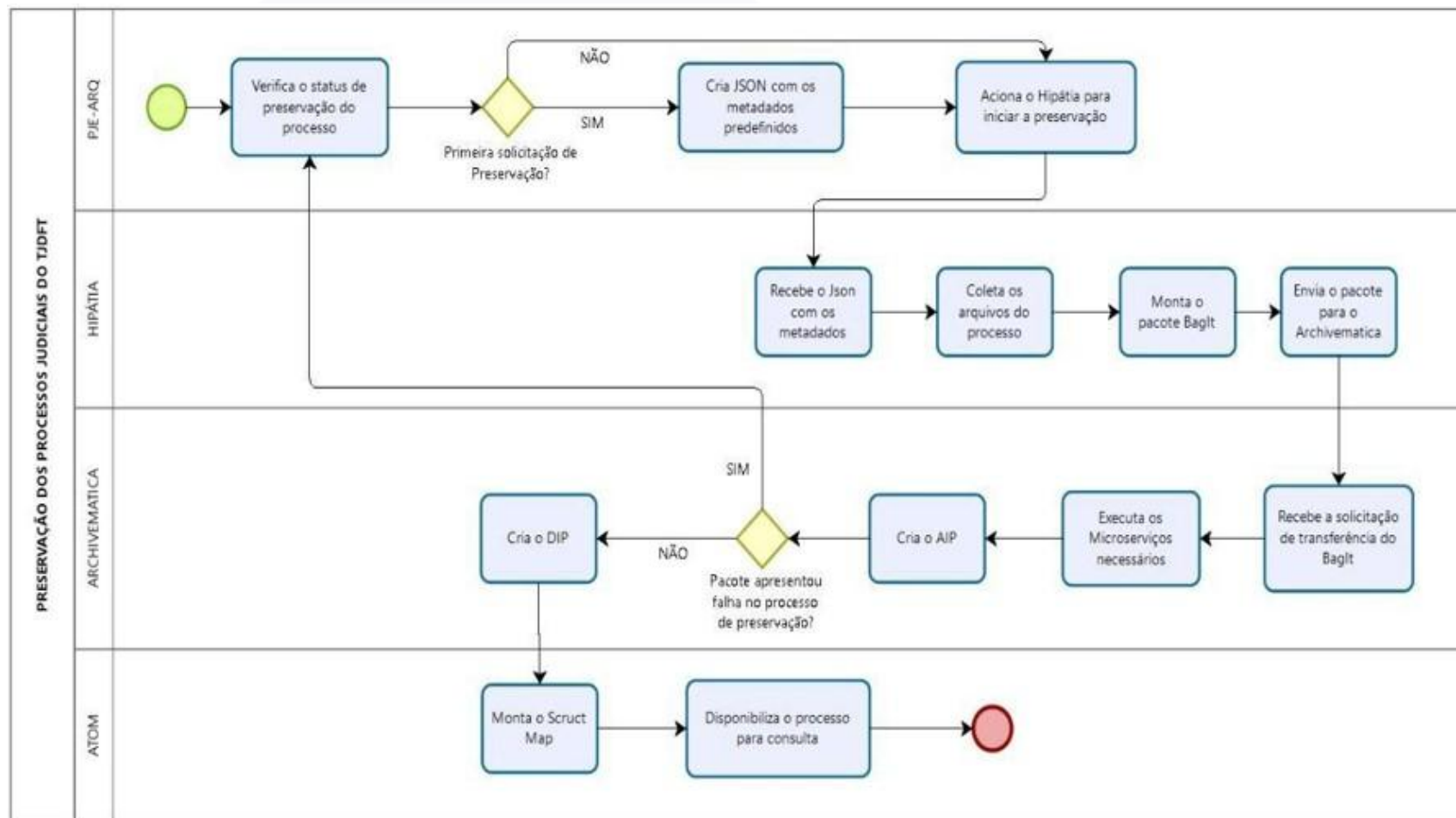
em conformidade com as diretrizes da Plataforma Digital do Poder Judiciário – PDPJ-Br, e utilizar a arquitetura baseada em eventos para comunicação e troca de informações

3.5.1 Estudo para implantação de barramento RDC-Arq orientado a eventos

Havia o planejamento de uma solução para que o barramento Hipátia fosse *OnDemand*, isto é, acionado de acordo com a demanda de preservação por intermédio de algum comando dentro da aplicação PJE-Arq, conforme apresentado na Figura 21.

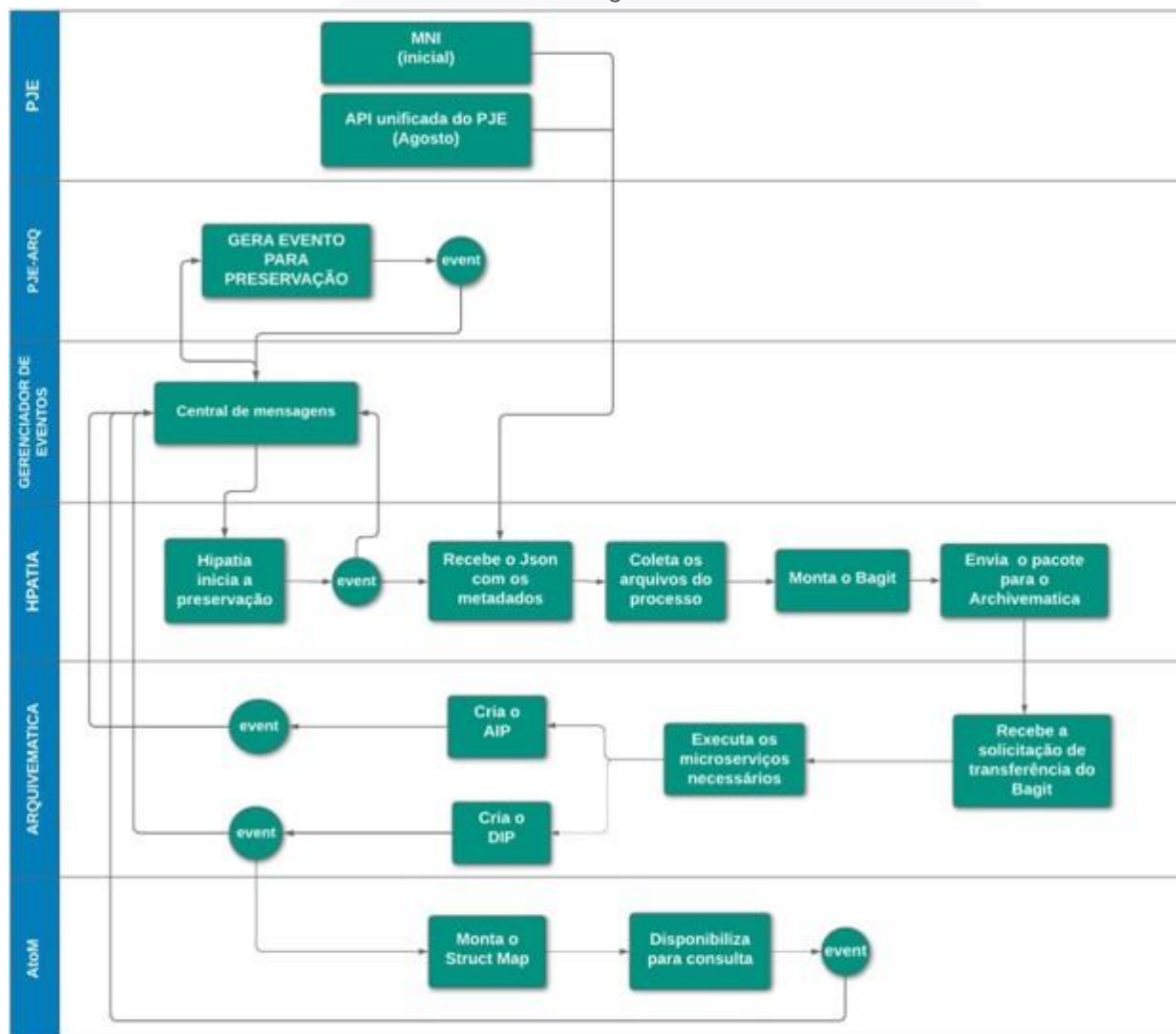
Entretanto, em reuniões para alinhamento da solução de integração PJE-Arq e Hipátia, foi apresentado o conceito de arquitetura baseada em eventos que o TJDFT vem adotando no desenvolvimento de suas aplicações. Nesse método, as aplicações não ficam acopladas aguardando os comandos, mas ligadas a um serviço de “mensageria” que alerta sobre eventos disponíveis nas diversas aplicações e inicia os processos específicos de cada um. Esse fluxo está apresentado na Figura 22 e mostra o novo conceito de execução baseada em eventos com o objetivo de alinhar as ações de cada equipe dentro da arquitetura da solução RDC-Arq.

Figura 21- Modelo de fluxo de processos para Hipátia PJE com ênfase no acionamento do *OnDemand*.



Fonte: Elaborada pelos autores (2021).

Figura 22 - Modelo de fluxo de processos para Hipátia PJE com a comunicação entre o Hipátia e a mensageria.



Fonte: Elaboração dos autores (2021).

Nesta versão ficam entendidas as comunicações com o sistema de mensageria e como o Hipátia recuperará as informações a partir dos eventos e quando ele irá gerar eventos para a infraestrutura.

→ Atividade executadas

- Reunião com a equipe para entendimento dos conceitos;
- Proposta inicial: Hipátia acionado *on-demand*;
- Sugestão para manter o Hipátia ativo com coleta agendada;
- Mudança no escopo: Arquitetura orientada a eventos;
 - Aprimoramento para estrutura de mensagens;
 - Foco na escalabilidade.

3.5.1.1 Estudo para integração com o serviço de mensageria Kafka

O *Apache Kafka* é um sistema de mensageria utilizado para processar informações oriundas de várias fontes, de maneira assíncrona, e disponibilizar esses dados para os diversos consumidores integrados a plataforma. De maneira simples, para que seja implantada uma estrutura onde aplicações se comunicam entre si através de trocas de mensagens ou, como a nomenclatura mais disseminada determina, eventos, é necessário a definição de três atores primordiais:

- **Broker:** Recebe os eventos dos produtores e as disponibiliza para os consumidores, funciona como uma espécie de central, pode ser configurado para atender diferentes necessidades nos mais variados casos, como por exemplo, garantir um armazenamento de eventos mais prolongado, ou até mesmo ser implantado em um ambiente “clusterizado”, visando uma melhor performance e garantindo a alta disponibilidade;
- **Consumer:** Consome os eventos armazenados no servidor do *Kafka*;
- **Producer:** Envia eventos para o servidor do *Kafka*.

Após a definição do papel de cada aplicação no decorrer do fluxo de execução do sistema é necessária a criação dos tópicos, que funcionam como agrupadores dos eventos, facilitando assim o consumo dos itens. Todo evento produzido é agrupado sob algum dos diversos tópicos que são criados no servidor do *Kafka*.

3.5.1.1.1 Integração com o Hipátia

Conforme definido no fluxo do processo de integração entre o PJE-ARQ e o Hipátia, o segundo se comportará como consumidor no início do fluxo, quando o processo for disponibilizado pelo PJE, e então passará a exercer o papel de produtor

de eventos, nas etapas subsequentes. Para facilitar o entendimento foi ilustrado como seria essa troca de mensagens nas imagens a seguir.

Figura 23 - Exemplo de tópicos criados no servidor.

```
raul@DESKTOP-IAGB5P3:/usr/local/kafka$ bin/kafka-topics.sh --list --bootstrap-server localhost:9092
HPT_AIP_CRIADO
HPT_START_EXECUCAO
HPT_STRUCT_MAP_CRIADO
PJE_NOVO_PROCESSO
```

Fonte: Da pesquisa (2021).

Figura 24 - Processo disponibilizado no PJE.

```
raul@DESKTOP-IAGB5P3:/usr/local/kafka$ bin/kafka-console-consumer.sh --bootstrap-server localhost:9092
--topic PJE_NOVO_PROCESSO --from-beginning
processo0008227000026201923,13072021
```

Fonte: Da pesquisa (2021).

Figura 25 - Exemplo nº do processo e data do arquivamento. Início de uma execução do Hipátia.

```
raul@DESKTOP-IAGB5P3:/usr/local/kafka$ bin/kafka-console-producer.sh --broker-list localhost:9092
--topic HPT_START_EXECUCAO
>0008227000026201923,534
```

Fonte: Da pesquisa (2021).

Figura 26 - Criação do AIP pelo Archivematica.

```
raul@DESKTOP-IAGB5P3:/usr/local/kafka$ bin/kafka-console-producer.sh --broker-list localhost:9092
--topic HPT_AIP_CRIADO
>0008227000026201923,534,809e18eb-74a9-436b-b200-c07c54126693
>
```

Fonte: Da pesquisa (2021).

Figura 27 - Exemplo nº de processo, id do processo e *hash* do arquivo. Criação do *Struct Map* e disponibilização do processo no AtoM.

```
raul@DESKTOP-IAGB5P3:/usr/local/kafka$ bin/kafka-console-producer.sh --broker-list localhost:9092
--topic HPT_STRUCT_MAP_CRIADO
>0008227000026201923,534
```

Fonte: Da pesquisa (2021).

O formato e conteúdo das mensagens são utilizadas para exemplificação, assim, podem ter mais ou menos conteúdo. Assim, para que seja integrado o barramento com o sistema de mensageria, deve ser implementado no código do barramento o sistema de consumo e produção de eventos, bem como as configurações de conexão (URL do servidor de broker e os tópicos).

3.5.2 Estudos para implantação de banco de dados no barramento Hipátia para gerenciamento dos dados de acesso aos sistemas

A informação é um dos bens mais valiosos das instituições, ela pode representar uma vantagem competitiva, ou se mal utilizada, ou mal protegida, tornar-se fonte de vulnerabilidade.

Essa necessidade de proteção, fica ainda mais evidenciada quando se trata dos dados de acessos aos sistemas dentro de um *RDC-Arq*. Por esse motivo e atendendo as recomendações do Guia de Boas Práticas de Desenvolvimento do TJDF, foi iniciado o estudo para implantação de um banco de dados para gerenciar alguns dos dados mais importantes para o bom funcionamento da aplicação.

O SGBD (Sistema Gerenciador de Banco de Dados) escolhido é o *MySQL*, por já ser o banco de dados usado no Archivematica, facilitando assim o processo de definição, construção, manipulação e compartilhamento do banco de dados e as aplicações.

Abaixo estão descritas as definições das tabelas e campos que serão utilizados na construção da nova versão do barramento Hipátia.

3.5.2.1 Definição das tabelas do Hipátia (*MySQL* versão 5.7 com *SSL*)

→ TABELA - Sistemas (SEI, PJE, DJE, AtoM, etc.)

- ID
- SIGLA_SISTEMA
- NOME_SISTEMA (DESCRIÇÃO)
- DRIVER_BANCO
- URL_ACESSO
- DATABASE
- USER
- PASSWORD a definir o tipo de criptografia)

- PORTA
- SISTEMA_NEGOCIO (!- TRUE/FALSE)
- QTE_ENVIO_SEQUENCIAL

→ **TABELA - WEBSERVICES_SISTEMAS**

- ID
- SIGLA_SISTEMA
- DESCRICAO (MNI, PJE-ARQ, ATOM, ARCHIVEMATICA, SEI)
- URL_WEBSERVICE

→ **TABELA - PARAMETROS**

- ID
- ID_WEBSERVICE_SISTEMAS
- CHAVE
- VALOR TABELA - ENVIADOS
- ID
- UUID (Archivematica)
- STATUS_AIP: (0-sucesso, 1-processando, 2-erro)
- STATUS_DIP: (a definir quais status)
- ID_PROCESSO
- N_PROCESSO
- ID_SISTEMA (sistema produtor)
- DESTINACAO
- DESCRICAO
- TIPO_PROCESSUAL
- FAILED/ERROS (ARCHIVEMATICA)
- TENTATIVAS (DE ENVIO)
- DATA_ENVIO (date_time)
- DATA_CONCLUSAO (date_time)

→ **TABELA - LISTA_PROCESSOS_MANUAIS**

- ID
- ID_SISTEMA
- ID_PROCESSO
- N_PROCESSO
- STATUS (0 - processado, 1-nao_processado (default))
- DATA (date_time)

→ **TABELA - LOGS_CONSULTAS**

- ID
- ID_ENVIADOS
- ID_SISTEMA
- ID_PROCESSO
- N_PROCESSO
- CONTEUDO (RETORNO DA CONSULTA)
- CONSULTA_ENVIADA
- DATA (date_time)

→ **TABELA - LOGS_GERAL**

- ID
- ID_SISTEMA
- ID_ENVIADOS
- CONTEUDO (payload-kafka (envio, recebimento), url de envio do Archivematica (pipeline), url de envio para o AtoM)
- TIPO (consumer_kafka, producer_kafka, envio_Archivematica, envio_AtoM)
- DATA (date_time)

→ **TABELA - Processing_configuration (gera XML com regras por tipo de documento)**

- ID
- ID_SISTEMA
- CLASSIFICACAO

- ARQUIVO_XML (? arquivo ou via api)
- STATUS (ativo ou inativo)

→ **TABELA - SLUG_ATOM**

- ID
- ID_SISTEMA
- CODIGO_CLASSIFICACAO (*solicitar ao sistema produtor)
- SLUG
- SLUG_DEFAULT (sim ou não)
- STATUS (ativo ou inativo)

3.5.3 Desenvolvimento do “Barrapres Gestão”

No âmbito do modelo de preservação Hipátia, foi desenvolvido um sistema para gerenciar as conexões entre os diferentes softwares que compõem o ecossistema. Esse sistema desempenha um papel fundamental na integração dos sistemas produtores, do Barramento, do Archivematica e do AtoM, garantindo a fluidez e eficiência das operações de preservação digital.

A criação desse sistema de gerenciamento de conexões envolveu a análise minuciosa dos requisitos de integração entre os sistemas. A equipe responsável conduziu estudos para entender as funcionalidades e a arquitetura de cada software envolvido, a fim de estabelecer as conexões apropriadas.

Em primeiro lugar, foi necessário definir os fluxos de comunicação entre os sistemas. Foram identificadas as principais interações e trocas de informações necessárias para o processo de preservação digital, levando em consideração os requisitos de cada etapa do fluxo de trabalho.

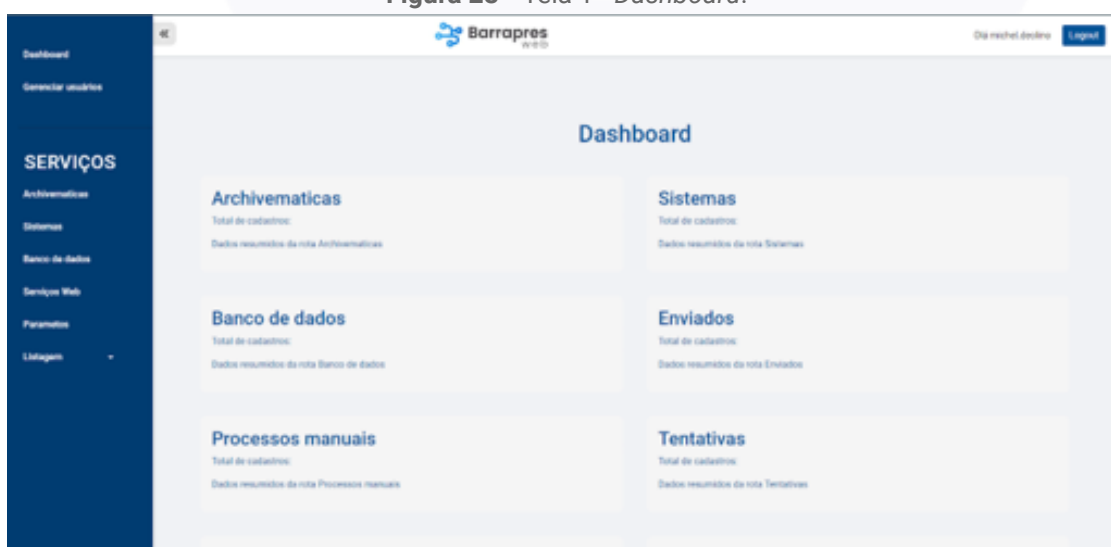
Com base nessas informações, o sistema de gerenciamento de conexões foi projetado e implementado. Esse sistema atua como uma camada intermediária entre os diferentes softwares, facilitando a comunicação e a troca de dados entre eles. Ele gerencia as conexões, estabelecendo canais de comunicação seguros e confiáveis.

A criação desse sistema, uma integração eficiente e harmoniosa entre os sistemas do TJDF, o Barramento, o Archivematica e o AtoM no contexto do modelo de preservação Hipátia. Ele permitiu que as rotinas de configuração das conexões fossem feitas, a partir de uma interface web, de forma mais segura.

Em resumo, o desenvolvimento do sistema de gerenciamento de conexões foi uma iniciativa crucial para estabelecer uma integração eficiente entre os sistemas, para facilitar a comunicação dentro do *RDC-Arq*.

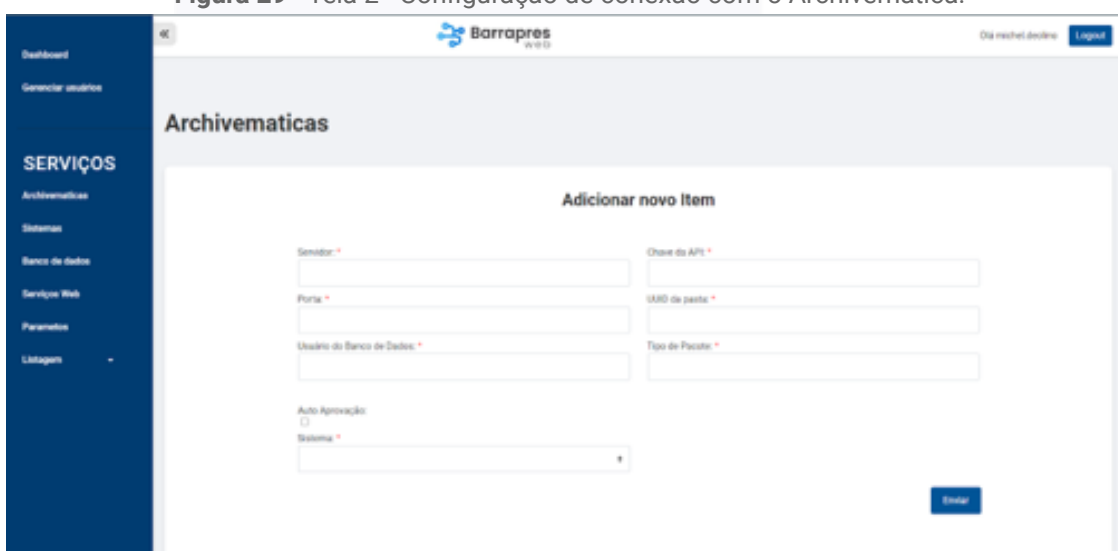
Telas do sistema desenvolvido

Figura 28 - Tela 1 - Dashboard.



Fonte: Da pesquisa (2022).

Figura 29 - Tela 2 - Configuração de conexão com o Archivematica.



Fonte: Da pesquisa (2022).

Figura 30 - Tela 3 - Configuração de conexão com o banco de dados.

Banco de dados

Adicionar novo Item

Driver *

URL *

Banco de Dados *

Sistema *

Usuário *

Senha *

Porta *

Mostrar senha

Enviar

Fonte: Da pesquisa (2022).

Figura 31 - Tela 4 - Configuração de parâmetros.

Parametros

Adicionar novo Item

Key *

Valor *

Serviço Web *

Enviar

Lista de Itens

ID	Chave	Valor	Serviço Web	Editar	Excluir
6	teste 2	221232	172.252.57.195:20000		

Fonte: Da pesquisa (2022).

Figura 32 - Tela 5 - Visualização dos processos.

Processos Manuais

Lista de Itens

ID	Código do processo	Número do processo	Status	Informações adicionais	Data de inclusão	Sistema	Editar	Excluir
1	067654	99999	Enviado	Teste add	12/01/2023	SIS teste		

Fonte: Da pesquisa (2021).

Figura 33 - Tela 6 - Configuração de serviços web.

Serviços Web

Adicionar novo Item

URL: Descrição: Sistema:

Lista de Itens

ID	URL	Descrição	Sistema	Editar	Excluir
3	173.252.57.109:20000	teste	Teste Serviço 2		

Fonte: Da pesquisa (2021).

3.5.4 Estudos dos metadados RDC-Arq do PJE

Metadados são dados que carregam informações sobre outros dados, eles reúnem informações estruturadas que descrevem e identificam dados, auxiliando no gerenciamento, localização e preservação da informação classificada.

3.5.5 Tipos de metadados

Existem 3 tipos principais de metadados (RILEY, 2017, p. 6, tradução nossa):

- **Metadados descritivos:** descrevem um recurso com o propósito, por exemplo, de descoberta ou identificação. Isso pode incluir elementos como título, resumo, autor e palavras-chave.
- **Metadados estruturais:** indicam como objetos compostos são colocados juntos, por exemplo, como é que páginas são ordenadas para formar capítulos.
- **Metadados administrativos:** fornecem informações para auxiliar no gerenciamento de um recurso, como por exemplo, quando e como ele foi criado, tipo de arquivo e outras informações técnicas, e sobre quem tem acesso a ele. Existem vários subconjuntos de dados administrativos; dois deles, às vezes, são listados separadamente como tipos metadados:
 - **Metadados para gerenciamento de direitos**, que tratam dos direitos de propriedade intelectual, e
 - **Metadados para preservação**, que contêm informações necessárias ao arquivamento e à preservação de um determinado recurso.

Para este projeto foram definidos e pesquisados os metadados necessários para a preservação dos processos judiciais no sistema PJE, bem como os metadados descritivos Dublin Core³ e ISAD(G)⁴.

³ Disponível em: <https://dublincore.org/>.

⁴ Disponível em: https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/isad_g_2001.pdf.

3.6 Meta 4: Estudos para extração de conteúdos AtoM >> Sistema de Gestão Documental

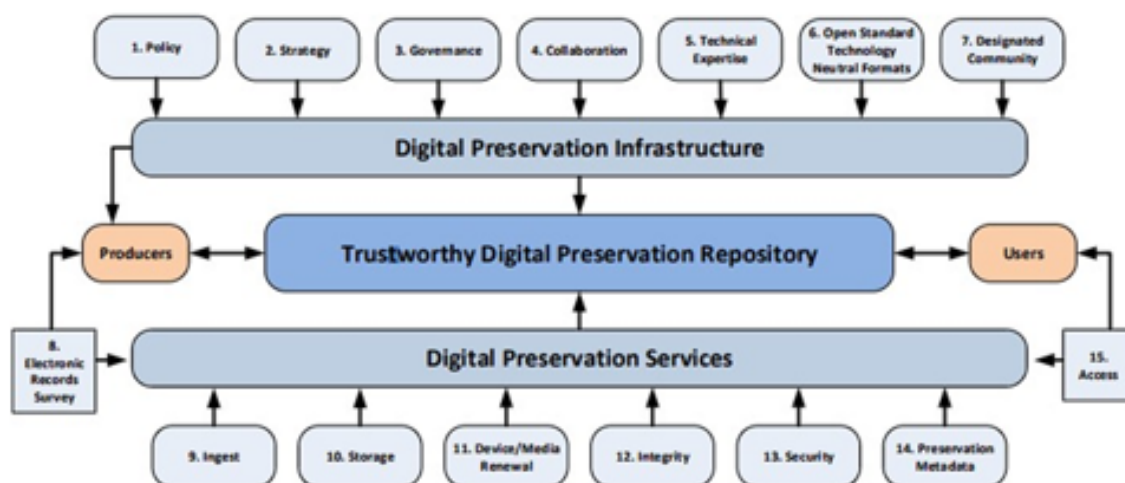
Os **Apêndices A, B, C, e D e E** apresentam os metadados levantados e validados pelas equipes de gestão da informação do Ibict e TJDFE em reuniões técnicas. E também os metadados do PJe - Arq validados em conjunto com a instituição.

3.7 Meta 5: Prova de Modelos

3.7.1 Diagnóstico de compliance da solução RDC Arq PJE com as normas arquivísticas, inclusive modelo OAIS

O DPCMM foi desenvolvido por Charles Dollar e Lori Ashley. Ele é baseado nos serviços e função identificados na ISO 14721 (OAIS) e nos atributos de auditoria e certificação de repositórios digitais confiáveis apresentados pela ISO 16363. Já que a preservação é efetuada pelos serviços dentro dos limites da infraestrutura, como podemos observar na figura a seguir:

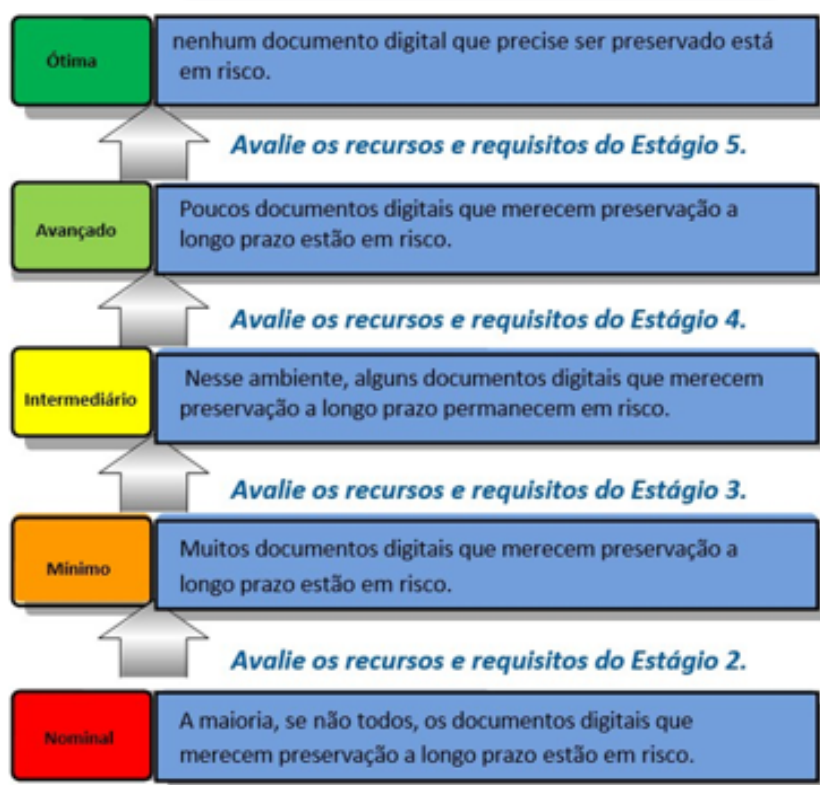
Figura 34 - Modelo de Maturidade da Capacidade de Preservação Digital.



Fonte: Da pesquisa (2021).

O modelo visa não só um modo de verificar o estágio de maturidade atual da instituição como também auxiliar no planejamento para a evolução de elementos com níveis de maturidade inferiores ao esperado. São cinco níveis ou estágios, baseados no ISO 3100:2009 de gestão de riscos, que variam de nominal a ótimo dependendo do risco de perdas decorrentes de problemas de preservação dos documentos digitais.

Figura 35 - Escala de Maturidade da Capacidade de Preservação Digital.



Fonte: Da pesquisa (2021).

A conformidade com as ISOs 14721 e 16363 se daria com o alcance do estágio intermediário (Estágio 3) conforme a escala de maturidade da figura 35, descritos pelo modelo como:

Quadro 3 - Descrição dos estágios de Maturidade da Capacidade de Preservação Digital.

	Estágio 5: Capacidade de preservação digital ideal O estágio 5 é o mais alto estágio de capacidade de prontidão de preservação digital que uma organização pode alcançar. Ele inclui um foco estratégico nos resultados de preservação digital, melhorando continuamente a maneira como o gerenciamento do ciclo de vida dos documentos digitais. A capacidade de preservação digital do estágio 5 também envolve o benchmarking de infraestrutura e serviços em relação a outros programas de preservação digital "melhores da categoria" e a realização de monitoramento proativo para tecnologias inovadoras que possam permitir que o programa melhore seu desempenho de preservação digital. Poucos ou nenhum documento digital que mereça preservação a longo prazo estão em risco.
--	--

	Estágio 4: Capacidade Avançada de Preservação Digital O estágio 4 é caracterizada por uma organização com uma infraestrutura robusta e serviços de preservação digital baseados nas especificações da ISO 14721 e no TRAC, o Repositório Confiável. Auditoria e Certificação: Critérios e Checklist e/ou ISO 16363. Nesta fase, a preservação dos documentos digitais é enquadrada inteiramente num ambiente colaborativo em que existem várias partes interessadas participantes. Os ensinamentos retirados deste quadro de colaboração servem de base para adaptar e melhorar as capacidades de identificar e integrar proativamente os documentos digitais a longo prazo em controle e gerenciamento do ciclo de vida. Alguns documentos digitais que merecem preservação a longo prazo ainda podem estar em risco.
	Estágio 3: Capacidade Intermediária de Preservação Digital O estágio 3 descreve um ambiente que abraça as especificações da ISO 14721 e outros padrões e esquemas de melhores práticas e, assim, estabelece a base para sustentar a preservação digital aprimorando suas capacidades ao longo do tempo. Essa base inclui a conclusão bem-sucedida de projetos e resultados repetíveis que suportam os recursos de preservação digital da instituição e promovem a colaboração, incluindo recursos compartilhados, entre as unidades produtoras e entidades responsáveis pela gestão e manutenção de repositórios digitais confiáveis. Nesse ambiente, muitos documentos digitais que merecem preservação a longo prazo provavelmente permanecerão em risco.
	Estágio 2: Capacidade mínima de preservação digital O estágio 2 descreve um ambiente onde um repositório de preservação baseado na ISO 14721 ainda não está em vigor. Algumas estratégias de preservação para os documentos digitais estão disponíveis para alguns produtores que satisfazem algumas, mas não todas, as especificações da ISO 14721. Há alguma compreensão das questões e estratégias de preservação digital, mas é limitada a relativamente poucos indivíduos. Pode não haver praticamente nenhuma relação entre o sucesso ou o fracasso de uma iniciativa de preservação digital e o sucesso ou fracasso de outra. O sucesso é em grande parte o resultado de ações excepcionais (talvez até heroicas) de um indivíduo ou de uma equipe de projeto. O conhecimento sobre tal sucesso não é amplamente compartilhado ou institucionalizado. A maioria dos documentos digitais que merecem preservação a longo prazo está em risco.
	Estágio 1: Capacidade nominal de preservação digital O Estágio 1 descreve um ambiente em que as especificações da ISO 14721 e de outras normas podem ser conhecidas e consideradas, mas não adotados ou implementados pela unidade responsável pela preservação ou por produtores. Geralmente, pode haver alguma compreensão das questões e preocupações de preservação digital, mas é provável que esse entendimento consista em práticas ad hoc de gerenciamento de documentos digitais, infraestruturas e iniciativas digitais contínuas. Embora possa haver alguns casos isolados de indivíduos tentando preservar os documentos digitais em uma rede ou mídia de armazenamento removível (por exemplo, DVD ou disco rígido), praticamente todos os documentos digitais que merecem preservação a longo prazo estão em risco.

Fonte: Elaborado pelos autores (2023).

São avaliados os 15 elementos apresentados na Figura 34, divididos em infraestrutura de preservação digital e serviços em preservação digital, a saber:

→ **Infraestrutura**

1. Política de Preservação Digital;
2. Estratégia de Preservação Digital;
3. Governança;
4. Colaboração;
5. Perícia Técnica;
6. Formatos *Open Standard Technology Neutral* ("OS/TN");
7. Comunidade designada; e
8. Pesquisa de Registros Eletrônicos.

→ Serviços

1. Admissão;
2. Área de Arquivamento (*Archival Storage*);
3. Renovação de mídia/dispositivo;
4. Integridade;
5. Segurança;
6. Metadados de preservação; e
7. Acesso.

Para cada um desses elementos é avaliado um dos 5 níveis de maturidade apresentados pelo modelo e imputada a pontuação de acordo com o nível definido. Após a somatória dos pontos da avaliação de cada um dos 15 elementos é definido o estágio de maturidade conforme tabela a seguir:

Quadro 4 - Avaliação dos níveis de Maturidade.

NÍVEIS DE CAPACIDADE		PONTUAÇÃO DO ÍNDICE
	Capacidade nominal de preservação digital	0
	Capacidade mínima de preservação digital	1-15
	Capacidade de preservação digital intermediária	16-30
	Capacidade avançada de preservação digital	31-45
	Capacidade de preservação digital ideal	46-60

Fonte: Elaborado pelos autores (2023).

O formulário foi preenchido pelo TJDFT e avaliado com o auxílio do Ibict. Vale salientar que esta primeira aplicação se deu em caráter experimental, já que um dos objetivos era avaliar o método em si.

O documento completo com os resultados estão no apêndice G deste relatório.

3.8 META 6: Transferência do Conhecimento

Os resultados da pesquisa foram amplamente disseminados em dois canais de comunicação com a comunidade de modo a repassar orientações sobre o uso do Hipátia.

A disseminação dos resultados da pesquisa é de suma importância em um projeto de pesquisa desenvolvido por um instituto público. Afinal, os atos da Administração Pública, como define a Constituição Federal em seu artigo 37, devem ser pautados pela publicidade. Além disso, a Lei de Acesso à Informação (Lei 12.527, de 2011) atribui aos órgãos de governo a responsabilidade de disseminação ativa de informações sobre sua gestão. Tais normativas e os princípios da Ciência Aberta definem a atuação do Ibict, que tem tradição na socialização do conhecimento científico e tecnológico.

3.8.1 Website

Foi criada uma página *web*, disponível em hipatia.ibict.br, que mostra informações relevantes do modelo de preservação digital para implementação de Repositórios Arquivísticos Digitais Confiáveis, conforme a Figura 36:

Figura 36 - Página inicial do portal Hipátia.



Fonte: Captura de tela da página inicial do portal Hipátia (2021).

Destacam-se a parceria com o TJDF e casos de uso do barramento. Para complementar a documentação do projeto, foram disponibilizadas três publicações em formatos de guia e manuais, elaboradas em outros projetos do IBICT que são:

- a) **Manual de instalação Hipátia:** O barramento Hipátia, é um programa que surgiu do projeto firmado com o TJDF, com a finalidade de automatizar o envio dos arquivos por parte do agente Produtor para o Repositório Digital Confiável Arquivístico (RDC-ARQ), proposto pelo Modelo OAIS de preservação digital. O seu funcionamento segue o padrão de se conectar ao sistema Produtor por meio de Banco de Dados ou *WebService*, extrair metadados e arquivos a serem preservados e criar o Pacote de Submissão de Informação (SIP), enviando para o RDC-ARQ⁵.

⁵ Disponível em: https://git.ibict.br/cgti/barrapres/_barramento/-/wikis/Manual-Hip%C3%A1tia.

- b) **Guia Archivemática**⁶: O guia é resultado de um trabalho coletivo e compartilhado entre todos os autores identificados nesta obra, desenvolvido pela tradução, interpretação, ou adequação terminológica ou revisão ou mesmo adequação do referencial do Archivemática aos referenciais do Conselho Nacional de Arquivos no tocante aos Repositórios Arquivísticos Digitais Confiáveis, os RDC-Arq. É uma primeira aproximação na questão de adequar a terminologia aos referenciais introduzidos pelos Repositórios Digitais, na medida em que esse software foi selecionado para apoiar esse projeto. Igualmente apoia outras instituições que aderem ao uso do Archivemática para o desenvolvimento de repositórios arquivísticos digitais confiáveis, com documentação técnica em português.
- c) **Guia AtoM**⁷: O guia se baseia na documentação oficial do AtoM, versão 2.2 abrangendo não apenas a operacionalização da ferramenta, mas contando com informações voltadas à equipe de tecnologia. Com isso, procura atender a todos os envolvidos na instalação, manutenção, aperfeiçoamento, administração e operação, na medida em que a relação entre a equipe de informática e o arquivo requer estar afinada para o uso eficaz da ferramenta.

Como forma de divulgação, duas apresentações foram realizadas virtualmente:

⁶ COSTA, Milene *et al.* **Guia do usuário Archivemática**. Brasília, DF: Instituto Brasileiro de Informação em Ciência e Tecnologia, 2016. 136 p. DOI: 10.18225/978-85-7013-122-5. Disponível em: <http://livroaberto.ibict.br/handle/123456789/1063>. Acesso em: 25 jul. 2023.

⁷ ABREU, Jorge Phelipe Lira de; CASTRO, Priscila de Paiva; SHINTAKU, Milton; SANTAREM SEGUNDO, José Eduardo. **Guia de usuário do AtoM**. Brasília, DF: Ibict, 2017. 164 p. Disponível em: <https://livroaberto.ibict.br/handle/123456789/1065>. Acesso em: 25 jul. 2023.



WEBINAR Preservação digital: o case do TJDF na implementação do RDC-Arq. 2020. 1 vídeo (2 horas e 22 minutos). Publicado pelo canal TJDFTofficial. Disponível em: <https://www.youtube.com/watch?v=kWKDIwQbk1k>. Acesso em: 25 jul. 2023.



O PAPEL da preservação em uma sociedade digital. 2020. 1 vídeo (1 hora e 52 minutos). Publicado pelo canal Instituto Brasileiro de Informação em Ciência e Tecnologia. Disponível em: <https://www.youtube.com/watch?v=00NJggHzJbs>. Acesso em: 25 jul. 2023.

3.8.2 Fórum de discussão

No âmbito da Web, a colaboração de usuários é cada vez mais presente. Um local adequado para essa interatividade é o fórum de discussão que também está contemplado nesta etapa do projeto.

Figura 37- Página inicial do Fórum do Ibict tópicos Hipátia.



Fonte: Captura de tela do tópico Hipátia no Fórum do Ibict (2021).

A Figura apresenta o Fórum de Discussão disponível no website que se destina a coletar insights, sugestões e críticas. Essa ferramenta está aberta a toda comunidade e se alinha às boas práticas do serviço público possibilitando a publicidade e a interação com os usuários.

3.8.3 Workshop de repasse tecnológico

O Workshop Técnico para fins de repasse tecnológico foi realizado conforme o quadro 5.

Quadro 5 - Workshop Técnico.

DATA	TEMA
03/05/2023	RDC - Arq: Conceitos arquivísticos
04/05/2023	RDC - Arq: Tecnologias usadas
05/05/2023	RDC - Arq: Ambiente de preservação em Openshift
10/05/2023	RDC - Arq: Código e configurações do sistema Barrapres,

Fonte: Elaboração dos autores (2023).

3.8.4 Publicações

Durante o período de execução do projeto foram feitas algumas publicações elencadas no quadro 6.

Quadro 6 - Publicações.

TÍTULO	TIPO DE PUBLICAÇÃO	LINK DE ACESSO
Os principais normativos relacionados ao RDC-Arq	Artigo	https://hipatia.ibict.br/publicacoes/os-principais-normativos-relacionados-ao-rdc-arq/?page=12&order=DESC&orderby=title&pos=1&source_list=collection&ref=%2Fpublicacoes
Hipátia: modelo de preservação para repositórios arquivísticos digitais confiáveis	Livro	http://labcotec.ibict.br/omp/index.php/edcotec/catalog/book/livrohipatia
A gestão dos formatos de preservação de arquivos no Archivematica: estudo de caso com o Processo Judicial Eletrônico	Artigo aceito para ser apresentado em evento	Aguardando publicação dos anais

Fonte: Elaboração dos autores (2023).

4 CONSIDERAÇÕES FINAIS

Este projeto elaborou um conjunto de propostas e vem realizando várias atividades que atendem a necessidade no TJDFR por melhorias e modernização na gestão documental aderente às melhores práticas nacionais e internacionais do mundo jurídico. Essas atividades foram pensadas e formuladas em conjunto com o Ibict que proveu sua expertise metodológica e científica na condução de projetos.

Nessa concepção, foram estabelecidos os objetivos específicos relacionados às entregas do projeto que se caracterizam como mapas que conduzem a equipe ao objetivo final e à entrega das atividades previstas. Assim, de forma a estabelecer explicitamente esses objetivos às entregas de trabalho, apresentamos o Quadro 7:

Quadro 7 - Objetivos Específicos X Entregas de Trabalho.

OBJETIVOS ESPECÍFICOS	ENTREGAS DE TRABALHO
Melhorar o desempenho e infraestrutura do barramento RDC-Arq	Estudos de infraestrutura para solução RDC-Arq Estudos dos metadados RDC-Arq do PJE
Disponibilizar novas formas de acesso ao RDC-Arq	Estudo para implantação de barramento RDC-Arq usando o modelo de mensageria

Fonte: Elaboração dos autores (2021).

O Quadro 5 mostra expressamente o andamento do projeto dado que as entregas estão relacionadas com o propósito inicial do projeto em que foram estabelecidos os objetivos específicos.

Portanto, a implantação do *software* Archivematica de acordo com o modelo de infraestrutura *DevOps*, no qual o TJDFR se embasa, foi realizada com sucesso. Os volumes foram definidos, os arquivos de configuração *DockerFile* e demais arquivos necessários estão versionados no repositório *GitLab*, as imagens *Docker* estão descritas no **gitlab-ci.yml** e a aplicação está sendo executada sem erros conforme as especificações do Termo de Referência.

De tal modo, neste documento, descrevemos as atividades desenvolvidas pelas equipes das duas instituições para a operacionalização do projeto. Implementar o Archivematica no ambiente *OpenShift* figurou como o maior desafio para o Ibict. A pesquisa pioneira servirá de base para outras instituições.

Também foi dada ênfase a pesquisa inicial para implantação de um ambiente Archivemática com dois pipelines. Uma forma mais eficaz de se implantar o sistema com múltiplos fluxos de trabalhos com diferentes regras de preservação. Ao se usar uma única instalação para trabalhar diferentes formas de gestão, otimiza-se recursos informacionais e humanos.

A programação orientada a eventos foi outro grande salto evolutivo no barramento Hipátia, de modo a não deixá-lo vinculado e dependente dos outros sistemas. Integrar em um ambiente de mensageria, permite que ele continue a coleta e comunicação com os outros softwares do *RDC-Arq*, mesmo que o sistema de origem esteja temporariamente inoperante.

Todas as inovações pesquisadas e aplicadas neste ano de 2021, permitiram que as recomendações de segurança descritas no Guia de Boas Práticas do TJDF, fossem avaliadas para que o ambiente Hipátia entre em conformidade com os itens apresentados e possa ser validado pela equipe responsável para entrar em produção.

O projeto evidencia a exitosa parceria entre o TJDF e o IBICT. Ambas instituições têm colaborado com a elaboração de ferramentas metodológicas e científicas para que as barreiras para implantação de um *RDC-Arq* sejam transpostas. Dessa maneira está sendo construído um modelo de Repositório Digital Confiável que poderá ser replicado em todos os Tribunais de Justiça e outras instituições interessadas.

BIBLIOGRAFIA CONSULTADA

ARCHIVEMATICA. [S. l.: s. n.], c2023. Disponível em: <https://www.archivematica.org/>. Acesso em: 24 set. 2021.

BACA, Murtha (ed.). **Introduction to Metadata**. 2. ed. Los Angeles, CA: The Getty Research Institute, 2008. Disponível em: <https://www.getty.edu/publications/resources/virtuallibrary/0892368969.pdf>. Acesso em: 24 set. 2021.

BRASIL. Conselho Nacional de Justiça. **Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Judiciário brasileiro** (MoReq-Jus). Brasília, DF: CNJ, 2009. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2011/01/manualmoreq.pdf>. Acesso em: 24 set. 2021.

BRASIL. Tribunal de Justiça do Distrito Federal e Territórios. **Relatório de gestão**. Brasília, DF: TJDF, 2020. https://www.tjdft.jus.br/transparencia/processo-de-contas-anual/rg-tcu-2020_final.pdf. Acesso em: 24 set. 2021.

BRASIL. Tribunal de Justiça do Distrito Federal e Territórios. **Relatório de gestão**. Brasília, DF: TJDF, 2019. Disponível em: https://www.tjdft.jus.br/institucional/governanca/governanca-e-gestao-estrategica/elatorio-de-gestao_tjdft.pdf. Acesso em: 24 set. 2021.

CONSELHO INTERNACIONAL DE ARQUIVOS (Conarq). **ISAD(G): Norma geral internacional de descrição arquivística: segunda edição**, adotada pelo Comitê de Normas de Descrição, Estocolmo, Suécia, 19-22 de setembro de 1999, versão final aprovada pelo CIA. 2. ed. Rio de Janeiro: Arquivo Nacional, 2000. Disponível em: https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/isad_g_2001.pdf. Acesso em: 24 set. 2021.

COSTA, Milene et al. **Guia do usuário Archivematica**. Brasília, DF: Instituto Brasileiro de Informação em Ciência e Tecnologia, 2016. 136 p. DOI: 10.18225/978-85-7013-122-5. Disponível em: <http://livroaberto.ibict.br/handle/123456789/1063>. Acesso em: 24 set. 2021.

DUBLIN CORE METADATA INITIATIVE. [S. l.: s. n.], [2023]. Disponível em: <https://dublincore.org/>. Acesso em: 24 jul. 2023.

FERRITER, MEGHAN. BagIt at the Library of Congress. **The Signal**. [United States of America], 4 apr. 2019. Disponível em: <https://blogs.loc.gov/thesignal/2019/04/bagit-at-the-library-of-congress/>. Acesso em: 24 set. 2021.

GAMMA, Erich et al. **Padrões de projetos**: soluções reutilizáveis de software orientado a objetos. Porto Alegre: Bookman, 2000.

GITLAB. GitLab CI/CD. [S.l.: s.n.], [201-]. Disponível em: <https://docs.gitlab.com/ee/ci/>. Acesso em: 24 set. 2021.

GOMES, Rafael. **Container versus máquina virtual**. iMasters. [S. l.], 24 fev. 2016. Disponível em: <https://imasters.com.br/devsecops/container-versus-maquina-virtual>. Acesso em: 24 set. 2021.

REDHAT. O que é DEVOps. [S. l.: s. n.], 2022. Disponível em: <https://www.redhat.com/pt-br/topics/devops>. Acesso em: 24 jul. 2023.

REDHAT. O que é Docker? [S. l.: s. n.], 2023a. Disponível em: <https://www.redhat.com/pt-br/topics/containers/what-is-docker>. Acesso em: 24 jul. 2023.

REDHAT. Introdução aos containers. [S. l.: s. n.], 2023b. Disponível em: <https://www.redhat.com/pt-br/topics/containers/what-is-kubernetes>. Acesso em: 24 jul. 2023.

RILEY, Jenn. **Understanding Metadata**: what is metadata, and what is it for? a primer. Bethesda, MD: NISO Press, 2017. Disponível em: https://groups.niso.org/apps/group_public/download.hp/17446/Understanding%20Metadata.pdf. Acesso em 24 set. 2021.

APÊNDICES

APÊNDICE A - Metadados de Gestão PJe (MoReq-Jus, e-Arq e Resolução nº 24 do conarq)

→ DADOS DO PROCESSO

- Número do Processo**

Descrição	Número do processo judicial, que deve estar de acordo com as regras definidas pela Resolução do CNJ nº 65, de 16 de dezembro de 2008.
Campo CSV	numeroProcesso
Campo WS	(nr_processo em core.tb_processo)
Exemplo	07196889620188070003

- Classe Processual - Código**

Descrição	Número identificador da classe processual, segundo o padrão estabelecido no Sistema de Gestão de Tabelas Processuais Unificadas ¹ . As classes estão disponíveis, de acordo com a configuração de classes para cada jurisdição.
Campo CSV	codigoClasseProcessual
Campo WS	(cd_classe_judicial em client.tb_classe_judicial)
Exemplo	6017

- Classe Processual - Nome**

Descrição	Descrição da classe processual, segundo o padrão estabelecido no Sistema de Gestão de Tabelas Processuais Unificadas ² . As classes estão disponíveis, de acordo com a configuração de classes para cada jurisdição.
Campo CSV	nomeClasseProcessual
Campo WS	(ds_classe_judicial em client.tb_classe_judicial)
Exemplo	Usucapião

- Código da Localidade da Jurisdição**

Descrição	Código da Localidade da Jurisdição
-----------	------------------------------------

Campo CSV	codigoDaLocalidade
Campo WS	(id_jurisdicao em client.tb_jurisdicao)
Exemplo	18

- **Nome da Localidade**

Descrição	Nome da Jurisdição.
Campo CSV	nomeDaLocalidade
Campo WS	(ds_jurisdicao em client.tb_jurisdicao)
Exemplo	Brasília - Fórum Des. Joaquim Sousa Neto

- **Identificador da Competência**

Descrição	Identificador da competência.
Campo CSV	idDaCompetencia
Campo WS	(id_competencia em client.tb_competencia)
Exemplo	4

- **Nome da Competência**

Descrição	Nome da competência.
Campo CSV	nomeDaCompetencia
Campo WS	(ds_competencia em client.tb_competencia)
Exemplo	Criminal

- **Processo Vinculado (São campos que se repetem)**

Descrição	Número do processo vinculado, no formato CNJ.
Campo CSV	processoVinculado
Campo WS	(tabela: client.tb_processo_trf_conexao)
Exemplo	0725943-26.2021.8.07.0016

- **Modalidade de vinculação de processo (São campos que se repetem)**

Descrição	Tipo de elemento destinado a permitir a identificação entre processos judiciais. As vinculações podem ser: 'AP' (apenso); 'AR' (ação rescisória); 'CD' (competência delegada); 'CT' (continência); 'CX' (conexão); 'DP' (dependência); 'OG' (originário); 'OR' (outro tipo de associação que não os anteriores); 'PU' (precedente de uniformização); 'RG' (repercussão geral); 'RR' (recurso repetitivo).
Campo CSV	modalidadeVinculacaoProcesso
Campo WS	(tp_tipo_conexao em client.tb_processo_trf_conexao)
Exemplo	Apenso

• Prioridade

Descrição	Elemento destinado a permitir a identificação da existência de prioridades processuais não óbvias, ou seja, aquelas que não são resultado direto da identificação da classe processual (ex.: habeas corpus ou mandado de segurança). Na versão 2.0, será texto livre, mas é recomendável utilizar os seguintes textos identificadores: "IDOSO" "RÉU PRESO" "PERECIMENTO" "MENOR"
Campo CSV	prioridade
Campo WS	(ds_prioridade em client.tb_prioridade_processo)
Exemplo	Idoso

• Valor da causa

Descrição	Valor da relação jurídica. Não usar caracteres especiais, apenas números.
Campo CSV	valorDaCausa
Campo WS	(vl_causa em client.tb_processo_trf)
Exemplo	5.000,00

• Nível de Sigilo

Descrição	Nível de sigilo a ser aplicado ao processo. Dever-se-á utilizar os seguintes níveis: - 0: públicos, acessíveis a todos os servidores do Judiciário e dos demais órgãos públicos de colaboração na administração da Justiça, assim como aos advogados e a qualquer cidadão - 1: segredo de justiça, acessíveis aos servidores do Judiciário, aos servidores dos órgãos públicos de colaboração na administração da Justiça e às partes do processo. - 2: sigilo mínimo, acessível aos servidores do Judiciário e aos demais órgãos públicos de colaboração na administração da Justiça - 3: sigilo médio, acessível aos servidores do órgão em que tramita o processo, à(s) parte(s) que provocou(ram) o incidente e àqueles que forem expressamente incluídos - 4: sigilo intenso, acessível a classes de servidores qualificados (magistrado, diretor de secretaria/escrivão, oficial de gabinete/assessor) do órgão em que tramita o processo, às partes que provocaram o incidente e àqueles que forem expressamente incluídos - 5: sigilo absoluto, acessível apenas ao magistrado do órgão em que tramita, aos servidores e demais usuários por ele indicado e às partes que provocaram o incidente.
Campo CSV	nivelDeSigilo
Campo WS	(cd_nivel_acesso em client.tb_processo_trf)
Exemplo	Segredo de Justiça

• Data da autuação

Descrição	Este atributo corresponde a data de autuação do processo e sempre virá preenchido nos dadosBasicos do processo após uma consulta. Observação: Na entrega da manifestação não é preciso preencher este atributo.
Campo CSV	dataDaAutuação
Campo WS	(dt_autuacao em client.tb_processo_trf)
Exemplo	01/01/2021 14:35:00 Formato: 'DD/MM/AAAA HH:MM:SS'

• Pedido de liminar

Descrição	Indica se houve pedido de liminar no processo.
Campo CSV	pedidoDeLiminar
Campo WS	(in_tutela_liminar em client.tb_processo_trf)
Exemplo	Sim / Não;

• Número SISPL

Descrição	Número do processo antigo do SISPL, para processos digitalizados.
Campo CSV	numeroSISPL

Campo WS	(numero_processo_sispl em client.tb_processo)
Exemplo	2010.01.1.032950-9

• Processo de Origem

Descrição	Número do processo de origem no formato do CNJ.
Campo CSV	processoDeOrigem
Campo WS	(nr_processo_origem em client.tb_processo)
Exemplo	2010.01.1.032950-9

• Incidental

Descrição	Indica se o processo é incidental.
Campo CSV	incidental
Campo WS	(in_tutela_liminar em client.tb_processo_trf)
Exemplo	Sim / Não

• Objeto do processo

Descrição	Campo utilizado internamente para classificar o objeto do processo.
Campo CSV	objetoDoProcesso
Campo WS	(ds_objeto em client.tb_processo_trf)
Exemplo	SISTJ (indica que foi digitalizado do SISTJ para o PJE)

• Justiça 100 Digital

Descrição	Campo que indica se houve pedido de juízo 100% digital.
Campo CSV	justica100Digital
Campo WS	(in_solicitado_juizo_100_digital em client.tb_processo_trf)
Exemplo	sim/não

• Processo Digitalizado

Descrição	Campo que indica se o processo foi digitalizado.
Campo CSV	processoDigitalizado (boolean)
Campo WS	(ds_codigo em client.tb_tipo_sit_processual / id_tipo_situacao_processual em client.tb_situacao_processual)
Exemplo	Sim/não

• Órgão Julgador - Código

Descrição	Identificador do órgão julgador do processo.
Campo CSV	codigoOrgaoJulgador
Campo WS	(id_orgao_julgador em client.tb_orgao_julgador)
Exemplo	144

• Órgão Julgador - Nome

Descrição	Descrição do órgão julgador do processo.
Campo CSV	nomeOrgaoJulgador
Campo WS	(ds_orgao_julgador em client.tb_orgao_julgador)
Exemplo	2ª Vara Cível de Ceilândia

• Plano Classificação e Tabela de Temporalidade Utilizada

Descrição	Descrever qual a versão do plano de classificação e tabela de temporalidade foi utilizado para extrair os metadados deste documento.
Campo CSV	versaoPCTT
Onde buscar	No Sistema de Gestão de Tabelas Processuais Unificadas (https://www.cnj.jus.br/sgt/versoes.php) <pre>function getDataUltimaVersao() /** * Retorna uma String contendo a data da última versão * * @return String */ </pre> (Obs: data extraída no momento do cálculo da temporalidade no PJE-Arq)
Exemplo	Plano de classificação e tabela de temporalidade de documentos - PCTT-AD TJDF (Minuta de Proposta do PCTT-TJDF - Versão 1-47)

- **Prazo de guarda**

Descrição	Indicação do prazo estabelecido em tabela de temporalidade para o cumprimento da destinação.
Campo CSV	prazoGuardaClassificacao
Onde buscar	PJe-Arq
Exemplo	Um (01) ano de guarda em arquivo corrente e depois é recolhido para o arquivo permanente.

- **Destinação prevista**

Descrição	Indicação da próxima ação de destinação (transferência, eliminação ou recolhimento) prevista para o documento, em cumprimento à tabela de temporalidade.
Campo CSV	destinacaoPrevista
Onde buscar	PJe-Arq
Exemplo	Repositório Arquivístico Digital - Tribunal de Justiça do Distrito Federal e dos Territórios

→ SUBMISSION DOCUMENTATION

Ficarão no JSON os dados que se repetem e não são possíveis de elaborar um **csv** com 2 ou mais linhas. São os campos referentes a: documento; partes; movimentação processual;

- **Identificador do documento**

Descrição	Identificador do Documento.
Campo CSV	idDocumento
Campo WS	(id_processo_documento_trf em client.tb_processo_documento_trf)
Exemplo	123456

- **Identificador do documento principal**

Descrição	Identificador do documento principal caso este documento seja um anexo.
Campo CSV	idDocumentoVinculado

Campo WS	(id_doc_associado em client.tb_proc_doc_associacao)
Exemplo	123456

- Tipo de documento**

Descrição	Código do tipo de documento disponível no serviço "ConsultaPJe" - Ex.: 58 - Petição Inicial, 118A - Informações. O código variará dependendo da instalação do PJe.
Campo CSV	codigoTipoDocumento
Campo WS	(id_tipo_processo_documento em core.tb_processo_documento)
Exemplo	123456

- Tipo de documento - Nome**

Descrição	Descrição do tipo de documento disponível no serviço "ConsultaPJe" - Ex.: 58 - Petição Inicial, 118A - Informações. Obs.: A ser desenvolvido pela SEDES/TJDFT.
Campo CSV	nomeTipoDocumento
Campo WS	(ds_tipo_processo_documento em core.tb_tipo_processo_documento)
Exemplo	Petição Inicial, 118A - Informações.

- Data e hora da criação**

Descrição	Sequência de ano+dia+mês/hora+minuto+segundo. Atributo destinado a permitir a informação do momento em que o documento foi recebido pelo Poder Judiciário. É opcional no caso de documento enviado para protocolo.
Campo CSV	dataHoraCriacao
Campo WS	(dt_inclusao em core.tb_processo_documento_bin)
Exemplo	12/12/2012 14:32:00

- Descrição**

Descrição	Descrição do documento.
Campo CSV	descricao
Campo WS	(ds_documento em core.tb_documento)
Exemplo	Sentença; Carteira de motorista.

- **Hash**

Descrição	Resumo matemático do documento enviado pelo algoritmo SHA-256.
Campo CSV	hash
Campo WS	(ds_md5_documento em core.tb_processo_documento_bin)
Exemplo	b0c020615d91c745a8cb54025cece674

- **Documento Sigiloso**

Descrição	Propriedade que indica se o documento é ou não sigiloso.
Campo CSV	documentoSigiloso
Campo WS	(in_documento_sigiloso em core.tb_tipo_processo_documento)
Exemplo	Sim / não

- **Mimetype**

Descrição	Tipo do arquivo que será enviado, seguindo o seguinte domínio: application/pdf ou html/text. O PJe suporta os seguintes tipos de arquivos: pdf (máximo até 3Mb), mpeg (máximo até 5Mb), ogg (máximo até 10Mb), vorbis (máximo até 5Mb), png (máximo até 3Mb), mp4 (máximo até 10Mb) e quicktime (máximo até 10Mb).
Campo CSV	mimetype
Campo WS	(ds_extensao em core.tb_processo_documento_bin)
Exemplo	video/mp4, application/pdf

- **Assinatura**

Descrição	Contém os dados em Base64 do arquivo de assinatura do documento. Para arquivos em PDF ou HTML, que não sejam P7S, é necessário informar os dados da assinatura.
Campo CSV	assinatura
Campo WS	(ds_signature em core.tb_processo_documento_bin)
Exemplo	assinaturadeteste

- **Usuário da assinatura**

Descrição	Identificador do usuário que realizou a assinatura. O MNI salva o ID do usuário, mas pode-se gravar o CPF ou ambos.
Campo CSV	usuarioDaAssinatura
Campo WS	(id_usuario_ultimo_assinar em core.tb_processo_documento_bin)
Exemplo	123456

- **Algoritmo hash**

Descrição	Algoritmo utilizado para gerar a assinatura: MD5withRSA, SHA1withRSA, SHA256withRSA ou ASN1MD5withRSA. Atualmente, o mais utilizado é o SHA256withRSA. Atualmente, o mais utilizado é o SHA256withRSA
Campo CSV	algoritmoHash
Campo WS	campo fixo com o valor MD5
Exemplo	MD5withRSA

- **Cadeia do certificado**

Descrição	String do certificado. Caso seja do tipo PEM é necessário incluir inclusive as strings "BEGIN CERTIFICATE" e "END CERTIFICATE".
Campo CSV	cadeiaDeCertificado
Campo WS	(ds_cert_chain em core.tb_processo_documento_bin)
Exemplo	-----BEGIN CERTIFICATE----- certchaindeteste= -----END CERTIFICATE-----

- **Codificação do certificado**

Descrição	Codificação utilizada no certificado: "PEM" ou "PkiPath".
Campo CSV	codificacaoDoCertificado
Campo WS	(ds_md5_documento em core.tb_processo_documento_bin)
Exemplo	PkiPath

- ***Data da assinatura**

Descrição	Data e Hora da assinatura, obedecendo a sequência de ano+dia+mês+minuto+segundo.
Campo CSV	dataAssinatura

Campo WS	(dt_primeira_assinatura em core.tb_processo_documento_bin)
Exemplo	20190725181340

- ***Signatário login**

Descrição	Informação referente a signatário que fez uso de login e senha para assinar o documento.
Campo CSV	signatarioLogin
Campo WS	(?)
Exemplo	-

- **Identificação do tipo de meio do documento**

Descrição	Documento/volume/processo/dossiê: digital, não digital (convencionais/analógicos) ou híbrido, para controlar as relações entre os meios e o monitoramento de preservação.
Campo CSV	meioDocumental
Onde buscar	Será um texto fixo.
Exemplo	Documento digital

- **Gênero Documental**

Descrição	É a configuração da informação no documento de acordo com o sistema de signos utilizado na comunicação do documento. Exemplos: Audiovisual; textual; cartográfico; iconográfico; multimídia.
Campo CSV	generoDocumental
Onde buscar	Será de acordo com o mime type do documento.
Exemplo	Textual

→ PARTES

- ***Polo**

Descrição	Sigla para identificação do tipo de polo. Para polo ativo, usar "AT"; Passivo, usar "PA"; "TC" = Terceiro; "FL" = Fiscal da lei diverso; "TJ" = Testemunha do juízo; "AD" = Assistente simples desinteressado (amicus curiae); "VI" = Vítima.
-----------	---

Campo CSV	polo
Campo WS	(ds_tipo_parte em client.tb_tipo_parte / client.tb_processo_parte)
Exemplo	Ativo

● ***Nome da parte**

Descrição	Nome da parte que compõe o polo do processo.
Campo CSV	nome
Campo WS	(ds_nome em acl.tb_usuario_login)
Exemplo	Vanessa Rocha

● ***Sexo da parte**

Descrição	Correspondente a pessoa parte, onde "M" masculino; "F" feminino; "D" desconhecido.
Campo CSV	sexo
Campo WS	(in_sexo em client.tb_pessoa_fisica)
Exemplo	Feminino

● ***Nome do genitor**

Descrição	Nome completo do pai da pessoa parte.
Campo CSV	nomeDoGenitor1
Campo WS	(nm_genitora em client.tb_pessoa_fisica)
Exemplo	Francisco Rocha

● ***Nome da genitora**

Descrição	Nome completo da mãe da pessoa parte.
Campo CSV	nomeDoGenitor2
Campo WS	(nm_genitor em client.tb_pessoa_fisica)
Exemplo	Maria Rocha

- **(Referenciado na tabela) Data de nascimento da parte**

Descrição	Data do nascimento no formato AAAAMMDD.
Campo CSV	dataDeNascimento
Campo WS	(dt_nascimento em tb_pessoa_fisica)
Exemplo	19900104

- **(Referenciado na tabela) Data de óbito da parte**

Descrição	Data do falecimento no formato AAAAMMDD.
Campo CSV	dataDeObito
Campo WS	(dt_obito em client. tb_pessoa_fisica)
Exemplo	20100529

- ***Número do documento principal**

Descrição	Número do documento principal da pessoa parte, devendo ser utilizado o RIC ou o CPF para pessoas físicas, nessa ordem, ou o CNPJ para pessoas jurídicas. O atributo é opcional em razão da possibilidade de haver pessoas sem documentos ou cujos dados não estão disponíveis.
Campo CSV	numeroDocumentoPrincipal
Campo WS	(nr_documento_identificacao em client.tb_pess_doc_identificacao)
Exemplo	99999999999

- ***Tipo de pessoa**

Descrição	Indicar qual o tipo de pessoa que será integrante do processo. Enviar um dos seguintes valores, sem acentos: "fisica"; "juridica"; "autoridade"; "orgaorepresentacao".
Campo CSV	tipoDePessoa
Campo WS	(ds_tipo_pessoa em client.tb_tipo_pessoa / in_tipo_pessoa em client.tb_pessoa)
Exemplo	Física

- **(Referenciado na tabela) Nome Fantasia**

Descrição	Nome fantasia, para o caso da parte pessoa jurídica.
-----------	--

Campo CSV	nomeFantasia
Campo WS	(nm_fantasia em client.tb_pessoa_juridica)
Exemplo	

- **(Referenciado na tabela) Pessoa vinculada**

Descrição	Indicação da existência de um relacionamento entre uma autoridade e uma pessoa jurídica ou ente que ela representa. Exemplo: a escola é vinculada a seu diretor ou reitor. Sugestão: Salvar o nome da pessoa ou criar outro campo, se necessário, para salvar o CPF.
Campo CSV	pessoaVinculada
Campo WS	(nr_cpf_responsavel em client.tb_pessoa_juridica OU id_pessoa em client.tb_autoridade_publica)
Exemplo	Cristiano

- **(Referenciado na tabela) Cidade natural**

Descrição	Local de nascimento da pessoa parte.
Campo CSV	cidadeNatural
Campo WS	(id_municipio_nascimento em client.tb_pessoa_fisica)
Exemplo	Brasília

- **(Referenciado na tabela) Estado natural**

Descrição	Estado de nascimento da pessoa parte. A implementação de codificação/decodificação deverá interpretar o valor do campo como se tratando da sigla de duas letras identificadoras das unidades federativas brasileiras.
Campo CSV	estadoNatural
Campo WS	(id_estado em core.tb_municipio / id_municipio_nascimento em client.tb_pessoa_fisica)
Exemplo	DF

- **(Referenciado na tabela) Nacionalidade da parte**

Descrição	País de nascimento da pessoa parte. Exemplo: "BR"-Brasil. Dever-se-á utilizar, preferencialmente, o código ISO-3166-1-alpha-2 (http://www.iso.org/iso/english_country_names_and_code_elements) pertinente ao país respectivo.
-----------	--

Campo CSV	nacionalidade
Campo WS	(id_pais em client.tb_pessoa_fisica)
Exemplo	BR

● ***Código do documento de identificação da parte**

Descrição	Número do documento identificador vinculado ao tipo de pessoa, podendo ser o número do CPF, CNPJ, RG, TIT, etc. São uma sequência de caracteres que tornam único o documento descrito sem os separadores característicos.
Campo CSV	codigoDoDocumentoDeIdentificacao
Campo WS	(nr_documento_identificacao em client.tb_pess_doc_identificacao)
Exemplo	99999999999

● ***Emissor do documento de identificação da parte**

Descrição	Entidade emissora do documento. Exemplo: SSP, Cartórios, Justiça Eleitoral, SRFB.
Campo CSV	emissorDoDocumentoDeIdentificacao
Campo WS	(dr_orgao_expedidor em client.tb_pess_doc_identificacao)
Exemplo	SSP

● ***Tipo do documento de identificação da parte**

Descrição	Elemento destinado a permitir a identificação dos diversos tipos de documentos de identificação existentes. Trata-se de enumeração dos seguintes tipos: [Quebra da Disposição de Texto]- CI: carteira de identidade[Quebra da Disposição de Texto]- CNH: carteira nacional de habilitação[Quebra da Disposição de Texto]- TE: título de eleitor[Quebra da Disposição de Texto]- CN: certidão de nascimento[Quebra da Disposição de Texto]- CC: certidão de casamento[Quebra da Disposição de Texto]- PAS: passaporte[Quebra da Disposição de Texto]- CT: carteira de trabalho[Quebra da Disposição de Texto]- RIC: registro individual do cidadão[Quebra da Disposição de Texto]- CMF: cadastro no Ministério da Fazenda Brasileiro [Quebra da Disposição de Texto]- PIS_PASEP: número no programa de integração social [Quebra da Disposição de Texto]- CEI: cadastro específico do INSS [Quebra da Disposição de Texto]- NIT: número de identificação do trabalho [Quebra da Disposição de Texto]- CP: cadastro em conselhos profissionais [Quebra da
-----------	---

	Disposição de Texto]- IF: identidade funcional[Quebra da Disposição de Texto]- OAB: número de cadastro na Ordem dos Advogados do Brasil [Quebra da Disposição de Texto]- RJC: número de inscrição empresarial; [Quebra da Disposição de Texto]- RGE: registro de identificação do estrangeiro
Campo CSV	tipoDoDocumentoDeldentificacao
Campo WS	(client.tb_pess_doc_identificacao em client.tb_pess_doc_identificacao)
Exemplo	CNH

- **Nome no documento de identificação**

Descrição	Nome da parte detentora do documento.
Campo CSV	nomeNoDocumentoDeldentificacao
Campo WS	(ds_nome_pessoa em client.tb_pess_doc_identificacao)
Exemplo	

- ***Outro nome da parte**

Descrição	Elemento destinado a permitir a inclusão de outros nomes da pessoa individualizada. Devem ser incluídos sob esse elemento os nomes que NÃO constam em documentos específicos. Em caso de nomes divergentes do principal existentes em documentos específicos, esses nomes devem ser indicados no atributo pertinente do documento.
Campo CSV	outroNome
Campo WS	(ds_pessoa_nome_alternativo em client.tb_pessoa_nome_alternativo)
Exemplo	

- ***CEP endereço da parte**

Descrição	CEP da parte do processo. Atributo indicador do código de endereçamento postal do endereço no diretório nacional de endereços da ECT. O valor deverá ser uma sequência de 8 dígitos, sem qualquer separador. O atributo é opcional para permitir a apresentação de endereços desprovidos de CEP e de endereços internacionais.
Campo CSV	cep
Campo WS	(nr_cep em core.tb_cep / id_cep em core.tb_endereco / id_endereco em tb_processo_parte_endereco)
Exemplo	

- ***Logradouro endereço da parte**

Descrição	Logradouro vinculado ao CEP, tais como as ruas, avenidas, praças, jardins, etc.
Campo CSV	logradouro
Campo WS	(nm_logradouro em core.tb_cep / id_cep em core.tb_endereco / id_endereco em tb_processo_parte_endereco)
Exemplo	

● ***Número endereço da parte**

Descrição	Número vinculado ao CEP, podendo ser número da casa, apartamento, etc.
Campo CSV	numero
Campo WS	(nm_logradouro em core.tb_endereco / id_endereco em tb_processo_parte_endereco)
Exemplo	

● ***Complemento endereço da parte**

Descrição	Dados adicionais do endereço.
Campo CSV	string
Campo WS	(ds_complemento em core.tb_endereco / id_endereco em tb_processo_parte_endereco)
Exemplo	

● ***Bairro endereço da parte**

Descrição	Parte que compõe a cidade, devendo ser vinculada ao CEP.
Campo CSV	bairro
Campo WS	(nm_bairro em core.tb_endereco / id_endereco em tb_processo_parte_endereco)
Exemplo	

● ***Cidade endereço da parte**

Descrição	Vinculada ao CEP, ou seja, nome da zona geográfica onde se agrupam as residências, comércios e indústrias.
Campo CSV	cidade

Campo WS	(nm_logradouro em core.tb_endereco / id_endereco em tb_processo_parte_endereco)
Exemplo	

● ***Estado endereço da parte**

Descrição	Sigla do Estado brasileiro, composto por duas letras.
Campo CSV	estado
Campo WS	(id_municipio em core.tb_cep / id_cep em core.tb_endereco / id_endereco em tb_processo_parte_endereco)
Exemplo	DF

● ***País endereço da parte**

Descrição	Sigla referente ao país do Estado que compõe o endereço, composto por duas letras. Dever-se-á utilizar, preferencialmente, o código ISO-3166-1-alpha-2 (http://www.iso.org/iso/english_country_names_and_code_elements) pertinente ao país respectivo.
Campo CSV	pais
Campo WS	(como o PJE não aceita endereço sem CEP ainda, o país referente aos endereços é sempre BR)
Exemplo	BR

→ **DADOS DOS REPRESENTANTES PROCESSUAIS**

● **(REFERENCIADO NA TABELA) NOME**

Descrição	Nome do advogado ou do escritório de advocacia ou órgão de representação processual.
Campo CSV	nome
Campo WS	(ds_nome em acl.tb_usuario_login)
Exemplo	"B & G Advogados" (Campo que se repete)

● **(REFERENCIADO NA TABELA) INSCRIÇÃO**

Descrição	Inscrição do advogado ou escritório de advocacia no cadastro da Ordem dos Advogados do Brasil. O campo é preenchido no formato CCDDDDDDDC, sendo os primeiros 'C' dois caracteres indicativos da unidade federativa brasileira em que há a inscrição, os sete dígitos 'D' seguintes o número da inscrição, devendo incluir zeros ('0') à esquerda caso o número tenha menos de 7 dígitos e o último caracter a letra identificadora do tipo de inscrição.
Campo CSV	inscricao
Campo WS	(nr_oab + ds_letra_oab + id_uf_oab em client.tb_dado_oab_pess_advogado)
Exemplo	1254DF

● **(REFERENCIADO NA TABELA) NÚMERO DO DOCUMENTO PRINCIPAL**

Descrição	O número RIC ou o CPF, para advogados, ou o CNPJ, para escritórios de advocacia e órgãos de representação processual (MP, advocacia pública e defensoria pública).
Campo CSV	numeroDoDocumentoPrincipal
Campo WS	(ds_login em acl.tb_usuario_login)
Exemplo	1111111

● **(REFERENCIADO NA TABELA) TIPO DE REPRESENTANTE**

Descrição	Atributo que permite indicar o tipo de representante processual.
Campo CSV	tipoDeRepresentante
Campo WS	(id_tipo_representante em client.tb_proc_parte_representante)
Exemplo	Advogado"; "Escritório de advocacia"; "Ministério público"; "Defensoria pública";

→ **DADOS DOS ASSUNTOS PROCESSUAIS**

● ***Principal**

Descrição	Indica se o assunto será o principal do processo.
Campo CSV	principal
Campo WS	(in_assunto_principal em client.tb_processo_assunto)
Exemplo	sim/não

● ***Código Nacional**

Descrição	Código do assunto processual, segundo SGT.
Campo CSV	codigoNacional
Campo WS	(cd_assunto_trf em client.tb_assunto_trf)
Exemplo	1945 (descrever o nome e código).

- **Código Pai Nacional**

Descrição	Atributo destinado à entrada do código de assunto nacional de que o assunto local é filho.
Campo CSV	codigoPaiNacional
Campo WS	(id_assunto_trf_superior. cd_assunto_trf em client.tb_assunto_trf)
Exemplo	4563

- ***DESCRIÇÃO IGUAL AO NOME**

Descrição	Texto descritivo do assunto processual.
Campo CSV	descricaoigualao nome
Campo WS	(ds_assunto_trf em client.tb_assunto_trf)
Exemplo	"Alimentos"

→ MOVIMENTAÇÃO PROCESSUAL

- ***Código da movimentação processual**

Descrição	Código da movimentação de acordo com a SGT.
Campo CSV	codigoDaMovimentacao
Campo WS	(cd_evento em core.tb_evento / core.tb_processo_evento)
Exemplo	390

- ***Nome da movimentação processual**

Descrição	Nome da movimentação processual, conforme SGT.
Campo CSV	nomeDaMovimentacao

Campo WS	(ds_evento em core.tb_evento / core.tb_processo_evento)
Exemplo	Sentença Proferida

● **Descrição completa da movimentação processual**

Descrição	Descrição completa da movimentação, já com os complementos preenchidos.
Campo CSV	descricaoCompletaDaMovimentacao
Campo WS	(ds_texto_final_interno em core.tb_processo_evento)
Exemplo	Decorrido prazo de Vanessa Rocha em 19/03/2021 23:59:59

● ***Data da movimentação processual**

Descrição	Data da movimentação em sequência de ano+dia+mês/hora+minuto+segundo.
Campo CSV	dataDaMovimentacao
Campo WS	(dt_atualizacao em core.tb_processo_evento)
Exemplo	2021/03/21 23:59:59

→ **ESTUDO DOS CAMPOS DO PJE COM OS CAMPOS DO MOREQ-JUS**

● **Nível de Sigilo**

Descrição	Nível de sigilo a ser aplicado ao processo. Dever-se-á utilizar os seguintes níveis: - 0: públicos, acessíveis a todos os servidores do Judiciário e dos demais órgãos públicos de colaboração na administração da Justiça, assim como aos advogados e a qualquer cidadão - 1: segredo de justiça, acessíveis aos servidores do Judiciário, aos servidores dos órgãos públicos de colaboração na administração da Justiça e às partes do processo. - 2: sigilo mínimo, acessível aos servidores do Judiciário e aos demais órgãos públicos de colaboração na administração da Justiça - 3: sigilo médio, acessível aos servidores do órgão em que tramita o processo, à(s) parte(s) que provocou(ram) o incidente e àqueles que forem expressamente incluídos - 4: sigilo intenso, acessível a classes de servidores qualificados (magistrado, diretor de secretaria/escrivão, oficial de gabinete/assessor) do órgão em que tramita o processo, às partes que provocaram o incidente e àqueles que forem expressamente incluídos - 5: sigilo absoluto, acessível apenas ao magistrado do órgão em que tramita, aos servidores e demais usuários por ele indicado e às partes que provocaram o incidente.
Moreq	Metadados segurança; MSG1.1.20 Sigilo_recebido

● **Usuário do cadastro do processo**

Descrição	Identificador do usuário que protocolou a ação. Identificação do perfil de usuário para alteração de documento ou processo/dossiê/volume
Moreq	Metadados segurança; MSG1.1.16 Perfil_alteração_corpo

● **Nome do usuário do protocolo**

Descrição	Nome do usuário que efetuou o protocolo do processo. Identificação do perfil de usuário para alteração de metadado de documento ou processo/dossiê/volume.
Moreq	Metadados segurança; MSG1.1.17 Perfil_alteração_metadado

● **Processo Digitalizado**

Descrição	Campo que indica se o processo foi digitalizado.
Moreq	Metadados preservação; MPR1.3.6

● **HASH**

Descrição	Resumo matemático do documento enviado pelo algoritmo SHA-256.
Moreq	Metadados preservação; MPR1.3.24 - Checksum

● **MIMETYPE**

Descrição	Tipo do arquivo que será enviado, seguindo o seguinte domínio: application/pdf ou html/text. O PJe suporta os seguintes tipos de arquivos: pdf (máximo até 3Mb), mpeg (máximo até 5Mb), ogg (máximo até 10Mb), vorbis (máximo até 5Mb), png (máximo até 3Mb), mp4 (máximo até 10Mb) e quicktime (máximo até 10Mb).
Moreq	Metadados preservação; MPR1.3.19 - Formato_arquivo_digital

● **ASSINATURA**

Descrição	Contém os dados em Base64 do arquivo de assinatura do documento.
Moreq	Metadados segurança; MSG1.1.4 - Assinatura_digital_assinatura

- **Usuário da assinatura**

Descrição	Identificador do usuário que realizou a assinatura. (Nesse campo, o MNI salva o ID do usuário, mas no novo serviço podemos gravar o CPF, ou o nome, ou ambos, o que for mais atemporal)
Moreq	Metadados segurança; MSG1.1.5 - Assinatura_digital_validador

- **Algoritmo hash**

Descrição	Algoritmo utilizado para gerar a assinatura: MD5withRSA, SHA1withRSA, SHA256withRSA ou ASN1MD5withRSA. Atualmente, o mais utilizado é o SHA256withRSA.
Moreq	Metadados preservação; MPR1.3.23 - Algoritmo_checksum

- **Cadeia de certificado**

Descrição	String do certificado. Caso seja do tipo PEM é necessário incluir inclusive as strings "BEGIN CERTIFICATE" e "END CERTIFICATE".
Moreq	Metadados segurança; MSG1.1.3 - Certificado_digital

- **Codificação de certificado**

Descrição	Codificação utilizada no certificado: "PEM" ou "PkiPath". Registro de que a assinatura digital foi verificada com sucesso.
Moreq	Metadados segurança; MSG1.1.2 - Assinatura_digital_validação

- **Data assinatura**

Descrição	Data e Hora da assinatura, obedecendo a sequência de ano+dia+mês+minuto+segundo.
Moreq	metadados segurança; MSG1.1 - Assinatura_digital_data.1

- **Signatário login**

Descrição	Informação referente a signatário que fez uso de login e senha para assinar o documento. (Esse campo é para identificar o usuário que assinou o documento, para os casos de terem utilizado o PJE Token, que é um aplicativo em que servidores do TJ conseguem assinar os documentos com login e senha, utilizando o token do próprio TJDFt para garantir a assinatura.)
Moreq	metadados segurança; MSG1.1.5 - Assinatura_digital_validador

- **Assinatura válida**

Descrição	Indica se a assinatura foi verificada com sucesso.
Moreq	metadados segurança; MSG1.1.2 - Assinatura_digital_validação

APÊNDICE B - Metadados Descritivos Dublin Core

CAMPO	CAMPOS DC CSV	EXEMPLO DE PREENCHIMENTO	ONDE BUSCAR?	PERMITE REPETIÇÃO NO ATOM
Título	dc.title	Processo no 07193054-20.2019.8.07.0003	Nro do Processo Não precisa estar com máscara no número do processo!	Não permite repetição.
Criador (Produtor)	dc.creator	Tribunal de Justiça do Distrito Federal e dos Territórios	Texto fixo	Permite repetição.
Assunto (Ponto de acesso de assunto)	dc.subject[Quebra da Disposição de Texto]	Campo de assunto da tabela Classe; Assuntos principais e secundários; Jurisdição; órgão julgador colegiado; órgão julgador; partes.	(Assuntos cobertos pelo conteúdo)	Permite repetição.
Descrição [Quebra da Disposição de Texto] (Âmbito e conteúdo)	dc.description		(Uma descrição resumida sobre o conteúdo)	Não permite repetição.

Editor [Quebra da Disposição de Texto](Sem correspondência)	dc.publisher		(Pessoa que fez a descrição)	Permite repetição.
Contribuidor / Colaborador [Quebra da Disposição de Texto](Ponto de acesso de local)	dc.contributor		(Pessoa que contribuiu com o conteúdo)	Permite repetição.
Data [Quebra da Disposição de Texto]	dc.date	2019-03-29	Campo vem dos metadados de gestão: Data de Ajuizamento <dataAjuizamento>	Permite repetição.
			Formato: AAAA-MM-DD ou AAAA-MM ou AAAA	
Tipo do Recurso [Quebra da Disposição de Texto] (Tipo)	dc.type	Texto	(Uma categoria para o tipo de conteúdo) Exemplos: Collection, Dataset, Event, Image, InteractiveResource, MovingImage, PhysicalObject, Service, Software, Sound, StillImage, Text. Campo fixo	Permite repetição.

Formato	dc.format	application/pdf	Mimetype Campo fixo	Não permite repetição.
Identificador do Recurso	dc.identifier	Processo no 07193054-20.2019.8.07.0003	Um identificador único para o seu conteúdo. Pode ser um texto ou um número gerado por um sistema de identificação formal - ou apenas uma URL	Não permite repetição.
Fonte	dc.source		Onde o conteúdo foi inicialmente publicado / originado. Um conteúdo que tem alguma relação intelectual com o conteúdo descrito. Se for conteúdo original, veiculado pela primeira vez e sem nenhuma relação intelectual com outros conteúdos, deve ser a URL para esse conteúdo. Campo fixo	Não permite repetição.
Idioma	dc.language	pt_BR	Em que linguagem o conteúdo foi escrito. Você precisa especificar o código correto da língua. Campo fixo	Permite repetição.
Relação	dc.relation	campo: processos vinculados	**Concatenação das informações.	Não permite repetição.

Abrangência / Cobertura (Ponto de acesso de local)	dc.coverage		Onde o conteúdo está localizado fisicamente. Normalmente inclui localização espacial (nome do lugar ou coordenadas geográficas), período temporal (data) ou jurisdição.	Permite repetição.
Gerenciamento de Direitos Autorais	dc.rights		Informação dos direitos autorais do conteúdo. Pode conter a declaração de Copyright ou outros tipos de licença. Sigilo absoluto, acessível apenas ao magistrado do órgão em que tramita, aos servidores e demais usuários por ele indicado e às partes que provocaram o incidente.	Não permite repetição.

APÊNDICE C - Metadados Descritivos ISAD(G)

CAMPO	CAMPOS DC CSV	EXEMPLO DE PREENCHIMENTO	ONDE BUSCAR?	PERMITE REPETIÇÃO NO ATOM
Título	dc.title	Processo no 07193054-20.2019.8.07.0003	Nro do Processo Não precisa estar com máscara no número do processo!	Não permite repetição.
Criador (Produtor)	dc.creator	Tribunal de Justiça do Distrito Federal e dos Territórios	Texto fixo	Permite repetição.
Assunto (Ponto de acesso de assunto)	dc.subject[Quebra da Disposição de Texto]	Campo de assunto da tabela Classe; Assuntos principais e secundários; Jurisdição; órgão julgador colegiado; órgão julgador; partes.	(Assuntos cobertos pelo conteúdo)	Permite repetição.
Descrição[Quebra da Disposição de Texto] (Âmbito e conteúdo)	dc.description	-	(Uma descrição resumida sobre o conteúdo)	Não permite repetição.
Editor[Quebra da Disposição de Texto](Sem correspondência)	dc.publisher		(Pessoa que fez a descrição)	Permite repetição.

Contribuidor / Colaborador[Quebra da Disposição de Texto](Ponto de acesso de local)	dc.contributor			Permite repetição.
[Quebra da Disposição de Texto]	dc.date	2019-03-29 [Quebra da Disposição de Texto]	Campo vem dos metadados de gestão: Data de Ajuizamento <dataAjuizamento>	Permite repetição.
			Formato: AAAA-MM-DD ou AAAA-MM ou AAAA	
Tipo do Recurso[Quebra da Disposição de Texto] (Tipo)	dc.type	Texto	(Uma categoria para o tipo de conteúdo) Exemplos: Collection, Dataset, Event, Image, InteractiveResource, MovingImage, PhysicalObject, Service, Software, Sound, StillImage, Text. Campo fixo	Permite repetição.
Formato	dc.format	application/pdf	Mimetype Campo fixo	Não permite repetição.
Identificador do Recurso	dc.identifier	Processo no 07193054-20.2019.8.07.0003	Um identificador único para o seu conteúdo. Pode	Não permite repetição.

			ser um texto ou um número gerado por um sistema de identificação formal - ou apenas uma URL	
Fonte	dc.source		Onde o conteúdo foi inicialmente publicado / originado. Um conteúdo que tem alguma relação intelectual com o conteúdo descrito. Se for conteúdo original, veiculado pela primeira vez e sem nenhuma relação intelectual com outros conteúdos, deve ser a URL para esse conteúdo. Campo fixo	Não permite repetição.
Idioma	dc.language	pt_BR	Em que linguagem o conteúdo foi escrito. Você precisa especificar o código correto da língua. Campo fixo	Permite repetição.
Relação	dc.relation	campo: processos vinculados	**Concatenação das informações.	Não permite repetição.

Abrangência / Cobertura (Ponto de acesso de local)	dc.coverage		Onde o conteúdo está localizado fisicamente. Normalmente inclui localização espacial (nome do lugar ou coordenadas geográficas), período temporal (data) ou jurisdição.	Permite repetição.
Gerenciamento de Direitos Autorais	dc.rights		Informação dos direitos autorais do conteúdo. Pode conter a declaração de Copyright ou outros tipos de licença. Sigilo absoluto, acessível apenas ao magistrado do órgão em que tramita, aos servidores e demais usuários por ele indicado e às partes que provocaram o incidente.	Não permite repetição.

APÊNDICE D - Outros Metadados ISAD(G)

Esses metadados foram extraídos na planilha oficial da *Artefactual*, para importação de metadados ISAD(G) à plataforma de difusão AtoM.

CAMPO	CAMPOS ISAD CSV	EXEMPLO DE PREENCHIMENTO	OBSERVAÇÃO
Locais	[isad.placeAccessPoints]	Brasília - DF	Campo igual ao dc.coverage. Onde o conteúdo está localizado fisicamente. Normalmente inclui localização espacial (nome do lugar ou coordenadas geográficas), período temporal (data) ou jurisdição Campo fixo.
Assuntos	[isad.subjectAccessPoints]	Campo de assunto da tabela Classe; Assuntos principais e secundários; Jurisdição; órgão julgador colegiado; órgão julgador; partes.	Campo igual ao dc.subject.

Pessoas / Entidades	[isad.nameAccessPoints]	Nomes das partes (ds_nome em acl.tb_usuario_login) Nomes dos representantes processuais (ds_nome em acl.tb_usuario_login)	Lista de pessoas ou entidades relacionadas ao documento.
Gênero	[isad.genreAccessPoints]	Textual	Campo fixo.
Repositório	[isad.repository]	Tribunal de Justiça do Distrito Federal e dos Territórios	Campo igual ao dc.relation (isLocatedAt). Campo fixo.
Sistema de Escrita	[isad.script]	Português ou latim	Registrar a escrita do documento Campo fixo
Notas sobre o Idioma	[isad.languageNote]		Especificar qualquer tipo de alfabeto, escrita, sistema de símbolos ou abreviaturas utilizadas.
URI do Objeto	[isad.digitalObjectURI]		URI enviada do Archivematica para o AtoM, preenchida pelo sistema.
Checksum	[isad.digitalObjectChecksum]	Esses metadados estão dentre aqueles que serão preservados do PJe. Sua extração deverá ser feita juntamente com os demais metadados.	Cálculo matemático do documento.

Identificador da Descrição	[descriptionIdentifier]		Identificador único dado pelo usuário da descrição.
Identificador da Instituição	[isad.institutionIdentifier]	Tribunal de Justiça do Distrito Federal e dos Territórios	Identificação da instituição responsável pela descrição. Campo fixo.
Status da Descrição	[isad.descriptionStatus]	Draft	Registrar o estado da descrição, indicando se está em elaboração (rascunho), revisada ou final (concluída). Campo fixo
Nível de detalhamento da Descrição	[isad.levelOfDetail]	Minimal	Indicar o nível de detalhe da descrição (mínima, parcial ou completa) de acordo com as regras ou diretrizes nacionais e internacionais. Campo fixo.
Idioma(s) da Descrição	[isad.languageOfDescription]	pt_BR	Indicar o idioma(s) utilizado para criar a descrição do material arquivístico. Campo fixo
Escrita(s) da descrição	[isad.scriptOfDescription]	Português ou Latim	Indicar a escrita utilizada para criar a descrição do material arquivístico. Campo fixo
Fontes	[isad.sources]	Site de pesquisa do PJe: https://pje.tjdft.jus.br/consultapublica/ConsultaPublica/listView.seam	Site do PJe Campo fixo

Status da publicação	[isad.publicationStatus]	Draft	Preencher entre Rascunho ou Publicado Campo fixo
Nome do Objeto físico	[isad.physicalObjectName]	Existe a possibilidade para aqueles processos judiciais que possuem documentos físicos (por algum motivo, em razão da digitalização para inserção no PJe e os documentos em papel tiverem sido preservados)	Ex.: Caixa Nro 10
Endereçamento do objeto físico	[isad.physicalObjectLocation]		Ex.: Arquivo Judiciário, Módulo 05, Estante 03, Prateleira 01
Tipo do objeto físico	[isad.physicalObjectType]		Exemplos: caixa, ficha, pasta, prateleira, armário, etc.
Identificador alternativo	[isad.alternativeIdentifiers]		Introduza um código de referência anterior, identificador alternativo, ou qualquer outra sequência alfanumérica associada ao registro.
Etiqueta do Id. alternativo	[isad.alternativeIdentifierLabels]		Digite um nome para o campo identificador alternativo que indique sua finalidade e uso. Ex. código de barras, AIP
Tipo de data	[isad.eventTypes]	Data de Ajuizamento <dataAjuizamento>	Indique se são data(s) em que os documentos de arquivo foram acumulados pelo produtor no exercício das suas atividades, ou seja, integrados num sistema de arquivo, ou, se são data(s) em que os documentos foram produzidos, ou seja, que inclui a data de cópias, edições, versões,

			anexos ou originais de peças produzidas antes da sua acumulação ou integração no sistema de arquivo. Escolher entre Produção ou Acumulação.
Data Inicial	[isad.eventStartDates]	Data de Ajuizamento <dataAjuizamento>	Indique a data de início.
Data Final	[isad.eventEndDates]	Data do arquivamento - Para documentos permanentes.	Indique a data final, se houver.
Descrição do evento	[isad.eventDescriptions]	Data da preservação digital no RDC-Arq	
Data Tópica	[isad.eventPlaces]	Tribunal de Justiça do Distrito Federal e dos Territórios.	Local de produção de um documento. Campo fixo.
Cultura	[isad.culture]		Dado automático, preenchido pelo sistema.

Apêndice E - Metadados PJe

Metadados de Gestão

Dados do Processo

Número do Processo

Descrição	Número do processo judicial, que deve estar de acordo com as regras definidas pela Resolução do CNJ nº 65, de 16 de dezembro de 2008.
Campo CSV	numeroProcesso
Campo PJEQL	data/consultaProcessoPeloNumero/numero
Exemplo	0700194-07.2021.8.07.0016

Classe Processual - Código

Descrição	Número identificador da classe processual, segundo o padrão estabelecido no Sistema de Gestão de Tabelas Processuais Unificadas ⁸ . As classes estão disponíveis, de acordo com a configuração de classes para cada jurisdição.
Campo CSV	codigoClasseProcessual
Campo PJEQL	data/consultaProcessoPeloNumero/classe/codigo
Exemplo	6017

Classe Processual - Nome

Descrição	Descrição da classe processual, segundo o padrão estabelecido no Sistema de Gestão de Tabelas Processuais Unificadas ⁹ . As classes estão disponíveis, de acordo com a configuração de classes para cada jurisdição.
Campo CSV	nomeClasseProcessual
Campo PJEQL	data/consultaProcessoPeloNumero/classe/descricao
Exemplo	Usucapião

Jurisdição - Código

Descrição	Código da Jurisdição, que compõe os quatro últimos dígitos do número do processo.
Campo CSV	codigoDaLocalidade
Campo PJEQL	data/consultaProcessoPeloNumero/ jurisdicao/nr_origem
Exemplo	18

⁸ https://www.cnj.jus.br/sgt/consulta_publica_classes.php

⁹ https://www.cnj.jus.br/sgt/consulta_publica_classes.php

Jurisdição - Nome

Descrição	Nome da Jurisdição.
Campo CSV	nomeDaLocalidade
Campo PJEQL	data/consultaProcessoPeloNumero/jurisdicao/descricao
Exemplo	Brasília - Fórum Des. Joaquim Sousa Neto

Competência - Nome

Descrição	Nome da competência.
Campo CSV	nomeDaCompetencia
Campo PJEQL	data/consultaProcessoPeloNumero/competencia/descricao
Exemplo	Criminal

Processo Vinculado - Número (São campos que se repetem)

Descrição	Número do processo vinculado, no formato CNJ.
Campo CSV	processoVinculado
Campo PJEQL	data/consultaProcessoPeloNumero/processosTrfConexao/numero
Exemplo	0725943-26.2021.8.07.0016

Processos Vinculados – Modalidade de vinculação

Descrição	Sigla que representa o tipo de vínculo do processo vinculado com o processo principal. Podem ser: DP("Dependência") DM("Desmembramento") PR("Prevenção") AS("Vinculação indireta") TR("Traslado") RE("Processo Referência")
Campo CSV	modalidadeVinculacaoProcesso
Campo PJEQL	data/consultaProcessoPeloNumero/processosTrfConexao/tipoConexao
Exemplo	0725943-26.2021.8.07.0016

Processos Vinculados – Situação

Descrição	Situação da vinculação processual. A propriedade verifica se o campo está ativo, logo, true = ativo e false = inativo
Campo CSV	situacaoVinculacaoProcesso

Campo PJEQL	data/consultaProcessoPeloNumero/processosTrfConexao/in_ativo
Exemplo	false / true

Prioridade

Descrição	Elemento destinado a permitir a identificação da existência de prioridades processuais não óbvias, ou seja, aquelas que não são resultado direto da identificação da classe processual (ex.: habeas corpus ou mandado de segurança). Na versão 2.0, será texto livre, mas é recomendável utilizar os seguintes textos identificadores: "IDOSO" "RÉU PRESO" "PERECIMENTO" "MENOR"
Campo CSV	prioridade
Campo PJEQL	data/consultaProcessoPeloNumero/prioridade
Exemplo	Idoso

Valor da causa

Descrição	Valor da relação jurídica. Não usar caracteres especiais, apenas números.
Campo CSV	valorDaCausa
Campo PJEQL	data/consultaProcessoPeloNumero/valorCausa
Exemplo	39000

Nível de Sigilo

Descrição	Nível de sigilo a ser aplicado ao processo. Dever-se-á utilizar os seguintes níveis: - 0: públicos, acessíveis a todos os servidores do Judiciário e dos demais órgãos públicos de colaboração na administração da Justiça, assim como aos advogados e a qualquer cidadão - 1: segredo de justiça, acessíveis aos servidores do Judiciário, aos servidores dos órgãos públicos de colaboração na administração da Justiça e às partes do processo. - 2: sigilo mínimo, acessível aos servidores do Judiciário e aos demais órgãos públicos de colaboração na administração da Justiça - 3: sigilo médio, acessível aos servidores do órgão em que tramita o processo, à(s) parte(s) que provocou(ram) o incidente e àqueles que forem expressamente incluídos - 4: sigilo intenso, acessível a classes de servidores qualificados (magistrado, diretor de secretaria/escrivão, oficial de gabinete/assessor) do órgão em que tramita o processo, às partes que provocaram o incidente e àqueles que forem expressamente incluídos - 5: sigilo absoluto, acessível apenas ao magistrado do órgão em que tramita, aos servidores e demais usuários por ele indicado e às partes que provocaram o incidente.
Campo CSV	nivelDeSigilo
Campo PJEQL	data/consultaProcessoPeloNumero/nivelAcesso
Exemplo	0

Data da autuação

Descrição	Este atributo corresponde a data de autuação do processo e sempre virá preenchido nos dadosBasicos do processo após uma consulta. Observação: Na entrega da manifestação não é preciso preencher este atributo.
Campo CSV	dataDaAutuação
Campo PJEQL	data/consultaProcessoPeloNumero/dataAutuação
Exemplo	2021-09-13T17:57:22.191Z Formato: 'AAAA/MM/DDTHH:MM:SS.SSSZ'

Pedido de liminar

Descrição	Indica se houve pedido de liminar no processo. Retorna os valores true (verdadeiro) ou false (falso)
Campo CSV	pedidoDeLiminar
Campo PJEQL	data/consultaProcessoPeloNumero/pedidoLiminar
Exemplo	false / true

Número SISPL

Descrição	Número do processo antigo do SISPL, para processos digitalizados.
Campo CSV	numeroSISPL
Campo PJEQL	data/consultaProcessoPeloNumero/numeroSispl
Exemplo	2010.01.1.032950-9

Processo de Origem

Descrição	Número do processo de origem no formato do CNJ.
Campo CSV	processoDeOrigem
Campo PJEQL	data/consultaProcessoPeloNumero/numeroProcessoOrigem
Exemplo	2010.01.1.032950-9

Incidental

Descrição	Indica se o processo é incidental.
Campo CSV	incidental
Campo PJEQL	data/consultaProcessoPeloNumero/incidental

Exemplo	false / true
---------	--------------

Objeto do processo

Descrição	Campo utilizado internamente, em formato de texto livre, para classificar o objeto do processo.
Campo CSV	objetoDoProcesso
Campo PJEQL	data/consultaProcessoPeloNumero/objetoProcesso
Exemplo	Processo referente ao cumprimento de sentença do processo nº 2013.01.1.186249-9

Justiça 100 Digital

Descrição	Campo que indica se houve pedido de juízo 100% digital.
Campo CSV	justica100Digital
Campo PJEQL	data/consultaProcessoPeloNumero/justica100Digital
Exemplo	false / true

Processo Digitalizado

Descrição	Campo que indica se o processo foi digitalizado.
Campo CSV	processoDigitalizado
Campo PJEQL	data/consultaProcessoPeloNumero/digitalizado
Exemplo	

Magistrados que atuaram no processo

Descrição	Nome do magistrado que atuou no processo
Campo CSV	magistradosQueAtuaram
Campo PJEQL	data/consultaProcessoPeloNumero/magistradosQueAtuaram
Exemplo	Maria da Silva

Órgão Julgador – Código

Descrição	Identificador do órgão julgador do processo.
Campo CSV	codigoOrgaoJulgador

Campo PJEQL	data/consultaProcessoPeloNumero/orgaoJulgador/id
Exemplo	144

Órgão Julgador - Nome

Descrição	Descrição do órgão julgador do processo.
Campo CSV	nomeOrgaoJulgador
Campo PJEQL	data/consultaProcessoPeloNumero/orgaoJulgador/descricao
Exemplo	2ª Vara Cível de Ceilândia

Plano Classificação e Tabela de Temporalidade Utilizada

Descrição	Descrever qual a versão do plano de classificação e tabela de temporalidade foi utilizado para extrair os metadados deste documento.
Campo CSV	versaoPCTT
Onde buscar	No Sistema de Gestão de Tabelas Processuais Unificadas (https://www.cnj.jus.br/sgt/versoes.php) <pre>Function getDataUltimaVersao() /** * Retorna uma String contendo a data da última versão * * @return String */ (Obs: data extraída no momento do cálculo da temporalidade no PJE-Arq)</pre>
Exemplo	Plano de classificação e tabela de temporalidade de documentos - PCTT-AD TJDF (Minuta de Proposta do PCTT-TJDF - Versão 1-47)

Prazo de guarda

Descrição	Indicação do prazo estabelecido em tabela de temporalidade para o cumprimento da destinação.
Campo CSV	prazoGuardaClassificacao
Onde buscar	PJe-Arq
Exemplo	Um (01) ano de guarda em arquivo corrente e depois é recolhido para o arquivo permanente.

Destinação prevista

Descrição	Indicação da próxima ação de destinação (transferência, eliminação ou recolhimento) prevista para o documento, em cumprimento à tabela de temporalidade.
-----------	--

Campo CSV	destinacaoPrevista
Onde buscar	PJe-Arq
Exemplo	Repositório Arquivístico Digital - Tribunal de Justiça do Distrito Federal e dos Territórios

Submission Documentation

Ficará no JSON os dados que se repetem e não são possíveis de elaborar um csv com 2 ou mais linhas. São os campos referentes a: documento; partes; movimentação processual;

Documento

Identificador do documento

Descrição	Identificador do Documento.
Campo CSV	idDocumento
Campo PJEQL	data/consultaProcessoPeloNumero/processosDocumento/id
Exemplo	123456

Identificador do documento principal

Descrição	Identificador do documento principal caso este documento seja um anexo. Se o campo estiver null, significa que este documento é principal
Campo CSV	idDocumentoVinculado
Campo PJEQL	data/consultaProcessoPeloNumero/processosDocumento/documentoPrincipalId
Exemplo	123456

Situação do documento

Descrição	Situação do documento. A propriedade informa se o campo está ativo, logo, true = ativo e false = inativo
Campo CSV	documentoAtivo
Campo PJEQL	data/consultaProcessoPeloNumero/processosDocumento/in_ativo
Exemplo	false / true

Tipo de documento - Código

Descrição	Código do tipo de documento disponível no serviço "ConsultaPJe" - Ex.: 58 - Petição Inicial, 118A - Informações. O código variará dependendo da instalação do PJe.
Campo CSV	codigoTipoDocumento
Campo PJEQL	data/consultaProcessoPeloNumero/processosDocumento/codigoTipoDeDocumento
Exemplo	123456

Tipo de documento - Nome

Descrição	Descrição do tipo de documento
Campo CSV	nomeTipoDocumento
Campo PJEQL	data/consultaProcessoPeloNumero/processosDocumento/descricaoTipoProcessoDocumento
Exemplo	Petição Inicial

Data e hora da criação

Descrição	Sequência de ano+dia+mês/hora+minuto+segundo. Atributo destinado a permitir a informação do momento em que o documento foi recebido pelo Poder Judiciário. É opcional no caso de documento enviado para protocolo.
Campo CSV	dataHoraCriacao
Campo PJEQL	data/consultaProcessoPeloNumero/processosDocumento/processoDocumentoBin/dataInclusao
Exemplo	12/12/2012 14:32:00

Descrição

Descrição	Descrição do documento.
Campo CSV	descricao
Campo PJEQL	data/consultaProcessoPeloNumero/processosDocumento/descricaoDocumento
Exemplo	Sentença; Carteira de motorista.

Hash

Descrição	Resumo matemático do documento enviado pelo algoritmo SHA-256.
-----------	--

Campo CSV	hash
Campo PJEQL	data/consultaProcessoPeloNumero/processosDocumento/processoDocumentoBin/descricaoMd5Documento
Exemplo	b0c020615d91c745a8cb54025cece674

Documento Sigiloso

Descrição	Propriedade que indica se o documento é ou não sigiloso.
Campo CSV	documentoSigiloso
Campo PJEQL	data/consultaProcessoPeloNumero/processosDocumento/documentoSigiloso
Exemplo	false / true

Mimetype

Descrição	Tipo do arquivo que será enviado, seguindo o seguinte domínio: application/pdf ou html/text. O PJe suporta os seguintes tipos de arquivos: pdf (máximo até 3Mb), mpeg (máximo até 5Mb), ogg (máximo até 10Mb), vorbis (máximo até 5Mb), png (máximo até 3Mb), mp4 (máximo até 10Mb) e quicktime (máximo até 10Mb).
Campo CSV	mimetype
Campo PJEQL	data/consultaProcessoPeloNumero/processosDocumento/processoDocumentoBin/descricaoExtensao
Exemplo	video/mp4, application/pdf

Assinatura

Descrição	Contém os dados em Base64 do arquivo de assinatura do documento. Para arquivos em PDF ou HTML, que não sejam P7S, é necessário informar os dados da assinatura.
Campo CSV	assinatura
Campo PJEQL	data/consultaProcessoPeloNumero/processosDocumento/processoDocumentoBin/descricaoSignature
Exemplo	assinaturadeteste

Usuário da assinatura

Descrição	Identificador do usuário que realizou a assinatura. O MNI salva o ID do usuário, mas pode-se gravar o CPF ou ambos.
Campo CSV	usuarioDaAssinatura
Campo PJEQL	data/consultaProcessoPeloNumero/processosDocumento/processoDocumentoBin/usuarioUltimoAssinar

Exemplo	123456
---------	--------

Algoritmo hash

Descrição	Algoritmo utilizado para gerar a assinatura: MD5withRSA, SHA1withRSA, SHA256withRSA ou ASN1MD5withRSA. Atualmente, o mais utilizado é o SHA256withRSA. Atualmente, o mais utilizado é o SHA256withRSA
Campo CSV	algoritmoHash
Onde buscar	Será uma campo fixo com o valor MD5
Exemplo	MD5withRSA

Cadeia do certificado

Descrição	String do certificado. Caso seja do tipo PEM é necessário incluir inclusive as strings "BEGIN CERTIFICATE" e "END CERTIFICATE".
Campo CSV	cadeiaDeCertificado
Campo PJEQL	data/consultaProcessoPeloNumero/processosDocumento/processoDocumentoBin/cadeiaCertificado
Exemplo	-----BEGIN CERTIFICATE----- certchaindeteste= -----END CERTIFICATE-----

Codificação do certificado

Descrição	Codificação utilizada no certificado: "PEM" ou "PkiPath".
Campo CSV	codificacaoDoCertificado
Campo MNI	Dentro da tag assinatura, campo codificacaoCertificado
Exemplo	PkiPath

Data da assinatura

Descrição	Data e Hora da assinatura, obedecendo a sequência de ano+dia+mês+minuto+segundo.
Campo CSV	dataAssinatura
Campo PJEQL	data/consultaProcessoPeloNumero/processosDocumento/processoDocumentoBin/dataPrimeiraAssinatura
Exemplo	2021-09-13T17:57:20.985Z

Identificação do tipo de meio do documento

Descrição	Documento/volume/processo/dossiê: digital, não digital (convencionais/analógicos) ou híbrido, para controlar as relações entre os meios e o monitoramento de preservação.
Campo CSV	meioDocumental
Onde buscar	Será um texto fixo.
Exemplo	Documento digital

Gênero Documental

Descrição	É a configuração da informação no documento de acordo com o sistema de signos utilizado na comunicação do documento. Exemplos: Audiovisual; textual; cartográfico; iconográfico; multimídia.
Campo CSV	generoDocumental
Onde buscar	Será de acordo com o mime type do documento.
Exemplo	Textual

Partes

Polo

Descrição	Descrição do polo processual da parte
Campo CSV	polo
Campo PJEQL	data/consultaProcessoPeloNumero/partes/polo
Exemplo	Ativo

Nome da parte

Descrição	Nome da parte que compõe o polo do processo.
Campo CSV	nome
Campo PJEQL	data/consultaProcessoPeloNumero/partes/nome
Exemplo	Vanessa Rocha

Nome social

Descrição	Nome da parte que compõe o polo do processo.
Campo CSV	nomeSocial
Campo PJEQL	data/consultaProcessoPeloNumero/partes/nomeSocial
Exemplo	Vanessa Rocha

Sexo da parte

Descrição	Correspondente a pessoa parte, onde "M" masculino; "F" feminino; "D" desconhecido.
Campo CSV	sexo
Campo PJEQL	data/consultaProcessoPeloNumero/partes/pessoaFisica/sexo
Exemplo	Feminino

Nome do genitor

Descrição	Nome completo do pai da pessoa parte.
Campo CSV	nomeDoGenitor1
Campo PJEQL	data/consultaProcessoPeloNumero/partes/pessoaFisica/nomeGenitor
Exemplo	Francisco Rocha

Nome da genitora

Descrição	Nome completo da mãe da pessoa parte.
Campo CSV	nomeDoGenitor2
Campo PJEQL	data/consultaProcessoPeloNumero/partes/pessoaFisica/nomeGenitora
Exemplo	Maria Rocha

Data de nascimento da parte

Descrição	Data do nascimento no formato AAAAMMDD.
Campo CSV	dataDeNascimento
Campo PJEQL	data/consultaProcessoPeloNumero/partes/pessoaFisica/dataNascimento
Exemplo	19900104

Data de óbito da parte

Descrição	Data do falecimento no formato AAAAMMDD.
Campo CSV	dataDeObito
Campo PJEQL	data/consultaProcessoPeloNumero/partes/pessoaFisica/dataObito
Exemplo	20100529

Número do documento principal

Descrição	Número do documento principal da pessoa parte, devendo ser utilizado o RIC ou o CPF para pessoas físicas, nessa ordem, ou o CNPJ para pessoas jurídicas. O atributo é opcional em razão da possibilidade de haver pessoas sem documentos ou cujos dados não estão disponíveis.
Campo CSV	numeroDocumentoPrincipal
Campo PJEQL	data/consultaProcessoPeloNumero/partes/cpfCnpj
Exemplo	99999999999

Situação da parte

Descrição	Situação do cadastro da parte no momento do arquivamento
Campo CSV	situacaoParte
Campo PJEQL	data/consultaProcessoPeloNumero/partes/situacao
Exemplo	Ativo

Tipo de pessoa

Descrição	Indicar qual o tipo de pessoa que será integrante do processo. Enviar um dos seguintes valores, sem acentos: "fisica"; "juridica"; "autoridade"; "orgaorepresentacao".
Campo CSV	tipoDePessoa
Campo PJEQL	data/consultaProcessoPeloNumero/partes/tipoPessoa/descricao
Exemplo	Física

Nome Fantasia

Descrição	Nome fantasia, para o caso da parte pessoa jurídica.
-----------	--

Campo CSV	nomeFantasia
Campo PJEQL	data/consultaProcessoPeloNumero/partes/pessoaJuridica/nomeFantasia
Exemplo	TJDFT

Pessoa vinculada

Descrição	Indicação da existência de um relacionamento entre uma autoridade e uma pessoa jurídica ou ente que ela representa. Exemplo: a escola é vinculada a seu diretor ou reitor. Sugestão: Salvar o nome da pessoa ou criar outro campo, se necessário, para salvar o CPF. Só temos o CPF da pessoa responsável. Não gravamos o nome da pessoa.
Campo CSV	pessoaVinculada
Campo PJEQL	data/consultaProcessoPeloNumero/partes/pessoaJuridica/cpfResponsavel
Exemplo	11122233344

Cidade natural

Descrição	Local de nascimento da pessoa parte.
Campo CSV	cidadeNatural
Campo PJEQL	data/consultaProcessoPeloNumero/partes/pessoaFisica/municipio
Exemplo	Brasília

Estado natural

Descrição	Estado de nascimento da pessoa parte. A implementação de codificação/decodificação deverá interpretar o valor do campo como se tratando da sigla de duas letras identificadoras das unidades federativas brasileiras.
Campo CSV	estadoNatural
Campo PJEQL	data/consultaProcessoPeloNumero/partes/pessoaFisica/estado
Exemplo	DF

Nacionalidade da parte

Descrição	País de nascimento da pessoa parte. Exemplo: "BR"-Brasil. Dever-se-á utilizar, preferencialmente, o código ISO-3166-1-alpha-2 (http://www.iso.org/iso/english_country_names_and_code_elements) pertinente ao país respectivo.
-----------	--

Campo CSV	nacionalidade
Campo PJEQL	data/consultaProcessoPeloNumero/partes/pessoaFisica/pais
Exemplo	BR

Código do documento de identificação da parte

Descrição	Número do documento identificador vinculado ao tipo de pessoa, podendo ser o número do CPF, CNPJ, RG, TIT, etc. São uma sequência de caracteres que tornam único o documento descrito sem os separadores característicos.
Campo CSV	codigoDoDocumentoDeIdentificacao
Campo PJEQL	data/consultaProcessoPeloNumero/partes/documentoIdentificacao/numeroDocumentoIdentificacao
Exemplo	999.999.999-99

Emissor do documento de identificação da parte

Descrição	Entidade emissora do documento. Exemplo: SSP, Cartórios, Justiça Eleitoral, SRFB.
Campo CSV	emissorDoDocumentoDeIdentificacao
Campo PJEQL	data/consultaProcessoPeloNumero/partes/documentoIdentificacao/orgaoExpedidor
Exemplo	SSP

Tipo do documento de identificação da parte

Descrição	Elemento destinado a permitir a identificação dos diversos tipos de documentos de identificação existentes. Trata-se de enumeração dos seguintes tipos: - CI: carteira de identidade - CNH: carteira nacional de habilitação - TE: título de eleitor - CN: certidão de nascimento - CC: certidão de casamento - PAS: passaporte - CT: carteira de trabalho - RIC: registro individual do cidadão - CMF: cadastro no Ministério da Fazenda Brasileiro - PIS_PASEP: número no programa de integração social - CEI: cadastro específico do INSS - NIT: número de identificação do trabalho - CP: cadastro em conselhos profissionais - IF: identidade funcional - OAB: número de cadastro na Ordem dos Advogados do Brasil - RJC: número de inscrição empresarial; - RGE: registro de identificação do estrangeiro
-----------	--

Campo CSV	tipoDoDocumentoDelidentificacao
Campo PJEQL	data/consultaProcessoPeloNumero/partes/documentoIdentificacao/tipoDocumento
Exemplo	CNH

Nome no documento de identificação

Descrição	Nome da parte detentora do documento.
Campo CSV	nomeNoDocumentoDelidentificacao
Campo PJEQL	data/consultaProcessoPeloNumero/partes/documentoIdentificacao/nomePessoa
Exemplo	José da Silva

Outro nome da parte

Descrição	Elemento destinado a permitir a inclusão de outros nomes da pessoa individualizada. Devem ser incluídos sob esse elemento os nomes que NÃO constam em documentos específicos. Em caso de nomes divergentes do principal existentes em documentos específicos, esses nomes devem ser indicados no atributo pertinente do documento.
Campo CSV	outroNome
Campo PJEQL	data/consultaProcessoPeloNumero/partes/nomesAlternativos
Exemplo	José da Venda

CEP endereço da parte

Descrição	CEP da parte do processo. Atributo indicador do código de endereçamento postal do endereço no diretório nacional de endereços da ECT. O valor deverá ser uma sequência de 8 dígitos, sem qualquer separador. O atributo é opcional para permitir a apresentação de endereços desprovidos de CEP e de endereços internacionais.
Campo CSV	cep
Campo PJEQL	data/consultaProcessoPeloNumero/partes/enderecos/cep/numeroCep
Exemplo	70300-000

Logradouro endereço da parte

Descrição	Logradouro vinculado ao CEP, tais como as ruas, avenidas, praças, jardins, etc.
Campo CSV	logradouro
Campo PJEQL	data/consultaProcessoPeloNumero/partes/enderecos/logradouro

Exemplo	Quadra 88
---------	-----------

Número endereço da parte

Descrição	Número vinculado ao CEP, podendo ser número da casa, apartamento, etc.
Campo CSV	numero
Campo PJEQL	data/consultaProcessoPeloNumero/partes/enderecos/numero
Exemplo	80

Complemento endereço da parte

Descrição	Dados adicionais do endereço.
Campo CSV	string
Campo PJEQL	data/consultaProcessoPeloNumero/partes/enderecos/complemento
Exemplo	Sala 10

Bairro endereço da parte

Descrição	Parte que compõe a cidade, devendo ser vinculada ao CEP.
Campo CSV	bairro
Campo PJEQL	data/consultaProcessoPeloNumero/partes/enderecos/bairro
Exemplo	Guará

Cidade endereço da parte

Descrição	Vinculada ao CEP, ou seja, nome da zona geográfica onde se agrupam as residências, comércios e indústrias.
Campo CSV	cidade
Campo PJEQL	data/consultaProcessoPeloNumero/partes/enderecos/cep/municipio/nome
Exemplo	Brasilia

Estado endereço da parte

Descrição	Sigla do Estado brasileiro, composto por duas letras.
Campo CSV	estado
Campo PJEQL	data/consultaProcessoPeloNumero/partes/enderecos/cep/municipio/uf/sigla

Exemplo	DF
---------	----

País endereço da parte

Descrição	Atualmente, para salvar o endereço é obrigatório informar um CEP válido. Portanto, mesmo não havendo campo específico para preencher o país, podemos auferir que o valor será sempre Brasil.
Campo CSV	pais
Campo fixo	Brasil
Exemplo	Brasil

Dados dos representantes processuais

Nome

Descrição	Nome do advogado ou do escritório de advocacia ou órgão de representação processual.
Campo CSV	nome
Campo PJEQL	data/consultaProcessoPeloNumero/partes/representantes/parte/nome
Exemplo	"B & G Advogados"

Situação

Descrição	Situação do cadastro do representante processual
Campo CSV	situacao
Campo PJEQL	data/consultaProcessoPeloNumero/partes/representantes/parte/situacao
Exemplo	"B & G Advogados"

Inscrição

Descrição	Inscrição do advogado ou escritório de advocacia no cadastro da Ordem dos Advogados do Brasil. O campo é preenchido no formato CCDDDDDDDC, sendo os primeiros 'C' dois caracteres indicativos da unidade federativa brasileira em que há a inscrição, os sete dígitos 'D' seguintes o número da inscrição, devendo incluir zeros ('0') à esquerda caso o número tenha menos de 7 dígitos e o último caracter a letra identificadora do tipo de inscrição.
Campo CSV	inscricao

Campo PJEQL	data/consultaProcessoPeloNumero/partes/representantes/parte/numeroOAB
Exemplo	1254DF

Número do documento principal

Descrição	O número RIC ou o CPF, para advogados, ou o CNPJ, para escritórios de advocacia e órgãos de representação processual (MP, advocacia pública e defensoria pública).
Campo CSV	numeroDoDocumentoPrincipal
Campo PJEQL	data/consultaProcessoPeloNumero/partes/representantes/parte/cpfCnpj
Exemplo	11122233344

Tipo de representante

Descrição	Atributo que permite indicar o tipo de representante processual.
Campo CSV	tipoDeRepresentante
Campo PJEQL	data/consultaProcessoPeloNumero/partes/representantes/tipoRepresentante/descricao
Exemplo	Advogado"; "Escritório de advocacia"; "Ministério público"; "Defensoria pública";

Dados dos assuntos processuais

Principal

Descrição	Indica se o assunto será o principal do processo.
Campo CSV	principal
Campo PJEQL	data/consultaProcessoPeloNumero/assuntos/principal
Exemplo	false / true

Código Nacional

Descrição	Código do assunto processual, segundo SGT.
Campo CSV	codigoNacional
Campo PJEQL	data/consultaProcessoPeloNumero/assuntos/codigo
Exemplo	1945

Descrição do assunto

Descrição	Texto descritivo do assunto processual.
Campo CSV	descricaoAssunto
Campo PJEQL	data/consultaProcessoPeloNumero/assuntos/descricao
Exemplo	"Alimentos"

Movimentação Processual

Código da movimentação processual

Descrição	Código da movimentação de acordo com a SGT.
Campo CSV	codigoDaMovimentacao
Campo PJEQL	data/consultaProcessoPeloNumero/movimentos/codigo
Exemplo	390

Situação da movimentação processual

Descrição	Campo que traz a informação se a movimentação está ativa no processo, ou seja, não foi excluída ou inativada.
Campo CSV	situacaoDaMovimentacao
Campo PJEQL	data/consultaProcessoPeloNumero/movimentos/ativo
Exemplo	390

Nome da movimentação processual

Descrição	Nome da movimentação processual, conforme SGT.
Campo CSV	nomeDaMovimentacao
Campo PJEQL	data/consultaProcessoPeloNumero/movimentos/descricao
Exemplo	Sentença Proferida

Descrição completa da movimentação processual

Descrição	Descrição completa da movimentação, já com os complementos preenchidos.
Campo CSV	descricaoCompletaDaMovimentacao

Campo PJEQL	data/consultaProcessoPeloNumero/movimentos/textoFinalInterno
Exemplo	Decorrido prazo de Vanessa Rocha em 19/03/2021 23:59:59

Data da movimentação processual

Descrição	Data da movimentação em sequência de ano+dia+mês/hora+minuto+segundo.
Campo CSV	dataDaMovimentacao
Campo PJEQL	data/consultaProcessoPeloNumero/movimentos/data
Exemplo	2021-09-13T17:57:39.730Z

Apêndice F - Avaliação das políticas de segurança da informação do Tribunal e o modelo Hipátia

Política Corporativa de Segurança da Informação

INTRODUÇÃO

O presente estudo tem por objetivo avaliar o atual estágio de desenvolvimento do barramento tecnológico, integrante do modelo Hipátia de preservação digital, frente ao Guia de Boas Práticas Desenvolvimento, Infraestrutura e Segurança das Aplicações do TJDFT e a Política Corporativa de Segurança da Informação baseada na RESOLUÇÃO 21 DE 8 DE NOVEMBRO DE 2016.

A premissa é seguir as recomendações e melhores práticas definidas pelo Guia em relação aos requisitos de segurança da informação, arquitetura, experiência dos usuários, ferramentas, infraestrutura e operação, obedecendo as melhores práticas de mercado, antes e durante a implantação, o desenvolvimento e a manutenção das aplicações.

O Ibict considera de extrema importância padronizar os procedimentos de desenvolvimento da ferramenta em relação aos critérios do TJDFT para implantação, manutenção, sustentação e eventual desligamento, de forma a garantir isonomia nos princípios de segurança de sistemas durante todo o ciclo de vida da aplicação.

RESOLUÇÃO 21 DE 8 DE NOVEMBRO DE 2016

Dispõe, no âmbito do Tribunal de Justiça do Distrito Federal e dos Territórios - TJDFT, sobre o Sistema de Gestão de Segurança da Informação - SGSI e a Política Corporativa de Segurança da Informação - PCSI.

Art. 1º O objetivo desta Resolução é estabelecer, implementar, manter e melhorar, continuamente, mecanismos e controles para promover a gestão da segurança da informação, de forma a garantir o direito de acesso previsto em Lei, a

proteção de dados, informações e conhecimentos gerados e custodiados, a redução de riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a disponibilidade, integridade, confiabilidade e autenticidade das informações, no âmbito do Tribunal de Justiça do Distrito Federal e Territórios - TJDF.

Art. 2º As normas desta Resolução aplicam-se a todas as autoridades, servidores, colaboradores e quaisquer pessoas que tenham acesso a informações do TJDF.

AValiação em relação ao Guia de Boas Práticas

REPOSITÓRIO DE CÓDIGO E VERSIONAMENTO

O código fonte da aplicação deve ser versionado no Gitlab institucional, preferencialmente. O controle das versões deve estar organizado com os branches e as tags adequadas. É necessário verificar quais usuários têm acesso ao projeto na ferramenta. É necessário verificar a visibilidade do projeto, sendo mais seguro defini-lo como PRIVATE.

Crítérios	Situação	Observação
Versionamento do Git institucional	OK	
Nomenclatura de branches	NÃO OK	Revisando de acordo com política interna
Nomenclatura de tags	NÃO OK	Revisando de acordo com política interna
Visibilidades do projeto	OK	
Controle de acesso ao projeto	OK	

AUTENTICAÇÃO ÚNICA

A ferramenta de SSO possibilita o controle de acesso único a vários sistemas, sejam eles conectados ou independentes. Recomenda-se a interação entre as aplicações e o SSO institucional para fins de login.

Critérios	Situação	Observação
integrada ao SSO institucional	não se aplica	-
Cadastros locais de usuários e senhas não devem ser usados	não se aplica	-
Mecanismos legados	não se aplica	-

LINGUAGENS DE PROGRAMAÇÃO E TECNOLOGIAS

As tecnologias e linguagens em que a aplicação será desenvolvida devem ser modernas e evoluídas por seus mantenedores, amplamente aceitas e validadas pela comunidade e deve-se observar o domínio da equipe técnica local.

Critérios	Situação	Observação
Front-Ends: Angular, Vue, React, Ember	não se aplica	-
Back-Ends: Spring Boot, Laravel, Django, Nodejs, Wildfly,	não se aplica	utiliza-se PYTHON
Plataformas: Jboss EAP, Kafka, RabbitMQ, Openshift	OK	-
Cache: Redis	OK	-
Bancos de dados: PostgreSQL, Oracle, MongoDB	não se aplica	utiliza-se MySQL (BD das soluções Arquivemática e AtoM)
Indexação: ElasticSearch, MeiliSearch	OK	-
Autenticação: Keycloak	não se aplica	-

REVISÃO DE CÓDIGO

A revisão de código visa garantir a qualidade por meio da conferência no código por outros desenvolvedores, de forma consciente e sistemática, para verificar se há erros ou falhas.

O código só estará pronto para ser implantado caso seja aprovado, segundo regras definidas, como por exemplo a necessidade de teste automatizado.

Critérios	Situação	Observação
Usar uma wiki, que é um documento formado por todas as atividades relacionadas ao projeto;	OK	utiliza-se a wiki e as issues do próprio Git do TJDFT
Usar checklists;	OK	Passo a passo de instalação e configurações
Estar atento às novas ameaças, para a segurança da aplicação;	OK	Por meio de grupos oficiais do Archivemática e AtoM
Usar a automação em conjunto com o trabalho manual, no intuito de identificar padrões e falhas recorrentes;	Não OK	reavaliando fluxo de trabalho
Usar ferramentas para otimizar o processo, como o Android Lint, o Findbugs e o Checkstyle.	Não se aplica	desenvolvimento em python

PADRÃO DE ARQUITETURA

Por padrão de arquitetura entende-se a adoção de uma solução anteriormente estudada, testada e documentada para um problema.

Critérios	Situação	Observação
Arquitetura Orientada a Mensagens (Eventos)	OK	-
desacoplamento entre aplicações	OK	-
Evitar a construção de sistemas monolíticos	OK	-
Comunicações entre sistemas devem ser feitas via serviço	OK	-
Aplicação deve ter seu próprio banco de dados	OK	-

TESTES AUTOMATIZADOS

Os testes automatizados são códigos implementados especificamente para testar o funcionamento da aplicação. Por meio desses, os programas tornam-se auto-testáveis.

Critérios	Situação	Observação
Testes automatizados dos tipos unitários	não OK	A ser implementado até o final do projeto
Cobertura mínima de 70%	não OK	A ser implementado até o final do projeto
Pipeline deve estar integrado com a ferramenta de qualidade	não OK	A ser implementado até o final do projeto

TESTES DE CARGA E TESTES DE STRESS

O teste de carga avalia o volume de transações, acessos simultâneos ou usuários que um servidor/software/ sistema suporta. O teste de stress pretende descobrir em que ponto a aplicação ultrapassa a sua capacidade de funcionamento.

Critérios	Situação	Observação
Teste de carga	não OK	avaliando metodologia, previsão de entrega até o final do projeto
Teste de stress	não OK	avaliando metodologia, previsão de entrega até o final do projeto

IMPLANTAÇÃO DE SOFTWARE TERCEIRO

Uma aplicação desenvolvida externamente - por contratação, cessão ou outro modelo - é necessária, primeiramente, a indicação formal de um indivíduo ou setor como responsável técnico. Esta designação deve compreender todo o ciclo de vida da solução - desde sua implantação, sustentação, eventuais evoluções e, fatalmente, seu desligamento. A necessidade de atualizações de versões, sempre que disponíveis, é medida crucial para a integridade e segurança do software. Da

mesma forma, as tecnologias de suporte devem seguir compatíveis, com suas respectivas modernizações.

Critérios	Situação	Observação
Técnico responsável pelo acompanhamento	OK	-

MONITORAMENTO DAS APLICAÇÕES

Percebe-se a necessidade de manter as aplicações e suas funcionalidades com alta disponibilidade. Para tanto, devem ser utilizados métodos para monitoramento da performance dos ambientes, bem como, sempre que possível, é recomendável a supervisão de funcionalidades críticas ou falhas frequentes conhecidas.

Critérios	Situação	Observação
Monitoramento de níveis 1, 2 e 3	em avaliação	previsão de entrega até o final do projeto
Ferramentas, tais como zabbix ou sentry	em avaliação	previsão de entrega até o final do projeto

DOCUMENTAÇÃO

É essencial para auxiliar usuários e programadores sobre as rotinas que estão contidas no software, facilitando o uso e o desenvolvimento de futuras evoluções.

Critérios	Situação	Observação
Documentação técnica no wiki do Gitlab	em avaliação	Atualizando wiki no Git do TJDF

INTEGRAÇÃO CONTÍNUA E ENTREGA CONTÍNUA

A aplicação da metodologia ágil de desenvolvimento, faz-se necessário adotar práticas alinhadas à aceleração de entregas de novas versões. O modelo de

MVPs (menor produto viável) exige maior frequência de atualizações, com a adoção de um método de trabalho que seja flexível e inteligente.

As etapas devem estar separadas, contendo passos de desenvolvimento, segurança e operação (DEVSECOPs) e sugere-se as seguintes: build -> test -> quality/security -> external.

Critérios	Situação	Observação
Pipeline configurado com as etapas adequadas no Gitlab institucional	OK	-
test são executados os testes automatizados	NÃO OK	em avaliação
quality/security a varredura do SonarQube	NÃO OK	em avaliação
external está a integração com a plataforma de gerenciamento de contêineres	OK	-
release automático no repositório	OK	-
deploy automático em produção	OK	-

BALANCEAMENTO DE CARGA

Importante uma boa distribuição do potencial tecnológico para garantir que todas as aplicações funcionem plenamente e atendam aos seus propósitos.

Critérios	Situação	Observação
Balanceamento de carga dos sistemas sobre múltiplas instâncias	em avaliação	• Estudo sobre o uso de pipelines no Archivematica. • Não se aplica ao barramento hipátia.

CONTÊINERES

O ambiente de contêiner é uma tecnologia que armazena todas as informações necessárias para que uma aplicação possa ser executada ou disponibilizada de forma isolada.

Critérios	Situação	Observação
Utilizar imagens de origem segura e minimalistas (com o mínimo de recursos necessários);	OK	-
Subir o serviço do contêiner sem o uso do usuário root (administrador);	OK	-
Utilizar volumes para persistência de dados de aplicação;	OK	-
Escolher protocolo de compartilhamento de arquivos adequado (NFS, iSCSI, Objeto), evitando o uso do CIFS (somente para exceções);	OK	-

ATUALIZAÇÃO DE TECNOLOGIAS UTILIZADAS

Toda a estrutura de linguagens, servidores de aplicação etc. precisa ser constantemente atualizada, tanto em suas versões mais recentes quanto para novas ferramentas que podem surgir.

Critérios	Situação	Observação
Atualizar as tecnologias usadas nas aplicações em produção	OK	-

IDENTIFICAÇÃO E TRATAMENTO DE VULNERABILIDADES

É fundamental a existência de um fluxo sistematizado, e de ação contínua, com foco em medidas de segurança das aplicações e na gestão de riscos. Some-se a isso a necessidade do uso cotidiano de critérios rígidos para o desenvolvimento, com observação das melhores práticas.

Critérios	Situação	Observação
Pipeline de sua aplicação deve estar integrado à ferramenta de qualidade	não OK	avaliar em qual ferramenta

ARMAZENAMENTO DAS CREDENCIAIS

As credenciais, chaves de acessos, keys, passphrases, tokens, entre outros, devem ser protegidos e armazenados da forma mais segura possível, evitando exposição em códigos e arquivos de configurações.

Critérios	Situação	Observação
Utilizar em suas aplicações, sempre que possível, as soluções de gerenciamento de credenciais homologadas e em uso pela SETI	não OK	ENV para OPENSIFT

PUBLICAÇÃO

Publicar uma aplicação é torná-la acessível aos usuários, por meio de uma URL, na rede interna ou na internet.

Critérios	Situação	Observação
Seguir o fluxo interno de requisição para publicação	OK	-

ITENS EM CONFORMIDADE COM A POLÍTICA DE SEGURANÇA

Itens	Observação
Repositório de Código e Versionamento	-
Versionamento do Git institucional	-
Visibilidades do projeto	-
Controle de acesso ao projeto	-
Linguagens de Programação e Tecnologias	-
plataformas: Jboss EAP, Kafka, RabbitMQ, Openshift	-
Cache: Redis	-
Indexação: Elasticsearch, MeiliSearch	-
Revisão de código	-
Usar uma wiki, que é um documento formado por todas as atividades relacionadas ao projeto;	-
Usar checklists;	-
Estar atento às novas ameaças, para a segurança da aplicação;	-
Padrão de Arquitetura	-

Arquitetura Orientada a Mensagens (Eventos)	-
desacoplamento entre aplicações	-
Evitar a construção de sistemas monolíticos	-
Comunicações entre sistemas devem ser feitas via serviço	-
Aplicação deve ter seu próprio banco de dados	-
Implantação de Software Terceiro	-
Técnico responsável pelo acompanhamento	-
Integração contínua e Entrega contínua	-
Pipeline configurado com as etapas adequadas no Gitlab institucional	-
external está a integração com a plataforma de gerenciamento de contêineres	-
release automático no repositório	-
deploy automático em produção	-
Contêineres	-
Utilizar imagens de origem segura e minimalistas (com o mínimo de recursos necessários);	-
Subir o serviço do contêiner sem o uso do usuário root (administrador);	-
Utilizar volumes para persistência de dados de aplicação;	-
Escolher protocolo de compartilhamento de arquivos adequados (NFS, ISCSI, Objeto), evitando o uso do CIFS (somente para exceções);	-
Atualização de Tecnologias Utilizadas	-
Atualizar as tecnologias usadas nas aplicações em produção	-
Publicação	-
Seguir o fluxo interno de requisição para publicação	-
Teste de stress	-
Monitoramento das Aplicações	-
Monitoramento de níveis 1, 2 e 3	-
Ferramentas, tais como zabbix ou sentry	-
Documentação	-
Documentação técnica no wiki do Gitlab	-
Integração contínua e Entrega contínua	-
test são executados os testes automatizados	-
quality/security a varredura do SonarQube	-
Balanceamento de Carga	-
Balanceamento de carga sobre múltiplas instâncias	-
Identificação e Tratamento de Vulnerabilidades	-

Pipeline de sua aplicação deve estar integrado à ferramenta de qualidade	-
Armazenamento das Credenciais	-
Utilizar em suas aplicações, sempre que possível, as soluções de gerenciamento de credenciais homologadas e em uso pela SETI	-

A análise do guia de boas práticas foi fundamental para avaliação do desenvolvimento do barramento Hipátia e das integrações com Archivematica e AtoM. A equipe de desenvolvimento do Ibict já iniciou a implementação de alguns dos itens e estuda a incorporação de metodologias para alinhar o código do sistema às conformidades apontadas no guia.

Apêndice G - Resultados do Diagnóstico de Maturidade

1. Política de Preservação Digital		
A preservação de documentos digitais acessíveis, autênticos e utilizáveis para o futuro, pelo tempo que for necessário, depende de tecnologias digitais de informação, mas depende igualmente de comprometimento organizacional e práticas. A organização com a obrigação de assegurar a preservação e acesso a documentos legais, fiscais e/ou históricos permanentes e de longo prazo, deve declarar sua política por escrito, comunicar a política a todas as partes interessadas, e periodicamente auditar a política, buscando garantir a conformidade. Uma política de preservação digital escrita inclui o propósito, o escopo, a responsabilidade e a abordagem da transferência de documentos, e o gerenciamento operacional e a sustentabilidade de repositórios de preservação confiáveis.		
Nível	Métricas de Capacidade em Política de Preservação Digital	
0	A organização não possui uma política de preservação digital escrita.	
1	A organização possui uma política de preservação digital em desenvolvimento, mas ainda não foi aprovada ou publicada.	
2	A organização publicou uma política de preservação digital, e ela é amplamente difundida entre as partes interessadas.	x
	Conformidade com a ISO 14721	
3	A organização conduz anualmente uma autoavaliação, e relata o nível de aderência à política de preservação digital para seu corpo dirigente.	
4	A organização providencia uma revisão paritária* periódica, ou auditoria externa da política de preservação digital, e revisa a política conforme apropriado.	
OBS: A instituição não promove auto avaliações ou auditorias internas sobre a aderência e efetividade da política, as atualizações e revisões são realizadas por demanda. Com relação à auditoria externa, essa não é uma prática comum no Brasil e, principalmente, não há entidade acreditada para promover esse tipo de serviço. Neste caso, acreditamos que o ciclo de autoavaliação e auditoria interna sejam suficientes para satisfazer o nível 4.		

OBS: A instituição não promove auto avaliações ou auditorias internas sobre a aderência e efetividade da política, as atualizações e revisões são realizadas por demanda.

Com relação à auditoria externa, essa não é uma prática comum no Brasil e, principalmente, não há entidade acreditada para promover esse tipo de serviço. Neste caso, acreditamos que o ciclo de autoavaliação e auditoria interna sejam suficientes para satisfazer o **nível 4**.

2. Estratégia de Preservação Digital

A organização com a obrigação de preservar documentos digitais permanentes e de longo prazo deve tratar proativamente os riscos associados com a obsolescência tecnológica. Enquanto nenhuma estratégia única é apropriada para todas as organizações, tipos de informação e recursos, deve haver planos para atualizar periodicamente os dispositivos e mídias de armazenamento, além de formatos de arquivo.

Se não for monitorada, a obsolescência de dispositivos e mídias de armazenamento eventualmente irá tornar ilegíveis as cadeias de bits dos documentos digitais. A inevitável obsolescência de formatos de arquivo, especialmente nativos e proprietários, significa que ao longo do tempo aplicativos de software não serão capazes de transformar cadeias de bits em documentos digitais inteligíveis e usáveis.

A estratégia geralmente aceita é mitigar a obsolescência de dispositivos/mídia de armazenamento através de renovações planejadas e periódicas, o que, no correr do tempo, assegura que "cadeias de bits" possam ser lidas pelas tecnologias atuais (ver Componente 11).

A estratégia geralmente aceita para mitigar a obsolescência de formato de arquivo, é contar com formatos tecnologicamente neutros, de padrão aberto e interoperáveis, que são considerados também "formatos preferenciais de preservação" (ver Componente 5).

Nível	Métricas de Capacidade em Estratégia de Preservação Digital	
0	A organização não possui uma estratégia formal para tratar a obsolescência tecnológica.	
1	A estratégia visa aceitar documentos digitais em formatos nativos em caráter <i>ad hoc</i> , e manter as cadeias de bits vivas até que software e outros recursos estejam disponíveis para transformar os documentos em formatos de arquivo tecnologicamente neutros e de padrão aberto.	
2	A estratégia visa encorajar os produtores de documentos a converter documentos digitais de longo prazo e valor permanente em sua custódia para formatos "prontos para preservação", no momento do recebimento e criação, ou próximo disso. A estratégia inclui monitoramento <i>ad hoc</i> de modificações em	

	tecnologias que possam impactar coleções de documentos digitais na custódia de produtores de documentos e repositórios de preservação.	
	Conformidade com a ISO 14721	
3	Adicionalmente à promoção de documentos “prontos para preservação”, a estratégia visa à transformação de documentos digitais em cinco (5) formatos de arquivo nativos selecionados, para formatos de preservação preferenciais durante a admissão, e monitoramento proativo de modificações em tecnologias que afetam a preservação de documentos digitais.	X
4	A estratégia visa à transformação de documentos digitais em formatos de arquivo nativos, para dez (10) ou mais formatos de preservação preferenciais durante a admissão. Documentos digitais no Armazenamento são automaticamente transformados em novos formatos interoperáveis, quando estes suplantarem os formatos atuais. O monitoramento proativo de modificações em tecnologias que afetem a preservação de documentos digitais é contínuo.	

Obs.: Aqui foram apontados possíveis problemas de tradução. Provavelmente o modelo define para o nível 3 que no mínimo 5 formatos de arquivos utilizados pelo produtor sejam convertidos para formatos de preservação além de mecanismos de monitoramento do contexto tecnológico e para o nível 4 que no mínimo 10 formatos de arquivo para formatos de preservação durante a admissão, além de mecanismos de monitoramento citados no nível 3 e que haja a conversão de formatos automática sempre que os formatos monitorados sofrerem risco de obsolescer.

Acreditamos que a variável de formatos de arquivo se dá pelo fato do modelo ser concebido para entidades preservadoras que tem pouca ou nenhuma gerência sobre o ambiente de produção e que deve estar preparada para receber os mais diversos formatos de arquivos oriundos dos produtores. Para o contexto do tribunal essa variável deve ser verificada pela capacidade de converter os formatos de produção definidos pelo programa de gestão e pela política de

preservação. Se a instituição for capaz de cumprir com 100% desses formatos haverá êxito em uma das variáveis para o nível 4 foi alcançada.

Tendo em vista que todos os formatos definidos pelo programa de gestão e pela política de preservação e que o monitoramento do contexto tecnológico é realizado ativamente, então o nível mais adequado para este item seria o nível 3.

Com relação a conversão automática de formatos, o Archivematica, em tese, deveria ser capaz de fazê-lo, no entanto, até a versão atual da ferramenta tal funcionalidade não foi implementada. Vale discutir se funcionalidade destacada pode ser integrada ao modelo com o uso de outras ferramentas.

3. Governança

Uma organização com obrigações em preservação digital deve possuir um processo formal de tomada de decisões, alinhado com sua estrutura de governança da informação corporativa, que atribua responsabilidades e autoridades para preservação de documentos digitais com valor permanente, e articule abordagens e práticas para que repositórios de preservação possam satisfazer as necessidades das partes interessadas. Essa capacidade, idealmente, faz proveito das regras, das práticas e dos protocolos existentes, bem como envolve as múltiplas partes interessadas.

A preservação de longo prazo, no entanto, pode exigir a criação de novas autoridades para tratar as ameaças da obsolescência tecnológica. Um repositório de preservação pode ser administrado por uma unidade administrativa ou de tecnologia, operada como um ou mais repositórios independentes sob o controle de uma unidade de Gestão de Arquivos ou Documentos; inclui a participação num sistema de repositórios federal ou regional, e/ou o uso de serviços de preservação digital fornecidos por terceiros. A organização exercita a governança de preservação digital em conjunto com arquivos, setores de tecnologia/gestão da informação, e com outros custodiadores e partes interessadas em preservação digital, como produtores de documentos e usuários. A estrutura de governança permite a conformidade do repositório de preservação com as leis aplicáveis, regulamentos, tabelas de temporalidade de documentos, instrumentos de destinação e padrões. Planos e decisões que sejam resultado de atividades de governança, incluindo estatísticas operacionais do repositório, são compartilhados com as partes interessadas internas e com operadores externos.

Nível	Métricas de Capacidade em Governança	
0	As atividades atuais de governança da informação da organização não abordam especificamente os requisitos de preservação digital.	
1	A organização possui uma estrutura de governança de preservação digital limitada, baseada em projetos, que está operacional ou foi concluída com sucesso.	
2	A organização está desenvolvendo uma estrutura de governança corporativa que identifica funções e responsabilidades para o gerenciamento do ciclo de vida de documentos digitais e preservação digital.	
	Conformidade com a ISO 14721	
3	A organização adotou uma estrutura de governança corporativa de preservação digital que inclui políticas abrangentes e procedimentos, e especifica um	x

	comprometimento contínuo com a sustentabilidade de um ou mais repositórios de preservação.	
4	A estrutura de governança corporativa de preservação digital mantém um ou mais repositórios de preservação, e é revisada e atualizada minimamente a cada dois anos, para absorver tecnologias e requisitos organizacionais em modificação.	
Obs.: Os ciclos de revisão e atualização se darão por demanda. Vale analisar se cabe o compromisso com ciclos periódicos de revisão.		

4. Colaboração

A preservação digital é uma disciplina multifacetada, que leva em conta a arquitetura de informação e o ambiente de tecnologia da organização, assim como as melhores práticas e padrões difundidos. Uma organização com a obrigação de preservar documentos digitais faz bem em manter e promover a colaboração entre as diversas partes interessadas.

Planos para diferentes tipos de documentos, modelos para abordagens de preservação e critérios, e uma estrutura de componentes e serviços de repositório exigem cooperação mais próxima e engajamento entre parceiros de longa data como TI, organizações semelhantes, fornecedores de serviços e software, e outras atividades de apoio. A colaboração deve reconhecer a interdependência entre as operações de produtores de documentos, requisitos legais e estatutários, políticas de tecnologia da informação e de governança, e responsabilidade histórica.

O engajamento ativo no tratamento dos desafios da preservação digital de longo prazo extrai melhor proveito dos recursos e das lições aprendidas. A estrutura colaborativa evolui em resposta às mudanças na tecnologia da informação e nas atividades de negócios dos Produtores de Documentos. Essa estrutura colaborativa procura alavancar recursos financeiros, humanos e técnicos, promover supervisão, e trocar conhecimento sobre o estado atual e futuro de iniciativas digitais. Essa estrutura colaborativa pode se estender além da organização, para incluir outros repositórios, agências federais ou de outro setor público, bem como consórcios de outras organizações com missão similar ou compartilhada.

Nível	Métricas de Capacidade em Colaboração	
0	Não existe nenhum ambiente de preservação digital colaborativo dentro da organização.	
1	A organização está atualmente trabalhando para estabelecer uma estrutura de engajamento colaborativo em gerenciamento de documentos digitais e problemas de preservação digital.	

2	Dentro de sua estrutura colaborativa de preservação digital, a organização contou com sucesso, ou está contando atualmente entidades interessadas selecionadas, para endereçar proativamente as necessidades de preservação digital. Esses contatos podem incluir iniciativas de preservação digital financiadas colaborativamente.	
	Conformidade com a ISO 14721	
3	Dentro de sua estrutura colaborativa de preservação digital, a organização contou com sucesso, ou está contando atualmente a maioria das partes interessadas, para identificar proativamente as necessidades de preservação digital e satisfazê-las.	
4	A organização monitora e atualiza continuamente sua estrutura colaborativa de preservação digital, estimulando o contato ativo com todas as partes interessadas, para identificar suas necessidades de preservação digital e satisfazê-las.	X
Obs.: Por se tratar de um projeto estratégico e de grande porte para instituição, todas as partes interessadas estão participando e colaborando ativamente com o desenvolvimento, governança e posterior manutenção de todo ecossistema de preservação. Pode-se verificar um grande compromisso institucional com a preservação digital e, portanto, cabe reavaliar se o nível 4 seria o mais adequado.		

5. Conhecimento Técnico

Uma capacidade de preservação digital viável exige das organizações que tenham conhecimento suficiente em gerenciamento de documentos digitais e preservação digital, para apoiar toda a infraestrutura e os processos-chave necessários, incluindo desenvolvimento profissional contínuo para o quadro funcional e certificação do repositório. O conhecimento técnico pode existir dentro do quadro funcional fixo ou de funcionários terceirizados, pode ser fornecido por um departamento centralizado, ou por prestadores de serviço externos.

NOTA: É provável que muitas organizações irão iniciar um programa de preservação digital de longo prazo com uma ou mais aplicações de gerenciamento eletrônico de documentos (GED) que estejam em conformidade com normas e padrões nacionais ou regionais, como a diretiva do Departamento de Defesa DoD 5015.2-STD, o *Model Requirements for the Management of Electronic Records* (MoReq2010), e a *Victorian Electronic Records Strategy* versão 2 (VERS2). Esses sistemas podem realizar algumas, mas não todas as funções ISO 14721.

Nível	Métricas de Capacidade em Conhecimento Técnico	
0	A organização tem pouco ou nenhum acesso operacional a conhecimento técnico especializado e profissional em preservação digital ou gerenciamento de documentos digitais.	
1	A organização tem acesso a conhecimento técnico profissional interno ou externo, que ampara apenas iniciativas de preservação digital baseadas em projetos e estritamente definidas. Isso pode também incluir conhecimento técnico em implantação de aplicações de gerenciamento eletrônico de documentos (GED) certificadas por um ou mais padrões.	
2	A organização tem acesso a conhecimento técnico profissional interno ou externo, que assessora produtores de documentos na criação de documentos prontos para preservação, e/ou executa serviços transitórios de Admissão e Armazenamento.	x
	Conformidade com a ISO 14721	
3	A organização tem acesso a conhecimento técnico profissional interno ou externo, que executa todas as funções de um repositório de preservação ISO 14721.	
4	A organização tem acesso a conhecimento técnico profissional interno ou externo, que executa todas as funções de um repositório de preservação ISO 14721, junto com a capacidade de avaliar o impacto de tecnologias emergentes que devem ser levadas em conta no planejamento de atividades de preservação digital de longo prazo.	
Obs.: A próxima etapa da autoavaliação será a aplicação de uma planilha de requisitos da resolução nº 43 do Conarq, que contempla as funcionalidades de um repositório de preservação de acordo com a ISO 14721.		

6. Formatos Tecnicamente Neutros e de Padrão Aberto

Um requisito para um programa sustentável de preservação digital, que assegure acesso de longo prazo a documentos digitais usáveis e inteligíveis, é a mitigação da obsolescência de formatos. As melhores práticas correntes para mitigação da obsolescência de formatos envolvem três ações separadas, porém relacionadas. A primeira ação é apoiar um Programa de Vigilância Tecnológica sobre a sustentabilidade de formatos de arquivo. Isso pode ser alcançado através de um serviço externo, como o fornecido pela Biblioteca do Congresso dos Estados Unidos¹⁵, ou o PRONOM¹⁶, o registro técnico do Arquivo Nacional do Reino Unido. A segunda ação envolve o comprometimento do repositório de preservação em adotar formatos de arquivo tecnicamente neutros e de padrão aberto (“OS/TN”) como formatos de preservação. A terceira ação refere-se ao engajamento proativo e a relações de trabalho colaborativas com produtores de documentos, para aconselhá-los sobre o uso de formatos de arquivo prontos para preservação quando eles criam e mantêm documentos digitais permanentes e de longo prazo, com valor histórico, legal ou financeiro, que serão transferidos para a custódia de um repositório de preservação. Arquivos neutros e de plataforma de padrão aberto são desenvolvidos em um contexto aberto e público, são especificados por uma organização padronizadora certificada, e possuem pouca ou nenhuma dependência tecnológica. Os formatos de arquivo OS/TN preferidos na atualidade incluem: CSV para planilhas HTML, Plain Text, XML, ODF, e PDF/A para texto JPGE 2000 para fotografias PDF/A, PNG, e TIFF para imagens escaneadas SVG para gráficos MPEG-4 e Motion JPEG2000 para vídeo WAVE_BWF LPCM para áudio WARC para páginas de internet Ao longo do tempo, ferramentas e soluções de preservação digital irão emergir, que exigirão novos formatos de arquivo tecnicamente neutros e de padrão aberto. Formatos tecnicamente neutros e de padrão aberto possuem retrocompatibilidade, para permitir a interoperabilidade entre plataformas tecnológicas, durante um período extenso de tempo. Métricas de Capacidade em Formatos Tecnicamente Neutros e de Padrão Aberto são fornecidos na próxima página.

Nível	Métricas de Capacidade em Formatos Tecnicamente Neutros e de Padrão Aberto	
0	A organização ainda não adotou nenhum formato de arquivo tecnicamente neutro e de padrão aberto (OS/TN) como formato preferencial de preservação.	
1	A organização adotou pelo menos um formato de arquivo OS/TN como formato preferencial de preservação.	
2	A organização adotou não mais que três formatos OS/TN como formatos preferenciais de preservação.	

Conformidade com a ISO 14721		
3	A organização adotou não mais que cinco formatos tecnologicamente neutros e de padrão aberto como formatos preferenciais de preservação digital (texto, planilhas, imagens escaneadas, gráficos vetoriais, fotos digitais, áudio, vídeo e páginas de internet). Um Programa de Vigilância Tecnológica é usado para monitorar a sustentabilidade desses formatos de arquivo OS/TN.	
4	A organização adotou dez ou mais formatos OS/TN como formatos de preservação digital preferenciais, e continuamente monitora a emergência de novos formatos de arquivo OS/TN, adotando-os, quando apropriado, para uso como formatos preferenciais de preservação digital.	X
Obs.: Os formatos de preservação foram definidos a partir das necessidades de formatos oriundos do ambiente de produção. Desta forma, a quantidade de formatos de preservação definidos são OS/TN e contemplam as demandas da instituição.		

7. Comunidade-Alvo

A organização que tem responsabilidade pela preservação e acesso a documentos digitais permanentes estará bem assessorada, se promover a expansão proativa e o engajamento com sua Comunidade-Alvo de produtores de documentos e usuários. Enquanto essa atividade tem sido tradicionalmente realizada por representantes de produtores de documentos, na forma de avaliação de documentos, revisão de tabela de temporalidade e autorização de destinação, os desafios da preservação digital demandam que profissionais de gestão de documentos se empenhem em ações “contracorrente” adicionais, no gerenciamento do ciclo de vida de documentos digitais permanentes e de longo prazo. Acordos de submissão 17 e protocolos de transferência devem ser padronizados, e acordos de nível de serviço definidos para as operações do repositório. Acordos e procedimentos formais com produtores de documentos registram o conteúdo, os direitos e condições sob os quais o repositório de preservação irá admitir, preservar e fornecer acesso a documentos digitais. Garantias específicas são dadas para assegurar o sigilo e a proteção de propriedade intelectual, onde apropriado. A organização mantém procedimentos escritos a respeito do acesso a suas coleções eletrônicas.

Pacotes de Informação para Disseminação (DIPs) são desenvolvidos e atualizados em conjunto com as suas comunidades de usuários (p. ex., estudantes, genealogistas, o público geral etc.). Procedimentos são regularmente revisados e atualizados para absorver práticas de negócio em evolução entre os produtores de documentos, bem como os interesses de pesquisa e a capacidade de acesso dos usuários.

Nível	Métricas de Capacidade em Comunidade-Alvo	
0	A organização não possui documentação formal que defina os direitos, obrigações e responsabilidades da Comunidade-Alvo, para documentos digitais serem transferidos para ou guardados por um repositório de preservação.	
1	A organização possui acordos <i>ad hoc</i> com produtores de documentos selecionados, que auxiliam a transferência de documentos digitais para um repositório de preservação.	
2	A organização possui acordos formais e escritos com poucos produtores de documentos, que auxiliam a transferência de SIPs transitórios, e contata proativamente usuários selecionados para identificar suas necessidades específicas e requisitos para acessar documentos digitais em sua custódia.	
	Conformidade com a ISO 14721	
3	A organização contata a maioria dos produtores de documentos em sua esfera de atividade, para estabelecer acordos escritos sobre seus direitos, obrigações e responsabilidades ao transferir Pacotes de Informação para Submissão (SIPs) para o repositório de preservação. A organização trabalha intimamente com a maioria dos usuários, para estabelecer perfis de DIPs que atendam suas necessidades e requisitos.	
4	A organização contata ativamente todos os produtores de documentos em sua esfera de atividade, para estabelecer acordos escritos sobre seus direitos, obrigações e responsabilidades ao transferir SIPs. Perfis de SIPs em conformidade são regularmente revisados e atualizados, para absorverem as práticas de negócio em evolução de produtores de documentos. A organização trabalha intimamente com todos os usuários para estabelecer perfis de DIPs que atendam suas necessidades e requisitos em evolução.	x

8. Pesquisa sobre Documentos digitais

Todas as organizações públicas e privadas são responsáveis por documentos criados, recebidos e adquiridos que sejam evidência de suas atividades de negócio, independentemente do formato ou mídia usados. Eles possuem a obrigação de assegurar a autenticidade, a integridade, a usabilidade e a fidedignidade dos documentos, pelo tempo que eles forem necessários.

Documentos com requisitos de guarda de longo prazo ou valor permanente eram tradicionalmente transferidos de uma área ou unidade administrativa para a custódia de uma atividade centralizada de Gestão Documental e/ou Arquivo, para preservação. Devido a fragilidade dos documentos digitais, organizações são aconselhadas a tratar proativamente a preservação digital, o mais próximo possível do momento da criação ou captura de documentos digitais. Isso é especialmente importante para documentos operacionais de longo prazo, quer dizer, documentos que irão permanecer na custódia da unidade administrativa e são considerados documentos "ativos".

Uma maneira efetiva de alcançar a preservação proativa é manter um inventário abrangente de documentos digitais e sistemas, bem como das relações de trabalho colaborativas entre as partes interessadas, que incluem produtores de documentos, Departamento Legal/de Conformidade, Arquivos, Gestão Documental, Serviços de Informação/Tecnologia e provedores externos de serviços, soluções e aplicações.

Uma característica-chave de repositórios digitais em conformidade com a ISO 14721 é a confiança em formatos tecnologicamente neutros e de padrão aberto. Durante o processo de admissão, documentos digitais em formatos proprietários são transformados em formatos de preservação preferenciais que a organização e/ou o repositório adotaram. Ao longo do tempo, e com o volume crescente de documentos digitais, a transformação de formato durante o processo de admissão pode se tornar penoso. Essa obrigação pode ser mitigada em parte se documentos "prontos para preservação", isto é, documentos que estão em formatos tecnologicamente neutros, interoperáveis e de padrão aberto, são produzidos no momento em que produtores de documentos criam ou capturam seus documentos, ou próximo a isso.

O objetivo de uma Pesquisa sobre Documentos digitais é identificar três categorias amplas de documentos digitais com prazo de guarda de dez (10) anos ou mais, com o intuito de apoiar as atividades de planejamento e preservação:

- Documentos digitais "prontos para preservação".
- Documentos "quase prontos para preservação", que são documentos digitais em formatos para os quais existem ferramentas que podem exportar formatos nativos de documentos para formatos tecnologicamente neutros, interoperáveis e de padrão aberto. Um exemplo é o

Microsoft Word 2007, que contém uma ferramenta para transformar documentos Word em formato PDF/A.

• Documentos “legados”, isto é, documentos digitais em formato proprietário nativo para o qual não existem ferramentas de exportação. A transformação de formatos proprietários nativos em formatos tecnologicamente neutros, interoperáveis e de padrão aberto provavelmente exigirá escrever código para auxiliar essa transformação, o que, por sua vez, pode ser oneroso. A coleta e análise de dados para uma Pesquisa sobre Documentos digitais pode ser alcançada por uma variedade de meios, incluindo pesquisas realizadas pela internet com produtores de documentos; entrevistas com unidades de negócio selecionadas ou terceiros que rotineiramente criem, recebam ou adquiram documentos digitais; revisão de tabela de temporalidade e destinação de documentos; e análise do portfólio de tecnologia da informação da organização, bem como o uso de ferramentas de pesquisa e algoritmos para identificar formatos de arquivo específicos, atualmente utilizados na captura e armazenamento de documentos digitais em unidades de disco conectadas em rede.

Nível	Métricas de Capacidade em Pesquisa sobre Documentos digitais	
0	A organização possui pouca ou nenhuma capacidade, ou recursos para coletar e analisar informação sobre o volume, locação, mídia, tipos de formato e requisitos de gerenciamento do ciclo de vida de documentos digitais.	
1	A organização usa a tabela de temporalidade existente para identificar documentos digitais de valor permanente histórico, fiscal e legal, em custódia dos produtores de documentos. Pode também conduzir entrevistas únicas e ad hoc, e pesquisas para identificar outros documentos digitais de valor permanente histórico, fiscal e legal.	
2	A organização usa entrevistas, pesquisas e análise retrospectiva sistemática da tabela de temporalidade existente para identificar documentos digitais de valor permanente histórico, fiscal e legal, em custódia de produtores de documentos selecionados. Esse esforço pode ser aprimorado através do foco em documentos digitais que tenham sido identificados como “em risco”.	
	Conformidade com a ISO 14721	
3	A organização suplementa a análise de documentos digitais “em risco” através de coleta de informação sobre o volume e locação, mídia e tipos de formato (pronto para preservação e quase pronto para preservação) de documentos digitais permanentes em custódia de produtores de documentos.	x

4	A organização identificou e categorizou todos os documentos digitais permanentes prontos para preservação, quase prontos para preservação e legados, em custódia de todos os produtores de documentos.	
Obs.: O tribunal está desenvolvendo mecanismos para o monitoramento sistemático do ambiente e produção.		

9. Admissão		
Um repositório de preservação que está em conformidade com as especificações funcionais da ISO 14721 e melhores práticas associadas, possui a capacidade de admitir sistematicamente (receber e aceitar) documentos digitais de produtores de documentos na forma de Pacotes de Informação para Submissão (SIPs). O repositório de preservação aceita SIPs de produtores de documentos, válida acordos e a integridade do conteúdo digital, movimenta os SIPs para uma área de preparação onde são realizadas verificações de vírus e validações de conteúdo e formato, transforma documentos digitais em formatos de preservação designados como apropriados, extrai metadados de SIPs e reescreve-os em Informação Descritiva de Preservação (PDI), cria Pacotes de Informação para Arquivamento (AIPs), e transfere os AIPs para a funcionalidade de Armazenamento do repositório.		
Nível	Métricas de Capacidade em Admissão	
0	A organização não possui um repositório de preservação digital capaz de receber ou admitir documentos digitais permanentes e de longo prazo.	
1	O repositório de preservação recebe documentos digitais de produtores de documentos baseado em acordos ad hoc sem preocupação com formato, integridade, verificação de vírus e qualidade dos metadados. Nenhum desses itens alcança o nível de um SIP em conformidade com a ISO 14721.	
2	O repositório recebe SIPs transitórios que são mantidos numa área de preparação enquanto verificações de vírus e validações de formatos são executadas manualmente. AIPs transitórios são criados manualmente e transferidos para o Armazenamento.	
Conformidade com a ISO 14721		

3	O repositório de preservação admite SIPs através de meios semiautomatizados que validam a completude das seguintes propriedades significativas: Administração, Informação Técnica, Proveniência, Descrição de Conteúdo e Descrição de Preservação. As propriedades significativas são extraídas dos SIPs e reescritas em Informação Descritiva de Preservação (PDI). Pacotes de Informação para Arquivamento (AIPs) são criados e transferidos para a funcionalidade de Armazenamento do repositório.	
4	O repositório de preservação admite SIPs através de meios automatizados que validam a completude das seguintes propriedades significativas: Administração, Informação Técnica, Proveniência, Descrição de Conteúdo e Descrição de Preservação. As propriedades significativas são extraídas dos SIPs e reescritas em Informação Descritiva de Preservação (PDI). Pacotes de Informação para Arquivamento (AIPs) são criados e transferidos para a funcionalidade de Armazenamento do repositório.	x
Obs.: O pacote e o fluxo de admissão dentro do Hipátia, mais especificamente no Archivematica, seguem as definições das pelas principais normas que versam sobre o funcionamento de repositórios de preservação.		

10. Armazenamento

O modelo de referência para sistemas abertos de arquivamento de informação ISO 14721 delinea uma quantidade de serviços sistemáticos de armazenamento automatizado, que auxiliam o recebimento e validação de transferências bem sucedidas de AIPs da admissão, a criação de Informação Descritiva de Preservação (PDI) para cada AIP, que confirma sua fixidez (i.e., que nenhuma corrupção ocorreu) durante qualquer ação de preservação ao realizar captura e manutenção de logs de erro, atualizações para PDI, incluindo transformação (i.e., migração) de documentos digitais para novos formatos, instâncias múltiplas de repositórios geograficamente separados, produção de Pacotes de Informação para Disseminação (DIPs) para acesso, e coleta de estatísticas operacionais.

O Armazenamento é dependente de outros serviços de preservação descritos no modelo de diagnóstico de maturidade, incluindo Migração (Renovação de Dispositivos/Mídias), proteções de Integridade e Segurança, e da disponibilidade e aplicação dos padrões de Metadados de Preservação.

Nível	Métricas de Capacidade em Armazenamento	
0	O repositório de preservação não trata de documentos digitais, ou seu acervo está em armazenamento primitivo (p. ex., uma unidade de disco compartilhada ou CDs/DVDs), onde estiver disponível.	

1	Uma única instância de um repositório de preservação suporta o armazenamento de AIPs transitórios com metadados limitados, que podem ser mapeados em Informação Descritiva de Preservação (PDI).	
2	Uma única instância de um repositório de preservação transitório suporta o armazenamento de AIPs transitórios, que incluem captura manual de algumas propriedades significativas de Administração, Informação Técnica, Proveniência e Informação de Conteúdo, e ações de preservação reprodutíveis.	
	Conformidade com a ISO 14721	
3	Uma única instância de um repositório de preservação suporta o armazenamento de AIPs. Ferramentas semiautomatizadas confirmam a completude de propriedades significativas e capturam todas as ações de preservação reprodutíveis. Resultados são transferidos para Informação Descritiva de Preservação, o que constitui uma cadeia de custódia digital auditável.	x
4	Duas ou mais instâncias geograficamente separadas de um repositório de preservação suportam o armazenamento de AIPs. Ferramentas automatizadas confirmam a completude de propriedades significativas e capturam todas as ações de preservação reprodutíveis. Resultados são transferidos para Informação Descritiva de Preservação, o que constitui uma cadeia de custódia digital auditável. A captura de estatísticas de armazenamento e de operação do repositório de preservação auxilia o planejamento contínuo e abrangente da preservação digital.	

11. Migração (Renovação de Dispositivos/Mídias)

Não existe dispositivo ou meio de armazenamento digital conhecido que seja invulnerável à degradação e à obsolescência. Uma capacidade fundamental de preservação digital, para uma organização que possui a responsabilidade de preservar documentos digitais de valor permanente e de longo prazo, é garantir a legibilidade das cadeias de bits que compõem os documentos digitais. A ISO 14721 especifica que os dispositivos e mídias de armazenamento de um repositório digital confiável devem ser monitorados e renovados ("replicar"/"reempacotar") periodicamente, para assegurar que as cadeias de bits permaneçam legíveis ao longo do tempo.

A degradação de mídias de armazenamento magnético e óptico é inevitável. Testes de envelhecimento acelerado predizem que a maioria das mídias de armazenamento magnético e óptico possuem uma expectativa de vida de 100 anos ou mais, se armazenadas em um ambiente controlado. Entretanto, mídias com expectativas de vida de centenas ou mesmo milhares de anos possuem pouco benefício prático, porque o problema fundamental em dispositivos ou mídias de armazenamento, para um repositório de preservação, é a obsolescência tecnológica. Isso provavelmente ocorrerá quando:

- Houver uma modificação de forma física (p. ex., de rolos de fita magnética de 10,5 polegadas para cartuchos de fita)
- Houver uma modificação no método de codificar fisicamente a informação na superfície de gravação, que torne impossível transferir conteúdo eletrônico de uma fita ou unidade de disco obsoleta, para uma atual
- Um fabricante decidir descontinuar um produto
- Um sistema legado ou aplicação for descomissionada, sem exportação dos documentos digitais para o novo ambiente computacional

Um repositório de preservação deve possuir um programa robusto de migração para dispositivos/mídias de armazenamento. Dependendo dos recursos disponíveis, esse programa de migração pode variar de dispositivos/mídias de armazenamento fora de rede, a dispositivos/mídias de armazenamento baseados em rede local, passando por fornecedores externos que provêm serviços de armazenamento que incluam migração de dispositivos/mídias de armazenamento. Independentemente de como e quando a migração de dispositivos/mídias de armazenamento ocorra, uma exigência crítica é que haja um protocolo vigente que determine a captura e preservação dos resultados da validação periódica da integridade de documentos digitais, antes e depois da conclusão da migração de dispositivos/mídias de armazenamento.

Nível	Métricas de Capacidade em Migração (Renovação de Dispositivos/Mídias)
-------	---

0	O repositório de preservação não possui protocolo formal vigente de migração para dispositivos e mídias.	
1	O repositório de preservação determina migração de dispositivos e mídias quando eles estão no limiar de tornarem-se obsoletos.	
2	O repositório de preservação determina migração de dispositivos e mídias numa base regular programada (p. ex., a cada dez anos).	
	Conformidade com a ISO 14721	
3	O atual programa de migração para dispositivos e mídias realiza um programa anual de inspeção de mídias, que identifica as mídias de armazenamento do repositório de preservação que estão diante de perda de dados iminente e catastrófica, e executa migração de dispositivos e mídias conforme apropriado.	x
4	O atual programa de migração para dispositivos e mídias monitora continuamente a perda potencial de legibilidade de documentos digitais, e automaticamente repõem dispositivos e mídias de armazenamento e transfere os documentos para novas mídias de armazenamento conforme apropriado.	

12. Integridade

Uma competência-chave em repositórios de preservação aderentes à ISO 14721 é assegurar a integridade (“fixidez”) dos documentos em sua custódia. Modificações acidentais ou intencionais podem ocorrer durante a migração de dispositivos/mídias, transferências internas de dados e outras ações de preservação. Uma maneira de estabelecer a integridade é através do uso de resumos de dispersão* criptográfica, que são as impressões digitais dos documentos digitais em um SIP, um AIP ou em alguma agregação dos dois.

Um resumo de dispersão criptográfica computado antes da operação de preservação digital e depois de sua conclusão detectará quaisquer modificações, até mesmo de um único bit. Resumos de dispersão são armazenados na Informação Descritiva de Preservação (PDI), onde eles podem ser revisados para confirmar que nenhuma modificação ocorreu durante a migração de dispositivos/mídias, transferências internas de dados e outras ações de preservação, garantindo assim uma cadeia de custódia eletrônica ininterrupta. A força dos resumos de dispersão varia, a mais baixa sendo MD5, e a mais alta sendo a SHA-3.18

Resumos de dispersão não garantem a cadeia de custódia eletrônica quando a ação de preservação envolve transformação de formato, porque as cadeias de bits que compõem os documentos digitais transformados não corresponderão às cadeias de bits antes deles serem transformados. Entretanto, isso pode ser compensado através da coleta de informação sobre todas as ações de preservação encetadas com relação aos AIPs, e armazenar essa informação na Informação Descritiva de Preservação do AIP. Acrescentar uma assinatura digital aos AIPs encapsulados em XML depois de cada ação de preservação também resulta numa cadeia de custódia eletrônica forte.

Nível	Métricas de Capacidade em Integridade	
0	O repositório de preservação não possui procedimento documentado para proteção da integridade dos documentos digitais em sua custódia.	
1	O repositório de preservação gera e preserva resumos de dispersão MD-5 de documentos digitais, antes e depois da migração de dispositivos/mídias e outras ações de preservação no Armazenamento.	x
2	O repositório de preservação gera e preserva resumos de dispersão SHA-1 antes e depois da migração de dispositivos/mídias e outras ações internas de preservação.	
Conformidade com a ISO 14721		

3	O repositório de preservação gera e valida resumos de dispersão SHA-2, antes e depois de todas as ações de preservação repetíveis das propriedades significativas de AIPs, através de meios semiautomatizados, e armazena-os na Informação Descritiva de Preservação (PDI).	
4	O repositório de preservação gera e valida resumos de dispersão SHA-2, antes e depois de todas as ações de preservação repetíveis das propriedades significativas de AIPs, através de meios automatizados, encapsula-os em XML, e assina-os com uma assinatura digital. Os procedimentos de proteção de integridade são continuamente avaliados e atualizados, enquanto novas ferramentas e abordagens se tornam disponíveis.	

13. Segurança

A preservação digital exige processos que restrinjam acesso ao repositório físico onde o conteúdo digital está armazenado, assegurem a segurança dos documentos digitais através de técnicas que bloqueiam acesso não autorizado, protejam a confidencialidade e o sigilo de documentos e direitos de propriedade intelectual, apoiem a realização de cópias de segurança periódicas dos documentos digitais que são armazenados em repositórios offsite, e auxiliem a recuperação após sinistros e a continuidade dos negócios.

Nível	Métricas de Capacidade em Segurança	
0	O repositório de preservação não possui procedimentos formais de recuperação após sinistro, de cópias de segurança ou de firewall vigentes, para proteger a segurança dos documentos digitais.	
1	O repositório de preservação garante a segurança dos documentos digitais em sua custódia através de procedimentos de recuperação após sinistro.	
2	O repositório de preservação garante a segurança dos documentos digitais em sua custódia através de uma proteção de firewall abrangente.	
	Conformidade com a ISO 14721	
3	O repositório de preservação garante a segurança dos documentos digitais em sua custódia através de gerenciamento abrangente de direitos de acesso, baseado em perfis.	

4	O repositório de preservação garante a segurança dos documentos digitais em sua custódia através de monitoramento contínuo dos processos de proteção e segurança, e revisando-os em resposta à evolução das capacidades tecnológicas e das exigências do negócio.	x
Obs.: O tribunal conta com uma robusta infraestrutura de TI e segue os principais protocolos de segurança do seguimento.		

14. Metadados de Preservação		
Um repositório de preservação coleta e mantém metadados que descrevem ações de preservação associadas com a custódia de documentos digitais permanentes. Metadados de preservação incluem uma trilha de auditoria que documenta ações de preservação empreendidas, porque e quando elas foram realizadas, como elas foram realizadas e com quais resultados. Uma boa prática atual é o uso de um esquema de metadados de preservação baseado em PREMIS para todos os documentos digitais permanentes, para garantir uma cadeia de custódia eletrônica que documenta a autenticidade ao longo do tempo, enquanto as ações de preservação são executadas. A captura de todos os metadados relacionados, transferência de metadados para quaisquer novos formatos/sistemas e armazenamento seguro de metadados são críticos. Todos esses metadados associados são armazenados na Informação Descritiva de Preservação (PDI) e mapeados logicamente nos AIPs.		
Nível	Métricas de Capacidade em Metadados de Preservação	
0	Um repositório de preservação primitivo possui pouco ou nenhum metadado de preservação para documentos digitais em sua custódia.	
1	O repositório de preservação possui um esquema de metadados de preservação ad hoc e estabelece uma cadeia de custódia mínima para os documentos digitais em sua custódia.	
2	O repositório de preservação possui um esquema PREMIS transitório para os documentos digitais em sua custódia, que garante uma cadeia de custódia limitada.	
Conformidade com a ISO 14721		
3	O repositório de preservação possui um esquema baseado em PREMIS semi-automatizado para a maioria dos documentos digitais em sua custódia, que garante uma cadeia de custódia sistematicamente auditável.	

4	O repositório de preservação possui um esquema PREMIS automatizado para todos os documentos digitais em sua custódia, que garante uma cadeia de custódia sistematicamente auditável.	x
Obs.: O Hipátia implementa o esquema de metadados PREMIS de forma automatizada.		

15. Acesso

O propósito da preservação digital é assegurar que documentos digitais usáveis, inteligíveis e confiáveis estejam acessíveis no futuro, pelo tempo que for necessário, sujeitos a quaisquer restrições impostas pelos produtores de documentos. Consequentemente, as comunidades de usuários devem possuir acesso a Pacotes de Informação para Disseminação (DIPs) derivados de Pacotes de Informação para Arquivamento (AIPs) que um repositório de preservação digital preserva apropriadamente. Em alguns casos, o repositório pode postar DIPs irrestritos em seu website. Baseado em expectativas e interesses de usuários, o repositório pode escolher limitar as “propriedades significativas e ações associadas” incluídas em DIPs, com o entendimento que elas serão disponibilizadas por demanda. Essa capacidade de acesso pode incluir a criação e manutenção de metadados de usuários pesquisáveis e recuperáveis, que podem ser investigados para identificar informações de interesse liberadas para divulgação (editadas ou censuradas para proteger o sigilo, a confidencialidade, e outros direitos onde for apropriado). Em nenhuma hipótese os usuários terão acesso direto a Pacotes de Informação para Arquivamento (AIPs) ou Informação Descritiva de Preservação.

Nível	Métricas de Capacidade em Acesso	
0	O repositório de preservação não possui nenhum documento digital em sua custódia, ou não possui capacidade para disponibilizar acesso aos documentos digitais em sua custódia.	
1	O repositório de preservação garante acesso aos documentos digitais em um único formato (p. ex., JPEG ou PDF), ao mesmo tempo em que aplica todas as restrições de acesso.	
2	O repositório de preservação garante acesso aos documentos digitais em pelo menos três formatos tecnologicamente neutros e de padrão aberto (p. ex., formatos PDF/A, JPEG e TIFF), ao mesmo tempo em que aplica todas as restrições de acesso.	x
Conformidade com a ISO 14721		

3	O repositório de preservação possui uma funcionalidade de pesquisa integrada e robusta, que garante a produção semiautomatizada de DIPs, junto com suas propriedades significativas associadas. Documentação auditável para a produção de DIPs é capturada, e tendências de consulta de usuários são usadas para identificar a necessidade de ferramentas de acessibilidade atualizadas.	
4	O repositório de preservação possui uma funcionalidade de pesquisa integrada e robusta, que garante a produção automatizada de DIPs e suas propriedades significativas associadas. Tendências de consulta de usuários são usadas para identificar a necessidade de ferramentas de acessibilidade atualizadas, e auditar os resultados da produção de DIPs.	

Nível de Capacidade atual		
	Níveis de Capacidade	Pontuação Final
	Capacidade Nominal de Preservação Digital	0
	Capacidade Mínima de Preservação Digital	1 – 15
	Capacidade Intermediária de Preservação Digital	16 – 30
	Capacidade Avançada de Preservação Digital	31 – 45
	Capacidade Ótima de Preservação Digital	46 – 60

Pontuação
48

Estágio 5: Capacidade de preservação digital ideal

O estágio 5 é o mais alto estágio de capacidade de prontidão de preservação digital que uma organização pode alcançar. Ele inclui um foco estratégico nos resultados de preservação digital, melhorando continuamente a maneira como o gerenciamento do ciclo

de vida dos documentos digitais. A capacidade de preservação digital do estágio 5 também envolve o benchmarking de infraestrutura e serviços em relação a outros programas de preservação digital "melhores da categoria" e a realização de monitoramento proativo para tecnologias inovadoras que possam permitir que o programa melhore seu desempenho de preservação digital. Poucos ou nenhum documento digital que mereça preservação a longo prazo estão em risco.

Conclui-se que o TJDFT é, certamente, uma das maiores referências de preservação digital do Brasil, não só em seu segmento como também no âmbito do Poder Executivo federal. O que é comprovado pela avaliação de sua maturidade no estágio máximo de capacidade. Algumas ações pontuais que precisam ser implementadas para alcançar a excelência em termos de preservação digital já estão previstas para o projeto. Sugerimos a aplicação deste diagnóstico em ciclos anuais.