CONSELHO NACIONAL DE JUSTIÇA

Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário

MoReq-Jus

2ª Edição

2023
CONSELHO NACIONAL DE JUSTIÇA
SAF SUL Quadra 2 Lotes 5/6 - CEP: 70070-600
Endereço eletrônico: www.cnj.jus.br

CONSELHO
NACIONAL
DE JUSTIÇA

Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário

MoReq-Jus

2ª Edição

Brasílila
2023

GRUPO DE TRABALHO (PORTARIA CNJ N. 252/2021)

Adriano da Silva Araújo - Juiz Auxiliar da Presidência CNJ

Alexandre Libonati de Abreu (coord. suplente) - Juiz Auxiliar da Presidência CNJ;

Anita Job Lübbe - Juíza do Trabalho TRT4;

Carlos Alexandre Böttcher (coordenador) - Juiz de Direito TJSP;

Fábio Ribeiro Porto (coord. suplente) - Juiz Auxiliar da Presidência CNJ;

Ingrid Schroder Sliwka (coord. suplente) - Juíza Federal TRF4;

João Thiago de França Guerra - Juiz Auxiliar da Presidência CNJ;

Marco Bruno Miranda - Juiz Federal TRF5;

Servidores(as) e colaboradores(as):

Eduardo Henrique Pereira de Arruda - PNUD/CNJ

Fabiano de Andrade Lima - TST

Gustavo Monteiro de Barros Barreto - TRF2

João Tiago Ferreira Soares Pessoa - TJPE

Júlio Cesar de Andrade - STJ

Luciane Baratto Adolfo - TJRS

Maria Rosa Torres Susana - TJRJ

Manoel Pedro de Souza Neto - TJAM

Neide Alves Dias de Sordi - STJ (aposentada)

Otacílio Marques Guedes - TJDFT

Pâmela Tieme Barbosa Aoyama - CNJ

Reginaldo Pereira de Matos - TST

Sidnei Roberto Feliciano da Silva – TJRO

Tassiara Jaqueline Fanck Kich – TRF4

Thiago de Andrade Vieira - DTI CNJ

Yan Amaral Engelke - TSE

GRUPO DE ANÁLISE DA CONSULTA PÚBLICA

Salise Monteiro Sanchotene - Conselheira do CNJ e Presidente da Comissão Permanente de Gestão Documental e de Memória do Poder Judiciário

Ricardo Fioreze - Secretário Especial de Programas, Pesquisas e Gestão Estratégica do CNJ

Ana Lúcia Andrade de Aguiar - Juíza Auxiliar da Presidência CNJ e Coordenadora do Comitê do Proname

Alexandre Libonati de Abreu - Juiz Auxiliar Presidência CNJ

Carlos Alexandre Böttcher - Juiz de Direito TJSP

Ingrid Schroder Sliwka - Juíza Federal TRF4

Marivaldo Dantas de Araújo - Juiz de Direito TJRN

Paulo Cristóvão de Araújo Silva Filho - Juiz Federal TRF4

Luciane Baratto Adolfo - Servidora TJRS

Neide Alves Dias de Sordi - Servidora aposentada STJ

Pâmela Tieme Barbosa Aoyama - Servidora CNJ

Rodrigo Franco de Assunção Ramos - Servidor CNJ

Tassiara Jaqueline Fanck Kich - Servidora TRF4

C755m
Conselho Nacional de Justiça.
Modelo de requisitos para sistemas informatizados de gestão de processos e documentos do Poder Judiciário: MoReq-Jus / Conselho Nacional de Justiça – 2 ed. – Brasília: CNJ, 2023.

201 p.
ISBN: 978-65-5972-119-1
1. Gestão de processos 2. Gestão documental 3. Sistemas informatizados 4. Requisitos e metadados 5. MoReq-Jus I. Título
CDD: 340

SUMÁRIO

APRESENTAÇÃO

O **Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (MoReq-Jus)** foi instituído em razão da necessidade de se estabelecerem requisitos mínimos de Gestão Documental para os sistemas informatizados do Poder Judiciário, de forma a garantir a confiabilidade, a autenticidade e a acessibilidade dos documentos e processos geridos por referidos sistemas pelo prazo necessário ao atendimento da legislação.

Desde a aprovação do Modelo pela Resolução CNJ nº 91/2009, ocorreram inúmeras mudanças relacionadas à disciplina e à implementação da temática no âmbito do Poder Judiciário. Naquele mesmo ano de 2009, foi instituído o Comitê do Programa Nacional de Gestão Documental e Memória do Poder Judiciário (Proname) do Conselho Nacional de Justiça (CNJ), que fora lançado no final do ano anterior de 2008, por meio de cooperação técnica com o Conselho Nacional de Arquivos (Conarq).

Coube ao Comitê do Proname a iniciativa de disciplinar a Gestão Documental dos órgãos do Poder Judiciário por meio da propositura de instrumentos e normativos, que deram origem, inicialmente, às Recomendações CNJ nº 37/2011 e nº 46/2013 e, posteriormente, à Resolução CNJ nº 324/2020.

Com o passar dos anos, o aprimoramento das políticas e programas de Gestão Documental pelos órgãos do Poder Judiciário, o incremento da utilização dos sistemas informatizados de processos judiciais e administrativos, o advento de novas tecnologias e a evolução do regramento legal e normativo suscitaram a necessidade de rever o Modelo de Requisitos vigente.

Com o objetivo de atualizar o MoReq-Jus, em atenção às modificações tecnológicas, legais e normativas, sobretudo com a aprovação da nova disciplina do Proname pela mencionada Resolução CNJ nº 324/2020 e a implementação do Programa Justiça 4.0, o Conselho Nacional de Justiça instituiu, por meio da Portaria CNJ nº 252/2021, Grupo de Trabalho multidisciplinar, composto por magistrados(as) e servidores(as) de vários órgãos do Poder Judiciário do país, com formação nas áreas de Direito, Arquivologia, Tecnologia da Informação, entre outras, que apresentou proposta no final do ano de 2022.

A proposta apresentada foi submetida a consulta pública no período de 26/01/2023 a 10/03/2023, cujas contribuições apresentadas foram analisadas por grupo de magistrados e servidores que promoveram adequações no texto e propuseram sugestão de ato normativo à apreciação da Presidência da Comissão Permanente de Gestão Documental e de Memória do Poder Judiciário, sendo a matéria objeto de apreciação pelo Plenário do Conselho Nacional de Justiça no Ato nº 0005445-23.2023.2.00.0000, com aprovação em Sessão Virtual finalizada em 15 de setembro de 2023.

O MoReq-Jus deve ser observado no desenvolvimento de todos os sistemas informatizados de gestão de documentos e processos administrativos e judiciais dos órgãos do Poder Judiciário, os quais são instrumentos do Proname.

O aprimoramento dos sistemas informatizados existentes por meio da aderência aos requisitos do Modelo, ora atualizado, é fundamental para que os órgãos do Poder Judiciário possam realizar efetivamente a gestão de seus documen-

tos. A observância do MoReq-Jus, por meio de sistemas próprios e com o apoio de sistemas externos quando necessário para a implementação dos requisitos funcionais e não funcionais, permite a adequada produção, classificação, uso, avaliação, conservação e destinação dos documentos institucionais, seja para a eliminação daqueles sem valor secundário, seja para a guarda permanente daqueles que compõem o Patrimônio cultural arquivístico do Poder Judiciário.

"Quem tudo guarda, nada preserva": essa premissa de experiência é válida para qualquer tipo de documento ou processo, seja físico ou eletrônico. Grande desafio do Poder Judiciário é lograr efetivar a gestão dos documentos, eliminando aqueles que tiverem cumprido sua função primária institucional e não trouxerem nenhum valor secundário. Recursos são finitos e sempre serão. A humanidade jamais terá condições de armazenar todas as informações produzidas.

Para a preservação da Memória do Poder Judiciário oriunda de nossa produção documental física e digital, revestida de natureza de Patrimônio cultural nacional (artigo 216 da Constituição Federal), é necessário que tenhamos sistemas informatizados aderentes ao MoReq-Jus sem os quais não poderemos avaliar os processos para sua destinação final: eliminação ou guarda permanente.

Além de efetivar a gestão de documentos e processos físicos e digitais, a implementação do Modelo, ora atualizado, visa a garantir a Preservação Digital.

O GestãoDoc, nome dado aos sistemas elaborados com fundamento nos requisitos do MoReq-Jus, atende as funcionalidades de normas técnicas internacionais e inclui os metadados que garantirão a preservação de longo prazo de dados e documentos digitais do Poder Judiciário em Repositório Arquivístico Digital Confiável (RDC-Arq), nos termos do artigo 34 da Resolução CNJ nº 324/2020, como ambiente seguro para essa finalidade. Os metadados de preservação estabelecidos pelo MoReq-Jus permitem a manutenção da cadeia de custódia ininterrupta no GestãoDoc, visando a garantir esse ambiente seguro durante todo o ciclo de vida dos documentos.

Com o MoReq-Jus, a obrigatoriedade de implementação do RDC-Arq, o Programa Justiça 4.0 e a Plataforma Digital do Poder Judiciário (PDPJ-Br), o Conselho Nacional de Justiça procura dar efetividade às recomendações da Carta da UNESCO para a Preservação do Patrimônio Arquivístico Digital, de forma a minimizar os efeitos da fragilidade e da obsolescência da tecnologia, assegurando, ao longo do tempo, o acesso contínuo e o uso pleno da informação a toda a sociedade (Conarq, 2005). Para tanto, é necessário que haja ampla articulação e cooperação dos órgãos do Poder Judiciário por meio da mencionada Plataforma (PDPJ-Br) e com organismos nacionais e internacionais comprometidos com a preservação do Patrimônio Arquivístico Digital..

Por fim, a profícua interlocução dos profissionais de Tecnologia da Informação e de Gestão Documental, alcançada nas atividades do Grupo de Trabalho, é o que se espera das respectivas áreas dos órgãos do Poder Judiciário no desenvolvimento e na adaptação de seus sistemas informatizados ao MoReq-Jus, corroborando a constatação de que a construção do conhecimento acontecerá cada vez mais de forma colaborativa, coletiva e interdisciplinar.

PARTE I

ASPECTOS GERAIS

1. INTRODUÇÃO

O **Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (MoReq-Jus)** estabelece critérios a serem cumpridos na captura, na produção, na classificação, na tramitação, na guarda, na avaliação, na seleção, no armazenamento, na indexação, na preservação, no arquivamento e no recebimento, pelos sistemas de gestão de processos e documentos digitais, não digitais ou híbridos, a fim de garantir a sua confiabilidade, autenticidade e acesso.

O MoReq-Jus estabelece requisitos mínimos para um Sistema Informatizado de Gestão de Processos e Documentos (GestãoDoc), independentemente da plataforma tecnológica em que for desenvolvido e implantado.

Um GestãoDoc deve ser capaz de gerenciar documentos e processos digitais, não digitais e híbridos.

Para os documentos não digitais, o sistema registra as referências a esses documentos e as operações de produção, de tramitação, de guarda, de armazenamento, de preservação, de arquivamento e de recebimento, podendo conter versões digitais desses documentos físicos. No caso dos sistemas de documentos digitais, esses registram também os documentos e as operações mencionadas.

Os sistemas de gerenciamento de documentos, já existentes para o controle dos documentos físicos, tiveram um incremento com a produção de documentos digitais. Esses sistemas devem incorporar requisitos arquivísticos para assegurar que os documentos possam manter-se autênticos e confiáveis.

A gestão de documentos não é questão afeta apenas às unidades de Arquivo, de Gestão Documental ou às Comissões Permanentes de Avaliação Documental, pois visa a garantir a produção, a guarda e o acesso aos documentos durante todo o seu ciclo de vida. Portanto, envolve os diversos atores e unidades da instituição e precisa também atender as demandas dos cidadãos, que são o destinatário dos serviços judiciais.

Dessa forma, resulta evidente que os sistemas informatizados de documentos administrativos e judiciais são também sistemas de gestão de documentos. Referida gestão permeia todas as etapas de um processo desde o protocolo, a distribuição, a classificação, o uso, a tramitação, a baixa, o arquivamento até a destinação final com a eliminação ou o recolhimento para guarda permanente.

Para melhor compreensão desse Modelo de Requisitos, alguns conceitos são relacionados a seguir e outros devem ser conferidos no Glossário.

a) Sistema de Informação

Conjunto organizado de políticas, procedimentos, pessoas, equipamentos e programas computacionais que produzem, processam, armazenam e proveem acesso à informação proveniente de fontes internas e externas para apoiar o desempenho das atividades do Poder Judiciário brasileiro.

b) Gestão de Documentos

Conjunto de procedimentos e operações técnicas, que engloba a produção de documentos, a tramitação, a utilização, a avaliação e o arquivamento em fase corrente e intermediária, visando a sua eliminação ou o seu recolhimento para guarda permanente, conforme artigo 3º da Lei nº 8.159/91 e artigo 2º, inciso I, da Resolução CNJ nº 324/2020.

c) Sistema Informatizado de Gestão de Processos e Documentos (GestãoDoc)

Sistema desenvolvido para produzir, gerenciar a tramitação, receber, armazenar, dar acesso e destinar documentos em ambiente eletrônico. Pode compreender um *software* particular, um determinado número de ***softwares*** integrados — adquiridos ou desenvolvidos — ou uma combinação desses. Envolve um conjunto de procedimentos e operações técnicas característicos do sistema de gestão de processos e documentos, processado eletronicamente e aplicável em ambientes digitais ou em ambientes híbridos — documentos digitais e não digitais ao mesmo tempo.

Um GestãoDoc inclui diversas operações, tais quais, produção do documento, controle de sua tramitação, aplicação do plano de classificação, controle de versões, controle sobre os prazos de guarda e destinação, armazenamento seguro e procedimentos que garantam o acesso e a preservação a médio e longo prazo de documentos digitais e não digitais, mantendo-os confiáveis, íntegros e autênticos.

No caso dos documentos digitais, um GestãoDoc deve ser empregado por todos os órgãos do Poder Judiciário.

A partir dessas premissas, podemos fazer as seguintes considerações:

- Um sistema de informação pode abarcar todas as fontes de informação existentes nos órgãos do Poder Judiciário, incluindo, principalmente, os sistemas de gestão de processos judiciais, administrativos e de documentos;
- O GestãoDoc, mantém a organicidade dos documentos e sua inter-relação com as atividades da instituição;
- A concepção de um GestãoDoc, por ser um sistema de gestão de processos e documentos, tem que ocorrer concomitantemente com a adoção de uma política de gestão de documentos;
- O ciclo de vida dos documentos refere-se às sucessivas etapas pelas quais passam: produção, tramitação, uso, avaliação, arquivamento e destinação (guarda permanente ou eliminação).

Requisitos arquivísticos que caracterizam um GestãoDoc:

- Captura, armazenamento, indexação e recuperação de todos os tipos de documentos institucionais e de todos os componentes digitais do documento institucional como uma unidade complexa;
- Gestão dos documentos desde a sua produção, classificando-os para manutenção da relação orgânica entre eles;
- Implementação de metadados associados aos documentos para descrever o contexto em que se inserem (jurídico-administrativo, de proveniência, de procedimentos, documental e tecnológico);
- Integração da gestão de documentos físicos e digitais no mesmo sistema;

- Armazenamento seguro para garantir a integridade dos documentos;
- Avaliação e seleção dos documentos para recolhimento e preservação daqueles considerados de valor permanente, de acordo com os atos normativos do Conselho Nacional de Justiça e do órgão;
- Aplicação de critérios de classificação e guarda;
- Exportação dos documentos para fins de transferência e recolhimento;
- Manutenção da cadeia de custódia para garantir a autenticidade dos registros;
- Instrumentos para apoio à preservação dos documentos.

Diversos pressupostos à implementação de um GestãoDoc, especialmente de requisitos não funcionais, adiante explicitados, constam como critérios a serem observados nos desenvolvimentos dos sistemas eletrônicos da área fim no âmbito da Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br), instituída pela Resolução CNJ nº 335/2020, que aponta para a construção de soluções que abranjam conceitos de interoperabilidade, acessibilidade, usabilidade, segurança de informação, otimização de fluxos de trabalho, automação de atividades, adequação à Lei Geral de Proteção de Dados Pessoais (LGPD), entre outros.

O desenvolvimento colaborativo e compartilhado, também incluído na referida Resolução CNJ nº 335/2020, permitirá que as soluções que vierem a ser elaboradas por aplicações, módulos, microsserviços e sistemas promovam a necessária e desejável associação entre os requisitos funcionais e os não funcionais, mais diretamente relacionados às ações de gestão documental, aproximando as políticas para a governança e gestão do processo judicial eletrônico e a instituída para a gestão documental pelo Proname, que são, em verdade, relacionadas de forma necessária e direta.

Importante destacar que não é vedado o emprego de soluções e ferramentas externas aos sistemas informatizados de gestão de processos e documentos adotados pelos órgãos do Poder Judiciário para apoio no cumprimento dos requisitos do Modelo.

Atualmente, a Preservação Digital constitui uma preocupação crescente dos profissionais ligados à gestão da informação. Para o Poder Judiciário, em razão do valor probatório da informação, é preciso, cada vez mais, garantir o acesso continuado aos acervos digitais em condições que assegurem a sua localização, preservação, legibilidade, usabilidade, confiabilidade e autenticidade a médio e longo prazos.

Nesse contexto, o MoReq-Jus constitui importante ponto de partida para o desenvolvimento e a implementação do RDC-Arq (Repositório Arquivístico Digital Confiável), "desenvolvido como software livre, gratuito e de código aberto, projetado para manter os dados em padrões de preservação digital e o acesso em longo prazo", conforme artigo 34 da Resolução CNJ n.º 324/2020.

De fato, o atendimento dos requisitos do MoReq-Jus possibilitará a transferência e o recolhimento da documentação dos sistemas informatizados para o RDC-Arq e consequentemente a sua preservação com a aplicação do modelo OAIS ("*Open Archival Information System*"), que constitui referência para preservação digital.

A transformação digital é uma revolução sem precedentes, que está sendo promovida pelas tecnologias digitais nas estratégias, nos sistemas de trabalho e nas interações da sociedade, dos governos e das organizações. A redução de custos e o aumento da eficiência em decorrência da informação em suportes digitais são evidentes. A importância dos meios e técnicas digitais de codificação, de armazenamento e de transporte da informação é amplamente reconhecida. Contudo, não são elucidados a contento os perigos associados ao caráter efêmero dessa informação e as dificuldades para a sua preservação.

A preservação da informação impressa é concentrada na preservação do papel, uma vez que nele estão o texto, a estrutura e de certa forma também o contexto do documento. Em meio digital, a preservação digital compreende a preservação física e lógica dos documentos. A preservação física está focalizada nos suportes materiais utilizados para o armazenamento do conteúdo, sejam eles magnéticos, ópticos ou quaisquer outros existentes ou que venham a ser desenvolvidos.

A preservação lógica procura na tecnologia formatos atualizados para a introdução dos dados (material audiovisual, correio eletrônico etc.) e novas aplicações de *hardware e software*, que mantenham em atividade os seus *bits* para conservar a sua capacidade de leitura.

Desse modo, a busca por estratégias de preservação digital requer não apenas procedimentos de manutenção e recuperação de dados, no caso de perdas acidentais, para resguardar a mídia e seu conteúdo, mas também estratégias e procedimentos para manter sua acessibilidade e autenticidade ao longo do tempo, o que requer a aplicação de padrões de metadados e documentação.

A longo prazo, o fracasso na preservação dos documentos digitais acarretará a perda irreversível do registro, da prova, do testemunho e da memória. Assim, a questão da preservação tem repercussão em questões legais, comerciais e organizacionais, podendo ter impacto negativo na memória coletiva, pública e privada da sociedade.

Com a produção de documentos e processos em meio exclusivamente digital em grande parte dos órgãos do Poder Judiciário, torna-se premente a instituição de política de Preservação Digital com a definição de estratégias que garantam a preservação, a regulamentação de questões associadas ao valor probatório, a uniformização de procedimentos normativos e a definição de parâmetros para a certificação de qualidade.

De outra parte, em caso de suspensão ou extinção de um GestãoDoc, devem ser preservados os dados e metadados, garantindo-se os direitos de acesso à informação e expedição de certidão. Ademais, o acesso ao sistema deve permanecer apenas para consulta e não inclusão de novos documentos, ao passo que aqueles já inseridos deverão ser submetidos a classificação, avaliação e destinação de acordo com normas do Proname ou transferidos para outros sistemas em que as atividades de gestão documental serão realizadas. Esse processo de suspensão ou extinção deve ser documentado, incluindo planos de conversão ou mapeamento dos dados, pois essas informações serão necessárias à verificação de autenticidade, integridade e manutenção da acessibilidade dos documentos contidos no sistema suspenso ou extinto.

1.1 Histórico

A crescente produção de documentos digitais sobretudo a partir do início do século XXI e da promulgação da Lei nº 11.419/2006, que disciplinou o processo judicial eletrônico, levaram o Conselho da Justiça Federal (CJF), em março de 2007, a constituir Grupo de Trabalho para o estabelecimento de um conjunto de requisitos, que garantissem confiabilidade, autenticidade e acessibilidade aos documentos digitais geridos por esses sistemas.

O Grupo de Trabalho, integrado por especialistas das áreas de Ciência da Informação, Arquivologia, Tecnologia da Informação e Direito, contou com consultoria externa e iniciou seus estudos pelo e-Arq Brasil, aprovado pela Resolução Conarq nº 25/2007, e pelo "Model Requirements for the Management of Electronic Documents and Records – MoReq" de 2002, desenvolvido pela Comissão Europeia, com o objetivo de analisar a possibilidade de adoção desses modelos pela Justiça Federal.

No entanto, em razão das peculiaridades do processo judicial, o referido Grupo de Trabalho optou pela elaboração de modelo próprio, qual seja, o Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos da Justiça Federal (MoReq-Jus), que foi colocado em consulta pública e aprovado pela Resolução CJF nº 7, de 7 de abril de 2008, que disciplinou a obrigatoriedade da utilização do MoReq-Jus no desenvolvimento de novos sistemas informatizados para as atividades judiciais e administrativas, no âmbito do Conselho e da Justiça Federal de primeiro e segundo graus. Os metadados de segurança, auditoria e preservação foram posteriormente elaborados e incorporados ao MoReq-Jus.

Em março de 2009, o Conselho Nacional de Justiça (CNJ) instituiu Grupo de Trabalho para realizar a adaptação do MoReq- Jus Versão 1.1 do Conselho da Justiça Federal (CJF) para todo o Poder Judiciário brasileiro (DE SORDI, 2011). Em julho de 2009, uma nova versão do MoReq-Jus foi disponibilizada para consulta pública pelo CNJ e em 29 setembro do mesmo ano, essa nova versão foi aprovada pela Resolução CNJ nº 91, que instituiu o MoReq-Jus e disciplinou a obrigatoriedade da sua utilização no desenvolvimento e manutenção de sistemas informatizados para as atividades judiciais e administrativas no âmbito do Poder Judiciário. (MoReq-Jus 1ª edição). Naquele momento, não havia ato normativo do Conselho Nacional de Justiça, que disciplinasse a gestão documental.

Em 2010, o CNJ instituiu um outro Grupo de Trabalho para o desenvolvimento do Programa de Avaliação da Conformidade dos sistemas de gestão de processos e documentos do Poder Judiciário com o MoReq-Jus, em consonância com o programa de melhoria contínua de *software* previsto na Resolução nº 91/2009 (DE SORDI, 2010). Contudo, o programa não chegou a ser aprovado.

Transcorrida mais de uma década da aprovação do MoReq-Jus, o CNJ constituiu novo Grupo de Trabalho, por meio da Portaria CNJ nº 252/2021, composto por magistrados(as) e servidores(as) de vários órgãos do Poder Judiciário, com formação nas áreas de Direito, Arquivologia, Tecnologia da Informação, entre outras, com o escopo de atualizar o Modelo de Requisitos para adequá-lo ao arcabouço normativo vigente e ainda atender as necessidades da transformação digital em curso, incrementada pelo Programa Justiça 4.0, que tem trazido

inovações tecnológicas sem precedentes para a sociedade e o Poder Público em geral.

Partindo-se do modelo vigente, nos estudos para a atualização do MoReq-Jus, foram analisadas diversas referências normativas e bibliográficas, realizadas várias reuniões remotas e presenciais concentradas e também organizado um webinário, que contou com a participação dos membros do Grupo de Trabalho e de especialistas convidados. Desse modo, buscou-se elaborar uma nova versão, que continuasse a atender as especificidades e peculiaridades do processo judicial. Houve também a promoção de segundo webinário para estimular a participação na consulta pública.

Para esse processo de elaboração da nova versão do MoReq-Jus, dois documentos foram as principais referências:

- *MoReq 2: Model Requirements for the Management of Electronic Records - Update and Extension*. 2008;
- Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-Arq Brasil Versão 2), aprovado pela Resolução Conarq nº 50/2022 (Conarq, 2022).

Embora o MoReq 2010, publicado pelo DLM Fórum em 2011, seja a versão mais recente do Modelo de Requisitos da União Europeia, que serviu de base para desenvolvimento do MoReq-Jus, a opção por fazer essa atualização ainda fundamentada no MoReq 2 decorreu do estabelecido pela Portaria de criação do Grupo de Trabalho, que o definiu como atualização e não como a elaboração de nova especificação de requisitos.

Com efeito, o MoReq 2010 é uma especificação diferente das suas versões anteriores, especialmente em razão da sua estrutura modular, o que, inclusive, levou à mudança de nome para "MoReq – Modular Requirements for Records System" (Requisitos Modulares para Sistemas de Documentos de Arquivo). No entanto, muitas inovações do MoReq 2010 foram adotadas, como a separação dos requisitos funcionais e não funcionais, assim como os conceitos de entidades, eventos de gestão e o aprimoramento na especificação dos níveis de acesso.

Também o e-Arq Brasil, em razão da sua recente atualização pela mencionada Resolução Conarq nº 50/2022, com o seu anexo de metadados, serviu de referência para o desenvolvimento dos metadados correspondentes da nova versão do MoReq-Jus.

Além das referências mencionadas, para elaboração da proposta, o Grupo de Trabalho levou em consideração a evolução tecnológica, legislativa e normativa, com ênfase na ocorrida no âmbito do Conarq e do CNJ, que impacta na formulação de requisitos para a gestão de documentos.

Para facilitar a leitura e a compreensão do destinatário final, na metodologia de elaboração do novo MoReq-Jus, optou-se por não se mencionar a fonte direta ou referência de cada requisito.

1.2 Objetivos

O MoReq-Jus descreve o modelo de requisitos necessários para o desenvolvimento de um sistema informatizado de gestão de documentos e processos judiciais e administrativos, incluindo módulos e outros microsserviços, denominado genericamente GestãoDoc.

O MoReq-Jus tem por objetivo fornecer especificações técnicas e funcionais, para orientar a aquisição, o detalhamento e o desenvolvimento de sistemas de gestão da documentação digital, não digital e híbrida no âmbito do Poder Judiciário brasileiro.

Os sistemas, módulos, aplicações e microsserviços, que vierem a ser introduzidos na PDPJ-Br (Plataforma Digital do Poder Judiciário), deverão ser aderentes aos requisitos do MoReq-Jus, naquilo que for cabível. A forma de aferição dos graus ou percentuais de aderência será disciplinada pelo Conselho Nacional de Justiça.

1.3 Destinatários

O MoReq-Jus é dirigido a:

- Desenvolvedores e fornecedores, como guia no desenvolvimento de sistemas, módulos, aplicações e microsserviços em forma conjunta com as Resoluções **CNJ nº 335/2020**, que institui política pública para a governança e a gestão de processo judicial eletrônico e integra os tribunais do país com a criação da Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br); **nº 370/2021**, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD); **nº 468/2022**, que dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça; e **nº 469/2022**, que disciplina a digitalização e a gestão de documentos digitalizados pelo Poder Judiciário.
- Profissionais da área de gestão de documentos, como orientação de execução das ações a partir de uma abordagem arquivística.
- Responsáveis pela auditoria ou inspeção dos sistemas existentes.
- Usuários de um GestãoDoc, em geral.

1.4 Organização do MoReq-Jus

Na Parte I, além deste capítulo introdutório, o capítulo 2 apresenta a Gestão Documental do Poder Judiciário e as questões relativas à política arquivística e aos respectivos instrumentos.

Nas Partes II e III, são apresentados os capítulos com os requisitos propriamente ditos categorizados em funcionais e não funcionais, que são explicados no capítulo 1.7.

Cada capítulo inclui um texto introdutório que apresenta o assunto e a relação dos requisitos correspondentes. Os requisitos são apresentados em

quadros numerados com o respectivo enunciado, a classificação dos níveis de obrigatoriedade e a categorização quanto ao tipo de requisito.

Ao final, são apresentados o Glossário, as Referências e os Anexos A. Quadro de Referências Normativas e B. Metadados.

1.5 Fundamentos legais e normativos

O MoReq-Jus foi instituído pela Resolução CNJ nº 91/2009, na mesma ocasião em que editada a Resolução CNJ nº 90/2009, que dispunha sobre os requisitos de nivelamento de tecnologia da informação no âmbito do Poder Judiciário.

Na época, conforme referido acima, não havia regramento sistematizado de Gestão Documental por parte do Conselho Nacional de Justiça, incidindo apenas a disciplina da Constituição Federal de 1988, da legislação e de atos normativos do Conselho Nacional de Arquivos (Conarq).

Da Constituição Federal, destacava-se a aplicação dos dispositivos relacionados à proteção da intimidade e do sigilo das comunicações (art. 5º, X e XII), ao acesso à informação (arts. 5º, XIV e XXXIII; 37, § 3º, II) e às fontes da cultura nacional (art. 215), aos deveres estatais de proteção de documentos (art. 23, III a V), de proteção e promoção do Patrimônio Cultural (art. 216, § 1º) e de gestão da documentação (art. 216, §2º). Pela recente Emenda Constitucional nº 115/2022, foi incluída, de forma expressa, a proteção de dados pessoais, inclusive em meios digitais (art. 5º, LXXIX).

No plano infraconstitucional, aplicava-se o regramento oriundo das Leis nºs 8.159/1991 (Lei Geral de Arquivos) e 11.419/2006 (Lei do processo eletrônico).

Várias leis foram promulgadas nos últimos anos, que influem na disciplina da matéria relacionada à gestão de documentos pelo Poder Judiciário, entre as quais cabe destacar as Leis nºs 12.527/2011 (Lei de Acesso à Informação - LAI), 12.682/2012 (Lei de Digitalização), 13.105/2015 (Novo Código de Processo Civil), 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) e 14.063/2020 (Lei da Assinatura Digital).

Da mesma forma, vários atos normativos do Conselho Nacional de Justiça e do Conselho Nacional de Arquivos foram editados, que são relacionados nos itens seguintes.

1.5.1 Constituição Federal e Legislação

Na formulação dos requisitos constantes do MoReq-Jus, foram considerados os dispositivos da Constituição Federal e a legislação a seguir elencados, com relação intrínseca com a gestão de documentos judiciais e administrativos, os quais devem ser observados no desenvolvimento e na atualização de um GestãoDoc:

1) **Constituição Federal**: proteção da intimidade e do sigilo das comunicações (art. 5º, X e XII), acesso à informação (arts. 5º, XIV e XXXIII, 37, § 3º, II), proteção de dados pessoais (art. 5º, LXXIX, incluído pela Emenda Constitucional nº 115/2022) e deveres estatais de proteção de documentos (art. 23, III a V), de proteção e promoção

do Patrimônio Cultural (art. 216, § 1º) e de promover a gestão da documentação (art. 216, §2º).

2) **Lei nº 8.159, de 8 de janeiro de 1991**, que dispõe sobre a política nacional de arquivos públicos e privados, em seu art. 20, define a competência e o dever inerente aos órgãos do Poder Judiciário Federal de proceder à gestão de documentos produzidos em razão do exercício de suas funções;
3) **Medida Provisória nº 2.200-2, de 24 de agosto de 2001**, que institui a Infraestrutura de Chaves Públicas Brasileira — ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências;
4) **Lei nº 11.419, de 19 de dezembro de 2006**, que dispõe sobre a informatização do processo judicial;
5) **Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI)**, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências;
6) **Lei nº 12.682, de 9 de julho de 2012 (Lei da Digitalização)**, que dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos;
7) **Lei nº 13.105, de 16 de março de 2015 (Código de Processo Civil)**;
8) **Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD)**; e
9) **Lei nº 14.036, de 23 de setembro de 2020 (Lei da Assinatura Digital)**, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de *softwares* desenvolvidos por entes públicos; e altera a Lei nº 9.096, de 19 de setembro de 1995, a Lei nº 5.991, de 17 de dezembro de 1973, e a Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

1.5.2 Conselho Nacional de Justiça

O Conselho Nacional de Justiça (CNJ) é órgão do Poder Judiciário, ao qual compete o controle da atuação administrativa e financeira do Poder Judiciário (artigo 103, parágrafo 4º, da Constituição Federal), podendo para tanto expedir atos regulamentares, no âmbito de sua competência ou recomendar providências.

Além das preexistentes Resolução CNJ nº 46/2007, que cria as tabelas unificadas, e Resolução CNJ nº 65/2008, que dispõe sobre a uniformização do número dos processos nos órgãos do Poder Judiciário, já considerados quando da elaboração do MoReq-Jus, ora atualizado, sobrevieram diversos normativos que se relacionam com a matéria.

A seguir, são relacionados os atos normativos do CNJ, examinados na construção desta nova versão do MoReq-Jus, que devem ser contemplados em sistemas, aplicações, módulos e microsserviços de gestão de documentos e processos, das áreas fim e meio, no que couberem:

1) **Resolução nº 46/2007**, que cria as Tabelas Processuais Unificadas do Poder Judiciário;
2) **Resolução nº 65/2008**, que dispõe sobre a uniformização do número dos processos nos órgãos do Poder Judiciário;

3) **Resolução nº 100/2009**, que dispõe sobre a comunicação oficial, por meio eletrônico, no âmbito do Poder Judiciário;
4) **Resolução nº 105/2010**, que dispõe sobre a documentação dos depoimentos por meio do sistema audiovisual e realização de interrogatório e inquirição de testemunhas por videoconferência;
5) **Resolução nº 121/2010**, que dispõe sobre a divulgação de dados processuais eletrônicos na rede mundial de computadores e a expedição de certidões judiciais;
6) **Resolução nº 185/2013**, que institui o Sistema Processo Judicial Eletrônico - PJe como sistema de processamento de informações e prática de atos processuais e estabelece os parâmetros para sua implementação e funcionamento;
7) **Resolução Conjunta CNJ-CNMP 3-2013**, que institui Modelo Nacional de Interoperabilidade do Poder Judiciário e do Ministério Público;
8) **Resolução nº 215/2015**, que dispõe, no âmbito do Poder Judiciário, sobre o acesso à informação e a aplicação da Lei 12.527, de 18 de novembro de 2011;
9) **Recomendação nº 52/2016**, que recomenda a adoção de medidas preventivas e maior rigor no controle quanto à forma como são geradas, armazenadas e disponibilizadas informações judiciais de caráter sigiloso e/ou sensíveis;
10) **Resolução nº 324/2020**, que institui diretrizes e normas de Gestão de Memória e de Gestão Documental e dispõe sobre o Programa Nacional de Gestão Documental e Memória do Poder Judiciário – PRONAME;
11) **Resolução nº 326/2020**, que altera a Resolução nº 46/2007, entre outras;
12) **Resolução nº 331/2020**, que institui a Base Nacional de Dados do Poder Judiciário – DataJud como fonte primária de dados do Sistema de Estatística do Poder Judiciário – SIESPJ para os tribunais indicados nos incisos II a VII do art. 92 da Constituição Federal;
13) **Resolução nº 332/2020**, que dispõe sobre a ética, a transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário;
14) **Resolução nº 335/2020**, que institui política pública para a governança e a gestão de processo judicial eletrônico e integra os tribunais do país com a criação da Plataforma Digital do Poder Judiciário Brasileiro – PDPJ-Br. Mantém o sistema PJe como sistema de Processo Eletrônico prioritário do Conselho Nacional de Justiça;
15) **Resolução nº 337/2020**, que dispõe sobre a utilização de sistemas de videoconferência no Poder Judiciário;
16) **Portaria nº 253/2020**, que institui os critérios e diretrizes técnicas para o processo de desenvolvimento de módulos e serviços na Plataforma Digital do Poder Judiciário Brasileiro – PDPJ-Br;
17) **Resolução nº 354/2020**, que dispõe sobre o cumprimento digital de ato processual e de ordem judicial e dá outras providências;
18) **Resolução nº 358/2020**, que regulamenta a criação de soluções tecnológicas para a resolução de conflitos pelo Poder Judiciário por meio da conciliação e mediação;
19) **Resolução nº 363/2021**, que estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais;
20) **Resolução nº 370/2021**, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
21) **Resolução nº 390/2021**, que dispõe sobre a extinção de soluções de Tecnologia da Informação e Comunicações e serviços digitais, que foram substituídos ou se encontram inoperantes e fixa regras para a criação de novas soluções de tecnologia;

22) **Resolução nº 396/2021**, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
23) **Resolução nº 408/2021**, que dispõe sobre o recebimento, o armazenamento e o acesso a documentos digitais relativos a autos de processos administrativos e judiciais;
24) **Resolução nº 417/2021**, que institui e regulamenta o Banco Nacional de Medidas Penais e Prisões (BNMP 3.0);
25) **Resolução nº 420/2021**, que dispõe sobre a adoção do processo eletrônico e o planejamento nacional da conversão e digitalização do acervo processual físico remanescente dos órgãos do Poder Judiciário;
26) **Resolução nº 427/2021**, que amplia a proteção a vítimas e testemunhas por meio da proteção à sua identidade, endereço e dados qualificativos;
27) **Resolução nº 428/2021**, que dispõe sobre procedimentos e rotinas quanto ao uso do Cadastro de Entidades Devedoras Inadimplentes de Precatórios (CEDINPREC), sistema informatizado por meio do qual serão centralizadas as informações relativas à não liberação tempestiva de recursos para o pagamento de parcelas mensais indispensáveis ao cumprimento do regime especial de que tratam os artigos 101 a 105 do Ato das Disposições Constitucionais Transitórias (ADCT);
28) **Resolução nº 446/2022**, que institui a plataforma Codex como ferramenta oficial de extração de dados estruturados e não estruturados dos processos judiciais eletrônicos em tramitação no Poder Judiciário Nacional;
29) **Resolução nº 455/2022**, que institui o Portal de Serviços do Poder Judiciário (PSPJ), na Plataforma Digital do Poder Judiciário (PDPJ-Br), para usuários externos;
30) **Resolução nº 462/2022**, que dispõe sobre a gestão de dados e estatística, cria a Rede de Pesquisas Judiciárias (RPJ) e os Grupos de Pesquisas Judiciárias (GPJ) no âmbito do Poder Judiciário e dá outras providências;
31) **Resolução nº 468/2022**, que dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça;
32) **Resolução nº 469/2022**, que estabelece diretrizes e normas sobre a digitalização de documentos judiciais e administrativos e de gestão de documentos digitalizados do Poder Judiciário; e
33) **Resolução nº 480/2022**, que restabelece os efeitos da Resolução n. 182/2013, que dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça, e dá outras providências.

1.5.3 Conselho Nacional de Arquivos

No âmbito do Conselho Nacional de Arquivos (Conarq), órgão central do Sistema Nacional de Arquivos (SINAR), que define a política nacional de arquivos, foram considerados os seguintes normativos na construção dos requisitos do Modelo, atendidas as peculiaridades do Poder Judiciário e a normatização existente por parte do Conselho Nacional de Justiça:

1) **Resolução Conarq nº 20/2004**, que dispõe sobre a inserção dos documentos digitais em programas de gestão arquivística de documentos dos órgãos e entidades integrantes do Sistema Nacional de Arquivos;

2) **Resolução Conarq nº 24/2006**, que estabelece diretrizes para a transferência e recolhimento de documentos arquivísticos digitais para instituições arquivísticas públicas;
3) **Resolução Conarq nº 27/2009**, que dispõe sobre a adoção da Norma Brasileira de Descrição Arquivística - NOBRADE pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR, institui o Cadastro Nacional de Entidades Custodiadoras de Acervos Arquivísticos e estabelece a obrigatoriedade da adoção do Código de Entidades Custodiadoras de Acervos Arquivísticos - CODEARQ;
4) **Resolução Conarq nº 31/2010**, que dispõe sobre a adoção das Recomendações para Digitalização de Documentos Arquivísticos Permanentes;
5) **Resolução Conarq nº 37/2012**, que aprova as diretrizes para a presunção de autenticidade de documentos arquivísticos digitais;
6) **Resolução Conarq nº 39/2014**, que estabelece diretrizes para a implementação de repositórios digitais confiáveis para a transferência e recolhimento de documentos arquivísticos digitais;
7) **Resolução Conarq nº 41/2014**, que dispõe sobre a inserção dos documentos audiovisuais, iconográficos, sonoros e musicais em programas de gestão de documentos arquivísticos dos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR, visando a sua preservação e acesso;
8) **Resolução Conarq nº 48/2021**, que estabelece diretrizes e orientações aos órgãos e entidades integrantes do Sistema Nacional de Arquivos quanto aos procedimentos técnicos a serem observados no processo de digitalização de documentos públicos ou privados; e
9) **Resolução Conarq nº 50/2022**, que dispõe sobre o Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-Arq Brasil.

1.6 Manuais, normas e orientações técnicas

1.6.1 Engenharia de *software* e segurança da informação

1) **ISO/IEC/IEEE 24765:2017** - "Systems and software engineering";
2) **ISO/IEC 25010:2011** - "Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE)" — "System and software quality models";
3) **ISO/IEC 27002:2022** - "Information security, cybersecurity and privacy protection — Information security controls";
4) **Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da Repúblic**a; e
5) **Padrão "British Standard (BS) Swebok"**, guia para o conjunto de melhores práticas e conhecimentos de engenharia de *software*.

1.6.2 Gestão de documentos, preservação e metadados

1) **ABNT NBR ISO30301:2016**, que trata dos requisitos de sistemas de gestão de documentos;
2) **ABNT NBR ISO30302:2017,** que trata das diretrizes para implementação de sistemas de gestão de documentos de arquivo;
3) **ABNT NBR ISO23081-1:2019,** que trata dos princípios dos processos de gestão de documentos de arquivo no que concerne aos metadados para documentos;
4) **ABNT NBR ISO23081-2:2020**, que trata dos problemas conceituais e de implementação do gerenciamento de metadados para documentos de arquivo;
5) **ABNT NBR ISO14721:2021**, modelo de referência para Sistemas Abertos de Arquivamento de Informação (SAAI);
6) I**SO 639-2:1998** - "Codes for the representation of names of languages — Part 2: Alpha-3 code";
7) **ISO 14721:2012** – "Reference model for an open archival information system (OAIS)", 2012;
8) **ISO15836-1:2017,** que descreve "The Dublin Core Metadata Initiative";
9) **ISO 8601:2019**, "Date and time - Representations for information interchange";
10) Manual de Gestão Documental do Poder Judiciário (CNJ, 2021a);
11) Manual de Gestão de Memória do Poder Judiciário (CNJ, 2021b);
12) Manual de Digitalização de Documentos do Poder Judiciário (CNJ, 2023);
13) **Padrão de Metadados do Governo Eletrônico – e-PMG,** Brasil, versão 1.1, 2014; e
14) **PREMIS Data Dictionary for Preservation Metadata** – version 3, 2015.

1.6.3 Padrões de interoperabilidade e acessibilidade

1) **Modelo de Acessibilidade em Governo Eletrônico (e-MAG)**. v. 3.1, 2014; e
2) **Padrões de Interoperabilidade de Governo Eletrônico (e-PING)**, versão 2018.

1.6.4 Modelos de Requisitos para sistemas informatizados de gestão de documentos

1) MoReq 2: Model Requirements for the Management of Electronic Records - Update and Extension. 2008;
2) MoReq 2010 – Modular Requirements for Records Systems, 2011; e
3) Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-Arq Brasil Versão 2), aprovado pela Resolução Conarq nº 50/2022.

1.7 Requisitos funcionais (RF) e não funcionais (RNF)

Para organização do MoReq-Jus, os requisitos foram categorizados em **funcionais** e **não funcionais**. Esta categorização visa a direcionar os esforços de construção e endereçamento interno na área de tecnologia da informação. Nessa linha, os requisitos não funcionais foram subdivididos em requisitos de **produto**, **organizacionais** e **externos**.

Categoria de requisitos	Anotação utilizada	Descrição
Requisito funcional	RF	Declaração que especifica uma funcionalidade que um sistema informatizado deve ser capaz de executar. Em geral, define uma função a ser implementada no sistema informatizado. Declaração de serviços que o sistema deve fornecer, de como deve reagir a entradas específicas e de como deve comportar-se em determinadas situações. Um requisito funcional define características de um código de computador que será construído e integrado como uma funcionalidade operacional no *software* GestãoDoc.
Requisito não funcional	RNF	Define uma característica que afeta o comportamento geral do sistema informatizado, influenciando na implementação das funcionalidades. Institui restrições ou limitações de serviços ou funções oferecidos pelo sistema, de *timing*, do processo de desenvolvimento e de normas impostas pelo próprio negócio. Afeta diretamente a qualidade do sistema informatizado.
Requisito não funcional de produto	RNF-P	Requisito não funcional que especifica comportamento geral do sistema em questão de desempenho, usabilidade e interoperabilidade. Influencia na qualidade do produto entregue, em relação ao usuário e às funcionalidades intrínsecas. Pode indicar a construção de requisitos funcionais para a implementação.
Requisito não funcional organizacional	RNF-O	Requisito não funcional que especifica questões de ambiente de funcionamento, procedimentos operacionais e desenvolvimento. Diz respeito à parte organizacional da área tecnológica em prover suporte para o funcionamento do sistema. Constituem exemplos desse requisito:: processo de *software*; definição, configuração e manutenção de servidores; ambientes diversos para homologação, produção, testes etc.; gerenciamento de *backup*; segurança e proteção de ativos de informação; gerenciamento de redes etc.
Requisito não funcional externo	RNF-E	Requisito não funcional que especifica requisitos legais, normativos e questões éticas. Possui influência na definição de outros requisitos funcionais e não funcionais.

Fonte: adaptado de ISO/IEC 24765 e Sommerville (2019)

Não obstante o MoReq-Jus descreva conjunto de requisitos aplicáveis aos sistemas informatizados utilizados pelo Poder Judicíario, cada sistema GestãoDoc possui os seus próprios que, em geral, são mais abrangentes e específicos para

o fim para o qual é construído. Assim, cada sistema GestãoDoc deve detalhar os seus próprios requisitos, os quais devem ser aderentes ao MoReq-Jus.

Os requisitos funcionais e não funcionais previstos neste Modelo são apresentados de forma individualizada nos seguintes capítulos:

Capítulo	Título	Requisito Funcional	Não Funcional
3	Organização dos documentos institucionais:	X	
4	Captura	X	
5	Fluxo de Trabalho e Tramitação	X	
6	Avaliação: temporalidade e destinação	X	
7	Pesquisa, localização e apresentação de documentos	X	
8	Segurança: controle de acessos e auditoria	X	
9	Armazenamento		X
10	Preservação		X
11	Segurança: aspectos estruturais		X
12	Disponibilidade		X
13	Usabilidade		X
14	Interoperabilidade		X
15	Desempenho e escalabilidade		X
16	Implementação, manutenção e evolução		X

As siglas dos requisitos funcionais e não funcionais correspondem ao tema tratado no capítulo e seção às quais estão vinculadas:

Requisitos funcionais:

RPC REQUISITOS DE PLANO DE CLASSIFICAÇÃO
RCA REQUISITOS DE CAPTURA
RFT REQUISITOS DE FLUXO DE TRABALHO E TRAMITAÇÃO
RAD REQUISITOS DE AVALIAÇÃO E DESTINAÇÃO
RPA REQUISITOS DE PESQUISA E APRESENTAÇÃO
RSC REQUISITOS DE SEGURANÇA
RTA REQUISITOS DE TRILHA DE AUDITORIA

Requisitos não funcionais:

RAR REQUISITOS DE ARMAZENAMENTO
RPR REQUISITOS DE PRESERVAÇÃO
RSE REQUISITOS DE SEGURANÇA
RDI REQUISITOS DE DISPONIBILIDADE
RUS REQUISITOS DE USABILIDADE
RIN REQUISITOS DE INTEROPERABILIDADE
RDE REQUISITOS DE DESEMPENHO E ESCALABILIDADE
RME REQUISITOS DE MANUTENÇÃO E EVOLUÇÃO

1.8 Níveis de obrigatoriedade dos Requisitos

Os requisitos foram classificados em obrigatórios e desejáveis de acordo com o grau de exigência para que o GestãoDoc desempenhe suas funções.

Cada requisito numerado é classificado como:

O (Obrigatório) — O requisito é imprescindível;

D (Desejável) — Podem existir razões válidas em circunstâncias particulares para não se adotar um determinado item, mas a totalidade das implicações deve ser cuidadosamente examinada antes da escolha de uma proposta diferente.

Na implementação dos requisitos obrigatórios e desejáveis e na interoperabilidade entre sistemas, deve ser assegurado que:

- Um sistema GestãoDoc que implemente um requisito desejável, quando operar com um outro sistema, deve comportar-se observando a possibilidade de o requisito não ter sido nele implementado e deixando de exigir desse outro sistema a referida implementação; e
- Um sistema que não tenha implementado um requisito desejável, quando interoperar com um que tenha implementado o requisito, deve ser capaz de descartar as informações a ele pertinentes.

2. GESTÃO DOCUMENTAL NO PODER JUDICIÁRIO

Os documentos produzidos e recebidos no decorrer das atividades do Poder Judiciário, independentemente do suporte em que se apresentam, registram suas funções, procedimentos, ações, decisões e políticas.

O processo de informatização dos órgãos do Poder Judiciário teve início na década de 1980.

Os sistemas de gerenciamento passaram a ser utilizados para os documentos não digitais e digitais.

Os documentos digitais e as alterações na legislação processual trouxeram várias vantagens na produção, na transmissão, no armazenamento e no acesso aos documentos. Contudo, provocaram novos desafios, como a necessidade de proteção contra invasões e intervenções não autorizadas, de forma a evitar adulterações ou perda dos documentos, preservação a longo prazo e acesso.

As mudanças, aceleradas com a aprovação da Lei nº 11.419/2006, que dispôs sobre a informatização do processo judicial e instituiu critérios à sua tramitação, acarretaram transformação lógica e conceitual e resultaram na necessidade de instituição de políticas próprias e adequadas para a tramitação com segurança e para a preservação de documentos institucionais.

Para conferir essa capacidade, os documentos precisam ser confiáveis, autênticos, acessíveis, compreensíveis e preserváveis, o que só é possível com a implantação de um sistema de gestão de documentos baseado em uma política de Gestão Documental.

O MoReq-Jus considera as diretrizes e normas do Programa Nacional de Gestão Documental e Memória do Poder Judiciário (Proname), prevendo requisitos para o desenvolvimento de sistemas informatizados em conformidade com o que estabelece a Resolução CNJ nº 324/2020 , que institui o Programa, e demais Resoluções aplicáveis, do CNJ e do Conarq, indicadas nos capítulos 1.5.2 e 1.5.3.

As operações técnicas cujos requisitos estão relacionados no MoReq-Jus destinam-se à gestão dos documentos em todas as fases de seu ciclo de vida, visando ao acesso, à segurança, à proteção e à preservação dos , à eficácia administrativa quanto à recuperação da informação disponível, ao apoio na tomada de decisões e ao cumprimento da missão institucional do Poder Judiciário..

2.1 Política de Gestão Documental

Para a coordenação e a normatização das políticas de Gestão Documental, o Conselho Nacional de Justiça (CNJ), a quem compete o controle administrativo do Poder Judiciário, instituiu o Programa Nacional de Gestão Documental e Memória do Poder Judiciário (Proname).

O Proname provê os órgãos do Poder Judiciário com diretrizes e normas de Gestão Documental em conformidade com a legislação vigente.

Os princípios, diretrizes e normas de Gestão Documental estão elencados na Resolução CNJ nº 324/2020, cujo artigo 2º, inciso I, conceitua a Gestão Documental como o "conjunto de procedimentos e operações técnicas referentes à produção, à tramitação, ao uso, à avaliação e ao arquivamento de documentos e processos recebidos e tramitados pelos órgãos do Poder Judiciário no exercício das suas atividades, inclusive administrativas, independentemente do suporte de registro da informação". O artigo 15, parágrafo único, da mencionada Resolução complementa o conceito ao referir-se à destinação final da documentação, "seja a preservação por meio de guarda permanente, seja a eliminação depois de sua avaliação", se não houver valor secundário.

As especificações dos princípios, diretrizes e normas elencados na Resolução CNJ nº 324/2020 constam do Manual de Gestão Documental do Poder Judiciário que é um dos instrumentos do Proname, previsto no artigo 5º, inciso VIII. O Manual descreve os principais elementos que estruturam o funcionamento de um programa de Gestão Documental e se constitui em material de consulta e de orientação para o planejamento, implementação e execução do tema nos diversos órgãos do Poder Judiciário.

A Resolução CNJ nº 469/2022, por sua vez, estabelece diretrizes e normas sobre a digitalização de documentos judiciais e administrativos e de gestão de documentos digitalizados do Poder Judiciário, as quais são especificadas no Manual de Digitalização de Documentos do Poder Judiciário.

Além disso, a política de Gestão de Documentos deve ser formulada com base na análise do perfil institucional, isto é, seu contexto jurídico-administrativo, estrutura organizacional, missão, competências, funções e atividades, de forma que os documentos produzidos e seu tratamento sejam os mais adequados, completos e necessários.

Essa política deverá definir um conjunto de procedimentos e operações técnicas que compreendem a gestão de documentos na instituição, que deverá observar as seguintes características:

- Promover a instituição de Comissões Permanentes de Avaliação Documental (CPADs) responsáveis pela avaliação dos documentos, que deve ser integrada também por um servidor da unidade de tecnologia da informação (artigo 12, inciso III, da Resolução CNJ n.º 324/2020).
- As unidades de Gestão Documental devem atuar como responsáveis pela seleção e destinação documental, tratamento técnico do acervo arquivístico da instituição e pelo acesso aos documentos sob sua guarda, entre outras atribuições.
- Prever a existência de instrumentos de classificação, destinação e temporalidade.
- Estabelecer que a guarda do documento, independentemente do suporte (papel ou digital), deve garantir sua autoria, integridade e tempestividade.

As dúvidas relacionadas às questões de gestão documental, tratadas ou não no Manual de Gestão Documental do Poder Judiciário, no Manual de Digitalização de Documentos do Poder Judiciário e neste Modelo, devem ser encaminhadas ao Comitê do Proname pelo e-mail**: proname@cnj.jus.br**.

2.2 Instrumentos de Gestão Documental

O artigo 5º da Resolução CNJ nº 324/2020 elenca os seguintes instrumentos do Programa Nacional de Gestão Documental e Memória do Poder Judiciário (Proname):

I. os sistemas informatizados de gestão de documentos e processos administrativos e judiciais, bem como os metadados desses sistemas, essenciais à identificação do documento institucional de modo inequívoco em sua relação com os outros documentos.
II. o Plano de Classificação (Tabelas Processuais Unificadas) e a Tabela de Temporalidade dos Processos Judiciais do Poder Judiciário;
III. o Plano de Classificação e a Tabela de Temporalidade dos Documentos da Administração do Poder Judiciário;
IV. a Listagem de Verificação para Baixa Definitiva de Autos;
V. a Listagem de Verificação para Eliminação de Autos Findos;
VI. o Fluxograma de Avaliação, Seleção e Destinação de Autos Findos;
VII. o Plano para Amostra Estatística Representativa;
VIII. o Manual de Gestão Documental do Poder Judiciário;
IX. o Manual de Gestão de Memória do Poder Judiciário;
X. o Manual de Digitalização de Documentos do Poder Judiciário; e
XI. a Listagem de Verificação para Seleção e Eliminação antecipadas de autos digitalizados.

Esses instrumentos compõem ferramentas de aplicação das diretrizes, princípios e normas de Gestão Documental e de Memória e devem ser adotados pelos órgãos do Poder Judiciário, nos termos do artigo 41 da Resolução CNJ nº 324/2020.

Depois de implementados os instrumentos de Gestão Documental, cabe aos referidos órgãos o monitoramento da sua aplicação efetiva, sistemática e integrada às rotinas de implantações internas e auditorias.

2.3 Designação de responsabilidades

A designação de responsabilidades é um dos fatores que garante o êxito da gestão de processos e documentos. Nesse sentido, as autoridades responsáveis terão o dever de assegurar o cumprimento das normas e dos procedimentos previstos na política de gestão.

As responsabilidades devem ser distribuídas a todos os colaboradores de acordo com a função e a hierarquia de cada um. Ademais, devem abranger as seguintes categorias:

a) Presidentes de Tribunais, Corregedores, Diretores de foro e juízes assessores ou auxiliares da alta administração dos órgãos do Poder Judiciário: responsáveis pela viabilidade da política e normas aplicáveis, a quem caberá apoiar integralmente a implantação dos requisitos estabelecidos neste documento, alocando recursos humanos, materiais e financeiros e promovendo o envolvimento de todos na política de gestão de processos e documentos;

b) Gestores de unidades organizacionais ou grupos de trabalho: responsáveis por garantir que os membros de sua equipe produzam e mantenham documentos, de acordo com os critérios previstos para a produção e tramitação de documentos;

c) Comissões Permanentes de Avaliação de Documentos (CPAD): responsáveis por propor, acompanhar e orientar a aplicação dos instrumentos de gestão documental, além de outras atribuições previstas no art. 11 da Resolução CNJ nº 324/2020 e nos normativos de cada órgão;

d) Gestores das unidades de Gestão Documental e Arquivos: responsáveis por gerenciar o sistema GestãoDoc, em tarefas como as de configuração e atribuição de perfis. No MoReq-Jus, são tratados como "gestor". As unidades também são responsáveis pela implantação da política de gestão documental e pela avaliação e controle dos trabalhos executados no âmbito de suas instituições;

e) Arquivistas: responsáveis pela proposição de estudos e projetos de gestão de documentos, elaboração de instrumentos de gestão documental e acesso, bem como pela disseminação das técnicas e funções arquivísticas e a preservação do acervo de guarda permanente;

f) Administradores dos sistemas de informação e de tecnologia da informação: responsáveis pelo projeto, desenvolvimento e manutenção da infraestrutura em que o GestãoDoc, os documentos digitais e não digitais são mantidos. No MoReq-Jus, são tratados como "administrador"; e

g) Usuários: responsáveis, em todos os níveis, pela produção, tramitação e uso dos documentos institucionais em suas atividades rotineiras.

2.4 Princípios e diretrizes para Política de Gestão Documental

De acordo com o art. 15 da Resolução CNJ nº 324/2020, a política de gestão documental dos órgãos do Poder Judiciário deve estar baseada nos princípios da legalidade, transparência, proteção de dados, eficiência e na segurança da informação.

A política de Gestão Documental deve atender também as seguintes diretrizes:

a) Contemplar o ciclo de vida dos documentos;

b) Garantir o acesso aos documentos;

c) Manter os documentos em ambiente seguro;

d) Proteger os dados pessoais;

e) Reter os documentos somente pelo período estabelecido nos instrumentos de classificação, temporalidade e destinação;

f) Implementar estratégias de preservação dos documentos desde sua produção e pelo tempo que for necessário; e

g) Garantir as características do documento institucional: relação orgânica, unicidade, confiabilidade, integridade, autenticidade, não-repúdio, tempestividade e confidencialidade.

A cada uma das mencionadas qualidades do documento institucional, corresponde novo conjunto de diretrizes a ser cumprido pela política de gestão, conforme especificação a seguir:

- **Relação orgânica** — O documento arquivístico, físico ou digital, caracteriza-se pela relação orgânica, ou seja, pelas relações que mantém com os demais documentos do órgão ou entidade e que refletem suas funções e atividades. Os documentos arquivísticos não são coletados artificialmente, mas estão ligados uns aos outros por um elo que se materializa por meio do registro ou do plano de classificação ou do arquivamento, que os contextualiza no conjunto ao qual pertencem. Os documentos arquivísticos apresentam um conjunto de relações que devem ser mantidas;
- **Unicidade** — O documento é único no conjunto documental ao qual pertence; podem existir cópias em um ou mais grupos de documentos, mas cada cópia é única em seu lugar, porque o conjunto de suas relações com os demais documentos do grupo é sempre único. A fim de evitar duplicação dos documentos, o GestãoDoc deve prever a identificação de cada documento individualmente, sem perder de vista o conjunto de relações que o envolve, utilizando referências lógicas para essa individualização dos documentos digitais;
- **Confiabilidade** — O documento confiável é aquele dotado de todos os elementos exigidos pela organização e pelo sistema jurídico-administrativo a que pertence, de forma a produzir consequências no mundo administrativo e jurídico. Além disso, é criado por usuário autorizado e todos os procedimentos de criação foram controlados pelo GestãoDoc. Assim, pode-se garantir a autoria do documento e que este não foi alterado. Os documentos digitais deverão ser assinados eletronicamente, conforme legislação vigente;
- **Integridade** — O documento institucional deve ter a garantia de que se encontra completo e que não sofreu nenhum tipo de corrupção ou alteração não autorizada nem documentada. O programa de gestão documental deve definir estratégias de armazenamento e preservação e regras para a transmissão dos documentos;
- **Autenticidade** — O documento institucional autêntico é aquele que é o que diz ser, independentemente de se tratar de original ou cópia. O documento autêntico deve ter a garantia de sua autoria, apresentar o mesmo grau de confiabilidade que tinha no momento de sua produção e ser transmitido e preservado sem adulteração ou qualquer outro tipo de corrupção. O programa de gestão documental deve implementar políticas e procedimentos que controlem a transmissão, a manutenção, a avaliação, a destinação e a preservação dos documentos, impedindo-os de sofrerem qualquer alteração, exclusão ou ocultação indevidas;
- **Não repúdio** — O documento institucional deve ter garantida a sua autoria, evitando-se que haja qualquer dúvida quanto ao produtor do documento. O programa de gestão documental deve garantir a identificação do autor do documento, que deverá ser realizada por meio de sua identificação única e inequívoca;
- **Tempestividade** — O documento institucional deve ter garantida a hora legal do momento de sua produção, alteração e registros dos eventos de sua tramitação, para assegurar a tempestividade. O programa de gestão documental deve possuir um mecanismo de protocolo para os documentos. No caso do documento digital, deverá ser prevista a utilização de uma Autoridade de Tempo com data e hora sincronizada com o Observatório Nacional e periódica auditagem por ele, conforme legislação vigente;
- **Confidencialidade** — O documento institucional só poderá ser acessado e manipulado por pessoas ou unidades previamente autorizadas. O programa de gestão documental deve garantir que os dados não estarão disponíveis nem serão divulgados a indivíduos, entidades ou processos sem autorização, de acordo com a legislação vigente referente ao segredo de justiça e à classificação da informação sigilosa.

PARTE II

REQUISITOS FUNCIONAIS

3. ORGANIZAÇÃO DOS DOCUMENTOS INSTITUCIONAIS

Os processos, dossiês e documentos institucionais compõem o acervo dos órgãos do Poder Judiciário e refletem as funções e atividades da organização, representadas no Plano de Classificação das áreas meio (administrativa) e fim (judicial).

Os prazos em que essa documentação institucional deve estar nas fases corrente, intermediária e permanente estão registrados nas respectivas Tabelas de Temporalidade.

Na área meio ou administrativa, devem ser adotados o Plano de Classificação e a Tabela de Temporalidade dos Documentos da Administração do Poder Judiciário (art. 5º, III, da Resolução CNJ nº 324/2020) e, no mínimo, os prazos da Tabela de Temporalidade dos Documentos da Administração do Poder Judiciário (artigo 20, § 1º, da Resolução CNJ nº 324/2020).

Em relação à área fim ou judicial, devem ser utilizados o Plano de Classificação (Tabelas Processuais Unificadas, aprovadas pela Resolução CNJ nº 46/2007), subdividido em Tabelas de Classes, Assuntos, Movimentos e Documentos e, no mínimo, os prazos da Tabela de Temporalidade dos Processos Judiciais do Poder Judiciário (arts. 5º, II, e art. 20, § 2º, da Resolução CNJ nº 324/2020).

> ***ATENÇÃO!*** *A referência utilizada neste Modelo de Requisitos ao termo "**CLASSE**" corresponde a qualquer das classificações em níveis e subníveis existentes nas estruturas dos Planos, como por exemplo classes e assuntos da área meio, e classes, assuntos, movimentos e documentos da área fim, incluindo seus desdobramentos.*

As atividades relacionadas à organização e ao gerenciamento de documentos institucionais sofrem influência direta da fase em que se encontra a documentação em seu ciclo de vida.

Processos, dossiês e documentos em tramitação na fase corrente são geridos pelas unidades produtoras (judiciais ou administrativas). Na fase intermediária, ou seja, quando não mais em tramitação, processos, dossiês e documentos passam a ser geridos pela unidade responsável pela gestão documental para fins de destinação. Isso porque, cessada a fase intermediária, é necessária a seleção da documentação para a sua destinação: eliminação ou guarda permanente.

Além dos Planos de Classificação, é de fundamental importância para as ações relacionadas às etapas da gestão documental que os sistemas informatizados contemplem:

a) Temporalidades e o registro dos termos iniciais e finais das fases diversas; e

b) Funcionalidades que permitam, após cumpridas as temporalidades, a transferência da documentação da etapa corrente para a intermediária e o recolhimento da documentação de guarda longa ou permanente para Repositório Digital Confiável (RDC – Arq).

A pesquisa e a obtenção de relatórios acerca dos conjuntos que se encontram em cada uma das fases estão contempladas nos requisitos RPC3.3.16 e RAD6.1.4, com base em metadados de Classe, apresentados no Anexo B.

Nos itens 3.1 a 3.6 deste capítulo são especificados os requisitos de um GestãoDoc para:

- Gerenciamento de planos de classificação e de tabelas de temporalidade.
- Formação, classificação e inclusão de metadados em processos, dossiês e documentos.
- Gerenciamento de processos, dossiês, documentos e volumes.
- Manutenção de documentos não digitais e híbridos.

3.1 Configuração e administração dos Planos de Classificação e Tabelas de Temporalidade

Os requisitos desta seção referem-se às funcionalidades que deverão ser desenvolvidas no sistema para apoiar a configuração dos instrumentos utilizados na classificação e destinação dos documentos e processos/dossiês.

Tais requisitos especificam como gerir os Planos de Classificação e as Tabelas de Temporalidade das áreas meio e fim dentro de um GestãoDoc, o que deve ser feito por usuários autorizados e em conformidade com as normas de gestão documental aplicáveis no órgão.

REQ	REQUISITO	OBRIG	TIPO
RPC3.1.1	Prover funcionalidades para a manutenção dos planos de classificação e tabelas de temporalidade a eles associadas, para documentos e processos/dossiês.	O	RF
RPC3.1.2	Permitir a criação de níveis dos planos de classificação de acordo com as normas e o método de codificação adotado. Para processos judiciais, permitir a criação de níveis de classes, assuntos, movimentos e documentos, de acordo com as definições dos órgãos competentes.	O	RF
RPC3.1.3	Permitir a usuários autorizados o acréscimo de novos níveis na forma do requisito RPC3.1.2.	O	RF
RPC3.1.4	Registrar no respectivo metadado as datas de abertura, reclassificação, movimentação e modificação de uma nova classe ou de um nível das tabelas processuais unificadas ou do plano de classificação.	O	RF
RPC3.1.5	Registrar no respectivo metadado a mudança de nome, de identificador e de código de uma classe ou de um nível específico das tabelas processuais unificadas ou do plano de classificação.	O	RF
RPC3.1.6	Permitir o deslocamento de um nível completo, incluindo seus subordinados, e os documentos ali classificados para outra localização, bem como o desmembramento ou fusão de níveis no plano de classificação ou nas tabelas processuais unificadas. Nesse caso, é necessário registrar o deslocamento nos metadados desses instrumentos.	O	RF

RPC3.1.7	Permitir que o gestor torne inativa e inacessível aos demais usuários, para utilização futura, uma classe ou um nível específico em que não mais serão classificados documentos..	O	RF
RPC3.1.8	Impedir a eliminação de uma classe ou nível de classificação ativa ou inativa.	O	RF
RPC3.1.9	Permitir a associação de metadados à classe ou nível específico dos planos de classificação e restringir a inclusão e alteração desses mesmos metadados somente a usuários autorizados.	O	RF
RPC3.1.10	Permitir a identificação da classe ou nível específico dos planos de classificação por meio de, pelo menos, um código numérico ou alfanumérico e um termo que a identifique, possibilitando a utilização desses identificadores separadamente ou em conjunto.	O	RF
RPC3.1.11	Associar atributos para identificar o nível hierárquico específico para classificação de documentos/processos/dossiês, de modo a impedir classificações genéricas. Em casos excepcionais e por meio de um usuário privilegiado, um documento/processo/dossiê pode ser classificado em nível genérico.	O	RF
RPC3.1.12	Utilizar o termo completo para identificar uma classe ou nível específico dos planos de classificação. Exemplo da Tabela Unificada de Assuntos do Judiciário: Vigilância Sanitária e Epidemiológica - Pública - Direito da Saúde	D	RF
RPC3.1.13	Assegurar que a identificação de cada classe ou nível específico seja única em um plano de classificação.	O	RF
RPC3.1.14	Importar e exportar total ou parcialmente os instrumentos de classificação e temporalidade.	O	RF
RPC3.1.15	Prover funcionalidades de pesquisa e navegação na estrutura do plano de classificação e da tabela de temporalidade para elaboração de relatórios de apoio à gestão desses instrumentos, incluindo a capacidade de gerar relatório: • Completo de todo o plano de classificação e tabela de temporalidade; • Parcial do plano de classificação e tabela de temporalidade, a partir de um ponto determinado na hierarquia; • Dos documentos/processos/dossiês classificados em uma ou mais classes ou níveis específicos do plano de classificação; • Dos documentos/processos/dossiês aos quais foi atribuído um determinado prazo de guarda; • De documentos classificados por unidade administrativa.	O	RF
RPC3.1.16	Permitir a gestão da tabela de temporalidade com as seguintes informações: • identificador da classe, assunto(s), movimento(s) e documento(s); • prazo de guarda na idade corrente; • evento que determina o início de contagem do prazo de retenção na idade corrente; • prazo de guarda na idade intermediária; • evento que determina o início de contagem do prazo de retenção na idade intermediária; • destinação final; • sigilo associado à classe ou nível específico dos planos de classificação; • observações.	O	RF

RPC3.1.17	Prever, pelo menos, as seguintes situações para destinação e a possibilidade de vinculá-las ao identificador da classe, assunto(s), movimento(s) e documento(s): • apresentação dos documentos para reavaliação em data futura; • eliminação; • exportação para transferência; • exportação para recolhimento (guarda permanente).	O	RF
RPC3.1.18	Prever a iniciação automática da contagem dos prazos de guarda referenciados nas tabelas de temporalidade a partir de, pelo menos, algum dos seguintes eventos • Data da produção de documento avulso; • Data do arquivamento definitivo ou rearquivamento (no caso de retomada de tramitação) de processo/dossiê/documento; • Data da retirada do sigilo em processo/dossiê/documento, na forma do art. 24 da Lei nº 12.527/2011 (Lei de Acesso à Informação); • acontecimentos específicos descritos em tabela de temporalidade ou na política de gestão documental aplicável ao órgão, quando não puderem ser detectados automaticamente pelo sistema. Nesses casos, deverá haver informação ao GestãoDoc por usuário autorizado. Exemplo: "cinco anos a contar da data de aprovação das contas".	O	RF
RPC3.1.19	Prever que a definição dos prazos de guarda seja expressa por: • um número inteiro de meses ou; • um número inteiro de anos.	O	RF
RPC3.1.20	Limitar a definição e a manutenção (alteração, inclusão e exclusão) da tabela de temporalidade a usuários autorizados de forma individualizada ou em bloco.	O	RF
RPC3.1.21	Permitir que um usuário autorizado altere o prazo ou destinação prevista em um item da tabela de temporalidade e garantir que a alteração tenha efeito em todos os documentos ou processos/dossiês associados àquele item. Obs: As alterações na tabela de temporalidade nos órgãos do Poder Judiciário só poderão ser feitas após a autorização dessas modificações pelos órgãos responsáveis pela aprovação dos instrumentos.	O	RF
RPC3.1.22	Permitir a automação de fluxos que auxiliem a identificação da temporalidade de processos judiciais.	O	RF
RPC3.1.23	Prover ferramentas que auxiliem a classificação e a seleção de documentos e processos/dossiês conforme as Tabelas de Classificação e Temporalidade dos Processos Judiciais e Administrativos do Poder Judiciário. Obs: A partir das tabelas, as ferramentas devem auxiliar a classificação e a seleção se dá a partir das temporalidades e destinações estabelecidas.	D	RF
RPC3.1.24	Manter o histórico das alterações realizadas nos planos de classificação e tabelas de temporalidade.	O	RF

3.2 Classificação e metadados dos documentos e processos/dossiês

Os requisitos desta seção referem-se à formação e classificação de processos e dossiês e à associação a eles de metadados, assim como à classificação e associação de metadados na produção de documentos avulsos.

REQ	REQUISITO	OBRIG	TIPO
RPC3.2.1	Permitir a classificação dos documentos e processos/dossiês somente nas classes ou níveis específicos autorizados.	O	RF
RPC3.2.2	Permitir a classificação de um número ilimitado de documentos/processos/dossiês dentro de uma classe ou nível específico.	O	RF
RPC3.2.3	Utilizar o termo completo da classe ou nível específico para identificar um documento/processo/dossiê, tal como especificado em RPC3.1.12.	O	RF
RPC3.2.4	Permitir a associação de metadados aos documentos/processos/dossiês.	O	RF
RPC3.2.5	Restringir a inclusão e alteração de metadados associados a documentos/processos/dossiês somente a usuários autorizados.	O	RF
RPC3.2.6	Associar os metadados dos documentos/processos/dossiês conforme estabelecido nos elementos de metadados (vide Anexo B - Metadados).	O	RF
RPC3.2.7	Permitir que um novo documento/processo/dossiê herde, da classe ou nível específico na qual foi classificado, determinados metadados predefinidos. Exemplos: temporalidade prevista e restrição de acesso.	O	RF
RPC3.2.8	Relacionar os metadados herdados de forma que qualquer alteração no metadado de uma classe ou nível específico seja automaticamente incorporada ao documento/processo/dossiê que herdou esse metadado.	O	RF
RPC3.2.9	Permitir a alteração conjunta de um determinado metadado em um grupo de documentos/processos/dossiês previamente selecionado.	O	RF

3.3 Gerenciamento dos processos/dossiês/documentos

Os requisitos desta seção referem-se ao gerenciamento dos documentos institucionais no que diz respeito a:

- controle de abertura e encerramento de processos/dossiês e seus volumes;
- inclusão de novos documentos em processos/dossiês e seus volumes; e
- procedimentos de arquivamento e reclassificação de processos/dossiês/documentos.

Entre os requisitos, os relacionados ao arquivamento possuem especial importância no contexto da gestão documental, visto que marcam o início da temporalidade constante das Tabelas para os fins de seleção e destinação.

O arquivamento consiste na "ação pela qual uma autoridade determina a guarda de um documento, cessada a sua tramitação" (ARQUIVO NACIONAL,

2005) e deve ocorrer quando não há mais diligências pendentes por parte do órgão/unidade processante ou de terceiros (art. 19 da Resolução CNJ nº 324/2020).

O arquivamento definitivo de processos judiciais inaugura a temporalidade na fase intermediária, visto que não há registro de temporalidade na fase corrente na Tabela de Temporalidade dos Processos Judiciais do Poder Judiciário.

Nesta seção, são também apresentados requisitos aptos a atender a necessidade de estabelecer relações entre documentos, processos ou dossiês, que podem ser de dependência ou de simples referência.

A relação de dependência enseja tramitação no mesmo órgão ou seleção conjunta de processos ou dossiês diversos. Constituem exemplos dessa relação processos judiciais autônomos que se originam de um processo principal como embargos à execução, embargos de terceiro, incidentes processuais etc.

Por sua vez, a relação de referência ocorre entre processos que não ensejam tramitação no mesmo órgão ou destinação comum consoante as regras de gestão documental aplicáveis, de que são exemplo, entre outros, os cumprimentos individuais de sentenças coletivas.

A referência feita a volumes nesta seção diz respeito a processos físicos.

REQ	REQUISITO	OBRIG	TIPO
RPC3.3.1	Registrar automaticamente a data de abertura, encerramento, arquivamento ou baixa definitiva do processo/dossiê.	O	RF
RPC3.3.2	Garantir que um processo/dossiê/documento seja marcado como arquivado ou não arquivado.	O	RF
RPC3.3.3	Permitir que um processo/dossiê/documento transite entre a unidade produtora e a responsável pela gestão documental (destinação), mediante procedimentos regulamentares.	O	
RPC3.3.4	Permitir que um processo/dossiê/documento arquivado definitivamente seja desarquivado ou reativado mediante procedimentos regulamentares.	O	RF
RPC3.3.5	Permitir que um processo/dossiê e seus respectivos volumes e documentos sejam reclassificados por um usuário autorizado e que todos os documentos já inseridos permaneçam nos processos/dossiês e volumes que estão sendo reclassificados, de modo a conservar a relação entre os documentos, volumes e processos/dossiês.	O	RF
RPC3.3.6	Manter o registro das classificações anteriores quando um documento/processo/dossiê é reclassificado, de forma a obter-se um histórico.	O	RF
RPC3.3.7	Permitir que o usuário autorizado introduza justificativa quando um processo/dossiê ou documento é reclassificado.	O	RF
RPC3.3.8	Permitir a geração de referências (links) entre documentos e processos/dossiês afins.	D	RF
RPC3.3.9	Permitir o estabelecimento de relação de dependência, ou apenas de referência, entre documentos, processos e dossiês.	O	RF
RPC3.3.10	Registrar, por referência ou inclusão/anexação, múltiplas capturas de um documento digital em mais de um processo/dossiê.	O	RF

RPC3.3.11	Impedir a eliminação de um documento/processo/dossiê digital ou de qualquer parte de seu conteúdo em qualquer momento, exceto quando se tratar de eliminação definitiva, consoante os critérios de classificação e guarda, ou na hipótese do RPC3.4.6. A eliminação será devidamente registrada em trilha de auditoria.	O	RF
RPC3.3.12	Impedir o acréscimo de novos documentos a processos/dossiês já encerrados. Para receber novos documentos, os processos/dossiês encerrados deverão ser reabertos.	O	RF
RPC3.3.13	Permitir o desarquivamento de documentos e/ou a reabertura de processos/dossiês encerrados.	O	RF
RPC3.3.14	Garantir a integridade da relação hierárquica entre classe, processo/dossiê, volume e documento nas operações dos usuários e nos procedimentos de manutenção do sistema.	O	RF
RPC3.3.15	Permitir operações em lotes relacionadas à produção, juntadas, assinaturas, movimentações, classificações e reclassificações dos processos/dossiês. Exemplos: abertura e encerramento de processos/dossiês, citação, intimação, sentença, decisão, despacho etc.	O	RF
RPC3.3.16	Fornecer ao gestor relatórios flexíveis para o gerenciamento dos volumes e documentos e sua utilização, que apresentem no mínimo: • Quantidade de processos/dossiês, volumes e documentos a partir de parâmetros ou atributos definidos (tempo, classe, unidade administrativa etc.). • Estatísticas de operações relativas a processos/dossiês, volumes e documentos. • Relatórios de operações por usuário.	O	RF

3.4 Processos

A formação e a manutenção de processos no Poder Judiciário obedecem a regras específicas que os diferenciam dos dossiês.

O dossiê é entendido como um conjunto de documentos relacionados entre si, tratados como uma unidade, e agregados por se reportarem a um mesmo assunto (ação, evento, pessoa, lugar, projeto). Exemplo: dossiê de evento de capacitação). O processo diferencia-se do dossiê, basicamente, por ser constituído de documentos oficialmente reunidos no decurso de uma ação administrativa ou judicial (ARQUIVO NACIONAL, 2005).

O detalhamento dessas regras está previsto na legislação e em atos normativos, que deverão ser observados pelos órgãos de acordo com seu âmbito de atuação.

REQ	REQUISITO	OBRIG	TIPO
RPC3.4.1	Prever a formação/autuação de processos conforme estabelecido nas leis e regulamentações vigentes.	O	RF
RPC3.4.2	Permitir que os documentos integrantes do processo sejam organizados de forma cronológica e contextualizada, seja por paginação, seja por eventos ou outros meios.	D	RF
RPC3.4.3	Permitir apensamento de processos. Nos processos judiciais, o apensamento ocorre por determinação legal ou judicial e nos administrativos, por determinação da autoridade competente. Esse procedimento deverá ser registrado nos metadados do processo. Quando se tratar de processo judicial, deve-se lançar o evento correspondente da Tabela Unificada de Movimentação Processual do Judiciário Brasileiro (apensamento) e seu complemento obrigatório (número do processo).	O	RF
RPC3.4.4	Permitir o registro do relacionamento entre processos, na hipótese de não haver apensamento. Exemplos: prevenção, prejudicialidade, cumprimento de títulos coletivos.	O	RF
RPC3.4.5	Permitir desapensamento. Nos processos judiciais, geralmente, o desapensamento ocorre por decisão judicial e nos administrativos, por determinação da autoridade competente. Esse procedimento deverá ser registrado nos metadados do processo. Quando se tratar de processo judicial, deve-se lançar o evento correspondente da Tabela Unificada de Movimentação Processual do Judiciário Brasileiro (desapensamento) e seu complemento obrigatório (número do processo).	O	RF
RPC3.4.6	Permitir o registro de exclusão de relacionamento entre processos.	O	RF
RPC3.4.7	Desentranhar peças dos processos judiciais em atenção à decisão judicial ou segundo a legislação específica, e dos administrativos, por determinação da autoridade competente. Esse procedimento deverá ser registrado nos metadados do processo. Quando se tratar de processo judicial, deve-se lançar o evento correspondente da Tabela Unificada de Movimentação Processual do Judiciário Brasileiro.	O	RF
RPC3.4.8	Permitir a inclusão de documentos anexos a um determinado processo. Esse procedimento deverá ser registrado nos metadados do processo.	O	RF

3.5 Volumes: abertura, encerramento e metadados

Em alguns casos, para facilitar o gerenciamento e a utilização, os processos e dossiês são compartimentados em volumes ou partes, de acordo com convenções predeterminadas ou com base em critérios como a dimensão, o número de documentos, o conteúdo específico, os períodos de tempo em que produzidos, entre outros.

Nesta seção são definidos os requisitos de sistema para a utilização de volumes em processos/dossiês físicos.

Em relação aos processos digitais, há um requisito desejável, já que o uso de volumes facilita questões de navegabilidade, visualização e operações de *download*.

REQ	REQUISITO	OBRIG	TIPO
RPC3.5.1	Gerenciar volumes para subdividir processos/dossiês, distinguindo entre processos/dossiês e volumes.	O	RF
RPC3.5.2	Permitir a associação de metadados aos volumes e restringir a inclusão e a alteração desses mesmos metadados somente a usuários autorizados.	O	RF
RPC3.5.3	Permitir que um volume herde automaticamente do processo/dossiê ao qual pertence determinados metadados predefinidos. Por exemplo: volume juntado em processo sigiloso também é sigiloso.	O	RF
RPC3.5.4	Permitir a abertura de volumes a qualquer processo/dossiê que não esteja encerrado.	O	RF
RPC3.5.5	Assegurar que, ao abrir um novo volume, o volume precedente seja automaticamente encerrado, registrando a data de encerramento. Apenas o volume produzido mais recentemente pode estar aberto; todos os outros volumes existentes nesse processo/dossiê têm de estar fechados.	O	RF
RPC3.5.6	Impedir a reabertura de um volume já encerrado para acréscimo de documentos.	O	RF
RPC3.5.7	Assegurar que um volume somente conterá documentos. Não é permitido que contenha outro volume ou um outro processo/dossiê.	O	RF
RPC3.5.8	Permitir que um volume seja encerrado por meio de procedimentos regulamentares.	O	RF
RPC3.5.9	Para processos/dossiês digitais, manter o conjunto de documentos organizados em volumes pré-definidos de páginas, com vistas a facilitar procedimentos de navegação no processo/dossiê e de download.	D	RF

3.6 Manutenção de documentos institucionais não digitais e híbridos

O Poder Judiciário possui documentos e processos digitais e não digitais. Esses últimos podem estar registrados em papel ou em outros suportes, tais como registros sonoros, audiovisuais etc.

Os documentos ou processos/dossiês híbridos podem ser nato-digitais com partes físicas ou documentos e mídias que não podem ser mantidas no GestãoDoc, físicos digitalizados para tramitação eletrônica ou ainda físicos com mídia ou parte digital.

Um GestãoDoc deve registrar os documentos ou processos/dossiês não digitais e digitais, utilizando os Planos de Classificação e as Tabelas de Temporalidade aplicáveis às áreas meio e fim, além de possibilitar a gestão de documentos ou processos/dossiês híbridos, formados por uma parte digital e uma parte não digital.

REQ	REQUISITO	OBRIG	TIPO
RPC3.6.1	Capturar documentos ou processos/dossiês não digitais e gerenciá-los como os digitais. Para conceito de captura, vide capítulo 4 - Captura.	O	RF
RPC3.6.2	Gerenciar os documentos ou processos/dossiês híbridos, associando-os ao mesmo número identificador, atribuído pelo sistema, e título, além de indicar que se trata de um documento institucional híbrido.	O	RF
RPC3.6.3	Permitir que um conjunto específico de metadados seja configurado para os documentos ou processos/dossiês não digitais e incluir informações sobre o local onde se encontram.	O	RF
RPC3.6.4	Possuir mecanismos para acompanhar a movimentação física do documento, processo/dossiê não digital, de forma que se evidencie ao usuário a localização atual. Exemplo: Documentos cuja digitalização seja tecnicamente inviável, processos judiciais físicos etc.	O	RF
RPC3.6.5	Oferecer ao usuário funcionalidades para solicitar vista, carga ou desarquivamento de um documento e/ou processo não digital.	O	RF
RPC3.6.6	Incluir mecanismos de impressão e reconhecimento de códigos de barra para automatizar a introdução de dados e acompanhar as movimentações de documentos ou processos/dossiês não digitais.	D	RF
RPC3.6.7	Assegurar que a recuperação de um documento ou processo/dossiê híbrido permita igualmente a recuperação dos metadados tanto da parte digital como da parte não digital.	O	RF
RPC3.6.8	Sempre que os documentos ou processos/dossiês híbridos estiverem classificados quanto ao grau de sigilo, garantir que o grau de sigilo seja estendido ao todo ou à parte, independentemente do suporte.	O	RF
RPC3.6.9	Registrar na trilha de auditoria todas as alterações efetuadas nos metadados dos documentos ou processos/dossiês não digitais ou híbridos.	O	RF

4. CAPTURA

A captura é a inserção de um documento/processo/dossiê no GestãoDoc para tramitação e processamento. A captura poderá dar-se mediante a geração de documento nato-digital ou a incorporação de documento digitalizado ao sistema e inclui as seguintes ações:

a) Produção e Registro;
b) Classificação;
c) Indexação;
d) Atribuição de restrição de acesso; e
e) Arquivamento.

Tradicionalmente, nos sistemas de gestão de processos e documentos em papel, a captura é feita quando o documento é registrado, classificado e identificado.

Em um GestãoDoc, o documento pode ser produzido diretamente no sistema, capturado e registrado automaticamente neste momento ou pode ser produzido fora do sistema e capturado e registrado para tramitação e acesso.

A política de gestão de documentos do Poder Judiciário é única para documentos nato-digitais, físicos e híbridos. O GestãoDoc deve capturar todos os documentos produzidos ou recebidos pela instituição no exercício das suas atividades, independentemente do suporte. Após a captura, os documentos serão retidos pelo tempo definido nos instrumentos de gestão documental aprovados.

A captura compreende ainda o preenchimento automático ou manual de metadados (Anexo B), tais como:

- classificação;
- assuntos (descritores);
- número do documento/processo/dossiê e seu identificador;
- data e hora da produção; e
- nome do autor e do destinatário.

Esses metadados podem ser registrados em vários níveis de detalhe, dependendo das previsões normativas.

Os metadados são essenciais para identificar o documento institucional de modo inequívoco e mostrar sua relação com os outros.

A captura tem como pré-requisitos definir:

- Que documentos (produzidos e recebidos) serão capturados pelo sistema de gestão de processos e documentos;
- Quem deve ter acesso a esses documentos e em quais níveis; e
- A classificação e previsão de prazos de guarda dos documentos.

As ações relativas à captura do documento no sistema são descritas a seguir:

a) Produção e Registro

As atividades de produção e registro de documentos compreendem o conjunto de operações que visam a propiciar o registro dos documentos produzidos no GestãoDoc e o controle de entrada dos documentos produzidos e recebidos fora do sistema nos órgãos do Poder Judiciário, assegurando sua localização, tramitação, recuperação e acesso.

O GestãoDoc atribui número e data da entrada ou da produção do documento e registra a classificação atribuída, com base nos instrumentos aprovados na instituição.

b) Registro do processo judicial

O registro é a ação para a formação do processo judicial, quando lhe é atribuído um número identificador e uma descrição informativa.

O registro tem por objetivo demonstrar que o documento foi produzido ou recebido e capturado pelo GestãoDoc, assim como facilitar sua recuperação. Consiste na formalização da captura do documento judicial no GestãoDoc.

Para os processos físicos, empregava-se o termo "autuação", que abrangia as ações de inclusão dos documentos em capa, preenchimento do termo correspondente e numeração de suas folhas, formando os "autos" judiciais ou administrativos.

Os documentos judiciais são os vinculados diretamente ao processo (petição inicial, contestação, sentença, certidão de trânsito em julgado, recurso etc.).

Os processos judiciais receberão a numeração com base no sistema de Numeração Única de Processos, conforme disposições da Resolução CNJ nº 65/2008, que estabeleceu a uniformização do número dos processos nos órgãos do Poder Judiciário.

Além de numerados, os processos serão classificados de acordo com as Tabelas Processuais Unificadas do Poder Judiciário, criadas pela Resolução CNJ nº 46/2007.

c) Produção e registro de documentos e processos administrativos

Consiste na formalização da captura do documento administrativo no GestãoDoc.

A atividade visa à incorporação do documento por meio da produção, assinatura e registro ou da captura dos dados informacionais (o número recebido na origem, o assunto, a data da produção, a data do registro no sistema etc.) dos documentos recebidos, com a finalidade de informar, de forma rápida e precisa, a sua situação e localização.

Os documentos produzidos no âmbito de cada um dos órgãos do Poder Judiciário (pareceres, ofícios, informações etc.) receberão numeração e serão classificados com base no Plano de Classificação e Tabela de Temporalidade dos Documentos da Administração do Poder Judiciário, disponível na página

do Proname/CNJ. O mesmo se aplica aos documentos de apoio às atividades forenses (pauta de julgamento, requisições, precatórios etc.).

d) Classificação

A classificação arquivística representa o ato ou efeito de analisar e identificar o conteúdo dos documentos e de selecionar a classe sob a qual serão recuperados, para fins de distribuição, tramitação, acesso, padronização, estatísticas e destinação. Essa classificação é feita a partir dos Planos de Classificação adotados pelo órgão, referidos nos subitens anteriores.

A classificação deve refletir a atividade que gerou o documento e determinar o uso da informação nele contida. Ela também define a organização física dos documentos não digitais, constituindo-se em referencial básico para sua recuperação.

Objetivos da classificação:

- Estabelecer a relação orgânica dos documentos;
- Assegurar que os documentos sejam identificados de forma consistente ao longo do tempo;
- Auxiliar a recuperação de todos os documentos relacionados a uma determinada função ou atividade; e
- Possibilitar a avaliação de um grupo de documentos de forma que aqueles associados sejam transferidos, recolhidos ou eliminados em conjunto.

e) Indexação

A indexação de assuntos envolve duas etapas principais; e

- Análise conceitual — atividade de definição dos assuntos tratados no documento.
- Tradução — atividade de conversão dos conceitos identificados na análise para uma linguagem de indexação (vocabulário controlado e/ou lista de descritores, tesauro e o próprio plano de classificação).

O principal objetivo da indexação é assegurar a recuperação de qualquer documento em um sistema de informações e pode ser feita de forma manual ou automática.

No caso de documentos administrativos, a indexação ocorre pelo Plano de Classificação e há a possibilidade de uso de outros indexadores, como títulos, cabeçalhos, datas, anexos etc. Em processos judiciais, há indexações pré-definidas e aplicáveis com base nas Tabelas Processuais Unificadas do Poder Judiciário, que têm enorme potencial facilitador de recuperação de documentos, sem prejuízo de outras formas de indexação aplicáveis.

f) Atribuição de restrição de acesso

De forma geral, os documentos dos órgãos do Poder Judiciário são públicos, devendo o acesso a eles ser restringido apenas em casos de segredo de justiça e de aplicação das Leis nº 12.527/2011 (Lei de Acesso à Informação – LAI) e nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

Os documentos podem ser ostensivos ou sigilosos. No caso dos sigilosos, a legislação vigente estabelece procedimentos específicos para seu tratamento, incluindo a definição de graus de sigilo e demais restrições de acesso a serem atribuídas a cada documento.

Os documentos que dizem respeito à segurança da sociedade e do Estado, bem como aqueles necessários à utilidade do processo e ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas estarão sujeitos às restrições de acesso, conforme legislação em vigor.

A atribuição de restrições pode ser feita em qualquer fase da tramitação, com base no esquema de classificação de segurança e sigilo elaborado pelos órgãos do Poder Judiciário e envolve as seguintes etapas:

a) Identificar a ação ou a atividade que o documento registra;
b) Identificar a unidade administrativa ou judicial à qual o documento pertence;
c) Verificar a precaução de segurança e o grau de sigilo;
d) Atribuir o grau de sigilo e as restrições de acesso ao documento;
e) Registrar o grau de sigilo e as restrições de acesso no sistema informatizado de gestão de processos e documentos; e

Os requisitos de segurança são apresentados no Capítulo 8.

G) Arquivamento

As operações de arquivamento dos documentos digitais e não digitais são distintas.

Em relação aos documentos não digitais, o arquivamento é, ao mesmo tempo, operação intelectual e física. Assim, por exemplo, o arquivamento de um relatório é feito em pasta física na unidade produtora ou custodiadora e o registro no sistema informatizado é feito de forma a permitir sua recuperação pelo metadado apropriado.

No documento digital, por sua vez, a operação de arquivar significa que o GestãoDoc enviará o(s) arquivo(s) a um dispositivo de armazenamento ou a um Repositório Arquivístico Digital confiável (RDC-Arq), após validação da destinação prevista pela área responsável pela gestão documental, e registrará, em metadados, elementos obrigatórios previamente determinados (operação lógica).

Para mais informações sobre arquivamento de documentos, consulte o capítulo 3.3 deste Modelo e o Manual de Gestão Documental do Poder Judiciário.

4.1 Captura: procedimentos gerais

REQ	REQUISITO	OBRIG	TIPO
RCA4.1.1	A captura deve garantir a execução das funções relacionadas a seguir, de acordo com o sistema de classificação do Poder Judiciário: • Registrar e gerenciar todos os documentos não digitais. • Registrar e gerenciar todos os documentos digitais, independentemente do contexto tecnológico. • Classificar todos os documentos de acordo com o Plano de Classificação • Validar a introdução de metadados.	O	RF
RCA4.1.2	Capturar documentos digitais das seguintes formas: • Documento individual produzido em arquivo digital fora do GestãoDoc. • Documento individual produzido em outros sistemas integrados ou no próprio GestãoDoc. • Documentos em lote.	O	RF
RCA4.1.3	Permitir a automatização da produção de documentos por meio da exibição de formulários e modelos predefinidos pela política de gestão documental do órgão.	O	RF
RCA4.1.4	Aceitar o conteúdo do documento, bem como as informações que definem sua aparência, mantendo as associações entre os vários componentes digitais do documento.	O	RF
RCA4.1.5	Capturar e manter todos os componentes digitais do documento. Os componentes digitais armazenam informações de conteúdo, da forma documental e as relações entre elas. No caso de documentos constituídos por mais de um componente digital, o GestãoDoc deve: • tratar o documento como uma unidade indivisível, assegurando a relação entre os componentes digitais; • preservar a integridade do documento, mantendo a relação entre os componentes digitais; • garantir a integridade do documento quando de sua recuperação, visualização e gestão posteriores; • gerenciar a destinação de todos os componentes digitais que compõem o documento como uma unidade indivisível.	O	RF
RCA4.1.6	Permitir a inserção de todos os metadados, obrigatórios e facultativos suportados pelo sistema, apresentados no Anexo B, e garantir que eles se mantenham associados ao documento ou processo/dossiê.	O	RF
RCA4.1.7	Atribuir um número identificador a cada processo/dossiê e documento capturado, que serve para identificá-lo desde o momento da captura até sua destinação final dentro do GestãoDoc a fim de manter a integridade.	O	RF
RCA4.1.8	O formato do número identificador atribuído pelo sistema deve ser definido no momento da configuração do GestãoDoc. O identificador pode ser numérico ou alfanumérico, ou pode incluir os identificadores encadeados das entidades superiores no ramo apropriado da hierarquia.	O	RF
RCA4.1.9	O identificador atribuído pelo sistema deve: • Ser único e gerado automaticamente, vedada sua introdução manual e alteração posterior; ou • Ser atribuído pelo usuário e validado pelo sistema antes de ser aceito.	O	RF
RCA4.1.10	Utilizar sistemas de indexação automática do conteúdo do documento para atribuição do metadado assunto.	D	RF

RCA4.1.11	Garantir que os metadados associados a um documento sejam alterados somente por gestores e usuários autorizados e devidamente registrados em trilhas de auditoria.	O	RF
RCA4.1.12	Inserir automaticamente os metadados previstos no sistema para o maior número possível de documentos. Por exemplo, para diminuir as tarefas do usuário do sistema e garantir maior exatidão e eficiência na inserção dos metadados, no caso de documentos com forma padronizada (formulários, modelos de requerimentos, memorandos etc.) alguns metadados podem ser inseridos automaticamente, tais como: número identificador, título, prazo de guarda.	D	RF
RCA4.1.13	Visualizar o registro de entrada do documento dentro do sistema com todos os metadados que possam ser inseridos automaticamente e os demais a serem atribuídos pelo usuário. Por exemplo, o sistema pode atribuir automaticamente o número identificador, a data de captura, o título, o originador e requerer que o usuário preencha os demais metadados.	O	RF
RCA4.1.14	Garantir a inserção de outros metadados após a captura. Por exemplo, data e hora de alteração e mudança de suporte.	O	RF
RCA4.1.15	Permitir o registro de versões do documento enquanto não for dada publicidade.	D	RF
RCA4.1.16	Registrar a versão final do documento institucional após ter sido dada publicidade ou assinado digitalmente.	O	RF
RCA4.1.17	Facilitar a classificação dos documentos, por meio de algumas ou de todas as ações que se seguem: • Tornar acessível ao usuário somente o subconjunto do plano de classificação que diz respeito à sua atividade. • Indicar as últimas classificações feitas pelo usuário. • Indicar processos/dossiês que contenham documentos institucionais relacionados. • Indicar classificações possíveis a partir dos metadados já inseridos. • Indicar classificações possíveis a partir do conteúdo do documento.	D	RF
RCA4.1.18	Permitir que diversos usuários atuem colaborativamente, de forma concorrente, na captura de documentos para compor um único processo/dossiê.	D	RF
RCA4.1.19	No caso de documentos constituídos por mais de um objeto digital: • Tratar o documento como uma unidade indivisível, assegurando a relação entre os objetos digitais. • Preservar a integridade do documento, mantendo a relação entre os objetos digitais. • Garantir a integridade do documento quando da recuperação, visualização e gestão posteriores. • Gerenciar a destinação de todos os objetos digitais que compõem o documento como uma unidade indivisível.	O	RF
RCA4.1.20	Emitir aviso caso o usuário tente inserir documento digital detectado como idêntico a outro anteriormente registrado no mesmo processo/dossiê, devendo ser observados os metadados dos documentos como parâmetro de comparação.	O	RF
RCA4.1.21	Impedir a reinserção de documentos digitais que forem detectados como idênticos.	O	RF
RCA4.1.22	Identificar e associar informações de metadados a partir dos documentos digitais, por meio de técnicas de automatização.	D	RF
RCA4.1.23	Atribuir a cada componente digital do documento, no momento da captura, um código de manutenção de integridade baseado em criptografia robusta.	O	RF

4.2 Captura em lote

REQ	REQUISITO	OBRIG	TIPO
RCA4.2.1	Capturar documentos em lote gerados por outros sistemas autorizados pelo órgão do Poder Judiciário. Esse procedimento deve: • Permitir importação de transações predefinidas de arquivos em lote; • Registrar automaticamente cada um dos documentos importados contidos no lote; • Permitir e controlar a edição do registro dos documentos importados; • Validar a integridade dos metadados. Exemplos de lote de documentos podem ser: mensagens do sistema de comunicação eletrônica, correspondência digitalizada por meio de escâner, documentos provenientes de uma unidade administrativa/órgão, de um grupo ou indivíduo, transações de aplicações de um computador ou ainda documentos oriundos de um sistema de gestão de processos e documentos.	O	RF

4.3 Captura de mensagens de sistemas de comunicação digital

Os sistemas de comunicação digital são utilizados para criar, transmitir e receber mensagens eletrônicas e outros documentos digitais por meio de redes de computadores, sendo o correio eletrônico (e-mail) a forma mais usada pelos órgãos do Poder Judiciário.

As características do sistema de comunicação digital podem dificultar seu gerenciamento, cabendo ao GestãoDoc permitir controles de gestão que possibilitem ao usuário capturar apenas as mensagens e os anexos previamente selecionados e permitir o envio e recebimento de forma vinculada aos processos e dossiês a que estejam relacionadas.

REQ	REQUISITO	OBRIG	TIPO
RCA4.3.1	Permitir o envio e recebimento de mensagens por meio de interfaces públicas de serviços externos, quando relacionados a comunicações que normativamente possam ser feitas por tais serviços.	O	RF
RCA4.3.2	Assegurar que as mensagens enviadas sejam capturadas e vinculadas aos processos/dossiês em que foram produzidas.	O	RF
RCA4.3.3	Permitir que mensagens recebidas e vinculadas a processos/dossiês possam ser selecionadas e capturadas.	O	RF
RCA4.3.4	Assegurar que o conteúdo original das mensagens seja armazenado sem alterações, assim como os respectivos metadados.	O	RF

4.4 Formato de arquivo e estrutura dos documentos a serem capturados

Os órgãos do Poder Judiciário realizam a captura de quantidade diversificada de documentos com formatos de arquivo e estruturas diferentes. Os requisitos técnicos para a captura variam de acordo com a complexidade dos documentos.

Em alguns ambientes, não é possível identificar antecipadamente todos os formatos de arquivo e estruturas possíveis dos documentos, sendo comum a recepção a partir de fontes externas. Considerando a captura de documentos produzidos fora dos sistemas de GestãoDoc, entre os requisitos foi incluída a previsão de recursos aptos ao reconhecimento de caracteres textuais, tais como OCR (Reconhecimento Óptico de Caracteres) e ICR (Reconhecimento Inteligente de Caracteres), aplicáveis aos documentos digitalizados. O uso dessas tecnologias está previsto na Resolução CNJ nº. 469/2022 e é abordado no capítulo 9.4 do Manual de Digitalização de Documentos do Poder Judiciário.

REQ	REQUISITO	OBRIG	TIPO
RCA4.4.1	Possuir a capacidade de capturar documentos nos formatos previamente definidos como padrão.	O	RF
RCA4.4.2	Fornecer recursos que possibilitem o reconhecimento de caracteres a partir de documentos textuais digitalizados.	O	RF
RCA4.4.3	Fornecer recursos que possibilitem a extração e reconhecimento do conteúdo de documentos de áudio, vídeo e outras mídias.	D	RF
RCA4.4.4	Capturar documentos que se apresentam com as seguintes estruturas: • Simples: texto, imagens, mensagens de sistema de comunicação digital, *slides* digitais, som e vídeo; e • Composta: mensagens enviadas ou recebidas por meio de sistema de comunicação digital, com ou sem anexos, páginas *web* e publicações eletrônicas.	O	RF
RCA4.4.5	Permitir que um documento composto seja capturado das seguintes formas: • Um único documento de arquivo contendo todas as peças; • Uma série de arquivos simples, um para cada documento, relacionado.	O	RF
RCA4.4.6	Ser capaz de armazenar, suportar e tratar os formatos de arquivos adotados pelo Poder Judiciário.	O	RF
RCA4.4.7	Registrar em metadados as informações relativas à dependência de *software*, quando capturar documentos em formatos diferentes dos previstos pela política de gestão documental do órgão.	D	RF

4.5 Documentos automodificáveis

Documentos automodificáveis podem ter seus conteúdos alterados sem intervenção do usuário. O documento lógico, no entanto, não se modifica, mas apenas sua exibição (documento conceitual) sofre alterações conforme o *software* utilizado para visualizá-lo.

Constituem exemplos de documentos automodificáveis:

- um modelo de mandado de citação ou intimação, cuja data é colocada automaticamente pelo sistema e armazenada como um "campo" ou "código". Nesse caso, cada vez que o documento é exibido, a data apresentada é atualizada.
- Uma folha de cálculo com uma "macro" sofisticada que a altera (mediante *software* de aplicações utilizado para visualização) e, em seguida, guarda-a automaticamente.

Os documentos automodificáveis devem ser evitados. Na impossibilidade, os documentos dessa natureza devem ser armazenados em formatos estáveis, como o PDF, que desativem o código automodificador ou visualizados por meio de *software* que não desencadeie a alteração.

Quando não for possível converter os documentos automodificáveis para formato estável ou visualizá-los por meio de *software* que não desencadeie a alteração, no momento da captura desses documentos no GestãoDoc, o armazenamento deve ser feito em formato que desative o código automodificador.

REQ	REQUISITO	OBRIG	TIPO
RCA4.5.1	Capturar documentos automodificáveis, desativando seu código automodificador. Exemplos: • Informações de outros aplicativos: contabilidade, folha de pagamento, desenho assistido por computador (CAD); • Agenda digital; • Diagramas e mapas digitais; • Dados estruturados (EDI); • Bases de dados; e • Páginas *web*.	D	RF
RCA4.5.2	Armazenar em formato que desative o código automodificador quando da captura de documento automodificável.	O	RF

4.6 Estrutura dos procedimentos de gestão

A gestão de documentos digitais prevê o estabelecimento de três domínios dentro do ambiente informatizado:

- Espaço individual — Designado a cada usuário autorizado;
- Espaço do grupo — Designado a cada grupo de trabalho, equipe, comitê etc; e
- Espaço geral — Ambiente no qual o documento não pode mais ser alterado e onde ocorre sua publicidade.

Nos sistemas informatizados de gestão de documentos são necessárias algumas definições sobre os espaços, conforme e-Arq Brasil (Conarq, 2022a):

- *os espaços em que os documentos podem ser produzidos, recebidos, alterados, capturados (registrados, classificados, indexados e arquivados ou encaminhados), armazenados e eliminados;*
- *o espaço em que os metadados serão incluídos;*
- *os direitos de acesso a cada espaço e a maneira como os documentos tramitarão dentro e fora do órgão ou entidade.*

Uma vez capturados no espaço geral, os documentos e seus metadados devem ser mantidos em versão definitiva e protegidos contra alterações deliberadas ou acidentais, em relação ao seu conteúdo, contexto e forma ao longo de todo o seu ciclo de vida.

REQ	REQUISITO	OBRIG	TIPO
RCA4.6.1	Assegurar que as ações desempenhadas dentro do sistema GestãoDoc possam ser executadas dentro dos três espaços de domínio: individual, grupo e geral.	O	RF
RCA4.6.2	Operacionalizar as regras estabelecidas pelo sistema de gestão de processos e documentos nos três espaços.	O	RF
RCA4.6.3	Impedir que o conteúdo de um documento seja alterado por usuários, gestores e administradores, exceto nos casos em que a alteração fizer parte do processo documental, conforme tratado na seção 8.4- Alteração, ocultação e exclusão de documentos institucionais.	O	RF
RCA4.6.4	Emitir um aviso, ao se tentar capturar um documento cujos dados estruturados estejam incompletos, e impedir a captura quando estiverem inconsistentes.	O	RF
RCA4.6.5	Implementar controles para assegurar a autenticidade dos documentos capturados.	O	RF

4.7 Captura de documentos não digitais ou híbridos

A política de gestão documental de um órgão é única para documentos não digitais, digitais e híbridos. Assim, o GestãoDoc tem que capturar todos esses tipos de documentos.

A captura do documento não digital será realizada pelo GestãoDoc por meio das atividades de registro, classificação e indexação.

O arquivamento será feito da forma apropriada ao suporte, formato e tipo de documento.

REQ	REQUISITO	OBRIG	TIPO
RCA4.7.1	Capturar também os documentos não digitais e/ou híbridos.	O	RF
RCA4.7.2	Acrescentar aos metadados dos documentos não digitais informações sobre sua localização. Obs: Essa informação só será acessada por usuários autorizados.	O	RF
RCA4.7.3	Garantir que a parte digital de um documento ou processo/ dossiê híbrido seja tratada de forma análoga aos documentos ou processos/ dossiês inteiramente digitais.	O	RF
RCA4.7.4	Tratar um documento ou processo/dossiê híbrido como uma unidade indivisível, assegurando a relação entre a parte digital e a não digital.	O	RF

5. FLUXO DE TRABALHO E TRAMITAÇÃO

Os requisitos deste capítulo tratam das situações em que o GestãoDoc prevê recursos de automação de fluxo de trabalho (*workflow*), que consiste na substituição de atividades rotineiras ou sequenciais por ações de sistemas.

Esse conjunto de requisitos está abrangido nos conceitos introduzidos pela Resolução CNJ nº 335/2020, que cria a Plataforma Digital do Poder Judiciário - PDPJ-BR, devendo as soluções contemplar, também em um GestãoDoc, a otimização dos fluxos de trabalho (*workflow*), padronizando-os sempre que possível.

Os requisitos abrangem funções para controle do fluxo de trabalho e atribuição de metadados para registro da tramitação dos documentos, incluindo-se o *status* do documento (minuta, original ou cópia).

Os recursos de um GestãoDoc para controle do fluxo de trabalho podem compreender a produção e a tramitação de processos/dossiês/documentos antes e após seu registro ou captura. Esse fluxo não se confunde com a tramitação de documentos controlada pelo sistema de protocolo, o qual realiza registro e autuação para formação de processos.

Conforme especificado no e-Arq Brasil (Conarq, 2022a):

> Um participante de um fluxo de trabalho pode ser um indivíduo específico, um grupo de trabalho ou mesmo um software. Um participante é o responsável pela realização de uma tarefa estabelecida ao longo de um fluxo de trabalho predefinido. Caso o participante seja um indivíduo, a tarefa é direcionada a um usuário com uma identificação específica. Se o participante for um grupo de trabalho, a tarefa é dirigida ao grupo (formado por vários usuários, cada um com sua identificação no SIGAD). A tarefa tem que ser distribuída entre os usuários do grupo, e, após ser cumprida por um membro desse grupo, o documento segue o fluxo previsto. Quando o participante é um software, a tarefa é direcionada a uma função de programa, que a realiza automaticamente e reencaminha o documento ao fluxo previsto.

5.1 Controle do fluxo de trabalho

REQ	REQUISITO	OBRIG	TIPO
RFT5.1.1	Fornecer os passos necessários para o cumprimento de trâmites preestabelecidos ou fluxos alternativos. Nesse caso, cada passo significa o deslocamento de um documento ou processo/dossiê, a fim de serem objeto de ações.	O	RF
RFT5.1.2	Permitir a automação dos fluxos de trabalho.	D	RF
RFT5.1.3	Possuir capacidade, sem limitações, para estabelecer o número necessário de trâmites nos fluxos de trabalho.	O	RF
RFT5.1.4	Disponibilizar uma função para avisar a um participante do fluxo que um documento lhe foi enviado, especificando a ação necessária.	O	RF
RFT5.1.5	Permitir a automação dos avisos aos participantes do fluxo de trabalho.	D	RF

RFT5.1.6	Permitir a utilização de sistema de comunicação eletrônica validado pelo órgão para que um usuário possa informar outros usuários sobre documentos que requeiram sua atenção.	D	RF
RFT5.1.7	Permitir que fluxos de trabalho pré-programados sejam definidos, alterados e mantidos exclusivamente por usuário autorizado.	O	RF
RFT5.1.8	Possibilitar que tarefas e ações sejam redistribuídas em um fluxo de trabalho, quando necessário, a um usuário ou grupo diferente do que havia sido previsto.	O	RF
RFT5.1.9	Registrar na trilha de auditoria todas as alterações ocorridas no fluxo de trabalho.	O	RF
RFT5.1.10	Registrar a tramitação de todos os documentos no processo.	O	RF
RFT5.1.11	Efetuar a gestão dos documentos em filas de espera que possam ser examinadas e controladas pelo usuário autorizado.	O	RF
RFT5.1.12	Permitir que os usuários visualizem a fila de espera do trabalho a eles destinado e que selecionem os itens a trabalhar.	O	RF
RFT5.1.13	Fornecer fluxos condicionais de acordo com os dados de entrada do usuário ou do GestãoDoc.	O	RF
RFT5.1.14	Fornecer histórico de movimentação dos documentos. O histórico de movimentação corresponde a um conjunto de metadados de datas de entrada e saída; nomes de responsáveis; título do documento, providências etc.	O	RF
RFT5.1.15	Permitir que usuários autorizados interrompam ou suspendam temporariamente um fluxo com o objetivo de executar outro trabalho. O fluxo só prosseguirá com a autorização do usuário.	D	RF
RFT5.1.16	Incluir processamento condicional, permitindo que um fluxo de trabalho seja suspenso aguardando algum evento para continuar. Por exemplo, aguardar a chegada de um documento para prosseguimento, assim que o documento for recebido, conforme definido pelo próprio fluxo.	O	RF
RFT5.1.17	Permitir associar limites de tempo a trâmites e/ou procedimentos individuais em cada fluxo e comunicar os itens que expiraram, de acordo com tais limites.	O	RF
RFT5.1.18	Reconhecer indivíduos e grupos de trabalho como participantes do fluxo.	O	RF
RFT5.1.19	Prever a forma de distribuição dos documentos entre os membros do grupo, sempre que o participante do fluxo for um grupo de trabalho.	O	RF
RFT5.1.20	Permitir que a captura de documentos desencadeie automaticamente fluxos de trabalho.	O	RF
RFT5.1.21	Fornecer meios de elaboração de relatórios completos para permitir que gestores monitorem a tramitação dos documentos e o desempenho dos participantes.	O	RF
RFT5.1.22	Registrar a tramitação de um documento em seus metadados. Os metadados referentes à tramitação devem registrar, entre outros, data e hora de envio e de recebimento e identificação dos usuários.	O	RF
RFT5.1.23	Manter versões dos fluxos alterados e estabelecer vínculos entre os documentos já processados ou em processamento nos fluxos alterados.	O	RF
RFT5.1.24	Assegurar que qualquer modificação nos atributos dos fluxos, como extinção ou ampliação do número de pessoas ou extinção de autorização, leve em conta os documentos vinculados.	O	RF

5.2 Controle de versões e do status do documento

Um GestãoDoc deve ser capaz de estabelecer — pelo seu recurso de fluxo de trabalho — o *status* do documento: minuta, original ou cópia. No caso dos documentos nato-digitais, esse *status* é estabelecido de acordo com o fluxo do documento no GestãoDoc (Conarq, 2022a):

Assim, por exemplo:

- *um documento criado no espaço individual ou do grupo, mas não transmitido, é uma minuta;*
- *um documento transmitido do espaço individual ou do grupo para o espaço geral, onde não pode mais ser alterado, e deste para fora da instituição, será sempre recebido como um original e armazenado no espaço de origem (individual, do grupo ou gerencial) como uma última minuta. Isso porque a transmissão acrescenta metadados ao documento (como data e hora da transmissão) que o tornam mais completo;*
- *um documento enviado do espaço individual para outro espaço individual ou para o espaço do grupo, para receber comentários, é uma minuta, que deve ter seu número de versões devidamente controlado;*
- *quando um usuário autorizado recupera um documento do espaço geral e o armazena em seu próprio espaço, ele cria uma cópia. O mesmo acontece nos casos em que o usuário reencaminha um documento para outro usuário.*

REQ	REQUISITO	OBRIG	TIPO
RFT5.2.1	Registrar o status de transmissão do documento: minuta, original ou cópia.	O	RF
RFT5.2.2	Manter o identificador único do documento e registrar, em metadados específicos, o controle de versões.	O	RF

5.3 Acompanhamento de transferência

Durante a tramitação ou conforme a fase do ciclo de vida, os processos/dossiês/documentos institucionais e os respectivos metadados podem ser transferidos de uma mídia de suporte ou de um local para outro, conforme necessário, adequado ou previsto.

Essa movimentação não está circunscrita a ações de *backup*, redundância, escalabilidade e situações similares para melhoria de desempenho e segurança do acervo.

Essa transferência pode envolver, entre outros, a mudança:

- de sistemas *online* para sistemas *offline;*
- de suporte de armazenamento; e
- do local de armazenamento conforme competências de atuação.

São necessários recursos de acompanhamento, a fim de registrar a mudança de local, tanto para facilitar o acesso quanto para cumprir requisitos regulamentares.

REQ	REQUISITO	OBRIG	TIPO
RFT5.3.1	Manter, para cada documento/processo/dossiê, o histórico das movimentações e transferências de meios de armazenamento ocorridas.	O	RF
RFT5.3.2	Fornecer recurso de acompanhamento para monitorar e registrar informações acerca da localização atual e do deslocamento dos meios de armazenamento de documento/processo/dossiê digital e não digital.	O	RF
RFT5.3.3	A função de acompanhamento de mudança de suporte ou de local tem que registrar metadados (Anexo B) que incluam: • identificador do documento atribuído pelo GestãoDoc; • localização atual e localizações anteriores (definidas pelo usuário); • data e hora do envio/deslocamento; • data e hora da recepção no novo local; • destinatário; • usuário responsável pela mudança de suporte ou de local (sempre que for adequado); e • método da mudança de suporte ou de local.	O	RF

6. AVALIAÇÃO: TEMPORALIDADE E DESTINAÇÃO

Os requisitos deste capítulo referem-se a funcionalidades que servem para apoiar os procedimentos de avaliação, seleção e destinação dos documentos gerenciados pelo GestãoDoc.

Os valores dos documentos, observados durante a avaliação, definem a necessidade de sua guarda e preservação por diferentes períodos, bem como a destinação de cada um: eliminação ou guarda permanente.

Prazos de guarda e destinação são comumente registrados em tabelas de temporalidade. No Poder Judiciário, adotam-se a Tabela de Temporalidade dos Processos Judiciais e a Tabela de Temporalidade dos Documentos da Administração.

Além delas, alguns critérios definidores de prazos e destinação, resultantes da avaliação, estão registradas em outros instrumentos que compõem o Programa Nacional de Gestão Documental e Memória do Poder Judiciário (Proname) e as políticas locais.

O GestãoDoc deve adotar e aplicar os prazos e destinação definidos durante a avaliação, a fim de permitir a seleção facilitada dos documentos e processos/dossiês geridos.

Para cumprir a destinação, um documento deve ser exportado do GestãoDoc. Além disso, um GestãoDoc pode exportar documentos para outro sistema por outras razões, como cumprimento de trâmite e migração.

Este capítulo estabelece requisitos para a implementação da avaliação e para a exportação e eliminação de documentos de um GestãoDoc.

a) Avaliação, temporalidade e destinação

A avaliação é uma atividade vital em um programa de gestão de documentos, pois permite racionalizar o acúmulo dos documentos nas fases corrente e intermediária, facilitando a constituição dos arquivos permanentes (vide teoria das três idades).

A avaliação é o processo de análise dos documentos e visa a estabelecer os prazos de guarda e a destinação, de acordo com os valores primário e secundário que lhes são atribuídos. Uma vez avaliados, a seleção dos documentos permite a separação dos permanentes daqueles passíveis de eliminação.

Os prazos de guarda referem-se ao tempo necessário para o trâmite, manutenção e arquivamento dos documentos nas fases corrente e intermediária, visando a atender as necessidades jurídicas e administrativas que levaram à sua produção. Os prazos de guarda e as ações de destinação são formalizados em instrumentos de temporalidade e destinação.

O Poder Judiciário adota duas Tabelas de Temporalidade, uma para os processos judiciais (atividade-fim) e outra para os documentos da administração (atividades-meio), conforme mencionado acima.

Para os processos judiciais, adotam-se prazos de guarda e destinação em algumas classes, nos assuntos processuais, em alguns movimentos, e ainda em alguns documentos, os quais compõem as Tabelas Processuais Unificadas utilizadas em todo o Poder Judiciário.

A aplicação requer a observância de critérios apresentados em fluxogramas que apoiam a identificação da temporalidade, constantes do Manual de Gestão Documental do Poder Judiciário. Em outras palavras, a temporalidade de classes, assuntos, movimentos e documentos não é aplicada diretamente, mas mediante critérios a serem contemplados no GestãoDoc.

Em muitos casos, a temporalidade e a destinação previstas podem ser constatadas no momento da captura e do registro dos documentos no GestãoDoc. Essa informação deve ser registrada em um metadado associado ao documento.

Após a tramitação e transcorridos os prazos de guarda, o sistema também deve ter capacidade de identificar aqueles que já cumpriram sua temporalidade para que se implemente a destinação prevista, com possibilidade de alteração, uma vez que documentos originalmente eliminâveis podem ter sua destinação alterada para guarda permanente em razão da identificação de valor secundário.

As determinações sobre a destinação devem ser aplicadas aos documentos de forma sistemática no curso rotineiro das atividades do órgão. Essas mesmas determinações não poderão ser implementadas nos processos em tramitação, nos documentos que estejam com pendências, sob litígio ou investigação.

O sistema de gestão de documentos deve prever as seguintes ações:

- Retenção dos documentos, por determinado período, em arquivo corrente e intermediário do órgão;
- Transferência;
- Recolhimento à unidade de arquivo permanente ou ao Repositório Arquivístico Digital Confiável (RDC-Arq); e
- Eliminação física e eliminação lógica.

b) Transferência

Transferência é a passagem de documentos do arquivo corrente para o arquivo intermediário, para aguardar o cumprimento dos prazos após o qual se farão a seleção e a destinação final.

c) Recolhimento

Recolhimento é a passagem dos documentos do arquivo intermediário para o arquivo permanente, sob a guarda da unidade de arquivo do órgão.

No âmbito do Poder Judiciário, o recolhimento deve ser feito a um Repositório Arquivístico Digital Confiável (RDC-Arq), conforme estabelece o art. 34 da Resolução CNJ nº 324/2020.

Os procedimentos de recolhimento de arquivos digitais para a unidade de arquivo do órgão, que implicam a transposição desses documentos de um GestãoDoc para outro sistema, deverão adotar algumas providências elencadas no e-Arq Brasil(Conarq, 2022a), em relação a:

- compatibilidade de suporte e formato, de acordo com as normas previstas pela instituição arquivística recebedora;
- documentação técnica necessária para interpretar o documento digital (processamento e estrutura dos dados);
- instrumento descritivo que inclua os metadados atribuídos aos documentos digitais e informações que possibilitem a presunção de autenticidade dos documentos recolhidos à instituição arquivística;
- informações sobre as migrações realizadas no órgão produtor.

d) Eliminação

Eliminar significa destruir os documentos que, na avaliação, foram considerados sem valor para a guarda permanente.

A eliminação deve ser precedida da elaboração de listagem de eliminação e da publicação de edital de ciência de eliminação, que visam a garantir o controle e a publicidade acerca da destruição de documentos públicos.

A eliminação deverá sempre ser autorizada pela Comissão Permanente de Avaliação Documental (CPAD), com base na política de gestão documental do órgão.

A eliminação deverá ser realizada de forma a impossibilitar a recuperação posterior de informações contidas nos documentos eliminados. Todas as cópias, inclusive aquelas de segurança e de preservação, independentemente do suporte, deverão ser destruídas.

6.1 Aplicação dos instrumentos de temporalidade e destinação

Estes requisitos referem-se à aplicação da tabela de temporalidade, ou seja, aos procedimentos de controle e verificação dos prazos e da destinação previstos, que devem ser realizados antes de se proceder às ações de destinação propriamente ditas.

REQ	REQUISITO	OBRIG	TIPO
RAD6.1.1	Fornecer recursos integrados à tabela de temporalidade para implementar as ações de destinação.	O	RF
RAD6.1.2	Para cada processo/dossiê ou documento avulso, acompanhar automaticamente os prazos de guarda determinados para a classe, assuntos, movimentos ou documentos a ele relacionados.	O	RF
RAD6.1.3	Prover funcionalidades para informar ao usuário autorizado sobre os documentos ou processos/dossiês que já cumpriram ou estão para cumprir o prazo de guarda previsto.	O	RF
RAD6.1.4	Prover funcionalidades para gerenciar o processo de destinação, que tem de ser iniciado por usuário autorizado e cumprir os seguintes passos: • identificar automaticamente os documentos ou processos/dossiês que atingiram os prazos de guarda previstos; • informar o usuário autorizado sobre todos os documentos ou processos/dossiês que foram identificados no passo anterior, permitindo a geração de relatórios e listas que subsidiam editais de eliminação, exportáveis em formato aberto, que possibilitem publicação; • possibilitar a alteração do prazo ou destinação previstos para aqueles documentos ou processos/dossiês, caso necessário; • proceder à ação de destinação quando confirmada pelo usuário autorizado.	O	RF
RAD6.1.5	Pedir confirmação antes de realizar as ações de destinação.	O	RF
RAD6.1.6	Prever, em determinados casos, dispositivo de aviso antes do início de uma ação de destinação. Por exemplo, emitir aviso ao gestor, caso um documento arquivístico possua restrição de acesso.	D	RF
RAD6.1.7	Restringir as funcionalidades de destinação a usuários autorizados da unidade de gestão documental.	O	RF
RAD6.1.8	Adotar automaticamente a temporalidade e a destinação vigente em nova classe, assunto, movimento ou documento quando reclassificado por usuário autorizado.	O	RF
RAD6.1.9	Impedir a eliminação de documentos/processos/dossiês definidos como de guarda permanente pela política de gestão documental.	O	RF
RAD6.1.10	Adotar o prazo mais abrangente quando um documento/processo/dossiê - não previamente definido pela política de gestão documental como de guarda permanente - for dependente de outro(s) e os prazos de guarda forem diversos. Sendo o caso de referência entre documentos/processos/dossiês, deverá ser observada a temporalidade própria de cada um.	O	RF

6.2 Exportação de documentos

Um GestãoDoc deve ter capacidade de exportar documentos para apoiar as ações de transferência e recolhimento ou ainda para realizar migrações ou enviar cópias para outros locais ou sistemas.

Em alguns casos, os documentos serão eliminados do GestãoDoc após a exportação; em outros, serão mantidos. As ações relacionadas devem ser executadas de maneira controlada, com o registro nos metadados e na trilha de auditoria e verificação dos documentos relacionados.

REQ	REQUISITO	OBRIG	TIPO
RAD6.2.1	Exportar documentos e processos/dossiês digitais e seus metadados para outro sistema, dentro ou fora do órgão. Exemplo: para transferência ou recolhimento ao RDC-Arq	O	RF
RAD6.2.2	Exportar um documento e processo/dossiê ou grupo de documentos e processos/dossiês em uma sequência de operações, de modo que: • O conteúdo, o contexto e a estrutura dos seus documentos não se degradem. • Todos os componentes de um documento digital sejam tratados como uma unidade indissociável. • Todos os metadados do documento sejam relacionados a ele, de forma que os vínculos sejam mantidos no novo sistema. • Todas as ligações entre documentos, volumes e processos/dossiês sejam mantidas.	O	RF
RAD6.2.3	Exportar documentos e processos/dossiês: • Em seu formato nativo ou no formato para o qual foi migrado; • De acordo com os formatos definidos em padrões de interoperabilidade adotados pelo Poder Judiciário.	O	RF
RAD6.2.4	Exportar metadados nos formatos previstos em padrões de interoperabilidade adotados pelo Poder Judiciário.	O	RF
RAD6.2.5	Exportar todos os formatos de documentos que estiver apto a capturar.	D	RF
RAD6.2.6	Produzir um relatório detalhado sobre qualquer falha que ocorra durante uma exportação. O relatório tem que identificar os documentos e processos/dossiês que originaram erros de processamento ou cuja exportação não tenha sido bem-sucedida.	O	RF
RAD6.2.7	Conservar todos os documentos e processos/dossiês digitais que foram exportados, pelo menos até que tenham sido importados no sistema destinatário com êxito.	O	RF
RAD6.2.8	Manter metadados relativos a documentos e processos/dossiês que foram exportados. O gestor deve indicar o subconjunto de metadados que deverá ser mantido.	D	RF
RAD6.2.9	Possibilitar a inclusão de metadados necessários à gestão do arquivo permanente nos documentos e processos/dossiês que serão exportados para recolhimento.	O	RF
RAD6.2.10	Possibilitar a ordenação dos documentos e processos/dossiês digitais a serem exportados de acordo com elementos de metadados selecionados pelo usuário.	D	RF
RAD6.2.11	Quando se exportarem documentos e processos/dossiês híbridos, exigir do usuário autorizado a confirmação de que a parte na forma não digital dos mesmos documentos e processos/dossiês tenha passado pelo procedimento de destinação adequado antes de confirmar a exportação da parte na forma digital.	D	RF

RAD6.2.12	Permitir que documentos sejam exportados mais de uma vez. Exemplo: remessa de processo eletrônico para o Superior Tribunal de Justiça (STJ) e para o Supremo Tribunal Federal (STF).	O	RF

6.3 Eliminação

A eliminação de documentos arquivísticos deve ser realizada de acordo com o previsto nas tabelas de temporalidade das áreas meio e fim e na política de gestão documental do órgão, após a avaliação e seleção dos documentos.

As ações para eliminação de documentos arquivísticos em um GestãoDoc devem ser executadas de forma controlada, fazendo-se registro nos metadados e na trilha de auditoria, com verificação dos documentos relacionados.

Estes requisitos referem-se a funcionalidades que apoiam o responsável pela execução da eliminação dos documentos.

REQ	REQUISITO	OBRIG	TIPO
RAD6.3.1	Restringir a função de eliminação de documentos ou processos/dossiês a usuários autorizados.	O	RF
RAD6.3.2	Impedir a eliminação de um documento ou dossiê/processo ou de qualquer parte de seu conteúdo, a não ser quando estiver de acordo com a tabela de temporalidade. A eliminação será devidamente registrada em trilha de auditoria.	O	RF
RAD6.3.3	Avisar o usuário autorizado quando um documento ou processo/dossiê, em fase de eliminação, for dependente/relacionado a outro. O procedimento deve ser suspenso até que seja tomada uma das medidas abaixo: • produção de um relatório, especificando os documentos ou processos/dossiês envolvidos e todas as ligações com outros processos/dossiês/documentos; e • confirmação pelo usuário autorizado para prosseguir ou cancelar o procedimento.	O	RF
RAD6.3.4	Permitir a eliminação de documentos ou processos/dossiês de forma irreversível a fim de que não possam ser restaurados por meio da utilização normal do GestãoDoc seja por meio de rotinas auxiliares do sistema operacional seja por aplicações especiais de recuperação de dados.	O	RF
RAD6.3.5	Garantir que todas as referências armazenadas de um documento sejam verificadas antes da eliminação de um arquivo digital. Esse requisito deve ser considerado quando um GestãoDoc relacionar um documento digital a mais de um processo ou dossiê, sem a duplicação física do arquivo digital.	O	RF
RAD6.3.6	Produzir relatório detalhado de qualquer falha que ocorra durante uma eliminação. O relatório tem que identificar os documentos cuja eliminação não tenha sido bem sucedida.	O	RF
RAD6.3.7	Quando eliminar documentos e processos/dossiês híbridos, exigir do usuário autorizado a confirmação de que a parte na forma não digital seja também eliminada antes de confirmar a destinação da parte digital.	O	RF

RAD6.3.8	Gerar relatório com os documentos e processos/dossiês: • passíveis de eliminação (edital); • selecionados para guarda permanente pela aplicação do plano amostral e demais critérios de guarda permanente previstos na Política de Gestão Documental do órgão; e • definitivamente eliminados (termo de eliminação).	O	RF
RAD6.3.9	Manter metadados relativos a documentos e processos/dossiês eliminados. O gestor deve indicar o subconjunto de metadados que deverá ser mantido.	O	RF
RAD6.3.10	Controlar editais de eliminação e respectivas listagens, com contagem de prazos e metadados mínimos: • Número de edital; • Data de início e fim do prazo de edital; • Listagem de eliminação;	O	RF

6.4 Avaliação e destinação de documentos arquivísticos não digitais e híbridos

Estes requisitos referem-se a funcionalidades para avaliação, seleção e destinação de documentos não digitais e híbridos.

REQ	REQUISITO	OBRIG	TIPO
RAD6.4.1	Aplicar os mesmos instrumentos de classificação e temporalidade para os documentos e processos/dossiês não digitais, digitais ou híbridos.	O	RF
RAD .4.2	Acompanhar os prazos de guarda dos documentos e processos/dossiês não digitais e dar início aos respectivos procedimentos de eliminação, transferência ou recolhimento, tomando em consideração suas especificidades.	O	RF
RAD6.4.3	Alertar ao usuário autorizado sobre a existência e localização de uma parte não digital associada a um documento ou processo/dossiê híbrido que esteja destinado a ser exportado, transferido, recolhido ou eliminado.	O	RF
RAD6.4.4	Permitir a exportação de metadados de documentos e processos/dossiês não digitais.	O	RF
RAD6.4.5	Permitir ao usuário autorizado selecionar outra destinação final aos documentos e processos/dossiês, diferente daquela originalmente existente na tabela de temporalidade, somente quando a nova destinação for a guarda permanente. Aplica-se exemplificativamente para implementação de plano amostral e decisões da CPAD.	O	RF
RAD6.4.6	Assegurar que as ações de destinação somente possam ser deflagradas sobre processo/dossiê ou sobre documento que esteja definitivamente arquivado.	O	RF

7. PESQUISA, LOCALIZAÇÃO E APRESENTAÇÃO DE DOCUMENTOS

Um GestãoDoc deve contemplar funcionalidades de recuperação e consulta aos documentos arquivísticos. Na recuperação, incluem-se os recursos de pesquisa, localização e apresentação dos documentos.

Todos os recursos de pesquisa, localização e apresentação de documentos devem ser submetidos aos controles de acesso e segurança descritos na seção específica.

7.1 Recuperação de informação

Um GestãoDoc deve disponibilizar interfaces com o usuário que permitam a apresentação, a localização e a pesquisa de documentos. Em geral, essas interfaces são dispostas por telas gráficas com áreas nas quais o usuário insere textos que serão utilizados pelo GestãoDoc na busca de documentos pertinentes.

No procedimento de recuperação da informação, os resultados devem ser validados e filtrados quanto ao nível de acesso (credenciais) atribuído ao usuário.

REQ	REQUISITO	OBRIG	TIPO
RPA7.1.1	Fornecer recursos de pesquisa, localização e apresentação dos documentos.	O	RF
RPA7.1.2	Dispor de interfaces de pesquisa, localização e apresentação acessíveis via ambiente web.	O	RF
RPA7.1.3	Dispor de interfaces de pesquisa e localização acessíveis via aplicativos móveis ou via serviços que não sejam em ambiente web	D	RF
RPA7.1.4	Dispor de navegação gráfica no plano de classificação, proporcionando a visualização das classes e assuntos (e dos movimentos e seus documentos para a área fim), bem como a seleção, recuperação e apresentação direta da documentação e de seu conteúdo por meio desses mecanismos.	O	RF
RPA7.1.5	Limitar a recuperação da informação (em todas as etapas) a usuários com credenciais adequadas, observando-se as restrições de acesso e questões de segurança, especialmente as restrições de sigilo e segredo de justiça.	O	RF

7.2 Pesquisa e localização

A pesquisa é o processo de identificação de documentos por meio de parâmetros definidos pelo usuário com o objetivo de localizar e recuperar esses documentos e seus respectivos metadados.

REQ	REQUISITO	OBRIG	TIPO
RPA7.2.1	Contemplar conjunto flexível de funcionalidades que atuem sobre os metadados relacionados com os diversos níveis de agregação (documento, unidade de arquivamento, classe etc.) e sobre os conteúdos dos documentos institucionais, por meio de parâmetros definidos pelo usuário, com o objetivo de localizar e acessar os documentos e/ou metadados, individualmente ou em grupo.	O	RF
RPA7.2.2	Executar pesquisas de forma integrada, apresentando todos os documentos e processos/dossiês, sejam digitais, híbridos ou não digitais, que satisfaçam os parâmetros da pesquisa.	O	RF
RPA7.2.3	Permitir pesquisa em plataformas integradas nacionalmente, apresentando todos os documentos e processos/dossiês, sejam eles digitais, híbridos ou não digitais que satisfaçam os parâmetros de pesquisa.	D	RF
RPA7.2.4	Permitir que todos os metadados de eventos de gestão de um documento ou processo/dossiê sejam pesquisados e exibidos, de acordo com a política de acesso e sigilo.	O	RF
RPA7.2.5	Permitir que sejam pesquisados os conteúdos dos documentos textuais nato-digitais.	O	RF
RPA7.2.6	Permitir que sejam pesquisados os conteúdos dos documentos digitais, em qualquer forma em que se apresentem (texto, imagem, vídeo etc.)	D	RF
RPA7.2.7	Permitir que sejam pesquisados os conteúdos textuais de documentos digitais (imagem, áudio, vídeo etc.). O documento digital pode sofrer tratamento, como por exemplo por OCR, para possibilitar a pesquisa.	D	RF
RPA7.2.8	Permitir a pesquisa ao conteúdo de documentos digitais não textuais (imagem, áudio, vídeo etc.), por meio de metadados registrados no GestãoDoc.	O	RF
RPA7.2.9	Permitir que um documento ou processo/dossiê seja recuperado por meio de todas as formas de identificação implementadas, incluindo no mínimo: • Identificador; • Número do documento; • Número do processo/dossiê; • Título ou descrição abreviada; • Datas; • Unidade de origem/destino; • Autor/redator/parte/advogado/magistrado/interessado; e • Classificação de acordo com os instrumentos de classificação.	O	RF
RPA7.2.10	Fornecer uma interface que possibilite a pesquisa combinada de metadados e de conteúdo do documento por meio dos operadores booleanos “e”, “ou” e “não”.	D	RF
RPA7.2.11	Permitir que os termos utilizados na pesquisa sejam qualificados, especificando-se um metadado ou o conteúdo do documento como fonte de busca.	O	RF

RPA7.2.12	Permitir o uso de critérios de pesquisa por data, como, por exemplo, “semana anterior”, “a partir de 01/01/2022” ou “antes de 31/12/2022”.	O	RF
RPA7.2.13	Pesquisar foneticamente nos metadados ou conteúdo de documentos por meio de operadores lógicos de proximidade de termos, coringas, truncagem, similaridade, pesquisa semântica etc. Por exemplo, o argumento de pesquisa “Bra*il” pode recuperar “Brasil” e “Brazil”, e o argumento de pesquisa “Arq*” pode recuperar “Arquivo”, “Arquivística”.	D	RF
RPA7.2.14	Permitir a pesquisa por proximidade, isto é, que uma palavra apareça no conteúdo do documento a uma distância máxima de outra.	D	RF
RPA7.2.15	Permitir que os usuários possam armazenar pesquisas para reutilização posterior.	O	RF
RPA7.2.16	Permitir que os usuários possam refinar as pesquisas já realizadas.	O	RF
RPA7.2.17	Permitir a pesquisa dos documentos e processos/dossiês por meio da navegação em tesauro ou vocabulário controlado, quando o órgão utilizar estes instrumentos.	D	RF
RPA7.2.18	Permitir a pesquisa previamente parametrizada, de acordo com o perfil ou necessidade do usuário.	D	RF
RPA7.2.19	Permitir a pesquisa de termos já em desuso, fazendo relação com os termos atualizados, com o apoio de um tesauro ou vocabulário controlado.	D	RF
RPA7.2.20	Permitir que usuários autorizados configurem e alterem os campos padronizados de pesquisa, com a definição dos metadados que poderão ser pesquisados.	D	RF
RPA7.2.21	Permitir a pesquisa e recuperação de uma unidade de arquivamento e exibir a lista de todos os documentos que o compõem.	O	RF
RPA7.2.22	Permitir que o usuário mantenha em área própria (pasta virtual) acervo com documentos (*link*) que queira salvar.	D	RF

7.3 Apresentação: texto, imagem, som e vídeo

A apresentação envolve a disponibilização da informação localizada pela chave indexada, em algum dispositivo de apresentação (tais como monitor de vídeo, impressora, caixa de som etc.) ou serviço de informação (um agente, um robô, um sistema inteligente) para tratamento da informação.

Um GestãoDoc pode conter documentos institucionais com os mais diversos formatos e estruturas e deve ter a capacidade para apresentá-los sem adulterações ao usuário, utilizando-se adequadamente de suportes tecnológicos para texto, imagem, som, vídeo etc., como a exibição na tela do computador, emitindo som, por exemplo.

O sistema deverá informar os programas adicionais e as configurações necessárias para a exibição, por exemplo, *softwares*, aplicativos, *plug-in*, configuração de navegador etc.

REQ	REQUISITO	OBRIG	TIPO
RPA7.3.1	Apresentar o resultado da pesquisa como uma lista de documentos e processos/dossiês digitais, não digitais ou híbridos que cumpram os parâmetros da consulta e informar se o resultado for nulo.	O	RF
RPA7.3.2	Sugerir outros parâmetros aproximados que possam ser satisfeitos quando o resultado de uma pesquisa for nulo. Por exemplo: no caso de uma pesquisa inicial com o parâmetro "*Habes Corpos*", o sistema poderá sugerir por meio de uma mensagem: "Você não quis dizer '*Habeas Corpus*'"?	D	RF
RPA7.3.3	Permitir que os documentos e processos/dossiês apresentados em uma lista de resultados sejam selecionados e, em seguida, abertos.	D	RF
RPA7.3.4	Permitir ao gestor a configuração de pesquisas, possibilitando as seguintes parametrizações: • determinação do número máximo de itens recuperáveis em uma pesquisa; e • definição dos metadados que devem ser exibidos nas listas de resultados de pesquisa.	O	RF
RPA7.3.5	Permitir a configuração do formato da lista de resultados de pesquisa pelo usuário, incluindo as funcionalidades: • seleção da ordem em que os resultados de pesquisa são apresentados; • determinação do número de resultados de pesquisa exibidos na tela de cada vez; e • armazenamento dos resultados de uma pesquisa.	D	RF
RPA7.3.6	Fornecer recursos que permitam a um usuário "navegar" para o nível imediatamente superior ou inferior, como, por exemplo: • de um documento para a unidade de arquivamento em que está incluído; • de uma unidade de arquivamento para os documentos nela incluídos; • de uma unidade de arquivamento para a classe respectiva; e • de uma classe para as unidades de arquivamento a ela relacionadas.	D	RF
RPA7.3.7	Apresentar o conteúdo de todos os documentos capturados, preservando as características e os formatos.	O	RF
RPA7.3.8	No caso de necessidade de apresentação de documentos em formato de arquivo não previstos na política de gestão documental, deve-se permitir o *download* do documento para que possa ser visualizado em outro ambiente, quando legalmente permitido.	O	RF
RPA7.3.9	Reproduzir (copiar) os documentos capturados, preservando o formato produzido pelas aplicações geradoras.	O	RF
RPA7.3.10	Permitir que os metadados e/ou documentos de um processo/dossiê sejam impressos ou baixados para o dispositivo do usuário.	O	RF
RPA7.3.11	Permitir a exportação da lista dos documentos e dossiês/processos resultantes de uma pesquisa.	O	RF
RPA7.3.12	Apresentar em outros formatos padronizados, além daquele nativo, documentos destinados à publicação digital.	O	RF
RPA7.3.13	Realizar pesquisa e exibição de documentos e processos/dossiês simultaneamente para diversos usuários.	O	RF
RPA7.3.14	Proporcionar ao usuário formas de visualização e impressão de documentos com seus metadados e possibilitar a definição dos metadados a serem visualizados ou impressos.	O	RF
RPA7.3.15	Permitir que o usuário defina quais metadados serão exibidos nas listas de documentos.	D	RF
RPA7.3.16	Apresentar os documentos arquivísticos em formatos alternativos, tais como .XML, .HTML ou outros.	D	RF

8. SEGURANÇA: CONTROLE DE ACESSOS E AUDITORIA

O sistema de gestão de documentos deve prever controles de acesso e procedimentos de segurança que garantam a confidencialidade, a integridade, a disponibilidade e a autenticidade dos documentos. Dentre esses procedimentos, pode-se destacar a utilização de controles técnicos e programáticos, diferenciando tipos de documentos, perfis de usuários e características de acesso aos dados, manutenção de trilhas de auditoria, rotinas de cópias de segurança, políticas, procedimentos e instrumentos instituídos pela Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ), instituída pela Resolução CNJ nº 396/2021.

Problemas de segurança não são resolvidos apenas com tecnologia, já que envolvem características do comportamento humano.

Nesse sentido, o GestãoDoc deve ser projetado, desenvolvido e mantido em consonância com uma Política de Segurança de Informação e de acordo com a Estratégia Nacional referida acima.

Além disso, também devem ser consideradas exigências e procedimentos de segurança da infraestrutura das instalações.

a) Controle de acesso

Um GestãoDoc deve limitar ou autorizar o acesso a documentos, por usuário e/ou papéis. Nessa acepção, papéis representam conjuntos de usuários com mesmos perfis de atividade do ponto de vista do GestãoDoc, tendo os mesmos direitos de acesso.

O controle de acesso deve garantir, no mínimo, as seguintes funções:

- Restrição de acesso aos documentos.
- Exibição dos documentos, criptografados ou não, e dos metadados somente aos usuários autorizados.
- Uso e intervenção nos documentos somente pelos usuários autorizados.

A confidencialidade atribuída aos documentos: ostensivos, reservados, sigilosos etc. influencia na especificação das funções referidas conforme os perfis de usuários. Regras, normas e legislação estabelecem diferentes razões para o sigilo e diferentes graus a serem atribuídos a cada documento e as autoridades competentes para fazê-lo. (Ver Capítulo 4, Captura — Atribuição de restrição de acesso), destacando-se a Lei nº 12.527/2011 (Lei de Acesso à Informação) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais).

Um GestãoDoc deve garantir que apenas usuários autorizados tenham acesso à informação sigilosa. O acesso aos metadados dos documentos sigilosos deve ser estabelecido com base nas diretrizes para o tratamento de processos e investigações sigilosas ou que tramitam em segredo de justiça, no que diz respeito à autuação, processamento, transporte, inserção de dados no sistema eletrônico de informações processuais, consulta e arquivamento, conforme estabelecido nos atos normativos dos órgãos do Poder Judiciário.

O monitoramento e mapeamento das permissões de acesso são um processo contínuo em todos os sistemas de gestão de documentos.

No que diz respeito ao controle de acesso, essa especificação contempla três tipos de requisitos:

- Controle de acesso baseado em papéis de usuário.
- Controle de acesso por grupos.
- Classificação quanto ao grau de sigilo.

Os três tipos de controle de acesso podem ser combinados e os requisitos de administração de controle de acesso devem ser adaptados a cada um dos tipos referidos anteriormente ou a combinação deles, de acordo com as normas institucionais.

b) Acesso e rastreamento

O acesso aos documentos pelo usuário deve ser registrado e sua gestão inclui:

- Identificação da permissão de acesso dos usuários, isto é, o que ele pode acessar.
- Identificação dos níveis de segurança e da categoria de sigilo dos documentos.
- Garantia de que somente os indivíduos autorizados tenham acesso aos originalmente sigilosos ou aos posteriormente classificados.
- Registro de todos os acessos, tentativas de acesso e usos dos documentos (visualização, impressão, transmissão e cópia para a área de transferência) com identificação de usuário, data, hora e, se possível, a estação de trabalho.
- Revisão periódica das classificações de acesso a fim de garantir sua atualização.

O rastreamento dos documentos em trilhas de auditoria é uma medida de segurança que tem por objetivo verificar a ocorrência de acesso aos documentos e seu uso indevido. O grau de controle de acesso e o detalhamento do registro na trilha de auditoria dependem da natureza do órgão, dos documentos produzidos e deverá refletir o nível de preocupação da Política de Segurança da informação dos órgãos do Poder Judiciário.

c) Trilha de auditoria sobre intervenções no documento e no GestãoDoc

A trilha de auditoria é o conjunto de informações registradas, que permite o rastreamento de intervenções ou tentativas de intervenções feitas no documento institucional digital ou no GestãoDoc.

A trilha de auditoria deve registrar o movimento e a utilização dos documentos institucionais dentro de um GestãoDoc (captura, produção, registro, classificação, indexação, arquivamento, armazenamento, recuperação da informação, acesso e utilização, preservação e destinação), informando quem operou, a data, a hora e as ações tomadas. A trilha de auditoria tem o objetivo de fornecer informações sobre o cumprimento das políticas e regras da gestão de documentos das instituições do Judiciário e serve para:

- Identificar os autores de cada operação sofrida pelos documentos.
- Prevenir a perda de documentos.
- Monitorar todas as operações realizadas no GestãoDoc.
- Garantir a segurança e a integridade do GestãoDoc.

No caso de procedimentos que tenham prazos a serem cumpridos pelos órgãos do Judiciário, devem-se implementar ações de rastreamento de forma a:

- Determinar os passos a serem dados em resposta às atividades ou ações registradas em um documento.
- Atribuir responsabilidade por uma ação a uma pessoa.

8.1 Controle de acesso

Esta seção trata dos requisitos de identificação e autenticação de usuários, controle de acesso baseado em papéis de usuários, bem como dos requisitos comuns a qualquer tipo de controle de acesso.

Os requisitos a seguir tratam do mapeamento da identidade do usuário e das permissões concedidas a ele, imediatamente após sua autenticação.

Usuários acessam informações e funcionalidades por meio da interface do programa. A associação entre identidade do usuário e as autorizações de acesso é feita durante a fase de identificação e autenticação do usuário por meio da interface do programa, com base nas credenciais de autenticação.

REQ	REQUISITO	OBRIG	TIPO
RSC8.1.1	Implementar o controle de acesso, mantendo pelo menos os seguintes atributos dos usuários, de acordo com a política de segurança da informação dos órgãos do Poder Judiciário: • identificador do usuário; • autorizações de acesso; e • credenciais de autenticação.	O	RF
RSC8.1.2	Utilizar, para efeito de autenticação, um sistema de gerenciamento de identidade externo utilizado pela Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br) ou pelo próprio órgão.	O	RF
RSC8.1.3	Exigir que o usuário esteja devidamente identificado e autenticado antes que este inicie qualquer operação no sistema.	O	RF
RSC8.1.4	Garantir que as credenciais de autenticação sejam alteradas em conformidade com a política de segurança do órgão do Poder Judiciário.	O	RF
RSC8.1.5	Permitir avaliação periódica dos direitos de acesso dos usuários do sistema.	O	RF

8.2 Aspectos gerais de controle de acesso

Os requisitos desta seção são aplicáveis independentemente do modelo de controle de acesso adotado, de acordo com a política de segurança da informação.

REQ	REQUISITO	OBRIG	TIPO
RSC8.2.1	Permitir o acesso às funções administrativas do sistema somente a usuários autorizados pelo gestor do sistema.	O	RF
RSC8.2.2	Garantir que a pesquisa feita por metadados diversos do número de documento/processo/dossiê somente retorne resultado positivo em caso de grau de sigilo acessível ao usuário.	O	RF
RSC8.2.3	Garantir que, na consulta feita exclusivamente por número de documento/processo/dossiê cujo grau de sigilo seja maior que o do usuário, resulte apenas a existência do documento/processo/dossiê e a informação de restrição de acesso, sem qualquer outro metadado.	O	RF
RSC8.2.4	Garantir que somente o gestor do GestãoDoc seja capaz de criar, alterar, remover ou revogar as permissões associadas a perfis de usuários, grupos de usuários ou usuários individuais.	O	RF
RSC8.2.5	Implementar imediatamente alterações ou revogações dos atributos de segurança de usuários e de documentos digitais.	O	RF
RSC8.2.6	Oferecer ferramentas de aumento de produtividade ao gestor do GestãoDoc, tais como a realização de operações sobre lotes ou grupos de usuários e lotes de documentos digitais, agenda de tarefas, análises de trilhas e geração de alarmes.	O	RF
RSC8.2.7	Controlar o acesso por grupos de usuários, papéis de usuários e usuários individuais, obedecendo a uma hierarquia de permissões preestabelecida na política de segurança da informação dos órgãos do Poder Judiciário.	O	RF

a) Controle de acesso por grupos de usuários

Grupos são conjuntos de usuários (possivelmente com papéis diferentes) reunidos para a realização de alguma atividade em comum.

Estes requisitos só são aplicáveis aos órgãos em que há controle de acesso por grupos de usuários

REQ	REQUISITO	OBRIG	TIPO
RSC8.2.8	Aplicar a política de controle de acesso a documentos por grupos de usuários considerando: • a identidade do usuário e sua participação em grupos; e • os atributos de segurança, associados ao documento arquivístico digital, às classes e/ou aos dossiês/processos.	O	RF
RSC8.2.9	Conceder o acesso a documentos, a dossiês/processos ou classes, se a permissão requerida para a operação estiver associada a pelo menos um dos grupos aos quais pertença o usuário.	O	RF
RSC8.2.10	Permitir que um usuário pertença a mais de um grupo.	O	RF
RSC8.2.11	Permitir que alguns usuários habilitados estipulem que outros usuários ou grupos de usuários possam ter acesso aos documentos sob sua responsabilidade. Essa permissão deve ser atribuída pelo gestor do GestãoDoc, de acordo com a política de segurança do órgão.	O	RF

c) Controle de acesso por papéis de usuários

O controle de acesso é um "conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais" (BRASIL, 2021), requerendo para isso procedimentos de autenticação.

O usuário é habilitado a utilizar um GestãoDoc no devido procedimento de credenciamento, momento no qual lhe é atribuído o conjunto de operações do que pode realizar sobre um determinado documento/processo/dossiê (perfil de acesso).

O controle de acesso baseado em papéis é uma abordagem que define os direitos e permissões de um usuário baseado no papel que ele desempenha na organização, simplificando o gerenciamento das permissões dadas aos usuários (BRASIL, 2021). Dessa forma, por exemplo, um magistrado, ao ser credenciado em um GestãoDoc, já recebe um conjunto de perfis de acesso condizentes com o papel que desempenha na organização.

REQ	REQUISITO	OBRIG	TIPO
RSC8.2.12	Utilizar os seguintes atributos do usuário ao implementar a política de controle de acesso por papéis de usuários sobre documentos: • identificação do usuário; e • papéis associados ao usuário.	O	RF
RSC8.2.13	Utilizar os seguintes atributos dos documentos ao implementar a política de controle de acesso por papéis: • identificação do documento; e • operações permitidas para os vários perfis de usuários, sobre as unidades a que pertence o documento.	O	RF
RSC8.2.14	Conceder acesso a documentos, processos/dossiês somente se a permissão requerida para a operação estiver presente em pelo menos um dos perfis associados ao usuário.	O	RF
RSC8.2.15	Impedir que um usuário assuma papéis com direitos conflitantes.	O	RF
RSC8.2.16	Permitir a criação de hierarquias de papéis e o conceito de herança de permissões entre eles.	O	RF
RSC8.2.17	Permitir ao gestor a definição do limite de tentativas de acesso. Quando esse valor for atingido, o acesso deve ser bloqueado.	O	RF
RSC8.2.18	Permitir que o gestor, de maneira controlada, recupere, identifique, visualize e reconfigure os parâmetros do sistema e os atributos dos perfis dos usuários.	O	RF

8.3 Classificação da informação quanto ao grau de sigilo e restrição de acesso

Os requisitos descritos nesta seção dizem respeito ao acesso a processos/dossiês e documentos, com base na classificação do grau de sigilo e em restrições a dados pessoais e/ou dados pessoais sensíveis.

As hipóteses de segredo, sigilo e restrição de acesso constam, entre outros diplomas legais, no Código de Processo Civil, na Lei nº 12.527/2011 (Lei de Acesso à Informação) e na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais).

A matéria é também disciplinada pelas Resoluções CNJ nºs 121/2010, 185/2013, 215/2015, 363/2021 e 408/2021, entre outras.

REQ	REQUISITO	OBRIG	TIPO
RSC8.3.1	Implementar a classificação de grau de sigilo, de perfis e demais caracterizações de restrição de acesso de documentos, dossiês/processos, movimentos e dos planos de classificação, e de todas as operações de usuários nos documentos	O	RF
RSC8.3.2	Implementar restrições legais de acesso, baseando-se nos seguintes atributos de segurança: • tipo de restrição legal de acesso; • credencial de segurança do usuário; e • os tipos de restrição previstas em legislação própria, determinação judicial ou administrativa.	O	RF
RSC8.3.3	Tratar a classificação de grau de sigilo baseando-se nos seguintes atributos de segurança: • grau de sigilo do documento; • perfil do usuário; • identificação da autoridade classificadora; O grau de sigilo tem que estar associado à credencial de segurança.	O	RF
RSC8.3.4	Permitir a formalização da decisão de classificação da informação em qualquer grau de sigilo, conforme legislação vigente.	O	RF
RSC8.3.5	Recusar o acesso de usuários a processos/dossiês e documentos que possuam um grau de sigilo superior à sua credencial de segurança.	O	RF
RSC8.3.6	Garantir que os processos/dossiês e documentos sem atribuição de grau de sigilo ou identificação de outras restrições de acesso, provenientes de fontes externas ao sistema, estejam sujeitos às políticas de controle de acesso e de sigilo.	O	RF
RSC8.3.7	Manter a marcação de sigilo original durante a importação de processos/dossiês e documentos marcados com graus de sigilo, a partir de fontes externas ao GestãoDoc.	O	RF
RSC8.3.8	Garantir que o grau de sigilo de um documento importado esteja associado a um usuário autorizado com a credencial de segurança pertinente para receber o documento.	O	RF
RSC8.3.9	Garantir a não ambiguidade na associação entre as marcações de grau de sigilo e os outros atributos de segurança (permissões) dos processos/dossiês e documentos importados.	O	RF
RSC8.3.10	Garantir que nos casos em que grau de sigilo e atributos de segurança incidam sobre um mesmo processo/dossiê e documento, o critério de acesso seja o de maior restrição.	O	RF

RSC8.3.11	Permitir que um dos itens abaixo seja selecionado durante a configuração: • graus de sigilo e restrições de acesso a serem atribuídos a classes e dossiês/processos e documentos; e • classes, dossiês/processos e documentos sem grau de sigilo ou outras restrições de acesso.	O	RF
RSC8.3.12	Possibilitar correção ou reavaliação de grau de sigilo ou outra restrição de acesso de todos os documentos arquivísticos de um dossiê/processo ou de uma classe em uma única operação. A informação quanto à desclassificação, reclassificação, redução do prazo de sigilo ou alteração de restrição de acesso deverá ser justificada conforme legislação em vigor.	O	RF
RSC8.3.13	Permitir que somente usuários autorizados sejam capazes de realizar as seguintes ações: • remover ou revogar os atributos de segurança dos documentos; e • criar, alterar, remover ou revogar as credenciais de segurança dos usuários.	O	RF
RSC8.3.14	Permitir somente ao gestor alterar a configuração dos valores predefinidos (padrão) para os atributos de segurança e marcações de graus de sigilo, quando necessário e apropriado.	O	RF
RSC8.3.15	Impedir que um documento sigiloso seja eliminado, antes de se tornar ostensivo e ser submetido ao processo de avaliação para definição de sua destinação final, salvo as exceções legais.	O	RF
RSC8.3.16	Implementar metadados nos níveis de processo/dossiê, documento ou cópia truncada de documento para controlar o acesso à informação com restrição de acesso.	O	RF

8.4 Alteração, ocultação e exclusão de documentos institucionais

As operações efetuadas com documentos arquivísticos não devem, em regra, ser canceladas e os documentos produzidos ou capturados em um GestãoDoc não devem ser eliminados, exceto nas hipóteses de seleção com essa destinação, ao término do ciclo de vida.

No entanto, os gestores podem necessitar efetuar cancelamento de ações de inclusão, alteração, ocultação e exclusão de documentos quando hajam sido indevidamente efetuadas, como nas hipóteses de inclusão em processos ou dossiês incorretos, equívocos de processamento que demandem retificação ou para cumprir requisitos jurídicos relacionados a sigilo e proteção de dados.

A ação de eliminar pode ter um dos seguintes significados: **eliminação definitiva** ou **retenção**, acompanhada de anotação nos metadados arquivísticos, informando que não mais está sob o controle da gestão de documentos arquivísticos.

Conforme explicitado no e-Arq Brasil (Conarq, 2022a):

> *A capacidade de apagar documentos deve ser, rigorosamente, controlada para proteger a integridade dos documentos arquivísticos. Todas as informações referentes a essa ação têm que ser registradas na trilha de auditoria e elementos indicativos da existência dos documentos arquivísticos apagados devem permanecer nos dossiês afetados.*

Caso haja necessidade de publicação ou disponibilização de documentos arquivísticos que possuam informações parcialmente sigilosas ou com restrição de acesso, aos gestores deve ser dada a possibilidade de ocultar a informação que não pode ser divulgada ou acessada, sem afetar o documento arquivístico correspondente. Nesse caso, o GestãoDoc armazenará o documento original e a cópia truncada ou anonimizada.

REQ	REQUISITO	OBRIG	TIPO
RAD8.4.1	Permitir o cancelamento da operação em caso de erro do usuário, de acordo com as normas vigentes. Esse cancelamento deve ser registrado nos metadados.	O	RF
RAD8.4.2	Impedir a exclusão (permanente ou lógica) de documentos ou lotes de documentos fora do processo regular de eliminação. O processo regular de eliminação é aquele previsto na política de gestão documental do órgão e acompanhado pela unidade de Gestão Documental e/ou Comissão Permanente de Avaliação Documental (CPAD).	O	RF
RAD8.4.3	Em situações excepcionais, permitir ao gestor autorizado apagar ou corrigir dossiês/processos, volumes e documentos. Nesse caso, um GestãoDoc deve: • registrar integralmente a ação de apagar ou corrigir na trilha de auditoria; • produzir um relatório de anomalias para o gestor do GestãoDoc; • eliminar todo o conteúdo de um dossiê/processo ou volume, quando houver esse procedimento; • garantir que nenhum documento seja eliminado se tal ação resultar na alteração de outro documento arquivístico; • informar o gestor do GestãoDoc sobre a existência de ligação entre um dossiê/processo ou documento prestes a ser apagado e qualquer outro dossiê/processo ou documento, solicitando confirmação antes de concluir a operação; • manter a integridade total do metadado, a qualquer momento.	O	RF
RAD8.4.4	Permitir aos usuários autorizados a retificação dos metadados com motivação em campo específico, com registro também na trilha de auditoria.	O	RF
RAD8.4.5	Permitir a um usuário autorizado fazer uma cópia truncada (anonimizada) de um documento, com o objetivo de não alterar o original. Se o GestãoDoc não fornecer, diretamente, esses recursos, deve permitir que outros pacotes de software os proporcionem.	O	RF

RAD8.4.6	Possibilitar que o usuário, ao elaborar cópia truncada, oculte informação sigilosa contida no documento original, por meio de: • retirada de páginas de um documento; • ocultação de nomes ou palavras sensíveis por meio da adição de retângulos opacos ou recursos semelhantes; • quaisquer outros recursos necessários para formatos de imagem, vídeo ou áudio, caso disponíveis. É essencial que, quando os recursos para truncar documentos forem empregados, nenhuma informação retirada ou ocultada seja passível de visualização na cópia truncada, na tela, nem quando impressa ou reproduzida por meios audiovisuais, independentemente da utilização de quaisquer recursos, tais como rotação, variação focal ou qualquer outra manipulação. A cópia truncada poderá ter graus de sigilo distintos..	O	RF
RAD8.4.7	Quando uma cópia truncada é produzida, um GestãoDoc deve registrar essa ação nos metadados do documento e da cópia truncada, incluindo, pelo menos, data, hora, motivo e quem a produziu.	O	RF
RAD8.4.8	Manter referência cruzada à(s) cópia(s) truncada(s) nos mesmos dossiês/processos e documentos em que se encontra o documento original.	O	RF
RAD8.4.9	Armazenar, na trilha de auditoria, qualquer alteração efetuada para satisfazer os requisitos desta seção.	O	RF

8.5 Trilha de auditoria

A trilha de auditoria consiste em um histórico de todas as intervenções, ou tentativas de intervenções, feitas no documento e no próprio GestãoDoc. Nesse sentido, é também um metadado sobre os documentos arquivísticos digitais, informando sobre sua autenticidade.

REQ	REQUISITO	OBRIG	TIPO
RTA8.5.1	Permitir que as informações da trilha de auditoria estejam disponíveis para inspeção a fim de que uma ocorrência específica possa ser identificada e que todas as respectivas informações sejam claras e compreensíveis.	O	RF
RTA8.5.2	Registrar, na trilha de auditoria, informações acerca das ações a seguir: • data e hora da captura de todos os documentos; • responsável pela captura; • reclassificação, desclassificação ou redução do grau de sigilo de um documento ou dossiê/processo, com a classificação inicial e final; • qualquer alteração na tabela de temporalidade e destinação de documentos; • qualquer ação de reavaliação de documentos; • qualquer alteração nos metadados associados a classes, dossiês/processos ou documentos; • data e hora de produção, aditamento e eliminação de metadados; • ações de exportação e importação envolvendo os documentos; • usuário, data e hora de acesso ou tentativa de acesso a documentos e ao GestãoDoc; • tentativas de acesso negado a qualquer documento; • ações de eliminação de qualquer documento e seus metadados; • tentativas de exportação (inclusive para backup) e importação (inclusive *restore*); • alterações efetuadas nas permissões de acesso que afetem um dossiê/processo, documento ou usuário; • infrações cometidas contra mecanismos de controle de acesso; • todas as ações administrativas sobre os atributos de segurança (papéis, grupos, permissões etc.); • todas as ações administrativas sobre dados de usuários (cadastro, ativação, bloqueio, atualização de dados e permissões, troca de senha etc.); e • todos os eventos de administração e manutenção das trilhas de auditoria (alarmes, cópias, configuração de parâmetros etc.).	O	RF
RTA8.5.3	Registrar, em cada evento auditado, informações sobre a identidade do usuário, respeitando a política de privacidade do órgão e a legislação vigente.	O	RF
RTA8.5.4	Permitir apenas aos usuários autorizados a leitura das trilhas de auditoria.	O	RF
RTA8.5.5	Possuir mecanismos para realização de buscas nos eventos das trilhas de auditoria. Para facilitar a visualização do relatório, os resultados podem ser apresentados de modo ordenado, mas essa ordenação não pode alterar os dados incluídos na trilha.	O	RF
RTA8.5.6	Impedir qualquer modificação de conteúdo da trilha de auditoria.	O	RF
RTA8.5.7	Quando o espaço de armazenamento da trilha de auditoria atingir o limite preestabelecido, um GestãoDoc deve permitir somente operações auditáveis originadas por administradores. Todas as outras operações estarão bloqueadas até a liberação pelo administrador.	D	RF

RTA8.5.8	Aplicar um conjunto de regras na monitoração de eventos auditados e, com base nessas regras, indicar a possível violação da segurança, como, por exemplo: • acumulação de um número predeterminado de tentativas consecutivas de *login* com erro (autenticação malsucedida), conforme especificado pela política de segurança do órgão; • ocorrência de vários *logins* simultâneos do mesmo usuário em locais (computadores) diferentes; e • *login* do usuário fora do horário autorizado após *logoff* no período normal.	O	RF
RTA8.5.9	Fornecer relatórios, em ordem cronológica, sobre as ações que afetam processos/dossiês, documentos e operações realizadas no sistema.	O	RF
RTA8.5.10	Garantir que somente gestores autorizados sejam capazes de configurar o conjunto de eventos auditáveis e seus atributos.	O	RF
RTA.5.11	Após a exclusão das trilhas de auditoria dos registros correntes do banco de dados do GestãoDoc, arquivá-las como documento arquivístico.	O	RF

PARTE III

REQUISITOS NÃO FUNCIONAIS

9. ARMAZENAMENTO

As decisões e as ações relativas ao armazenamento dos documentos institucionais não digitais e digitais permeiam todo o seu ciclo de vida, devendo ser aptas a garantir a sua integridade e o acesso a eles. Assim sendo, documentos, independentemente do suporte, requerem armazenamento criterioso desde o momento de sua criação para garantir sua preservação de longo prazo.

Em cenário híbrido, quando envolvidos documentos não digitais e digitais, devem ser observados requisitos de armazenamento que atendam igualmente às necessidades de ambos os suportes.

As condições de armazenamento devem:

- considerar o volume, o gênero documental e as propriedades físicas dos documentos;
- ser projetadas para a proteção contra acessos não autorizados e perdas por destruição, furto e sinistro.

No caso dos documentos digitais, os órgãos do Poder Judiciário devem dispor de políticas e diretrizes de preservação digital e empregar técnicas de preservação, descritas na próxima seção.

Fatores a serem considerados na escolha das opções de armazenamento estão indicados no e-Arq Brasil (Conarq, 2022a):

- *volume e estimativa de crescimento dos documentos: este fator deve ser levado em conta para se avaliar a capacidade de armazenamento, isto é, as áreas de depósito, os tipos e a quantidade de estantes e, para os documentos digitais, a capacidade dos dispositivos de armazenamento;*

- *segurança dos documentos: as instalações de armazenamento (depósitos, arquivos, computadores) deverão prever a limitação de acesso aos documentos, como, por exemplo, o controle das áreas de armazenamento e sistemas de detecção de entrada não autorizada. O depósito deve estar localizado em área que não seja de risco. No caso de documentos digitais, devem ser previstos procedimentos que previnam a perda de documentos por falha do SIGAD (...);*

- *características físicas do suporte e do ambiente: fatores como tipo de suporte, peso, grau de contaminação do documento e do ambiente, temperatura e umidade influenciam a adequação das condições de armazenamento. Nesse sentido, devem ser adotados procedimentos – como controle e verificação do tempo de vida útil e da estabilidade dos suportes – para prevenir danos aos documentos. É importante que os meios de acondicionamento sejam robustos e adequados ao formato e à quantidade de documentos. As áreas de depósito devem ter amplitude adequada, estabilidade de temperatura e de níveis de umidade, proteção contra sinistro, contaminação (isótopos radioativos, toxinas, mofo) e infestação de insetos ou micro-organismos. Os documentos digitais devem passar, periodicamente, pela troca de suporte, isto é, as informações contidas num suporte devem ser transferidas para outro. Essa técnica é denominada atualização (refreshing).*

- *frequência de uso: o uso mais ou menos frequente dos documentos deve ser levado em conta na seleção das opções de armazenamento. No caso dos documentos não digitais, as opções envolvem acondicionamento (pastas suspensas, caixas) e localização dos depósitos (próximos ou distantes da área de trabalho). Já em relação aos documentos digitais, as opções podem envolver armazenamento on-line (acesso imediato) ou off-line, nas chamadas "mídias removíveis" de armazenamento (disco óptico, fita magnética), em diferentes graus de disponibilidade e velocidade.*

- *custo relativo das opções de armazenamento dos documentos: além do custo dos dispositivos de armazenamento, devem ser considerados, para sua manipulação, os valores dos equipamentos e do software de controle.*

Para mais informações sobre conservação preventiva, consultem-se o Manual de Gestão Documental e o Manual de Gestão de Memória.

Os documentos digitais são armazenados em dispositivos de armazenamento eletrônicos (ou de estado sólido), magnéticos ou ópticos.

Do ponto de vista tecnológico, distinguem-se três tipos de memória: primária, secundária e terciária, cujas principais características são custo, capacidade e tempo de acesso.

As memórias secundária e terciária são adequadas para armazenamento.

O armazenamento secundário e terciário poderá ser contratado por provedores de serviços de infraestrutura *in loco* e em nuvem, observadas as políticas e definições estabelecidas pelo Conselho Nacional de Justiça e pelos órgãos do Poder Judiciário para a contratação de soluções de tecnologia da informação e comunicação, observadas a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) e a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), instituídas pelas Resoluções CNJ nºs 370/2021 e 396/2021.

Os equipamentos devem adequar-se às características das operações — *on-line* ou *off-line*. Operações *on-line* só podem ser realizadas por meio de GestãoDoc, ao passo que operações *off-line* podem ser realizadas em outros sistemas computacionais, desvinculadas do funcionamento do GestãoDoc.

Seja qual for a tecnologia empregada, um GestãoDoc deve garantir a integridade dos documentos institucionais.

Os itens seguintes enumeram requisitos de armazenamento organizados segundo os critérios de durabilidade, capacidade e viabilidade técnica.

9.1 Durabilidade

Os dispositivos de armazenamento de um GestãoDoc e os documentos nele armazenados devem estar sujeitos a ações de preservação que garantam sua conservação de longo prazo

REQ	REQUISITO	OBRIG	TIPO
RAR9.1.1	Utilizar dispositivos de armazenamento e padrões abertos, maduros, estáveis no mercado e de fornecedores consolidados, amplamente disponíveis.	O	RNF-O
RAR9.1.2	Avaliar periodicamente a escolha de dispositivos sempre que a evolução tecnológica indicar mudanças importantes.	O	RNF-O
RAR9.1.3	Efetuar migrações preventivas sempre que se tornar patente ou previsível a obsolescência do padrão corrente.	O	RNF-O
RAR9.1.4	Manter o registro de MTBF (*Mean Time Between Failures*)[1], MTTR (*Mean Time To Repair*)[2] e MTBSI (*Mean Time Between Service Incidents*)[3] para as memórias secundárias, bem como as datas de sua aquisição.	O	RNF-O
RAR9.1.5	Realizar o gerenciamento das mídias por meio do registro de durabilidade prevista, data de aquisição e histórico de utilização das memórias secundária e terciária. Informações técnicas sobre previsibilidade de duração de mídias referidas em RAR 9.1.4 devem ser obtidas preferencialmente a partir de órgãos independentes. Quando isso não for possível, podem ser utilizadas informações de fornecedores. A origem da informação deve ficar registrada em ambos os casos.	O	RNF-O
RAR9.1.6	Manter estatísticas da durabilidade efetivamente observadas das memórias secundária e terciária.	O	RNF-O
RAR9.1.7	Utilizar preferencialmente as redes de dados para o acesso às informações armazenadas em memória terciária. O objetivo é minimizar o acesso físico às mídias, visando à diminuição do desgaste. A manipulação direta das mídias deverá ser realizada preferencialmente por meio de sistemas automáticos de manipulação de mídias.	O	RNF-O
RAR9.1.8	Prever que as memórias de suporte sejam devidamente "sanitizadas", isto é, tenham suas informações efetivamente indisponibilizadas, quando se proceder à eliminação de documentos. A eliminação de um documento não implica a eliminação de seus metadados. Esse requisito aplica-se principalmente às memórias secundária e terciária, pela sua característica não volátil. As informações devem ser eliminadas de forma irreversível, incluindo, no caso de memória terciária, a possibilidade de destruição física das mídias.	O	RNF-O

1. *Mean Time Between Failures* (MTBF): tempo médio entre falhas. É um valor relativo ao período médio entre falhas de um sistema ou dispositivo e que permite a avaliação de sua confiabilidade ou vida útil.
2. *Mean Time To Repair* (MTTR): tempo médio de recuperação. É um valor relativo ao período médio para colocar um componente ou sistema defeituoso em funcionamento novamente.
3. *Mean Time Between Service Incidents* (MTBSI): é o tempo médio entre falhas. MTBSI = MTBF+MTTR.

9.2 Efetividade de armazenamento

Um GestãoDoc deve oferecer garantia de que o documento está sendo arquivado de forma segura e íntegra no sistema de armazenamento.

REQ	REQUISITO	OBRIG	TIPO
RAR9.2.1	Prever que os dispositivos de armazenamento suportem métodos de detecção de erros para leitura e escrita de dados e prover mecanismos automáticos de aviso ao administrador do sistema.	O	RNF-O
RAR9.2.2	Utilizar técnicas de restauração de dados em caso de falhas.	O	RNF-O
RAR9.2.3	Utilizar mecanismos de proteção que previnam alterações indevidas e mantenham a integridade dos dados armazenados.	O	RNF-O
RAR9.2.4	Prever a utilização de técnicas para garantir maior confiabilidade e desempenho. As técnicas recomendadas incluem redundância, paralelismo, espelhamento (*mirroring*) e participação de dados (*data stripping*).	O	RNF-O
RAR9.2.5	Verificar periodicamente a integridade dos dispositivos de armazenamento.	O	RNF-O
RAR9.2.6	Permitir o armazenamento dos documentos sigilosos em meios físicos ou lógicos distintos dos documentos não sigilosos.	D	RNF-O

9.3 Capacidade

Um GestãoDoc deve garantir a escalabilidade no armazenamento, permitindo a expansão ilimitada de seus dispositivos.

REQ	REQUISITO	OBRIG	TIPO
RAR9.3.1	Possuir capacidade de armazenamento suficiente para a acomodação de todos os documentos, metadados e suas cópias de segurança.	O	RNF-O
RAR9.3.2	Prever a possibilidade de expansão da estrutura de armazenamento. A quantidade de memória primária deve ser dimensionada adequadamente no momento da aquisição a fim de minimizar as indisponibilidades do GestãoDoc nas situações de expansão desse tipo de memória. Quando da aquisição de memória secundária e terciária, as possibilidades de expansão dos equipamentos de controle devem ser consideradas.	O	RNF-O
RAR9.3.3	Permitir ao administrador a configuração dos limites de capacidade de armazenamento dos diversos dispositivos.	O	RNF-O
RAR9.3.4	Oferecer ao administrador facilidades para a monitoração da capacidade de armazenamento. Esse controle indica, por exemplo, capacidade utilizada, capacidade disponível e taxa de ocupação. Tais informações são úteis para subsidiar ações de expansão em tempo hábil.	O	RNF-O
RAR9.3.5	Informar automaticamente ao administrador quando os dispositivos de armazenamento *on-line* atingirem níveis de alerta e níveis críticos de ocupação.	O	RNF-O
RAR9.3.6	Manter estatísticas de taxa de crescimento de utilização de memória secundária e terciária para fornecer ao administrador previsões de exaustão de recursos. Esse tipo de estimativa possibilita ao administrador antecipar ações de expansão antes que a utilização atinja níveis críticos.	O	RNF-O
RAR9.3.7	Permitir a definição de outras estatísticas referentes à capacidade de armazenamento de acordo com as necessidades do órgão.	O	RNF-O

10. PRESERVAÇÃO

A preservação de documentos arquivísticos físicos ou digitais não é um fim em si mesmo. Ela decorre de valor secundário desses documentos.

Os documentos arquivísticos digitais gerenciados por um GestãoDoc devem ser preservados durante todo o período previsto para sua guarda, conforme determinado nas Tabelas de Temporalidade.

Considerando que a degradação de suporte e a obsolescência tecnológica são os principais fatores de comprometimento da preservação dos documentos digitais, ameaçando o acesso ao conteúdo, a autenticidade e a integridade, no e-Arq Brasil (Conarq, 2022a) são apontadas técnicas para evitar esses riscos.

Em relação ao suporte, é recomendado

> *o uso de suportes de alta qualidade e com previsão de vida útil adequada aos propósitos de preservação, o monitoramento contínuo dos avanços tecnológicos e da degradação do suporte, a adoção de formatos abertos e a busca por soluções independentes de hardware, software e fornecedor.*

E, em relação aos riscos de obsolescência tecnológica, é recomendado o emprego das seguintes técnicas:

- *preservação da tecnologia: é a manutenção de um parque de equipamentos e programas para replicação de uma configuração mais antiga. Possibilita o acesso aos documentos originais no ambiente em que foram produzidos, porém, a manutenção e a integração com outros sistemas podem tornar-se problemáticas ao longo do tempo. A preservação do hardware, em especial, é uma alternativa cara, mesmo nas situações em que é compartilhado por mais de um usuário. Além disso, essa alternativa não é exequível no longo prazo, uma vez que o hardware pode ser danificado de forma irreversível, ficando completamente indisponível;*

- *emulação: é um processo que permite, por meio de software, a imitação de software e hardware em outro ambiente computacional. Permite que um computador moderno, possivelmente mais barato e de fácil manutenção, possa executar programas (software) antigos, desenvolvidos, originalmente, para outra plataforma. Para evitar possíveis perdas de informação e funcionalidades, deve ser realizada com bastante rigor. A probabilidade de perda de informações e funcionalidades aumenta à medida que são utilizadas diversas camadas de emulação, como resultado da aplicação desta técnica repetidas vezes;*

- *migração: é a transferência periódica dos documentos de um ambiente computacional para outro. Na preservação de documentos digitais a migração é correntemente realizada por meio da atualização de suporte e/ou conversão de formatos;*

- *atualização de suporte: consiste em copiar os documentos de um suporte para outro, sem mudar sua codificação, para evitar perdas decorrentes da deterioração do suporte. É amplamente utilizada e não provoca nenhuma perda ou alteração no documento, uma vez que a cadeia de bits copiada para o outro suporte é rigorosamente idêntica à inicial;*

- *conversão de formatos: é a conversão de um formato para outro, motivada principalmente para contornar a obsolescência tecnológica. Os documentos em formatos obsoletos são convertidos para novos formatos, apoiados em hardware e software mais atuais. Esse processo não está livre de problemas, podendo resultar em perda de informações e funcionalidades. A conversão também pode ser utilizada para reduzir a quantidade de formatos utilizados e, consequentemente, de sistemas a serem mantidos e gerenciados, de modo a facilitar as ações de preservação. Neste caso é chamada de normalização de formatos.*

No e-Arq Brasil recomenda-se, também que as estratégias e os procedimentos de preservação sejam bem definidos, documentados e periodicamente revisados.

O presente Modelo de Requisitos, no entanto, não tem como escopo principal a guarda permanente, que deve ocorrer no Repositório Arquivístico Digital Confiável (RDC-Arq), desenvolvido como *software* livre, gratuito e de código aberto, projetado para manter os dados em padrões de preservação digital e o acesso em longo prazo, para fins de preservação digital.

O Repositório Arquivístico Digital Confiável (RDC-Arq) pode ser definido como um conjunto de requisitos e procedimentos normativos e técnicos capazes de manter autênticos os documentos digitais nele custodiados, de modo a preservá-los e dar acesso a eles pelo tempo necessário.

Trata-se, dessa forma, de um ambiente de preservação dos documentos arquivísticos digitais, mantendo a sua autenticidade e sua relação orgânica, além de auxiliar nos processos de arranjo e descrição, com vistas ao acesso durante o tempo de guarda.

10.1 Aspectos físicos

REQ	REQUISITO	OBRIG	TIPO
RPR10.1.1	Prover que os suportes de armazenamento do GestãoDoc sejam acondicionados, manipulados e utilizados em condições ambientais compatíveis com sua vida útil prevista e/ou pretendida, de acordo com as especificações técnicas do fabricante e de entidades isentas e com base em estatísticas de uso.	O	RNF-O
RPR10.1.2	Permitir ao administrador especificar a vida útil prevista/pretendida dos suportes para implantação de estratégias de atualização.	O	RNF-O
RPR10.1.3	Permitir o controle da vida útil dos suportes para auxiliar a implementação da estratégia de atualização dos suportes.	O	RNF-O
RPR10.1.4	Informar automaticamente quais são os suportes que se encontram próximos do fim de sua vida útil.	D	RNF-O
RPR10.1.5	Permitir a identificação do suporte físico no qual a informação está registrada no caso de armazenamento local.	O	RNF-O

10.2 Aspectos lógicos

Um GestãoDoc deve garantir escalabilidade no armazenamento, permitindo expansão ilimitada dos dispositivos de armazenamento.

REQ	REQUISITO	OBRIG	TIPO
RPR10.2.1	Manter cópias de segurança, as quais devem ser guardadas em ambientes seguros e em locais diferentes de onde se encontra a informação original.	O	RNF-O
RPR10.2.2	Permitir a verificação periódica dos dados armazenados, visando à detecção de possíveis erros. Nesse caso, recomenda-se o uso de um *checksum* robusto, ou seja, que permita a constatação da integridade dos dados e seja seguro quanto a fraudes.	O	RNF-O
RPR10.2.3	Permitir a substituição de dados que apresentem erros em sistemas de armazenamento.	O	RNF-O
RPR10.2.4	Permitir a correção de erros de dados detectados em sistemas de armazenamento.	O	RNF-O
RPR10.2.5	Permitir a verificação dos dados armazenados, incluindo os erros detectados, substituições e correções de dados realizadas.	O	RNF-O
RPR10.2.6	Permitir manter o histórico dos resultados da verificação periódica dos dados armazenados.	D	RNF-O
RPR10.2.7	Realizar ações de preservação sempre que se torne patente ou previsível a obsolescência da tecnologia utilizada pelo GestãoDoc.	O	RNF-O

10.3 Aspectos gerais

REQ	REQUISITO	OBRIG	TIPO
RPR10.3.1	Registrar em trilhas de auditoria as operações de preservação realizadas.	O	RNF-O
RPR10.3.2	Utilizar suporte de armazenamento e recursos de *hardware* e *software* que sejam maduros, estáveis no mercado e amplamente disponíveis.	D	RNF-O
RPR10.3.3	Verificar as modificações em um GestãoDoc e em sua base tecnológica em ambiente exclusivo para essa finalidade, de modo a garantir que, após a implantação das alterações, os dados continuem sendo acessados sem alteração de conteúdo.	O	RNF-O
RPR10.3.4	Utilizar normas amplamente aceitas, descritas em especificações abertas e disponíveis publicamente, no que se refere a estruturas para codificação, armazenamento e banco de dados.	D	RNF-O
RPR10.3.5	Priorizar o uso de tecnologias abertas para codificação, armazenamento ou banco de dados, evitando o uso de soluções proprietárias e observando as diretrizes da Plataforma Digital do Poder Judiciário (PDPJ-Br). Ao adotar soluções proprietárias, devem estar plenamente documentadas e disponíveis ao administrador	O	RNF-O
RPR10.3.6	Gerir metadados relativos à preservação dos documentos e seus respectivos componentes.	O	RNF-P
RPR10.3.7	Possibilitar níveis de interoperabilidade com outros sistemas de produção documental, com sistemas de negócio e com Repositórios Arquivísticos Digitais Confiáveis (RDC-Arq), com finalidade de preservação digital.	O	RNF-P
RPR10.3.8	Suportar a transferência em bloco de documentos (incluindo as demais informações associadas a cada documento) para outros suportes e/ou sistemas, de acordo com as normas aplicáveis aos formatos utilizados. Exemplo: Recolhimento para o Repositório Arquivístico Digital Confiável (RDC-Arq).	D	RNF-P

11. SEGURANÇA: ASPECTOS ESTRUTURAIS

Em complementação aos requisitos funcionais definidos no Capítulo 8 - Segurança: controle de acessos e auditoria, são definidos os requisitos não funcionais de segurança a seguir. A segurança do GestãoDoc deve observar também as determinações da Resolução CNJ nº 396/2021, que trata da Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ).

O GestãoDoc deve prever controles para proporcionar a salvaguarda regular dos documentos institucionais e dos seus metadados. Deve também poder recuperá-los rapidamente em caso de perda devido a sinistros, falhas no sistema ou de segurança ou degradação do suporte. Esses mecanismos devem seguir a política de segurança da informação dos órgãos do Poder Judiciário, conforme Resolução CNJ nº 396/2021 referida acima.

No caso dos sistemas de gestão de documentos não digitais, pode-se prever a reprodução de documentos para outros suportes como medida de segurança, como, por exemplo, mediante processo de microfilmagem ou digitalização. No tocante à digitalização, os órgãos do Poder Judiciário deverão observar as diretrizes e normas instituídas pela Resolução CNJ nº 469/2022.

No caso dos sistemas de gestão de processos e documentos digitais, é aconselhável que o GestãoDoc contenha meios de monitoramento e acompanhamento da realização das cópias de segurança (*backup*). Esse processo consiste na realização de cópias periódicas das informações para sua restauração posterior, em caso de perda devido a falhas de *software*, *hardware* ou mesmo acidente. O processo reverso ao *backup* é o de restauração (*restore*), que consiste em recuperar as informações para o ambiente de produção do GestãoDoc para um estado consistente.

Como o objetivo é restaurar o sistema em caso de falhas, as informações serão armazenadas conforme definido na Política de Segurança da Informação dos órgãos do Poder Judiciário. O procedimento de cópias de segurança não pode ser confundido com uma estratégia de preservação de longo prazo.

11.1 Segurança da infraestrutura

Além dos dados inseridos nos sistemas, há necessidade de segurança da infraestrutura de instalações do acervo digital e dos ativos de tecnologia da informação que possibilite a resposta a incidentes a ela relacionados, a continuidade dos serviços e a prevenção de ameaças físicas e cibernéticas. Para isso, devem ser adotadas medidas que observem a política de segurança da informação, comunicação e cibernética, em conformidade com os normativos do CNJ e dos órgãos do Poder Judiciário.

11.2 Criptografia, certificação e assinatura digital

A criptografia é uma tecnologia que mistura a informação usando códigos e chaves criptográficas, impossibilitando que seja acessada por pessoas que não conheçam as chaves apropriadas.

A criptografia pode ser utilizada como mecanismo de garantia de sigilo na transmissão de documentos, seja na cifragem da conexão, estabelecendo canais seguros, seja na cifragem do documento transmitido ou capturado. Os requisitos de assinatura digital são necessários para as instituições que recebem documentos digitais assinados e onde são necessárias verificações de integridade e autenticidade.

O emprego de certificação e assinatura digital foi a princípio regulamentado pela Medida Provisória 2.200-2, de 2001, que instruía o reconhecimento do ICP-Brasil como órgão regulador para as autoridades certificadoras (AC´s). Atualmente, a Lei nº 14.063/2020 define três categorias de assinaturas eletrônicas possíveis para os sistemas de informação: assinatura eletrônica simples, assinatura eletrônica avançada, e assinatura eletrônica qualificada, que são tratadas no Capítulo 11.3 abaixo.

Esses requisitos não esgotam o tema segurança da informação, pois a segurança integral é sistêmica e abrange não somente a tecnologia, mas também pessoas, processos, ambiente e legislação.

11.3 Cópias de segurança

Procedimentos de *backup* destinados a gerar cópias de segurança aptas a prevenir a perda de informações e para garantir a disponibilidade do sistema devem ser feitos regularmente. Pelo menos uma cópia deve ser armazenada remotamente (*off-site*).

Nesses procedimentos devem ser incluídas informações necessárias ao funcionamento de um GestãoDoc, que compreendem: os documentos digitais, os metadados e informações de controle associadas às camadas de *software* relacionadas ao GestãoDoc (sistema operacional, gerenciador de bancos de dados, *software* aplicativo).

REQ	REQUISITO	OBRIG	TIPO
RSE11.3.1	Cumprir a política de segurança da informação do respectivo órgão e a nacional do Conselho Nacional de Justiça.	O	RNF-E
RSE11.3.2	Permitir que mecanismos de cópias de segurança criem cópias de todas as informações contidas no GestãoDoc (documentos arquivísticos, metadados e parâmetros do sistema, códigos do GestãoDoc etc.).	O	RNF-O
RSE11.3.3	Manter o controle das cópias de segurança, realizando testes de restauração.	O	RNF-O
RSE11.3.4	Prover as mídias removíveis com cópias em suportes equivalentes e armazenamento *off-site*.	O	RNF-O
RSE11.3.5	Prover os suportes de armazenamento com cópias de segurança armazenadas em pelo menos dois locais diferentes e fisicamente distantes.	O	RNF-O

RSE11.3.6	Realizar o agendamento, automaticamente, das cópias de segurança com periodicidade estipulada pela política de segurança da informação do órgão, devendo permitir cópias incrementais ou completas.	D	RNF-O
RSE11.3.7	Realizar assinatura digital das cópias de segurança, de modo a garantir a integridade dos dados e a identificação do responsável pelo procedimento.	D	RNF-O
RSE11.3.8	Restituir os documentos de arquivo e metadados a um estado conhecido, utilizando uma combinação de cópias restauradas e rotinas de auditoria.	O	RNF-O
RSE11.3.9	Prever mecanismos especiais de criação de cópias de segurança para dados críticos.	D	RNF-O
RSE11.3.10	Realizar, periodicamente, cópias das trilhas de auditoria.	D	RNF-O

11.4 Criptografia

Criptografia é a ciência do ocultamento de informações. Criptografar ou cifrar um arquivo significa alterar os *bits* de tal modo que a informação representada subsista, mas de forma ininteligível.

O processo inverso é descriptografar ou decifrar: recuperar a informação original, passível de interpretação e modificação. Atualmente a criptografia alcança diferentes aplicações, visando a prover segurança às relações estabelecidas no meio digital, cobrindo desde mecanismos de autenticação e controle de acesso, passando pela assinatura digital de documentos e, mais recentemente, pela implementação de mecanismos seguros de registros públicos, além de inúmeras funções básicas de segurança.

Um GestãoDoc deve utilizar métodos criptográficos para garantir a segurança na comunicação e em sessões *web*, bem como no armazenamento e recuperação de informações sigilosas.

Especial atenção deve ser dispensada quanto aplicados em documentos de longa temporalidade, em razão dos riscos de comprometimento ou obsolescência da chave, de indisponibilidade do portador da chave e de evoluções tecnológicas.

O conjunto desses requisitos é facultativo e a adoção e a obrigatoriedade apontadas nesta seção devem ser seguidas somente quando um GestãoDoc fizer uso de criptografia.

REQ	REQUISITO		TIPO
RSE11.4.1	Utilizar criptografia no armazenamento, transmissão e na apresentação de documentos digitais ao implementar a política de sigilo.	O	RNF-O
RSE11.4.2	Limitar o acesso aos documentos cifrados somente aos usuários portadores da chave de decifração.	O	RNF-P
RSE11.4.3	Registrar os seguintes metadados sobre um documento cifrado: • indicação se está cifrado ou não; • algoritmos usados na cifração; • identificação do detentor da chave pública; e • Identificação do detentor da chave privada.	O	RNF-P

RSE 11.4.4	Permitir a captura de documentos cifrados.	D	RNF-P
RSE 11.4.5	Habilitar a usuários autorizados a realização das seguir das operações: • incluir, remover ou alterar parâmetros dos algoritmos criptográficos instalados no GestãoDoc; • incluir, remover ou substituir chaves criptográficas de programas ou usuários do GestãoDoc; • cifrar e alterar a criptografia de documentos; e • remover a criptografia de um documento. A remoção da cifração pode ocorrer quando sua manutenção resultar na indisponibilidade do documento. Por exemplo, se a chave de cifração/decifração estiver embarcada em *hardware* inviolável cuja vida útil esteja prestes a se esgotar ou se o documento for desclassificado.	O	RNF-P
RSE 11.4.6	Garantir que somente o administrador seja capaz de alterar características dos mecanismos criptográficos internos. Em tais casos, deverão obrigatoriamente ser registradas, em trilha de auditoria, as seguintes informações: • descrição técnica da alteração; • data e hora da alteração; • identificação do executor da operação; e • motivo da alteração.	O	RNF-O
RSE 11.4.7	Nos casos de aplicação do item anterior, prover mecanismos para convivência temporária de dois mecanismos de criptografia distintos. O objetivo é viabilizar a transição para o novo sistema sem indisponibilizar a operação do GestãoDoc.	O	RNF-O
RSE 11.4.8	Em caso de remoção da cifração do documento, prover o registro dos seguintes metadados adicionais na trilha de auditoria: • data e hora da remoção da cifração; • identificação do executor da operação; • motivo da remoção da cifração.	O	RNF-P
RSE 11.4.9	Impedir a abertura (*disclosure*) de senhas, mesmo para o administrador. Casos de contingência, no impedimento de recuperação de informação sigilosa (por exemplo, pela morte do usuário detentor da senha) poderão ser tratados em sistemas externos ao GestãoDoc.	O	RNF-P
RSE11.4.10	Possuir arquitetura capaz de receber atualizações tecnológicas no que se refere à plataforma criptográfica.	O	RNF-O
RSE 11.4.11	Prover mecanismos de proteção como, por exemplo, criptografia, que permitam cópias de segurança de documentos confidenciais, preservando a inviolabilidade da informação.	O	RNF-O

11.5 Certificação Digital

Certificação digital é um conjunto de padrões, procedimentos e tecnologias voltados à garantia da vinculação inequívoca de uma chave pública a um indivíduo por meio da emissão de um documento eletrônico denominado "certificado digital", empregando para isso uma Infraestrutura de Chaves Públicas (ICP).

Uma ICP (no inglês, PKI – *Public Key Infrastructure*) é uma estrutura cartorial, mantida por uma organização pública ou privada com o objetivo de identificar de maneira inequívoca pessoas e computadores no ambiente digital, tendo como elemento central um certificado digital. Ela estabelece um conjunto de

papéis, políticas, padrões e procedimentos para emitir, gerenciar, distribuir, utilizar, armazenar e revogar certificados digitais.

No Brasil, o Governo Federal optou por adotar uma ICP de cadeia única, denominada Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

Conforme definição do Instituto Nacional de Tecnologia da Informação (ITI, 2021), autarquia federal responsável por manter e executar as políticas da ICP-Brasil, a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. Observa-se que o modelo adotado pelo Brasil foi o de certificação com raiz única, sendo que o ITI, além de desempenhar o papel de Autoridade Certificadora Raiz (AC-Raiz), também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.

Um certificado digital reúne uma série de informações sobre seu detentor, podendo ser considerado uma identidade digital. No caso de certificados digitais emitidos para pessoas físicas no âmbito da ICP-Brasil, os atributos de informação que os compõem incluem o nome de seu titular, o período de validade do certificado, um número de série, números de registro do CPF, RG, endereço, endereço eletrônico, entre outros.

11.6 Assinatura digital

A assinatura digital é um mecanismo para dar garantia de integridade e autenticidade a arquivos eletrônicos. A assinatura digital prova que a mensagem ou arquivo não foi alterado, e que foi assinado pela entidade ou pessoa que possui a chave privada, utilizada na assinatura.

A Medida Provisória nº 2.200-2, de 24 de agosto de 2001, instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), regulamentando o uso de certificados digitais como forma de assegurar a autenticidade, integridade e validade jurídica de documentos em forma eletrônica, prevendo a possibilidade de utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, quando admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

Posteriormente, a Lei nº 11.419/2006 estabeleceu duas formas de identificação inequívoca do signatário para fins de assinatura eletrônica: o uso de assinatura digital baseada em certificado digital emitido por Autoridade Certificadora credenciada e o cadastro do usuário no Poder Judiciário, atribuindo-lhe registro e meio de acesso ao sistema, usualmente mediante o uso de sigla de identificação do usuário e senha, de modo a preservar o sigilo, a identificação e a autenticidade de suas comunicações.

Mais recentemente, a Lei nº 14.063/2020 regulamentou o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre licenças de software desenvolvidos por entes públicos, definindo três classificações para as assinaturas digitais: a) assinatura simples: a que permite identificar o seu signatário e a que associa dados a ou-

tros dados em formato eletrônico do signatário; b) assinatura avançada: utiliza certificados não emitidos pela ICP-Brasil admitidos pelas partes como válidos; c) assinatura qualificada: a que utiliza certificado digital, nos termos do § 1º do art. 10 da Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

A obrigatoriedade apontada nesta seção deve ser observada de acordo com a modalidade de assinatura digital adotada pelo GestãoDoc.

11.6.1 Assinatura Digital com Certificados Digitais

A assinatura digital de documentos mediante a utilização de certificados digitais deve atender ao que estabelece a legislação referida no item anterior.

REQ	REQUISITO	OBRIG	TIPO
RSE11.6.1.1	Garantir a origem e a integridade dos documentos com assinatura digital.	O	RNF-P
RSE11.6.1.2	Permitir somente a administradores autorizados a inclusão, remoção ou atualização dos certificados digitais de computadores ou de usuários no GestãoDoc	O	RNF-O
RSE11.6.1.3	Verificar a validade da assinatura digital no momento da captura do documento, e caso não esteja válida, recusar a captura.	O	RNF-P
RSE11.6.1.4	No processo de verificação da assinatura digital, registrar, nos metadados do documento: · a validade da assinatura; · o registro de verificação da assinatura; e · a data e hora em que a verificação ocorreu.	O	RNF-P
RSE11.6.1.5	Armazenar juntamente com o documento as informações de certificação: · assinatura digital; e · certificado digital (cadeia de certificação) usado na verificação da assinatura.	D	RNF-P
RSE11.6.1.6	Receber atualizações tecnológicas quanto à plataforma criptográfica e padrões de assinatura digital.	D	RNF-O

11.6.2 Assinatura cadastrada mediante identificação do usuário e senha

Os sistemas GestãoDoc podem utilizar a identificação de usuário e senha para assinatura digital de documentos, conforme tratado pela legislação referenciada anteriormente (Lei nº 11.419/2006).

A assinatura de um documento digital pode se dar, também, por meio do registro em metadados da identificação do autor, realizado automaticamente pelo GestãoDoc, pela validação do nome de usuário e da senha ou de outra forma de identificação que seja reconhecida pelo GestãoDoc.

Esse conjunto de requisitos como um todo é facultativo e a adoção e a obrigatoriedade apontadas nesta seção somente ocorre quando um GestãoDoc fizer uso desta forma de autenticação.

REQ	REQUISITO	OBRIG	TIPO
RSE11.6.2.1	Garantir a autoria de um documento que tenha sido autenticado por meio da identificação do autor após confirmação de senha, nos documentos produzidos e mantidos dentro do GestãoDoc.	O	RNF-P
RSE11.6.2.2	Registrar a identificação do usuário como metadado de autenticação do documento após verificação da senha pessoal.	O	RNF-P
RSE11.6.2.3	Fazer uso de *checksum* para apoiar a verificação da integridade do documento que foi autenticado após confirmação de senha.	D	RNF-P

11.7 Carimbo digital do tempo

Carimbo digital do tempo

> É um documento eletrônico emitido por uma Autoridade de Carimbo do Tempo (ACT) que serve como evidência de que uma informação digital existia numa determinada data e hora. O timestamp, calculado a partir do hash do documento, é o registro da data e hora em que a requisição do timestamp (Time Stamp Request) chegou à Autoridade de Carimbo do Tempo, e não se refere à data e hora de criação do documento. É uma forma de autenticação do documento (Conarq, 2020, p. 15).

Seu uso pela administração pública, que é facultativo, foi padronizado e normalizado com a criação da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Para o perfeito funcionamento de carimbos de tempo, é imprescindível que a infraestrutura de TIC tenha os servidores todos sincronizados e com a data atualizada, conforme o padrão do horário brasileiro, respeitando-se os fusos horários.

Os requisitos a seguir são aplicáveis somente aos órgãos que adotarem o carimbo digital do tempo, pois há necessidade de assegurar autenticação, imputabilidade e irretratabilidade (ou irrefutabilidade) em relação a um determinado ponto no tempo. Assim, esse conjunto de requisitos como um todo é facultativo e a obrigatoriedade apontada nesta seção deve ser seguida somente quando o carimbo digital do tempo for utilizado no GestãoDoc.

REQ	REQUISITO	OBRIG	TIPO
RSE11.7.1	Acessar relógios e carimbador de tempo confiáveis para seu próprio uso.	O	RNF-P
RSE11.7.2	Verificar a validade do carimbo digital do tempo no momento da captura do documento.	O	RNF-P
RSE11.7.3	Registrar nos metadados do documento, na verificação do carimbo digital do tempo, o seguinte: · validade do carimbo digital do tempo; · registro da verificação do carimbo digital do tempo; e · data e hora em que ocorreu a verificação.	O	RNF-P

11.8 Marcas d'água digitais

Marcas d'água

> servem para marcar uma imagem digital com informação sobre a sua proveniência e características e são utilizadas para proteger a propriedade intelectual. As marcas-d'água sobrepõem no mapa de bits de uma imagem, um desenho complexo, visível ou invisível, o qual só pode ser suprimido mediante a utilização de um algoritmo e uma chave protegida (Conarq, 2020, p. 35).

Tecnologias semelhantes podem ser aplicadas a sons e a imagens em movimento digitalizadas.

Esses requisitos são aplicáveis somente aos órgãos em que são usadas marcas d'água digitais. Assim, esse conjunto de requisitos como um todo é facultativo e a obrigatoriedade apontada nesta seção deve ser seguida somente quando um GestãoDoc fizer uso de marcas d'água digitais.

REQ	REQUISITO	OBRIG	TIPO
RSE11.8.1	Permitir recuperar informação contida em marcas d'água digitais.	O	RNF-P
RSE11.8.2	Permitir armazenar documentos arquivísticos digitais que contenham marcas d'água digitais.	O	RNF-P
RSE11.8.3	Possuir uma arquitetura capaz de receber atualizações tecnológicas quanto à plataforma de geração e de detecção de marca d'água digital.	O	RNF-P

11.9 Autoproteção

A autoproteção consiste na capacidade do sistema de computação de verificar a integridade de programas e de dados de controle como medida de proteção.

Esta seção trata dos requisitos relativos à capacidade do GestãoDoc de se autoproteger contra quaisquer erros, falhas ou ataques ao próprio sistema.

Além dos requisitos de autoproteção, o GestãoDoc deverá interagir com outros sistemas de proteção, tais como: antivírus, *firewall*, *anti-spyware* etc.

Os arquivos digitais que não devam ser capturados pelo GestãoDoc em razão de *malware* ou similares, mas que devam ser armazenados ou arquivados como anexos externos e considerados nos processos ou dossiês por força de determinação judicial ou administrativa, deverão ser incluídos em Repositório Arquivístico Digital Confiável - RDC – Arq ou armazenados em dispositivos ou mídias externas ao GestãoDoc, com observância da cadeia de custódia e da garantia de acesso às partes.

Referidos arquivos deverão ser referenciados no processo/dossiê por certidão padronizada contendo, no mínimo, as seguintes informações:

a) descrição pormenorizada, acompanhada da justificativa acerca da não captura ou exclusão;

b) mídia ou dispositivo empregado para armazenamento;

c) local específico em que se encontra mantida a mídia ou dispositivo; e

d) data, nome, matrícula e assinatura do servidor responsável pela guarda e emissor da certidão.

REQ	REQUISITO	OBRIG	TIPO
RSE11.9.1	Realizar a verificação de *malware* e similares dos documentos destinados à captura ou capturados, identificando para o usuário aqueles que estiverem contaminados.	O	RNF-O
RSE11.9.2	Impedir o acesso e permitir a exclusão de documentos que sejam ou contenham *malware* ou similares quando a detecção foi posterior à captura.	O	RNF-O
RSE11.9.3	Possuir dispositivos e procedimentos que reduzam as possibilidades de erros, falhas e descontinuidades no seu funcionamento que causem danos ou perdas aos documentos digitais.	O	RNF-O
RSE11.9.4	Permitir a colocação do GestãoDoc em modo de manutenção após falha ou descontinuidade, quando a recuperação automática ocorrer, oferecendo a possibilidade de restaurar o GestãoDoc para um estado seguro. Na restauração ao estado seguro, um GestãoDoc deve ser capaz de garantir a recuperação de perdas, inclusive dos documentos de transações mais recentes.	O	RNF-O
RSE11.9.5	Garantir que os dados de segurança, quando replicados, sejam consistentes. Permissões de controle de acesso, chaves criptográficas e parâmetros de algoritmos criptográficos são exemplos de dados de segurança.	O	RNF-O
RSE11.9.6	Preservar um estado seguro de funcionamento, interrompendo completamente a interação com usuário comum, quando quaisquer dos seguintes erros ocorrerem: • falha de comunicação entre cliente e servidor; • perda de integridade das informações de controle de acesso; e • impossibilidade de registro em trilha de auditoria.	O	RNF-P
RSE11.9.7	Passar para o modo de manutenção quando não for possível escrever em trilha de auditoria, impedindo toda operação de qualquer usuário.	D	RNF-P

12. DISPONIBILIDADE

A disponibilidade está relacionada às exigências mínimas sobre prontidão de atendimento de um sistema.

Os requisitos de disponibilidade devem ser especificados pelo administrador do GestãoDoc de acordo com os períodos previstos de atendimento (por dia útil ou em atendimento contínuo) e o tempo máximo tolerável em interrupções previstas. O grau de disponibilidade a ser estabelecido deve levar em conta fatores como as regras de negócio da organização, a necessidade de realização de backup, manutenções planejadas, entre outros.

REQ	REQUISITO	OBRIG	TIPO
RDI12.1.1	Garantir disponibilidade de operação durante o período definido pela instituição.	O	RNF-O

13. USABILIDADE

Um sistema de *software* com boa usabilidade deve apoiar a realização de tarefas simples, diretas e objetivas, que garantam as metas de produtividade e qualidade de trabalho do usuário.

Sistemas com maior grau de usabilidade, segundo o e-Arq Brasil (Conarq, 2022a), devem ser fáceis de entender e operar, além de seguir padrões de boas práticas técnicas já conhecidas e bem estabelecidas.

Na descrição das características de um GestãoDoc, o e-Arq Brasil recomenda levar em consideração a facilidade de utilização da interface e de execução de tarefas, os tipos de usuários, o uso de equipamentos adequados, a ergonomia, o ambiente físico e organizacional e o contexto de uso.

REQ	REQUISITO	OBRIG	TIPO
RUS 13.1.1	Possuir documentação completa, clara, inteligível e organizada para utilização do *software*.	O	RNF-P
RUS13.1.2	Possuir sistema de ajuda *on-line*.	O	RNF-P
RUS13.1.3	Vincular o sistema de ajuda *on-line* à função ou tarefa executada (sensível ao contexto). Exemplo: Quando se executa uma operação de edição, uma vez acionada a ajuda, ela deve remeter para o tópico de ajuda da edição.	D	RNF-P
RUS13.1.4	Permitir ao gestor a personalização de conteúdo de ajuda *on-line* por adição de texto ou edição do texto existente. Exemplo: O responsável pela gestão do conteúdo da ajuda pode adicionar esclarecimentos ou alterar o conteúdo das descrições, de modo a facilitar o entendimento das funções.	D	RNF-P
RUS13.1.5	Permitir que toda mensagem de erro produzida seja clara e significativa, de modo a possibilitar ao usuário corrigir ou cancelar a operação.	O	RNF-P
RUS13.1.6	Prover a interface de padrões preestabelecidos e consolidados como boas práticas de projeto gráfico. Normas ou regras de interface podem ser relativas à utilização de padrão de identidade visual (ligado à logomarca da instituição ou algum normativo do órgão ou do Conselho Nacional de Justiça), assim como a utilização de guias de estilo para implementação e verificação da padronização da interface, observando os princípios básicos da ergonomia cognitiva.	O	RNF-P
RUS13.1.7	Utilizar conjunto simples e consistente de regras de interface, privilegiando a facilidade de aprendizado das operações pelos seus usuários. A utilização de um conjunto de regras em conformidade com o ambiente operacional em que o GestãoDoc será executado permite que ele apresente menus, comandos e outras facilidades consistentes em toda aplicação. Essas regras de interface, quando compatíveis com outras aplicações principais já instaladas, levam à padronização da terminologia utilizada para funções, rótulos e ações consistentes em toda a aplicação.	D	RNF-P
RUS13.1.8	Prover a interface de visualização dos documentos institucionais com o recurso de arrastar e soltar, caso apropriado no ambiente operacional do GestãoDoc.	D	RNF-P
RUS13.1.9	Permitir que a estrutura de classes, assuntos, movimentos e documentos seja visualizada em diferentes formas de apresentação.	D	RNF-P

RUS13.1.10	Personalizar a interface gráfica, quanto aos seguintes aspectos: • conteúdos de menus; • formatos de telas; • utilização de teclas de função; • alteração de cores, fontes e tamanhos de fontes em telas e janelas dentro de parâmetros ergonômicos; e • avisos sonoros, incluindo tom e volume.	D	RNF-P
RUS13.1.11	Utilizar barras de ferramentas, permitindo ao usuário a possibilidade de configuração e de habilitar/desabilitar esse tipo de recurso. Contudo, sem infringir a recomendação de utilização de um conjunto simples e consistente de regras de interface.	D	RNF-P
RUS13.1.12	Permitir a utilização de janelas e guias, sua movimentação, redimensionamento e gravação das modificações da aparência, possibilitando a personalização por perfil de usuário dentro de parâmetros ergonômicos.	D	RNF-P
RUS13.1.13	Permitir a gravação de opções default para entrada de dados de configuração: • valores iguais aos de um item anterior; • valores que possam ser selecionados de uma lista configurável; • valores derivados do contexto, como data, referência do processo/dossiê, identificador do usuário; e • valores predefinidos por um gestor (para campos de metadados como, por exemplo, o nome da organização que está utilizando o sistema).	D	RNF-P
RUS13.1.14	Possibilitar que a interface disponha de recursos de tecnologia assistiva para utilização por pessoa com deficiência, de modo a atender a legislação de acessibilidade e os atos normativos do Conselho Nacional de Justiça.	O	RNF-P
RUS13.1.15	Permitir que o usuário possa fazer anotações próprias nos documentos que foram salvos, sem que os documentos originais sejam alterados.	O	RNF-P
RUS13.1.16	Possibilitar o uso do GestãoDoc sem a obrigatoriedade de aparelho selecionador específico (mouse, por exemplo).	O	RNF-P
RUS13.1.17	Permitir a realização de transações ou tarefas mais frequentes com menor número de iterações (cliques de mouse, por exemplo) e sem mudanças excessivas de contexto.	D	RNF-P
RUS13.1.18	Integrar o GestãoDoc com ferramentas de comunicação digital da organização, de forma a permitir a geração de mensagens, compartilhamento de documentos e armazenamento de registros sem necessidade de sair do referido sistema.	D	RF
RUS13.1.19	Possibilitar, no caso de integração com as ferramentas de comunicação digital, o referenciamento direto os documentos institucionais por meio de links, sendo dispensável o envio de cópias ou anexos.	D	RF
RUS13.1.20	Possuir interface com sistema de edição de documentos.	D	RNF-P
RUS13.1.21	Permitir a definição e utilização de referências cruzadas entre documentos institucionais digitais correlacionados, possibilitando uma fácil navegação entre eles, inclusive com uso de hyperlinks.	D	RNF-P
RUS13.1.22	Impossibilitar a visualização das funcionalidades administrativas pelo usuário final.	O	RNF-P
RUS13.1.23	Considerar o ambiente de operação do sistema, como ruído, luminosidade, necessidade de rapidez na conclusão da tarefa, demandas específicas para dispositivos móveis, ambiente desktop/web e necessidade de instalação automática, para configurar as formas de interação com o usuário. Exemplo: não devem ser utilizados menus audíveis em ambientes que apresentam alto volume de ruído próximo aos terminais de usuários.	D	RNF-P
RUS13.1.24	Permitir o uso do GestãoDoc em dispositivos móveis.	D	RNF-P

14. INTEROPERABILIDADE

A adoção de regras e padrões de comunicação que estão consolidados permite a consulta e o intercâmbio de informações entre sistemas heterogêneos, sem que o usuário perceba as operações envolvidas (Conarq, 2022a).

O modelo nacional de interoperabilidade disponibilizado pelo Conselho Nacional de Justiça estabelece os padrões para intercâmbio de informações de processos judiciais e assemelhados entre os diversos órgãos de administração de justiça, e serve de base para implementação das funcionalidades pertinentes no âmbito do sistema processual.

Esta seção estabelece requisitos mínimos para que um GestãoDoc possa interoperar com outros sistemas de informação, inclusive sistemas legados, devendo ser respeitadas a política de segurança da informação do órgão e do Conselho Nacional de Justiça.

Pode-se entender a interoperabilidade "como uma característica que se refere à capacidade de diversos sistemas e organizações trabalharem em conjunto (interoperar) de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente" (BRASIL, 2012, p. 6). Isso se faz mediante a utilização de regras e padrões de comunicação.

O artigo 42 da Resolução CNJ nº 324/2020 dispõe que "os órgãos do Poder Judiciário, coordenados pelo CNJ, promoverão a interoperabilidade entre os sistemas de gestão documental e da memória".

Portanto, o GestãoDoc deverá adotar o padrão de interoperabilidade, observando também o previsto na Resolução CNJ nº 335/2020.

REQ	REQUISITO	OBRIG	TIPO
RIN14.1.1	Interoperar com outros sistemas, permitindo pelo menos consulta, recuperação, importação e exportação de documentos e seus metadados. As operações de interoperabilidade devem respeitar a legislação vigente e a política de segurança da informação do órgão e do Conselho Nacional de Justiça.	O	RNF-P
RIN14.1.2	Interoperar com outros sistemas por intermédio de padrões abertos de interoperabilidade regulamentados pelo CNJ.	O	RNF-P
RIN14.1.3	Aplicar os requisitos de segurança descritos neste documento ao executar operações de interoperabilidade. Isso é fundamental para que as operações, feitas em ambiente com interoperabilidade, não afetem a integridade dos documentos e possibilite acessos não autorizados.	O	RNF-P

15. DESEMPENHO E ESCALABILIDADE

Os requisitos de desempenho dizem respeito à eficiência no atendimento às requisições de usuários. O tempo de resposta a tais requisições é influenciado tanto por requisitos de qualidade do *software* quanto por fatores externos, como, por exemplo, infraestrutura de rede, volume de tráfego de dados e dimensionamento dos servidores e das estações de trabalho. O desempenho é medido avaliando-se a velocidade de processamento, o tempo de resposta e o consumo de recursos.

A escalabilidade de um componente ou de um *software* relaciona-se à capacidade do sistema manter o desempenho — tempo de resposta — quando há um aumento no número de usuários e/ou de requisições simultâneas.

Sobre desempenho e escalabilidade, investimentos em *hardware* devem refletir no aumento de desempenho do sistema. Quando se acrescentam mais máquinas, os investimentos em *hardware* caracterizam a melhor escalabilidade horizontal. Quando se aumenta o poder de processamento das máquinas existentes, a escalabilidade é vertical. Melhor escalabilidade possibilita distribuir e configurar a execução da aplicação para satisfazer vários volumes de transação. Um sistema é dito escalável quando o investimento necessário à melhoria do desempenho é proporcional ao resultado obtido.

A organização deve manter indicadores do valor da sua infraestrutura de informação, avaliando a relação entre o capital investido e os níveis de performance obtidos.

Para um GestãoDoc, entende-se escalabilidade como a capacidade de o sistema responder a um aumento de usuários e volume de documentos processados, mantendo-se o desempenho das respostas do sistema.

REQ	REQUISITO	OBRIG	TIPO
RDE15.1.1	Manter estatísticas dos tempos de atendimento, discriminados por tipo de operação.	D	RNF-O
RDE15.1.2	Ser expansível até comportar um número máximo preestabelecido de usuários simultâneos, provendo continuidade efetiva de serviços.	O	RNF-O
RDE15.1.3	Manter registros de atualização de versão de infraestrutura e do próprio sistema.	O	RNF-O
RDE15.1.4	Ser escalável, permitindo a adaptação a organizações de diferentes tamanhos e complexidades.	D	RNF-O
RDE15.1.5	Fornecer evidências do grau de escalabilidade ao longo do tempo, mantendo avaliações quantitativas de: · tamanho máximo do repositório; · número máximo de usuários simultâneos que possam ser atendidos com desempenho adequado; · sobrecarga administrativa, expectativa de crescimento do número de usuários; e · expectativa de crescimento das bases de dados.	D	RNF-O

16. IMPLEMENTAÇÃO, MANUTENÇÃO E EVOLUÇÃO

Esta seção trata dos requisitos relacionados à documentação de referência de ações de implementação, manutenção e evolução do GestãoDoc, que são relevantes para seu funcionamento, aprimoramento e para as auditorias, contribuindo também para o acompanhamento do grau de aderência aos requisitos do MoReq-Jus.

REQ	REQUISITO	OBRIG	TIPO
RME16.1.1	Possuir documentação de implementação, manutenção e evolução.	O	RNF-O
RME16.1.2	Ser aderente à normatização do CNJ nos aspectos de processo de desenvolvimento de *software*.	O	RNF-O
RME16.1.3	Possuir um ambiente de homologação para avaliação de novas versões de *software*, que permita testes: • funcionais; e • de preservação da integridade do acervo digital.	O	RNF-O
RME16.1.4	Permitir somente aos administradores a exportação e a transferência das trilhas de um suporte de armazenamento para outro, garantindo que em tais casos as informações não sejam comprometidas.	O	RNF-O
RME16.1.5	Gerar um alarme para os administradores se o tamanho da trilha de auditoria exceder um limite preestabelecido.	O	RNF-O
RME16.1.6	Documentar os aspectos de administração e operação do sistema, por meio de manual, roteiro, ajuda on-line ou outros meios.	O	RNF-P

REFERÊNCIAS

ARQUIVO NACIONAL. **Dicionário brasileiro de terminologia arquivística**. Rio de Janeiro: Arquivo Nacional, 2005. Disponível em: https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/dicionrio_de_terminologia_arquivistica.pdf. Acesso em: 31 ago. 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO 14721 Sistemas espaciais de transferência de dados e de informação**: Sistema Aberto de Arquivamento de Informação (SAAI): modelo de referência. Rio de Janeiro: ABNT, 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO 23081-1 Informação e documentação**: processos de gestão de documentos de arquivo: metadados para documentos de arquivo. Rio de Janeiro: ABNT, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO 23081-2 Informação e documentação**: gerenciamento de metadados para documentos de arquivo: parte 2: problemas conceituais e implementação. Rio de Janeiro: ABNT, 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO 30301 Informação e documentação**: sistemas de gestão de documentos de arquivo: requisitos. Rio de Janeiro: ABNT, 2016.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO 30302 Informação e documentação**: sistema de gestão de documentos de arquivo: diretrizes para implementação. Rio de Janeiro: ABNT, 2017.

BOURQUE, Piere; FAIRLEY, R. E (editores). **Guide to the software engineering body of knowledge:** version 3.0. Washington: IEEE Computer Society, 2014. Disponível em: https://www.computer.org/education/bodies-of-knowledge/software-engineering/v3. Acesso em: 31 ago. 2023.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14 out. 2022.

BRASIL. **Lei nº 11.419, de 19 de dezembro de 2006**. Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências. Brasília: Presidência da República, 2006. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm. Acesso em: 14 out. 2022.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**: Lei de Acesso à Informação. Regula o acesso informações previsto no inciso XXXIII do art. 5o, no inciso II do §3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei n. 8.112, de 11de dezembro de 1990; revoga a Lei n. 11.111, de 5 de maio de 2005, e dispositivos da Lei n.8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília: Presidência da República, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 14 out. 2022.

BRASIL. **Lei nº 12.682, de 9 de julho de 2012**. Dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos. Brasília: Presidência

da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Lei/L12682.htm. Acesso em: 14 out. 2022.

BRASIL. **Lei nº 13.105, de 16 de março de 2015**. Código de processo Civil. Brasília: Presidência da República, 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 14 out. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília: Presidência da República, 2018. Disponível em: https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-publicacaooriginal-156212-pl.html. Acesso em: 14 out. 2022.

BRASIL. **Lei nº 14.063, de 23 de setembro de 2020**. Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos; e altera a Lei nº 9.096, de 19 de setembro de 1995, a Lei nº 5.991, de 17 de dezembro de 1973, e a Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Brasília: Presidência da República, 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-n-14.063-de-23-de-setembro-de-2020-279185931. Acesso em: 14 out. 2022.

BRASIL. **Lei nº 8.159, de 8 de janeiro de 1991.** Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Brasília: Presidência da República, 1991. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8159.htm. Acesso em: 14 out. 2022.

BRASIL. **Medida provisória nº 2.200-2, de 24 de agosto de 2001.** Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Brasília: Presidência da República, 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm. Acesso em: 14 out. 2022.

BRASIL. Departamento de Governo Eletrônico. **Emag**: Modelo de acessibilidade em Governo Eletrônico: versão 3.1. Brasília: DGE, 2014. Disponível em: https://emag.governoeletronico.gov.br/. Acesso em: 14 out. 2022.

BRASIL. Gabinete de Segurança Institucional. **Glossário de segurança da informação**. Brasília: 2021. Publicado em 26/11/2021 e atualizado em 26/11/2021. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao-1. Acesso em: 14 out. 2022.

BRASIL. Instituto Nacional de Tecnologia da Informação. **Perguntas frequentes**: ICP-Brasil. Publicado em 20/07/2020 e atualizado em 10/08/2021. Brasília: ITI, 2021. Disponível em: https://www.gov.br/iti/pt-br/acesso-a-informacao/perguntas-frequentes/icp-brasil. Acesso em: 14 out. 2022.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. **Padrões de interoperabilidade de Governo Eletrônico**: guia de interoperabilidade: manual do gestor. Brasília: MPOG, 2012. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/Guia_de_Interoperabilidade_Manual_do_Gestor_2012.pdf. Acesso em: 14 out. 2022.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. **Padrões de interoperabilidade de Governo Eletrônico:** documento de referência. Brasília: MPOG,

2018. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/ePING_v2018_20171205.pdf. Acesso em: 15 out. 2022.

COMISSÃO EUROPEIA. **MoReq2 specification, model requirements for the management of electronic records**: update and extension. [s.l]: Publications Office, 2008. Disponível em: https://data.europa.eu/doi/10.2792/11981. Acesso em: 14 out. 2022.

COMISSÃO EUROPEIA. **MoReq2010, modular requirements for records systems**: core services & plug-in modules [version 1.1]. V. 1. [s.l]: Publications Office, 2011. Disponível em: https://data.europa.eu/doi/10.2792/2045. Acesso em: 14 out. 2022.

COMISSÃO EUROPEIA. **Requirements for Electronic records management systems**: revision: 2002. Disponível em: https://cdn.nationalarchives.gov.uk/documents/referencefinal.pdf. Acesso em: 14 out. 2022.

COMITÊ EXECUTIVO DE GOVERNO ELETRÔNICO. **Padrão de metadados do Governo Eletrônico**: e-PMG versão 1.1. Brasília: Comitê Executivo de Governo Eletrônico, 2014. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/PMGVersao1_1.pdf. Acesso em: 15 out. 2022.

CONSELHO DA JUSTIÇA FEDERAL. **Resolução CJF nº 7, de 7 de abril de 2008**. Institui o Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos da Justiça Federal - MoReq-Jus e disciplina a obrigatoriedade da sua utilização no desenvolvimento de novos sistemas informatizados para as atividades judiciárias e administrativas no âmbito do Conselho e da Justiça Federal de primeiro e segundo graus. Brasília: CJF, 2008. Disponível em: https://www.legisweb.com.br/legislacao/?id=109701. Acesso em: 15 out. 2022.

CONSELHO NACIONAL DE ARQUIVOS. **Carta para a preservação do patrimônio arquivístico digital**: 2005. Disponível em: http://www.conarq.arquivonacional.gov.br/Media/publicacoes/cartapreservpatrimarqdigitalconarq2004.pdf. Acesso em: 16 out 2022.

CONSELHO NACIONAL DE ARQUIVOS. **E-ARQ Brasil**: modelo de requisitos para sistemas informatizados de gestão arquivística de documentos [versão 2]. Rio de Janeiro: Câmara Técnica de Documentos Eletrônicos (CTDE), 2022a. Disponível em: https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/EARQV203MAI2022.pdf. Acesso em: 14 out. 2022.

CONSELHO NACIONAL DE ARQUIVOS. **Glossário dos documentos arquivísticos digitais.** Rio de Janeiro: Conarq, 2020. Versão 8.0 (Atual). Disponível em: https://www.gov.br/conarq/pt-br/assuntos/camaras-tecnicas-setoriais-inativas/camara-tecnica-de-documentos-eletronicos-ctde/glossario-da-ctde. Acesso em: 25 ago. 2023.

CONSELHO NACIONAL DE ARQUIVOS. **Resolução Conarq nº 20, de 16 de julho de 2004**. Dispõe sobre a inserção dos documentos digitais em programas de gestão arquivística de documentos dos órgãos e entidades integrantes do Sistema Nacional de Arquivos. Rio de Janeiro: Conarq, 2004. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-20-de-16-de-julho-de-2004. Acesso em: 15 out. 2022.

CONSELHO NACIONAL DE ARQUIVOS. **Resolução Conarq nº 24, de 3 de agosto de 2006.** Estabelece diretrizes para a transferência e recolhimento de documentos arquivísticos digitais para instituições arquivísticas públicas. Rio de Janeiro:

Conarq 2006. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-24-de-3-de-agosto-de-2006. Acesso em: 15 out. 2022.

CONSELHO NACIONAL DE ARQUIVOS. **Resolução Conarq nº 25, de 27 de abril de 2007**. Dispõe sobre a adoção do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-Arq Brasil pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR. Rio de Janeiro: Conarq 2007. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-25-de-27-de-abril-de-2007. Acesso em: 15 out. 2022.

CONSELHO NACIONAL DE ARQUIVOS. **Resolução Conarq nº 27, de 16 de junho de 2008**. Dispõe sobre o dever do Poder Público, no âmbito dos Estados, do Distrito Federal e dos Municípios, de criar e manter Arquivos Públicos, na sua específica esfera de competência, para promover a gestão, a guarda e a preservação de documentos arquivísticos e a disseminação das informações neles contidas. Rio de Janeiro: Conarq 2008. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-27-de-16-de-junho-de-2008. Acesso em: 15 out. 2022.

CONSELHO NACIONAL DE ARQUIVOS. **Resolução Conarq nº 31, de 28 de abril de 2010**. Dispõe sobre a adoção das Recomendações para Digitalização de Documentos Arquivísticos Permanentes. Rio de Janeiro: Conarq, 2010. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-31-de-28-de-abril-de-2010. Acesso em: 15 out. 2022.

CONSELHO NACIONAL DE ARQUIVOS. **Resolução Conarq nº 39, de 29 de abril de 2014**. Estabelece diretrizes para a implementação de repositórios arquivísticos digitais confiáveis para o arquivamento e manutenção de documentos arquivísticos digitais em suas fases corrente, intermediária e permanente, dos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR. [Redação dada pela Resolução nº 43 de 04 de setembro de 2015]. Rio de Janeiro: Conarq, 2014a. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-39-de-29-de-abril-de-2014. Acesso em: 15 out. 2022.

CONSELHO NACIONAL DE ARQUIVOS. **Resolução Conarq nº 41, de 9 de dezembro de 2014**. Dispõe sobre a inserção dos documentos audiovisuais, iconográficos, sonoros e musicais em programas de gestão de documentos arquivísticos dos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR, visando a sua preservação e acesso. Rio de Janeiro: Conarq, 2014b. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-41-de-9-de-dezembro-de-2014. Acesso em: 15 out. 2022.

CONSELHO NACIONAL DE ARQUIVOS. **Resolução Conarq nº 48, de 10 de novembro de 2021**. Estabelece diretrizes e orientações aos órgãos e entidades integrantes do Sistema Nacional de Arquivos quanto aos procedimentos técnicos a serem observados no processo de digitalização de documentos públicos ou privados. Rio de Janeiro: Conarq, 2021b. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-48-de-10-de-novembro-de-2021 Acesso em: 15 out. 2022.

CONSELHO NACIONAL DE ARQUIVOS. **Resolução Conarqnº 50**, **de 6 de maio de 2022**. Dispõe sobre o Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-Arq Brasil, Versão 2. Câmara Técnica de

Documentos Eletrônicos (CTDE). Rio de Janeiro: Conarq, 2022b. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-50-de-06-de-maio-de-2022. Acesso em: 14 out. 2022.

CONSELHO NACIONAL DE JUSTIÇA. **Manual de digitalização de documentos do poder Judiciário**. Brasília: CNJ, 2023. Disponível em: https://bibliotecadigital.cnj.jus.br/handle/123456789/608. Acesso em: 23 ago. 2023.

CONSELHO NACIONAL DE JUSTIÇA. **Manual de gestão documental do Poder Judiciário**. Brasília, CNJ, 2021a. Disponível em: https://bibliotecadigital.cnj.jus.br/jspui/bitstream/123456789/480/1/Manual_de_Gestao_Documental.pdf. Acesso em: 14 out. 2022.

CONSELHO NACIONAL DE JUSTIÇA. **Manual de gestão de memória do Poder Judiciário**. Brasília: CNJ, 2021b. Disponível em: https://bibliotecadigital.cnj.jus.br/jspui/bitstream/123456789/481/1/Manual_de_Gestao_de_Memoria.pdf. Acesso em: 14 out. 2022.

CONSELHO NACIONAL DE JUSTIÇA. **Portaria CNJ nº 252**, **de 5 de outubro de 2021.** Institui Grupo de Trabalho para a atualização do Modelo de Requisitos Informatizados de Gestão de Processos e Documentos do Poder Judiciário (MoReq-Jus). Brasília: CNJ, 2021c. Disponível em: https://atos.cnj.jus.br/atos/detalhar/4156. Acesso em: 15 out. 2021.

CONSELHO NACIONAL DE JUSTIÇA. **Recomendação CNJ nº 37**, **de 15 de agosto de 2011**. Recomenda aos Tribunais a observância das normas de funcionamento do Programa Nacional de Gestão Documental e Memória do Poder Judiciário – Proname e de seus instrumentos. Brasília: CNJ, 2011. Disponível em: https://atos.cnj.jus.br/atos/detalhar/846. Acesso em: 15 out. 2022.

CONSELHO NACIONAL DE JUSTIÇA. **Recomendação CNJ nº 46**, **de 17 de dezembro de 2013**. Altera a Recomendação n. 37, de 15 de agosto de 2011. Brasília: CNJ, 2013. Disponível em: https://atos.cnj.jus.br/atos/detalhar/1991. Acesso em: 2 nov. 2020.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução CNJ nº 46**, **de 18 de dezembro de 2007**. Cria as Tabelas Processuais Unificadas do Poder Judiciário e dá outras providências. Brasília: CNJ, 2007. Disponível em: https://atos.cnj.jus.br/atos/detalhar/167. Acesso em: 14 out. 2020.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução CNJ nº 65**, **de 16 de dezembro de 2008**. Dispõe sobre a uniformização do número dos processos nos órgãos do Poder Judiciário e dá outras providências. Brasília: CNJ, 2008. Disponível em: https://atos.cnj.jus.br/atos/detalhar/119. Acesso em: 14 out. 2022.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução CNJ nº 90**, **de 29 de setembro de 2009**. Dispõe sobre os requisitos de nivelamento de tecnologia da informação no âmbito do Poder Judiciário. Brasília: CNJ, 2009a. Disponível em: https://atos.cnj.jus.br/atos/detalhar/81. Acesso em: 14 out. 2022.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução CNJ nº 91**, **de 29 de setembro de 2009**. Institui o Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário e disciplina a obrigatoriedade da sua utilização no desenvolvimento e manutenção de sistemas informatizados para as atividades judiciárias e administrativas no âmbito do Poder Judiciário.

Brasília: CNJ, 2009b. Disponível em: https://atos.cnj.jus.br/atos/detalhar/78. Acesso em: 14 out. 2022.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução CNJ nº 324**, **de 30 de junho de 2020**. Institui diretrizes e normas de Gestão de Memória e de Gestão Documental e dispõe sobre o Programa Nacional de Gestão Documental e Memória do Poder Judiciário – Proname. Brasília: CNJ, 2020a. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3376. Acesso em: 15 out. 2022.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução CNJ nº 335**, **de 29 de setembro de 2020**. Institui política pública para a governança e a gestão de processo judicial eletrônico. Integra os tribunais do país com a criação da Plataforma Digital do Poder Judiciário Brasileiro – PDPJ-Br. Mantém o sistema PJe como sistema de Processo Eletrônico prioritário do Conselho Nacional de Justiça. Brasília: CNJ, 2020b. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3496. Acesso em: 15 out. 2022.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução CNJ nº 363**, **de 12 de setembro de 2021**. Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais. Brasília: CNJ, 2021d. Disponível em https://atos.cnj.jus.br/atos/detalhar/3668. Acesso em: 15 out. 2022.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução CNJ nº 370**, **de 28 de janeiro de 2021**. Estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD). Brasília: CNJ, 2021e. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3706. Acesso em: 15 out. 2022.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução CNJ nº 396**, **de 7 de junho de 2021**. Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Brasília: CNJ, 2021f. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3975. Acesso em: 15 out. 2022.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução CNJ nº 408**, **de 18 de agosto de 2021**. Dispõe sobre o recebimento, o armazenamento e o acesso a documentos digitais relativos a autos de processos administrativos e judiciais. Brasília: CNJ, 2021g. Disponível em: https://atos.cnj.jus.br/atos/detalhar/4065. Acesso em: 15 out. 2022.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução CNJ nº 468**, **de 15 de julho de 2022**. Dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça. Brasília: CNJ, 2022a. Disponível em: https://atos.cnj.jus.br/files/original155235202207186 2d581c34c4be.pdf. Acesso em: 14 out. 2022.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução CNJ nº 469**, **de 31 de agosto de 2022**. Estabelece diretrizes e normas sobre a digitalização de documentos judiciais e administrativos e de gestão de documentos digitalizados do Poder Judiciário. Brasília: CNJ, 2022b. Disponível em: https://atos.cnj.jus.br/atos/detalhar/4719. Acesso em: 15 out. 2022.

DE SORDI, Neide Alves Dias. Programa de Avaliação de Conformidade dos Sistemas Informatizados do Poder Judiciário ao MoReq-Jus: Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Judiciário. *In:* SEMINÁRIO NACIONAL DE DOCUMENTAÇÃO E INFORMAÇÃO JURÍDICA, 2., 2010, Brasília. **Anais**... Brasília: 2010. 1 CD. Republicado em: Cadernos de Informa-

ção Jurídica, Brasília, v. 6, n. 1, p. 141-171, jan./jun. 2019. Disponível em: https://www.cajur.com.br/index.php/cajur/article/view/228. Acesso em: 16 out.2022.

DE SORDI, Neide Alves Dias. MOREQ-JUS: uma contribuição do Centro de Estudos Judiciários à preservação da informação jurídica digital. **Revista CEJ**, Edição comemorativa: 20 anos do CEJ, Brasília, n. 15, p. 49-59, jul. 2011. Disponível em: https://revistacej.cjf.jus.br/cej/index.php/revcej/article/download/1514/1471/#:~:text=O%20MoReq%2DJus%20%C3%A9%20uma,%2C%20%C3%ADntegra%2C%20aut%C3%AAntica%20e%20acess%C3%ADvel. Acesso em: 15 out. 2022.

DEPARTAMENTO DE DEFESA (Estados Unidos). **Design Criteria Standard for Electronic Records Management Software Applications**. Washington: DoD, 2002. Disponível em: http://www.interpares.org/display_file.cfm?doc=dod_50152.pdf. Acesso em: 15 out. 2022.

INSTITUTO DOS ARQUIVOS NACIONAIS (Portugal). Torre do Tombo. **Recomendações para a gestão de documentos de arquivo electrónicos**: 2 modelo de requisitos para a gestão de arquivos electrónicos. Lisboa: IAN TT, 2002. Disponível em: https://arquivos.dglab.gov.pt/wp-content/uploads/sites/16/2013/10/siade_caderno2.pdf. Acesso em: 14 out. 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO 639-2:1998**: Codes for the representation of names of languages: Part 2: Alpha-3 code. Genebra: ISO, 1998.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO 8601:2019**: Date and time: Representations for information interchange. Genebra: ISO, 2019.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO 15836:2017**: Information and documentation: The Dublin Core metadata element. Genebra: ISO, 2017.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO 25010:2011**: Systems and software engineering: Systems and software Quality Requirements and Evaluation (SQuaRE): System and software quality models. Genebra: ISO, 2011.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO 27002:2022**: Information security, cybersecurity and privacy protection: Information security controls. Genebra: ISO, 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO/IEC/IEEE 24765:2017**: Systems and software engineering: Vocabulary. 2017. Genebra: ISO, 2017.

INTERPARES. **InterPARES Trust Terminology**. Disponível em: http://interpares-trust.org/terminology. Acesso em: 14 ago. 2023.

LIBRARY OF CONGRESS. **Dicionário de metadados PREMIS para metadados de preservação**. Washington, DC: Library of Congress, 2022. Disponível em: https://loc.gov/standards/premis/v3/index.html. Acesso em: 20 de julho de 2022, às 11:09.

PREMIS EDITORIAL COMITTEE. **PREMIS data dictionary for preservation metadata: version 3.0**. Washington, DC: Library of Congress, 2015. Disponível em: https://www.loc.gov/standards/premis/v3/premis-3-0-final.pdf. Acesso em: 15 out. 2022.

SOMMERVILLE, Ian. **Engenharia de software**. 9 ed. São Paulo: Pearson, 2019.

GLOSSÁRIO

Termo	Definição
Administrador	Responsável pelo projeto, desenvolvimento e manutenção da infraestrutura em que o GestãoDoc, os documentos digitais e não digitais são mantidos.
Administrador do sistema	Responsável pelo gerenciamento das regras de negócio do sistema. Cabe ao administrador do sistema, entre outras atividades, a configuração e atribuição de perfis de usuários. (termo similar ao de "Gestor")
Ambiente Computacional	Ambiente físico em que são acomodados equipamentos de informática, tais como racks, switches, equipamentos de comunicação, equipamentos servidores, robôs de backup etc. São exemplos de ambiente computacional os CPD´s, as salas-cofre, salas seguras etc.
Anexação	Ato de reunir documentos organizados em volumes próprios a um determinado processo. Os documentos que formam os anexos tramitam junto ao processo, mas não são autuados como um processo.
Anexo	Documentos organizados em volume próprio, que acompanham um processo, mas não são autuados como um processo. Documentos que acompanham e estão vinculados a um documento principal ou mensagem, independentemente do suporte em que se apresentam.
Apensação ou Apensamento	Reunião de dois ou mais processos, permanecendo cada processo com seu respectivo número. Nos processos judiciais, a apensação ocorre por determinação legal ou judicial em processos que estejam em movimento, suspensos ou baixados. Nos processos administrativos, a apensação ocorre por determinação da autoridade competente.
Arquivista	1. Profissional de nível superior, com formação em arquivologia ou experiência reconhecida pelo Estado (ARQUIVO NACIONAL, 2005, p. 26). 2. Responsável pela proposição de estudos e projetos de gestão de documentos, elaboração de instrumentos de gestão documental e acesso, bem como pela disseminação das técnicas e funções arquivísticas e a preservação do acervo de guarda permanente .
Atualização de suporte	Técnica de migração que consiste em copiar os dados de um suporte para outro sem mudar sua codificação, para evitar perdas de dados provocadas por deterioração do suporte. (Conarq, 2020, p. 11).
Autenticidade	Credibilidade de um documento enquanto documento, isto é, a qualidade de um documento ser o que diz ser e que está livre de adulteração ou qualquer outro tipo de corrupção. A autenticidade é composta de identidade e integridade (Conarq, 2020, p. 12).
Autuação	Formar autos. Reunir em forma de processo (a petição e documentos apresentados em juízo), designando número, identificando partes, procuradores, assunto, classe processual e outras informações relevantes.
Avaliação de Documentos	Processo de análise de documentos, que estabelece os prazos de guarda e a destinação, de acordo com os valores que lhes são atribuídos (Conarq, 2020, p. 13).
Captura	Incorporação de documento ao sistema.
Checksum	Sequência de *bits* obtida a partir de um conjunto de dados de origem calculado na origem e no destino, normalmente com o objetivo de assegurar que não houve erro durante a transmissão, armazenamento ou recuperação desses dados. Essa sequência pode ser resultado de uma função de verificação (função *checksum*) que pode utilizar diversos algoritmos, inclusive alguns *hash* criptográficos.
Ciclo de vida dos Documentos	As sucessivas etapas pelas quais os documentos passam: produção, tramitação, uso, avaliação, arquivamento e destinação (guarda permanente ou eliminação) (ARQUIVO NACIONAL, 2005, p.39).

Classe	Primeira divisão de um plano de classificação ou de um código de classificação. Nos requisitos e metadados do **MoReq-Jus**, o termo **classe** é compreendido como a designação genérica que inclui qualquer das classificações em níveis e subníveis existentes nas estruturas dos planos de classificação, como por exemplo classes, subclasses e assuntos da área meio e classes, assuntos, movimentos e documentos da área judicial, incluindo seus desdobramentos.
Código de classificação	Conjunto de símbolos, normalmente letras e/ou números, derivados de um plano de classificação.
Código *hash*	Sequência de *bits* de comprimento fixo resultado de uma função que mapeia uma sequência de *bits* de comprimento variável para um conjunto de *bits,* assegurando, a um só tempo, que seja computacionalmente improvável que: (a) para um dado conjunto de dados de entrada, outro conjunto de dados resulte no mesmo código *hash* (colisão); e b) para um dado código *hash* seja possível identificar o conjunto de dados de entrada.
Componente digital	Objeto digital que é parte de um ou mais documentos digitais, incluindo os metadados necessários para ordenar, estruturar ou manifestar seu conteúdo e forma, que requer determinadas ações de preservação. Um documento arquivístico digital pode ser composto por um ou mais componentes digitais (Conarq, 2020, p. 18). Exemplo: uma fotografia digital tem apenas um componente digital, que é o arquivo com a imagem, já um documento multimídia tem diversos componentes digitais, que são os arquivos com o código executável, os textos, as imagens e os registros sonoros.
Confiabilidade	Credibilidade quanto à produção de um documento arquivístico, e sua validação como afirmação do fato.
Conversão	Técnica de migração que pode se configurar de diversas formas, tais como: 1. conversão de dados: mudança de um formato para outro. 2. conversão de sistema computacional: mudança do modelo de computador e de seus periféricos.
Desapensação ou Desapensamento	Separação de processos que estavam apensados. Nos processos judiciais, geralmente, é o efeito de uma decisão judicial que determina a separação de processos que estavam reunidos. No caso dos processos administrativos, a desapensação ocorre por determinação da autoridade competente.
Desentranhamento	Ato de retirar peças juntadas em processo judicial ou administrativo.
Desmembramento	Ato de dividir um processo em dois ou mais processos. Ocorre nos processos judiciais por decisão judicial e nos administrativos por determinação da autoridade competente.
Destinação	Decisão, com base na avaliação, quanto ao encaminhamento dos documentos para a guarda permanente ou eliminação (Conarq, 2020, p. 23).
Documento automodificável	Aquele cujos conteúdos podem ser alterados sem intervenção do usuário.
Documento Digital	Informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional.
Documento não digital	Documento que se apresenta em suporte, formato e codificação diferente dos digitais, tais como: documentos em papel, documentos em películas e documentos eletrônicos analógicos (Conarq, 2020, p. 26).
Documento híbrido	Documento composto por parte digital e parte não digital.
Documento institucional	Documento produzido e/ou recebido por um órgão do Poder Judiciário, no decorrer das suas atividades, qualquer que seja o suporte, e dotado de organicidade.

Documento institucional digital	Documento codificado em dígitos binários, acessível por meio de sistema computacional.
Dossiê	Conjunto de documentos relacionados entre si por ação, evento, pessoa, lugar, projeto, que constitui uma unidade (Conarq, 2020, p. 26).
Emulação	Utilização de recursos computacionais que fazem uma tecnologia funcionar com as características de outra, aceitando as mesmas entradas e produzindo as mesmas saídas.
Ergonomia cognitiva	Processos mentais, tais como percepção, memória, raciocínio e resposta motora conforme afetem as interações entre seres humanos e outros elementos de um sistema. Os tópicos relevantes incluem o estudo da carga mental de trabalho, tomada de decisão, desempenho especializado, interação homem computador, estresse e treinamento conforme esses se relacionem a projetos envolvendo seres humanos e sistemas.
Fluxo de trabalho	Automatização de uma atividade, no todo ou em parte, durante a qual documentos, informação ou tarefas transitam de um participante para outro com vistas a serem submetidos a ações, de acordo com um conjunto de normas processuais.
Gestor	Responsável por gerenciar o sistema GestãoDoc, em tarefas tais como as de configuração e atribuição de perfis.
Memória primária	De funcionamento essencial, é necessária a qualquer sistema computacional. É nela que o software e os dados são armazenados durante a execução. Representantes típicas dessa classe são as memórias *Random Access Memory (*RAM). São memórias extremamente rápidas, de conteúdo dinâmico e volátil, permanecendo registrado apenas durante a execução do software.
Memória secundária	Apresenta volume maior de armazenamento que a primária; entretanto é mais lenta e não-volátil. São exemplos os discos rígidos magnéticos (*hard disk* - HD), que podem ser usados isolados ou combinados em *disk arrays*. Diversas tecnologias permitem, através do uso de *disk arrays*, obter-se maior desempenho e confiabilidade do que com os discos isoladamente..
Memória terciária	Compreende fitas magnéticas, discos ópticos e outros. Usos típicos incluem armazenamento do acervo digital e cópias de segurança. Outra nomenclatura corrente para essa classe de memória é “mídias de armazenamento”. A memória terciária tem característica não volátil na preservação de dados. Seu preço unitário é tão pequeno que requisitos de confiabilidade devem prevalecer: em caso de desastre, o prejuízo da perda de dados é superior ao preço das mídias que fisicamente os contêm.
Metadado	Informação que descreve e contextualiza o dado. Dado estruturado que descreve e permite encontrar, gerenciar, compreender e/ou preservar documentos arquivísticos ao longo do tempo (Conarq, 2020, p. 36).
Minuta	Versão preliminar de documento sujeita à aprovação (ARQUIVO NACIONAL, 2005, p. 123).
Objeto digital	1. Uma unidade de informação que inclui propriedades (atributos ou características do objeto) e também pode incluir métodos (meios de realizar operações no objeto). 2. Representação de uma unidade discreta de informação na forma digital. Um objeto digital pode ser uma representação (*representation*), um arquivo (*file*), uma cadeia de bits (*bitstream*) ou uma cadeia de arquivos (*filestream*).(Dicionário de Dados PREMIS, 2012).

Plano de classificação	1. Esquema de distribuição de documentos em classes, de acordo com métodos de arquivamento específicos, elaborado a partir do estudo das estruturas e funções de uma instituição e da análise do arquivo por ela produzido. Expressão geralmente adotada em arquivos correntes (ARQUIVO NACIONAL, 2005, p. 132); 2. Instrumento de gestão arquivística, que apresenta a organização hierárquica para classificação dos documentos, com o estabelecimento de classes, seguindo um critério funcional ou estrutural, como por exemplo, para uma instituição voltada para prestação jurisdicional, a conjugação das áreas do Direito (Assuntos) com o tipo de procedimento (Classes) adotado numa petição inicial e para a área administrativa a representação lógica das funções, subfunções e atividades do organismo produtor.
Preservação digital	Conjunto de ações gerenciais e técnicas exigidas para superar as mudanças tecnológicas e a fragilidade dos suportes, garantindo o acesso , a integridade e a interpretação de documentos digitais pelo tempo que for necessário (Conarq, 2020, p. 39)..
Processo	Conjunto de documentos oficialmente reunidos no decurso de uma ação administrativa ou judicial, que constitui uma unidade (Conarq, 2020, p. 39).
Recolhimento	Entrada de documentos em arquivos permanentes (ARQUIVO NACIONAL, 2005, p. 133).
Repositório Arquivístico digital Confiável - RDC-ARQ	Ambiente de preservação dos documentos arquivísticos digitais capaz de manter autênticos os materiais digitais nele custodiados, de modo a preservá-los e dar acesso a eles pelo tempo necessário.
Requisito Funcional	Descreve as funções que o software deve executar, sendo também conhecido como capacidade ou recurso. Um requisito funcional também pode ser descrito como aquele para o qual um conjunto finito de etapas de teste pode ser escrito para validar seu comportamento.
Requisito Não Funcional	Deve ser respeitado pela solução, sendo também conhecido como restrição ou requisito de qualidade. Ele pode ser classificado como requisito de desempenho, manutenção, segurança, confiabilidade, interoperabilidade ou um dos muitos outros tipos de requisitos de software.
Tabela de temporalidade	Instrumento de destinação, aprovado por autoridade competente, que determina prazos e condições de guarda tendo em vista a transferência, recolhimento, descarte ou eliminação de documentos. (ARQUIVO NACIONAL, 2005, p. 159)
Teoria das três idades	Base do conceito de gestão de documentos, essa teoria os classifica em três fases: Corrente: Documentos que estão em curso (tramitando ou arquivados), mas objeto de consultas frequentes. São conservados nos locais onde foram produzidos sob a responsabilidade do órgão produtor. Intermediária: Documentos que não são mais de uso corrente, mas que por conservarem ainda algum interesse administrativo, aguardam no arquivo intermediário o cumprimento do prazo estabelecido nos instrumentos de classificação, temporalidade e destinação, para serem eliminados ou recolhidos ao arquivo permanente. Permanente: Documentos que devem ser definitivamente preservados em função de seu valor histórico, probatório ou informativo.
Tramitação	Curso do documento desde sua produção ou recepção até o cumprimento de sua função administrativa ou judicial. Também chamado movimentação ou trâmite.
Transferência	Passagem de documentos do arquivo corrente para o arquivo intermediário (ARQUIVO NACIONAL, 2005, p. 165).

Trilha de auditoria	Conjunto de informações registradas que permite o rastreamento de intervenções ou tentativas de intervenções feitas no documento arquivístico digital ou no sistema computacional. (I) *Audit Trail*. (Conarq, 2020, p. 46).
Unidade de arquivamento	Documento tomado por base para fins de classificação, arranjo, armazenamento e notação. Uma unidade de arquivamento pode ser um dossiê, um processo ou ainda uma pasta em que estão reunidos documentos sob o mesmo código de classificação, como por exemplo, as folhas de ponto de um determinado ano, relatórios de atividades relativos a um determinado período ou atas de reunião.
Usuário	1.Gestão de documentos - Responsáveis, em todos os níveis, pela produção e uso dos documentos institucionais em suas atividades rotineiras, conforme estabelecido pelo programa de gestão. Aquele que é identificável, habilitado a interagir com o sistema. 2. GestãoDoc - Aquele que é cadastrado e que interage com o sistema.
Usuário autorizado	Aquele que possui níveis de acesso diferenciados atribuídos pelo gestor.
Valor primário	Atribuído aos documentos considerando sua utilidade administrativa imediata, que são, de fato, as razões pelas quais esses documentos foram criados.
Valor secundário	Refere-se ao valor atribuído aos documentos em função do interesse que possam ter para a entidade produtora e outros usuários, tendo em vista a sua utilidade para fins diferentes daqueles para os quais foram originalmente produzidos (ARQUIVO NACIONAL, 2005, p. 172)..
Versão	Estado de um documento em determinada fase de sua elaboração.
Via original	Primeiro documento completo e efetivo.

ANEXO A - QUADRO DE REFERÊNCIAS NORMATIVAS

As diretrizes gerais elencadas abaixo devem ser atendidas a fim de assegurar que o GestãoDoc seja concebido e opere em conformidade com as previsões legais, normativas e regulatórias estabelecidas para o Poder Judiciário, assim como de acordo com os padrões e práticas amplamente reconhecidos.

O arcabouço normativo definido no capítulo 1 constitui a base para o detalhamento das diretrizes elencadas abaixo.

MoReq-Jus.	Fundamentos legais, regulatórios, normativos e de padronização
Estar alinhado com as diretrizes e os objetivos definidos para a estratégia nacional do Poder Judiciário.	• Resolução CNJ 325/2020 - ENPJ - e atualizações posteriores periódicas; e • Resolução CNJ 370/2021 - ENTIC-JUD.
Ter como foco prioritário a redução da taxa de congestionamento dos processos e a significativa melhoria na qualidade dos serviços prestados..	• Resolução CNJ 325/2020 – ENPJ; e • Resolução CNJ 335/2021 - PDPJ-Br - art. 4º, XVII.
Seguir as diretrizes para o desenvolvimento de sistema estabelecidas pelo CNJ, boas práticas e princípios gerais amplamente reconhecidos no mercado.	• Resolução CNJ 370/2021 - ENTIC-JUD - art. 21, III e arts. 28 a 33; • Resolução CNJ 335/2021 - PDPJ-Br -art. 2º, III e art. 4º; • Resolução CNJ 185/2013 – PJe - arts. 31 e 47; e • SWEBOK.
Ser projetado para o desenvolvimento comunitário e compartilhamento entre todos os segmentos e esferas do Poder Judiciário.	• Resolução CNJ 370/2021 - ENTIC-JUD - art. 7º, IV e VI; art. 21, b e art. 28, § único; e • Resolução CNJ 335/2021 - PDPJ-Br - art. 2º, II e art. 4º, II.
Ser dada preferência ao uso de sistemas de informação já desenvolvidos, disseminados e experimentados no âmbito do Poder Judiciário.	• Resolução CNJ 370/2021 - ENTIC-JUD - art. 33, VI; e • Resolução CNJ 335/2021 - PDPJ-Br, art. 2º.
Ser desenvolvido em plataforma pública com a utilização preferencial de tecnologias com código aberto (*open source*).	• Resolução CNJ 335/2021 - PDPJ-Br art. 4º, I e XIX.
Assegurar a independência tecnológica de fornecedores quanto ao direito de propriedade do que for desenvolvido..	• Resolução CNJ 370/2021 - ENTIC-JUD – art.32; e • Resolução CNJ 335/2021 - PDPJ-Br, art. 5º.
Ser portável e interoperável.	• Resolução CNJ 370/2021 - ENTIC-JUD – art.15, II e art. 33, I; • Resolução CNJ 335/2021 - PDPJ-Br, art. 4º, VII e VIII; • Resolução CNJ 185/2013 – PJe – art. 29, § 3º; • Resolução Conjunta CNJ/CNMP 3/2013 – MNI – arts 1º e 2º; • Resolução CNJ 331/2020 – DataJud; • Resolução CNJ 446/2022 – CODEX; e • Padrões de Interoperabilidade de Governo Eletrônico (e-PING).

Estar em conformidade com a política de segurança da informação dos órgãos do Poder Judiciário e a nacional do CNJ.	• Resolução CNJ 396/2021 – ENSEC-PJ; • Resolução CNJ 370/2021 - ENTIC-JUD – art.21, II; art. 31; e 36 a 41; • Resolução CNJ 335/2021 - PDPJ-Br, art. 4º, XII; • Resolução CNJ 185/2013 – PJe – art.6º, § 2º; e • Norma NBR ISO27001:2013 – Segurança.
Estar em conformidade com a Lei de Acesso à Informação, com a Lei Geral de Proteção de Dados Pessoais e com as diretrizes de dados abertos definidas para o Poder Judiciário.	• Lei nº 13.709/2018 – Lei Geral de Proteção de dados Pessoais (LGPD); • Lei nº 12.527/2011 - Lei de Acesso à Informação (LAI); • Resolução CNJ 363/2021 - LGPD; • Resolução CNJ 334/2020 – Dados abertos; e • Resolução CNJ 21/2015 - LAI.
Prover autenticação uniformizada.	• Resolução CNJ 370/2021 - ENTIC-JUD – art.29; • Resolução CNJ 335/2021 - PDPJ-Br, art. 3º, VI e art. 9º, IV; e • Resolução CNJ 185/2013 – PJe – art. art. 4º - A, caput, § 1º, § 2º e § 3º.
Prover mecanismos de identificação inequívoca do signatário (assinatura digital).	• Lei 11.419/2006, art. 1º, § 2º, III; • Lei 14.063/2020 - Lei de Assinaturas Eletrônicas; • Resolução CNJ 370/2021 - ENTIC-JUD – art.33, IV; e • Resolução CNJ 185/2013 – PJe - art. 3º, I; art. 4º, caput, § 3º; art. 4º - A, caput, § 1º, § 2º e art. 4º -D.
Prover mecanismos de validação da autenticidade.	• Resolução CNJ 185/2013 – PJe - art. 4º, § 1º.
Prover mecanismos para assegurar o controle de acesso e sigilo dos documentos.	• Lei Federal nº 13.709/2018 - LGPD; • Lei nº 12.527/2011 - Lei de Acesso à Informação (LAI); • Resolução CNJ 185/2013 – PJe – arts. 27 e 28; • Resolução nº 215/2015; • Resolução CNJ 121/2010 – Divulgação de dados na rede mundial; e • Resolução CNJ 335/2021 - PDPJ-Br, art. 4º.
Adotar práticas de desenvolvimento de *software* preocupadas com a acessibilidade e a usabilidade.	• Lei nº 12.527/2011 - Lei de Acesso à Informação (LAI); • Resolução CNJ 401/2021; • Resolução CNJ 370/2021 - ENTIC-JUD – art.33, V; • Resolução CNJ 335/2021 - PDPJ-Br, art. 4º, X e XI; e art. 9º, VI; e • Modelo de Acessibilidade em Governo Eletrônico (e-Mag).
Prover automações de atividades rotineiras ou sequenciais e a otimização e a padronização de fluxos de trabalho.	• Resolução CNJ 370/2021 - ENTIC-JUD – art.3º e art. 18, § 2º; • Resolução CNJ 335/2021 - PDPJ-Br, art. 4º, XIV e XV; e art. 9º, V; e • Resolução CNJ 185/2013 – PJe - art. 4º -D; art. 5º, § 2º; art. 22; art. 28, § 3º; art. 29, § 3º.
Ser adaptável ao uso de ferramentas de aprendizado de máquina, ao incremento da robotização e a adoção de técnicas disruptivas de desenvolvimento de soluções.	• Resolução CNJ 335/2021 - PDPJ-Br, art. 4º e XII, XVI; e • Resolução CNJ 332/2020 – Inteligência Artificial.
Ser responsivo e disponível para dispositivos móveis.	• Resolução CNJ 370/2021 - ENTIC-JUD – art.33, II; e • Resolução CNJ 335/2021 - PDPJ-Br, art. 4º e IX.
Possuir ampla cobertura de testes, baixo acoplamento, alta coesão e modularização.	• Resolução CNJ 335/2021 - PDPJ-Br, art. 4º, III.

Possuir documentação atualizada.	• Resolução CNJ 370/2021 - ENTIC-JUD – art.33, III.
Adotar serviços em nuvem que simplifiquem a estrutura física, viabilizem segurança da informação, proteção de dados, disponibilidade e padronização do uso dessa tecnologia no Poder Judiciário.	• Resolução CNJ 370/2021 - ENTIC-JUD – art.35; e • Resolução CNJ 335/2021 - PDPJ-Br, art. 2º,IV, e 4º,V, XIV e XV; e art. 9º, V.
Estar em conformidade com as diretrizes e normas de gestão de memória e de gestão de documentos definidos para o Poder Judiciário.	• Resolução 324/2020 - Proname.
Receber, digitalizar, capturar, armazenar e prover acesso a documentos digitais conforme as diretrizes estabelecidas para o Poder Judiciário.	• Resolução CNJ 408/2021; • Resolução CNJ 420-2021 – Digitalização; • Resolução CNJ 469/2022; e • Resolução CNJ 185/2013.
Estar em conformidade com as políticas de sustentabilidade estabelecidas para o Poder Judiciário.	• Resolução CNJ 400/2021, art. 2º; • Resolução CNJ 335/2020 - PDPJ, art. 13, II; e • Resolução CNJ 468/2022 - STIC, art. 32.

ANEXO B - METADADOS

Metadado consiste em um "dado estruturado, que permite classificar, descrever e gerenciar documentos e processos" (Art. 2º, VIII da Resolução CNJ nº 469/2022).

Os metadados complementam o MoReq-Jus e identificam os documentos (documentos, processos ou dossiês, que podem apresentar-se em formato não digital, híbrido ou digital) e as ações de gestão documental.

Os metadados deste Modelo foram elaborados com base na Resolução Conarq nº 50/2022, que dispõe sobre o e-Arq Brasil versão 2, e adaptados para atender as normas do Programa Nacional de Gestão Documental e de Memória do Poder Judiciário (Proname) e as peculiaridades de seus órgãos compostos por Tribunais e Conselhos.

Os metadados estão presentes em todas as fases do sistema, desde a captura até a destinação final.

A metodologia adotada envolveu a análise do e-Arq Brasil e a inclusão de metadados previstos em normativos do Poder Judiciário e destinados a atender essas especificidades. Além disso, foram analisados os metadados utilizados no Dicionário de Dados PREMIS para aqueles relacionados à Preservação**.**

São premissas da entidade Documento no GestãoDoc:

- São incorporados quando capturados ou produzidos pelo GestãoDoc;
- Podem agregar-se formando processos/dossiês ou ainda serem gerenciados individualmente;
- Os processos/dossiês, por sua vez, podem ser divididos em volumes;
- Todos os documentos receberão uma classificação no momento da produção ou da captura. Aqueles inseridos em processo/dossiê receberão a classificação do processo/dossiê em que foram inseridos. Em caso de documentos em processos judiciais, deverá ser observada a classificação da tabela respectiva; e
- Todo documento digital é composto por um ou mais componentes digitais.

O **Documento** está sujeito a diferentes tipos de eventos:

- **Evento de gestão do ciclo de vida** - Uma série de eventos relativos à gestão do ciclo de vida incidem sobre o documento/processo/dossiê e devem ser registrados no GestãoDoc, quais sejam, captura, classificação, desclassificação, eliminação, transferência, recolhimento, entre outros. Um agente será responsável pelo registro dos eventos do ciclo de vida do documento.
- **Evento de gestão dos processos/dossiês** – refere-se aos procedimentos realizados com os processos/dossiês, como abertura de volume/processo/dossiê, encerramento de volume/processo/dossiê, tramitação, juntada, desapensação, desentranhamento, desmembramento, entre outros. Um evento de gestão dos processos/dossiês pode estar relacionado com um documento (quando aplicável), com um processo e com um agente responsável pela ação.

O **Documento** também pode ser segregado em classes:

- **Classe** - refere-se aos diversos níveis de agregação dos instrumentos de classificação adotados no Poder Judiciário brasileiro. Quando um requisito trata da classe ou nível específico de classificação, estão sendo considerados todos os níveis dos planos de classificação.

Em cada classe, estão também associadas informações a respeito da temporalidade e da destinação prevista para os documentos nela classificados. Os instrumentos de classificação são subdivididos em:

- Administrativo: por uma hierarquia de classes, subclasses, grupos, subgrupos numa estrutura de árvore, que podem ser identificados por códigos;
- Judicial: Tabelas Processuais Unificadas de classes, assuntos, movimentos e documentos (Resolução CNJ nº 46/2007).

Um documento/processo/dossiê não pode receber uma classificação genérica, havendo níveis ou classes subordinadas e mais específicas. As classes estão relacionadas a:

- outras classes a ela subordinadas;
- processo/dossiê;
- documentos; e
- evento de gerenciamento de classe.

As classes também estão sujeitas à ocorrência de eventos:

- **Evento de gerenciamento de classe -** refere-se às ações de manutenção dos planos de classificação e tabelas de temporalidade administrativa e judicial, tais como: alteração de nome da classe, alteração de subordinação, alteração de temporalidade prevista, entre outros.

Evento de gerenciamento de classe relaciona-se com a classe e com o agente responsável pela ação.

- **Componente digital** - refere-se aos objetos digitais que compõem o documento digital. De modo geral, pode-se dizer que componentes digitais são os arquivos de computador que contêm as informações de conteúdo, forma e composição necessárias à apresentação do documento arquivístico.

Uma série de eventos de preservação incidem sobre os componentes digitais para permitir o acesso ao longo do tempo, devendo ser registrados no GestãoDoc.

Em termos de relacionamentos, cada documento está relacionado a um ou mais componentes digitais, assim como cada componente digital está relacionado a uma série de eventos de preservação.

- **Evento de preservação** – são as ações de preservação realizadas nos componentes digitais, tais como migração (atualização, conversão), compressão, validação e decifração.

Um evento de preservação relaciona-se com o componente digital e com o agente responsável pela ação de preservação.

- **Agente** - refere-se aos usuários que utilizam o GestãoDoc. Um Agente pode relacionar-se e ser responsável por um ou mais dos seguintes eventos: gestão do ciclo de vida, gestão dos processos/dossiês, preservação e/ou gerenciamento de classe.

Em algumas situações, as ações podem ser realizadas automaticamente pelo sistema, sendo o próprio sistema o Agente.

O documento digital é a apresentação, em formato acessível ao ser humano ou a um sistema, de um ou vários componentes digitais que estão relacionados entre si. Os documentos arquivísticos digitais relacionam-se e formam agregações conceituais em processos e dossiês, que podem conter volumes e/ou documentos.

Os elementos de metadados referentes à informação de data e hora deverão ser registrados em conformidade com a ISO 8601:2019 *Date and time - Representations for information interchange*.

B.1.1 Documento

Os metadados previstos são:

- MDOC1 - Identificador do documento
- MDOC2 - Número do documento
- MDOC3 - Identificador do processo/dossiê
- MDOC4 - Número do processo
- MDOC5 - Tipo de meio
- MDOC6 - Status
- MDOC7 - Identificador de versão
- MDOC8 - Título
- MDOC9 - Descrição
- MDOC10 - Assunto
- MDOC11 - Autor
- MDOC12 - Destinatário
- MDOC13 - Originador
- MDOC14 - Redator
- MDOC15 - Interessado
- MDOC16 - Identificador do componente digital
- MDOC17 - Gênero
- MDOC18 - Espécie
- MDOC19 - Tipo
- MDOC20 - Idioma
- MDOC21 - Quantidade de folhas
- MDOC22 - Numeração sequencial dos documentos
- MDOC23 - Indicação de anexos
- MDOC24 - Indicação de anotação
- MDOC25 - Relação com outros documentos
- MDOC26 - Níveis de acesso

- MDOC27 - Previsão de desclassificação
- MDOC28 - Data de produção
- MDOC29 - Local de produção
- MDOC30 - Classe
- MDOC31 - Destinação prevista
- MDOC32 - Prazo de guarda
- MDOC33 - Indicação de precedente qualificado
- MDOC34 - Localização
- MDOC35 - Indicação de arquivamento

Para os elementos de metadados referentes à identificação do **Documento** foi elaborada uma ficha individual que detalha cada elemento e apresenta as seguintes informações:

Código de identificação			
Rótulo			
Definição			
Objetivo			
Aplica-se a	Processo/Dossiê	Volume	Documento
Repetibilidade			
Nota de aplicação			
Exemplos			
Regra de preenchimento			
Requisito			
Equivalência			

- **Código de identificação e Nome:** indicação do código e do nome atribuídos ao elemento.
- **Rótulo:** nome padrão utilizado para identificar o elemento a fim de facilitar a interoperabilidade de sistemas. O padrão de rotulagem especificado neste modelo pode ser alterado para adoção de padrão já utilizado para desenvolvimento de sistemas no órgão.
- **Definição:** indica que informação deve ser registrada no elemento de metadado.
- **Objetivo:** a referência do que se pretende alcançar com a aplicação do elemento.
- **Aplica-se a:** indica a obrigatoriedade da aplicação do elemento para cada nível de agregação: documento, volume, processo/dossiê. Os valores possíveis são: *obrigatório (O); obrigatório se aplicável (OA); facultativo (F);* ou *não se aplica (NA).*
- **Repetibilidade:** indica se a informação pode ser registrada mais de uma vez para um mesmo documento, volume ou processo/dossiê.
- **Nota de aplicação:** sugere formas de aplicação do elemento.
- **Exemplos:** apresenta alguns exemplos de aplicação que explicam o elemento.
- **Regra de preenchimento:** regra que especifica os valores, a codificação ou a lista de autoridades (lista de valores autorizados) convencionados para o preenchimento do elemento.
- **Requisito:** apresenta os requisitos relacionados com o elemento de metadado.
- **Equivalência:** referências para elementos equivalentes de outros esquemas de metadados.

Alguns elementos de metadados de identificação são aplicáveis aos três, em dois ou em apenas um dos níveis de agregação (processo/dossiê, volume e documento).

Código de identificação	**MDOC1 - Identificador do documento**		
Rótulo	**moreqjus.documento.id**		
Definição	Identificador único atribuído pelo GestãoDoc ao documento no ato de sua captura para o sistema.		
Objetivo	Identificar de forma unívoca o documento para que o GestãoDoc possa gerenciá-lo.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	NA	NA	O
	Ver elemento MDOC3		
Repetibilidade	Não repetível		
Nota de aplicação	Aplicável no âmbito do GestãoDoc. Esse identificador deve ser unívoco e persistente.		
Exemplos	documento.id: 215380731205429610290807115 47		
Regra de preenchimento	Deve, preferencialmente, ser gerado de forma automática pelo GestãoDoc. As instituições devem seguir normas específicas em seu âmbito de atuação ou esfera de competência para geração desse identificador.		
Requisito	RPC3.6.2 / RCA4.1.6 / RCA4.1.7 / RCA4.1.9 / RFT5.3.3/ RPA7.2.9		
Equivalência	e-PMG: identificador.idDoSistema (identifier.systemID)		

Código de identificação	**MDOC2 - Número do documento**		
Rótulo	**moreqjus.documento.numero**		
Definição	Número ou código alfanumérico atribuído ao documento no ato da sua produção.		
Objetivo	Permitir a identificação precisa de um documento.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	NA	NA	OA
	Ver elemento MDOC4		
Repetibilidade	Não repetível		
Nota de aplicação	Em geral é uma numeração seriada correspondente a uma espécie documental, tal como ofícios, avisos, portarias, ordens de serviço e outros. Pode ser acrescido da data de produção e da sigla do órgão produtor.		
Exemplos	OFÍCIO JUD - 4262855 - DILOG-DARQ Portaria CNJ nº 252/2021;		
Regra de preenchimento	Deve, preferencialmente, ser gerado de forma automática pelo GestãoDoc. As instituições devem seguir normas específicas em seu âmbito de atuação ou esfera de competência para geração desse número.		
Requisito	RCA4.1.6		
Equivalência	--		

Código de identificação	**MDOC3 - Identificador do processo/dossiê**		
Rótulo	**moreqjus.processoDossie.id**		
Definição	Identificador único atribuído pelo GestãoDoc ao processo ou dossiê no ato de sua captura para o sistema.		
Objetivo	Identificar de forma unívoca e persistente o processo ou dossiê para que o GestãoDoc possa gerenciá-lo. Estabelecer a relação entre o processo ou dossiê e os Volumes e Documentos que os integram.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	O	NA	NA
Repetibilidade	Não repetível	-	-
Nota de aplicação	Aplicável no âmbito do GestãoDoc. Pode ser um elemento identificador simples e conter um componente para localização em ambiente eletrônico. Esse identificador não está disponível para o usuário. É um controle interno do sistema. Esse identificador tem de ser unívoco e persistente.		
Exemplos	--		
Regra de preenchimento	Deve, preferencialmente, ser gerado automaticamente pelo GestãoDoc. As instituições devem seguir normas específicas em seu âmbito de atuação ou esfera de competência.		
Requisito	RPC3.6.2 / RCA4.1.7 / RCA4.1.9 / RPA7.2.9		
Equivalência	e-PMG: identificador.idDoSistema (identifier.systemID)		

Código de identificação	**MDOC4 - Número do processo**		
Rótulo	moreqjus.processo.protocolo		
Definição	Número ou código alfanumérico de registro no protocolo do processo.		
Objetivo	Identificar o número de registro no protocolo do processo. Permitir o controle dos registros de autuações de processos. Permitir a pesquisa sobre processos.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	O	NA	NA
			Ver elemento MDOC2
Repetibilidade	Não repetível	-	-
Nota de aplicação	Em alguns casos o número de registro no protocolo do documento avulso é atribuído seguindo a mesma sistemática do processo. Assim, os metadados MDOC2 e MDOC4 podem ser tratados como o mesmo elemento de metadados e registrados no mesmo campo.		
Exemplos	Processo judicial nº 0056516-25.2005.8.06.0001 Processo judicial nº 0196701-69.2012.8.06.0001 Processo administrativo nº 8.2022.7228/000002-2		
Regra de preenchimento	As instituições devem seguir normas específicas em seu âmbito de atuação ou esfera de competência. No âmbito do processo judicial observar a Resolução CNJ nº 65/2008, que dispõe sobre a uniformização do número dos processos nos órgãos do Poder Judiciário e dá outras providências. Deve, preferencialmente, ser gerado automaticamente pelo GestãoDoc.		
Requisito	RCA4.1.7 / RCA 4.1.8		
Equivalência	--		

Código de identificação	**MDOC5 - Tipo de meio**		
Rótulo	moreqjus.documento.meio moreqjus.processo.meio		
Definição	Identificação do meio do documento/volume/processo/dossiê: digital, não digital ou híbrido.		
Objetivo	Identificar se o documento/volume/processo/dossiê é digital, não digital ou híbrido para controlar as relações entre os meios e o monitoramento de preservação.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	F	NA	O
Repetibilidade	Não repetível	-	Não repetível
Nota de aplicação	No documento/volume/processo/dossiê híbrido, os relacionamentos deverão ser registrados para identificar a parte não digital e a parte digital. Ver elemento MDOC25 (Relação com outros documentos).		
Exemplos	--		
Regra de preenchimento	--		
Requisito	RPC3.6.2 / RCA4.6.1 / RCA4.6.3 / RAD6.2.11		
Equivalência	Nobrade: 1.5 Dimensão e suporte / 4.4 Características físicas e requisitos técnicos		

<table>
<tr><td>Código de identificação</td><td colspan="3">MDOC6 - Status</td></tr>
<tr><td>Rótulo</td><td colspan="3">moreqjus.documento.status</td></tr>
<tr><td>Definição</td><td colspan="3">Indicação do grau de formalização do documento:
· minuta - versão preliminar do documento;
· original – primeiro documento completo e efetivo; e
· cópia – resultado da reprodução do documento; representante digital, no caso da reprodução de documento físico.</td></tr>
<tr><td>Objetivo</td><td colspan="3">Identificar o grau de formalização do documento e as relações existentes entre os originais, as minutas e as cópias.
Manter um controle sobre a disposição de cópias.</td></tr>
<tr><td rowspan="2">Aplica-se a</td><td>Processo/Dossiê</td><td>Volume</td><td>Documento</td></tr>
<tr><td>NA</td><td>NA</td><td>O</td></tr>
<tr><td>Repetibilidade</td><td>-</td><td>-</td><td>Não repetível</td></tr>
<tr><td>Nota de aplicação</td><td colspan="3">Deverá haver relacionamento entre os vários graus de formalização dos documentos.
O órgão deverá ter um plano de organização e registro do status dos documentos e da forma de relacioná-los.
No caso de o GestãoDoc apoiar a elaboração de documentos, o metadado status registra o grau de formalização do documento: minuta, quando ainda está sendo elaborado; original, quando se torna completo e efetivo; cópia, quando é feita uma reprodução a partir do original. Em geral, as minutas não são capturadas, ou seja, não são registradas e arquivadas no espaço geral. No entanto, em alguns casos, minutas de documentos avulsos são inseridas em um processo/dossiê, para fins de análise e prosseguimento da ação.
No caso de documentos administrativos digitalizados, há que se especificar a natureza - cópia simples, cópia autenticada administrativamente ou cópia autenticada em cartório, conforme art. 16, inc. II, da Resolução CNJ nº 469/2022.</td></tr>
<tr><td>Exemplos</td><td colspan="3">--</td></tr>
<tr><td>Regra de preenchimento</td><td colspan="3">Deve, preferencialmente, ser gerado automaticamente pelo GestãoDoc.
Valores sugeridos: minuta, original, cópia.</td></tr>
<tr><td>Requisito</td><td colspan="3">RFT5.2.1</td></tr>
<tr><td>Equivalência</td><td colspan="3">--</td></tr>
</table>

Código de identificação	**MDOC7 - Identificador de versão**		
Rótulo	moreqjus.documento.versao		
Definição	Identificação da versão do documento.		
Objetivo	Identificar a versão do documento e estabelecer relação entre as versões anteriores e posteriores.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	NA	NA	OA
Repetibilidade	-	-	Não repetível
Nota de aplicação	Registrar informações relativas a: identificador da versão, descrição de alterações, data/hora da produção da versão e da transmissão, e o relacionamento entre as versões. Versões de documentos podem integrar processos e/ou dossiês.		
Exemplos	--		
Regra de preenchimento	É recomendável que seja gerado automaticamente pelo GestãoDoc.		
Requisito	RCA4.1.6 / RCA4.1.12 / RFT5.2.2		
Equivalência	e-PMG: identificador.versao		

Código de identificação	**MDOC8 - Título**		
Rótulo	dc.title		
Definição	Elemento de descrição que nomeia o documento ou processo/dossiê. Pode ser formal ou atribuído: formal - designação registrada no documento; atribuído - designação providenciada para identificação de um documento formalmente desprovido de título.		
Objetivo	Identificar o documento. Servir como elemento de acesso ao documento.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	F	NA	O
Repetibilidade	Não repetível	-	Não repetível
Nota de aplicação	--		
Exemplos	Fotografia da fachada do edifício sede do Superior Tribunal de Justiça; Processo de inventário da Princesa Isabel.		
Regra de preenchimento	Cada órgão deverá fixar critérios para títulos atribuídos.		
Requisito	RPC3.6.2 / RCA4.1.6 / RPA7.2.9		
Equivalência	Nobrade: 1.2 Título e-PMG: Título (Title) Dublin Core: Título (dc.title)		

Código de identificação	**MDOC9 - Descrição**		
Rótulo	**dc.description**		
Definição	Exposição concisa do conteúdo do documento, processo ou dossiê.		
Objetivo	Identificar o conteúdo do documento. Facilitar a pesquisa.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	F	NA	F
Repetibilidade	Não repetível	-	Não repetível
Nota de aplicação			
Exemplos	Termo de adesão ao pacto nacional pela primeira Infância celebrado entre o Conselho Nacional de Justiça e os atores da rede de atenção à primeira Infância (processo SEI CNJ nº 05906/2019)		
Regra de preenchimento	Cada órgão deverá fixar critérios e modelos com elementos básicos para a elaboração da descrição.		
Requisito	RCA4.1.6 / RCA4.1.10		
Equivalência	e-PMG: Descrição (description.abstract) Dublin Core: Descrição (dc.description)		

Código de identificação	**MDOC10 - Assunto**		
Rótulo	**dc.subject**		
Definição	Termos, palavras-chave ou descritores que representam o conteúdo do documento, propiciando a recuperação da informação.		
Objetivo	Referir de forma sucinta o teor geral do documento.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	F	NA	F
Repetibilidade	Repetível	-	Repetível
Nota de aplicação	Observar a política de indexação do órgão.		
Exemplos	--		
Regra de preenchimento	Pode ser de preenchimento livre ou com o uso de vocabulário controlado ou tesauro.		
Requisito	RCA4.1.6 / RCA4.1.10 / RPA7.2.9		
Equivalência	e-PMG: Assunto.palavra-chave (subject.keyword) Dublin Core: Assunto (dc.subject)		

Código de identificação	**MDOC11 - Autor**		
Rótulo	**moreqjus.documento.autor moreqjus.processo.autor**		
Definição	Pessoa física ou jurídica com autoridade para emitir o documento/processo e em cujo nome ou sob cuja ordem ou responsabilidade o documento/processo é emitido ou julgado.		
Objetivo	Identificar o autor do documento. Fornecer informação sobre o contexto de produção do documento. Demonstrar a autenticidade de um documento, indicando o responsável direto pela sua produção.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	O	NA	O
Repetibilidade	Repetível	-	Repetível
Nota de aplicação	Não confundir com autor de processo judicial (autor x réu).		
Exemplos	Santos, José ou José Santos Conselho Nacional de Justiça Superior Tribunal de Justiça Unidade processante - Vara Federal, Juizado, Divisão de precatórios, etc.		
Regra de preenchimento	Os órgãos devem estabelecer normas para controlar as entradas de nomes.		
Requisito	RCA4.1.6 / RPA7.2.9		
Equivalência	e-PMG: criador.autor (creator.autor)		

Código de identificação	**MDOC12 - Destinatário**		
Rótulo	**moreqjus.documento.destinatario moreqjus.processo.destinatario**		
Definição	Pessoa física e/ou jurídica a quem foi dirigida a informação contida no documento. Pode ser nominal ou geral: · nominal – pessoa(s) específica(s); · geral – refere-se a uma entidade maior, indeterminada. Ex.: cidadãos, povo, estudantes, a quem possa interessar, a todos os envolvidos.		
Objetivo	Identificar o destinatário do documento. Fornecer informação sobre o contexto de produção do documento. Demonstrar a autenticidade de um documento, indicando a quem ele é dirigido.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	AO	NA	OA
Repetibilidade	Repetível	-	Repetível
Nota de aplicação	--		
Exemplos	Santos, José ou José Santos Conselho Nacional de Justiça Partes do processo		
Regra de preenchimento	Os órgãos devem estabelecer normas para controlar as entradas de nomes.		
Requisito	RCA4.1.6 / RFT5.3.3		
Equivalência	e-PMG: Destinatário (addressee)		

Código de identificação	**MDOC13 - Originador**		
Rótulo	**moreqjus.documento.originador**		
Definição	Pessoa física ou jurídica designada no endereço eletrônico ou login em que o documento é gerado e/ou enviado.		
Objetivo	Identificar o originador do documento. Fornecer informação sobre o contexto de produção do documento. Demonstrar a autenticidade de um documento, indicando o responsável legal pela sua emissão.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	NA	NA	OA
Repetibilidade	-	-	Não repetível
Nota de aplicação	Aplica-se quando o nome do originador for diferente do nome do autor ou do redator.		
Exemplos	Santos, José ou José Santos Departamento de Gestão de Pessoas		
Regra de preenchimento	Os órgãos devem estabelecer normas para controlar as entradas de nomes.		
Requisito	RCA4.1.6 / RCA4.1.14 / RPA7.2.9		
Equivalência	--		

Código de identificação	**MDOC14 - Redator**		
Rótulo	**moreqjus.documento.redator**		
Definição	Responsável pela elaboração do conteúdo do documento.		
Objetivo	Identificar o redator do documento. Fornecer informação sobre o contexto de produção do documento. Demonstrar a autenticidade de um documento, indicando o responsável pela articulação de seu conteúdo.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	NA	NA	O
Repetibilidade	-	-	Repetível
Nota de aplicação	Registrar mesmo quando o nome do redator for igual ao nome do autor.		
Exemplos	Santos, José ou José Santos		
Regra de preenchimento	Os órgãos devem estabelecer normas para controlar as entradas de nomes.		
Requisito	RCA4.1.6 / RPA7.2.9		
Equivalência	--		

Código de identificação	**MDOC15 - Interessado**		
Rótulo	**moreqjus.documento.interessado**		
Definição	Nome e/ou identificação da pessoa física ou jurídica que tem envolvimento ou interesse no assunto do documento.		
Objetivo	Facilitar a pesquisa.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	O	NA	NA
Repetibilidade	Repetível	-	-
Nota de aplicação	O interessado pode ser qualificado como, por exemplo: réu, vítima, inventariante, inventariado, apelante, apelado, requerente, solicitante, procurador. Esse metadado deve ser registrado de forma estruturada, em três subelementos, conforme a seguir: interessadoNome, interessadoId, interessadoTipo.		
Exemplos	interessadoNome: José da Silva interessadoTipo: solicitante interessadoId: 987.745.465-73 (CPF) interessadoTipo: requerente interessadoId: 59873/0001-38 (CNPJ) interessadoTipo: apelado interessadoId: 8783000238 (número de matrícula) interessadoTipo: vítima		
Regra de preenchimento	Os órgãos devem estabelecer normas para controlar as entradas de nomes. Pode-se fazer o cadastro de interessados internos da organização por categorias para facilitar o registro automático, com dados de identificação. Ex.: número de matrícula, nome, documento de identificação.		
Requisito	RCA4.1.6 / RPA7.2.9		
Equivalência	--		

Código de identificação	**MDOC16 - Identificador do componente digital**		
Rótulo	**moreqjus.componente.id**		
Definição	Identificador dos componentes digitais que integram o documento.		
Objetivo	Estabelecer a relação entre o documento e os componentes digitais necessários para apresentá-lo.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	NA	NA	O
Repetibilidade	-	-	Repetível
Nota de aplicação	Um documento pode ser formado por um ou mais componentes digitais, que são os componentes físicos do documento. De forma geral, pode se dizer que os componentes digitais são os arquivos de computador que formam um documento. Cada componente deve ser identificado individualmente a fim de que o documento possa ser recuperado de maneira completa.		
Exemplos	Um documento multimídia pode estar armazenado em diversos arquivos com as informações de texto, imagens, som e relação entre eles. É necessário que o sistema computacional leia cada um deles para apresentá-lo ao usuário. Um documento em formato .pdf com assinatura digital externa a ele, armazenado em dois componentes digitais. A mesma situação aplica-se a documentos estruturados em bases de dados.		
Regra de preenchimento	Deve ser preenchido a partir do metadado Identificador do componente digital: componente.Id.		
Requisito	RCA4.1.5 / RCA4.1.6 / RCA4.1.7 / RCA4.1.9 / RCA4.1.20 / RCA4.1.26		
Equivalência	--		

Código de identificação	**MDOC17 - Gênero**		
Rótulo	**moreqjus.documento.genero**		
Definição	Indica o gênero documental, ou seja, a configuração da informação no documento de acordo com o sistema de signos utilizado na comunicação do documento.		
Objetivo	Monitorar os diversos gêneros documentais de um acervo para fins de gestão arquivística. Facilitar a pesquisa.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	NA	NA	F
Repetibilidade	--	--	Não repetível
Nota de aplicação	--		
Exemplos	Audiovisual; textual; cartográfico; iconográfico; multimídia.		
Regra de preenchimento	É necessário que o órgão elabore uma tabela com os gêneros e suas designações, para facilitar sua indicação no registro.		
Requisito	RCA4.1.6		
Equivalência	Nobrade: 1.5 Dimensão e suporte[4] e-PMG: Tipo[5] (type)		

Código de identificação	**MDOC18 - Espécie**		
Rótulo	**moreqjus.documento.especie**		
Definição	Indica a espécie documental, ou seja, a configuração da informação no documento de acordo com a disposição e a natureza das informações nele contidas.		
Objetivo	Complementar a descrição do documento ou a identificação de título. Facilitar a pesquisa.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	NA	NA	F
Repetibilidade	-	-	Não repetível
Nota de aplicação	Os órgãos podem preparar, como instrumento complementar de gestão, glossários de espécies de documentos que são produzidos no cumprimento de suas funções e atividades. Havendo tabela de classificação formalmente definida e de uso obrigatório, como é o caso das TPU, deve-se empregar o código específico. Relaciona-se com tipo documental; descrição e título.		
Exemplos	Processo; ofício; ata; relatório; projeto; prontuário; alvará.		
Regra de preenchimento	--		
Requisito	RCA4.1.6		
Equivalência	Nobrade: 1.5 Dimensão e suporte[6]		

4. A informação de dimensão deve ser registrada associada ao gênero.
5. No caso de documentos arquivísticos, deve-se informar o gênero do documento nesse elemento.
6. A informação de dimensão deve ser registrada associada ao gênero, espécie ou tipo. Conforme a Nobrade, à exceção dos documentos textuais, todos os demais gêneros devem ser, preferencialmente, quantificados por espécie ou tipo.

Código de identificação	**MDOC19 - Tipo**		
Definição	Indica o tipo documental, ou seja, a configuração da espécie documental de acordo com a atividade que a gerou.		
Objetivo	Complementar a descrição do documento ou a identificação do título. Permite a pesquisa limitada a um determinado tipo.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	NA	NA	F
Repetibilidade	-	-	Não repetível
Nota de aplicação	Há órgãos que preparam, como instrumento complementar de gestão de seus documentos, glossários de tipos documentais que são produzidos no cumprimento de suas funções e atividades. A existência dessas tabelas pode facilitar o registro desse elemento. Relaciona-se com espécie documental.		
Exemplos	Relatório de pesquisa; carta precatória; assentamento funcional; alvará de levantamento de valores para perícia.		
Regra de preenchimento	--		
Requisito	RCA4.1.6 / RPA7.2.9		
Equivalência	Nobrade: 1.5 Dimensão e suporte[7]		

Código de identificação	**MDOC20 - Idioma**		
Rótulo	**dc.language**		
Definição	Idioma(s) em que é (são) expresso(s) o conteúdo do documento.		
Objetivo	Identificar os idiomas do conteúdo do documento. Permitir a pesquisa limitada a um determinado idioma.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	NA	NA	F
Repetibilidade	-	-	Repetível
Nota de aplicação	Pode ser registrado mais de um idioma no caso de documentos multilíngues.		
Exemplos	--		
Regra de preenchimento	Os órgãos devem, preferencialmente, utilizar padrões para identificar idiomas, como, por exemplo, a norma ISO 639-2: 1998 – Part 2: alpha-3 code (Codes for the representation of names of languages).		
Requisito	--		
Equivalência	Nobrade: 4.3 Idioma e-PMG: Idioma (Language) Dublin Core: Linguagem (dc.Language)		

7. A informação de dimensão deve ser registrada associada ao gênero, espécie ou tipo. Conforme a Nobrade, à exceção dos documentos textuais, todos os demais gêneros devem ser, preferencialmente, quantificados por espécie ou tipo.

Código de identificação	**MDOC21 - Quantidade de folhas**		
Rótulo	**moreqjus.documento.folhaNum moreqjus.volume.folhaNum moreqjus.processo.folhaNum**		
Definição	Indicação da quantidade de folhas de um documento.		
Objetivo	Permitir o controle de folhas por processo e por volume. Facilitar o registro e o acesso a um documento específico dentro do processo ou dossiê.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	OA	OA	F
Repetibilidade	Não repetível	Não repetível	Não repetível
Nota de aplicação	Usado especialmente para gerenciamento de processos não digitais, que limitam a quantidade de folhas, sugerindo a abertura de volumes. Os órgãos devem determinar as normas para esse tipo de ação.		
Exemplos	--		
Regra de preenchimento	--		
Requisito	RPC3.3.2 Ver capítulo 3.5 (Volumes: abertura, encerramento e metadados)		
Equivalência	--		

Código de identificação	**MDOC22 - Numeração sequencial dos documentos**		
Rótulo	**moreqjus.documento.sequencia**		
Definição	Numeração sequencial dos documentos inseridos em um processo.		
Objetivo	Ordenar os documentos em um processo. Controlar a integridade do processo. Facilitar a referência a um documento específico.		
Aplica-se a	Processo/dossiê	Volume	Documento
	NA	NA	AO
			aplica-se somente aos documentos que integram um processo
Repetibilidade	-	-	Não repetível
Nota de aplicação	Usado para ordenar os documentos (e não as folhas) nos processos digitais.		
Exemplos	--		
Regra de preenchimento	Devem-se numerar os documentos na ordem em que são inseridos no processo a fim de garantir sua integridade.		
Requisito	RPC3.3.2 / RPC3.5.9 / RCA4.1.6		
Equivalência	--		

Código de identificação	**MDOC23 - Indicação de anexos**		
Rótulo	**moreqjus.documento.anexo**		
Definição	Indica se o documento/processo tem anexos.		
Objetivo	Registrar a existência de anexos de um determinado documento/processo para apoiar o controle de sua integridade e facilitar o acesso.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	O	NA	F
Repetibilidade	Não repetível	-	Não repetível
Exemplos	--		
Regra de preenchimento	--		
Requisito	RPC3.4.7 / RPC3.4.8 / RCA4.1.6 / RCA4.3.1 / RCA4.3.2 / RCA4.4.5		
Equivalência	--		

Código de identificação	**MDOC24 - Indicação de anotação**		
Rótulo	**moreqjus.documento.anotacao** **moreqjus.processo.anotacao**		
Definição	Indica se existem anotações relativas ao documento.		
Objetivo	Registrar a existência de anotações feitas em um documento para após sua emissão apoiar sua autenticidade.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	O	NA	O
Repetibilidade	Repetível		Repetível
Exemplos	Algumas anotações comuns são: ciente, circular para ciência, grifos, atribuição de tarefas.		
Regra de preenchimento	O sistema indica apenas se existe anotação. Os valores possíveis são: sim / não. A anotação em si é registrada em outro metadado ou em campo específico e deve ser exibida junto com o documento. Para processo/dossiê, o conteúdo do metadado deve ser registrado em evento de gestão do processo/dossiê. Para documento, deve ser registrado de forma estruturada, em dois subelementos, conforme a seguir: · moreqjus.documento.anotação: indica apenas se existe anotação. Os valores possíveis são: sim / não. · moreqjus.documento.nota – refere-se ao conteúdo da anotação em si e deve ser exibida junto com o documento quando houver indicação positiva no subelemento anterior.		
Requisito	RCA4.1.6 / RUS13.1.15		
Equivalência	--		

Código de identificação	**MDOC25 - Relação com outros documentos**		
Rótulo	**dc.Relation**		
Definição	Registro das relações significantes de um documento/processo com outros documentos/processos.		
Objetivo	Tornar explícito o relacionamento e facilitar o processamento automático e o gerenciamento arquivístico. Demonstrar a relação orgânica dos documentos. Facilitar a pesquisa de informações de documentos relacionados.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	AO	NA	AO
Repetibilidade	Repetível	-	Repetível
Nota de aplicação	Os órgãos devem estabelecer os tipos de relacionamentos que deverão ser controlados e suas restrições ou condições. Estas relações podem ser expressas, por exemplo: referenciado; ver também; apenso; relacionado; conexo; dependente.		
Exemplos	Apensamento, distribuição por dependência, conexões ou relacionamentos entre processos, recursos, processo físico digitalizado.		
Regra de preenchimento	--		
Requisito	RPC3.3.6 / RCA4.6.1 / RAD6.3.6 / RAD8.4.8 / RUS13.1.13 / RUS13.1.19 / RUS13.1.21		
Equivalência	e-PMG: Relação (Relation) Dublin Core: Relação (dc.Relation)		

Código de identificação	**MDOC26 - Níveis de acesso**		
Rótulo	**moreqjus.nivelDeAcesso**		
Definição	Indicação dos níveis de acesso ao documento e ao processo a partir da classificação de segredo de justiça, da classificação da informação quanto ao grau de sigilo (Seção II do Capítulo IV da Lei nº 12.527/2011) e da proteção de dados pessoais.		
Objetivo	Garantir o acesso somente a pessoas autorizadas.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	O	NA	O
Repetibilidade	Repetível	-	Repetível
Nota de aplicação	Os órgãos devem estabelecer as normas para as condições de acesso e indicação de sigilo, de acordo com seu contexto e com base na legislação. Relaciona-se com tabela de classificação de segurança.		
Exemplos	Ostensivo Segredo de justiça Reservado Secreto Ultrassecreto Sigilo fiscal Informação pessoal Patente		
Regra de preenchimento	Deve ser informado se o documento é ostensivo ou se possui algum grau de sigilo, indicando o nível de sigilo e demais hipóteses de sigilo.		

Requisito	RCA4.1.6 / RSE8.3.1 / RSE8.3.5 / RSE8.3.6 / RSE11.7.4 / RIN14.1.3
Equivalência	Nobrade: 4.1 condições de acesso e-PMG: Direitos.classificacaodoGrauDesigilo (rights.descriptor) Dublin Core: Direitos (dc.rights)

Código de identificação	**MDOC27 - Previsão de desclassificação**		
Rótulo	**moreqjus.documento.previsaoDesclassificacao moreqjus.processo.nivelDeAcesso**		
Definição	Indicação da data prevista para término da restrição de acesso.		
Objetivo	Permitir a identificação dos documentos que podem se tornar ostensivos por decurso de prazo		
Aplica-se a	Processo/Dossiê	Volume	Documento
	O	NA	O
Repetibilidade	Não repetível	-	Não repetível
Nota de aplicação	--		
Exemplos	--		
Regra de preenchimento	É recomendável seguir o padrão da ISO 8601.		
Requisito	RSE8.5.2		
Equivalência	--		

Código de identificação	**MDOC28 - Data de produção**		
Rótulo	dc.date.created		
Definição	Registro cronológico (data e hora) da produção do documento.		
Objetivo	Indicar data e hora em que foi produzido o documento.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	O	NA	O
Repetibilidade	Não repetível	--	Não repetível
Nota de aplicação	--		
Exemplos	--		
Regra de preenchimento	É recomendável seguir o padrão da ISO 8601.		
Requisito	RPC3.3.1 / RCA4.1.6 / RCA4.3.1 / RPA7.2.9 / RSE8.5.2 / RSE11.5.2		
Equivalência	Nobrade: 1.3 Data(s) e-PMG: data.criação (date.created) Dublin Core: Data (dc.date.created)		

Código de identificação	**MDOC29 - Local de produção**		
Rótulo	**moreqjus.documento.local**		
Definição	Registro do local da produção do documento, também denominado de data tópica.		
Objetivo	Indicar local em que foi produzido o documento.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	NA	NA	AO
Repetibilidade	-	-	Não repetível
Nota de aplicação	Usualmente adotado em documentos físicos e documentos notariais.		
Exemplos	--		
Regra de preenchimento	--		
Requisito	--		
Equivalência	Nobrade: 1.3 Data(s)		

Código de identificação	**MDOC30 - Classe**		
Rótulo	**moreqjus.classeId**		
Definição	Identificação da classe[8] ou nível específico de classificação com base nos planos de classificação do documento ou processo.		
Objetivo	Identificar a localização intelectual do documento no âmbito da estrutura orgânica ou funcional.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	O	NA	AO
Repetibilidade	Não repetível ou repetível, conforme regramento	-	Não repetível
Nota de aplicação	Os órgãos devem adotar os instrumentos de classificação previstos no Proname para aplicar esse elemento.		
Exemplos	--		
Regra de preenchimento	Pode se registrar o código e/ou o nome completo da classificação do documento. Para processos judiciais, no caso da tabela de assuntos, há possibilidade de repetibilidade.		
Requisito	RPC3.2.1 / RPC3.2.3 / RPC3.2.7 / RCA4.1.6 / RPA7.2.9		
Equivalência	--		

8. O termo *classe* deverá ser entendido como designação genérica que inclui qualquer das classificações em níveis e subníveis existentes nas estruturas dos planos, como por exemplo classes e assuntos da área meio, e classes, assuntos, movimentos e documentos da área judicial, incluindo seus desdobramentos.

Código de identificação	**MDOC31 - Destinação prevista**		
Rótulo	**moreqjus.documento.destinacao** **moreqjus.processo.destinacao**		
Definição	Indicação da próxima ação de destinação (transferência, eliminação ou recolhimento) prevista para o documento, em cumprimento às tabelas de temporalidade.		
Objetivo	Apoiar o controle do ciclo de vida do documento.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	O	NA	OA
Repetibilidade	Não repetível	-	Não repetível
Nota de aplicação	Para a finalidade deste instrumento, considera-se a transferência como uma ação de destinação. Os órgãos devem adotar as tabelas de temporalidade associadas aos planos de classificação para aplicar este elemento. Este elemento está relacionado ao 1.30 e 1.32 e, em casos de processos judiciais, à baixa do processo (evento de gestão). Complementarmente, o metadado deverá ser estruturado em dois subelementos: · moreqjus.processo.destinacao: indica a destinação propriamente dita; · (subelemento) moreqjus.processo.destinacao.criterio: indica o critério que definiu a destinação indicada. · moreqjus.documento.destinacao: indica a destinação propriamente dita; · (subelemento) moreqjus.documento.destinacao.criterio: indica o critério que definiu a destinação indicada. Exemplo de preenchimento do subelemento: Tabela de temporalidade, indicação CPAD, Corte cronológico, etc.		
Exemplos	Guarda permanente Eliminação		
Regra de preenchimento	Deve ser preenchido de forma automática pelo GestãoDoc. Valores permitidos: eliminação, transferência e recolhimento.		
Requisito	RPC3.1.16 / RPC3.1.17 / RPC3.1.21 / RPC3.2.7 / RAD6.1.4 / RSE8.5.2		
Equivalência	Nobrade: 3.2 Avaliação, eliminação e temporalidade[9] e-PMG: Destinação.ação (disposal.action)		

9. Registro de informações quanto a destinação, prazos de guarda e datas para cumprimento das ações previstas relativas à unidade de descrição. Recomendado na Nobrade para documentos em idade intermediária.

Código de identificação	**MDOC32 - Prazo de guarda**		
Rótulo	**moreqjus.documento.prazoGuarda moreqjus.processo.prazoGuarda**		
Definição	Indicação do prazo estabelecido em tabelas de temporalidade e destinação de documentos para o cumprimento da destinação.		
Objetivo	Apoiar o controle do ciclo de vida do documento.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	O	NA	OA
Repetibilidade	Não repetível	-	Não repetível
Nota de aplicação	Os órgãos devem estabelecer as tabelas de temporalidade associadas ao plano de classificação para aplicar esse elemento. Este elemento está relacionado ao MDOC30 e MDOC32 e, em casos de processos judiciais, à baixa do processo (evento de gestão).		
Exemplos	3 anos 5 anos 20 anos		
Regra de preenchimento	Deve ser preenchido de forma automática pelo GestãoDoc.		
Requisito	RPC3.1.6 / RPC3.1.19 / RPC3.1.21 / RPC3.2.7 / RCA4.1.13 / RAD6.1.2 / RAD6.1.3 / RAD6.1.4		
Equivalência	Nobrade: 3.2 Avaliação, eliminação e temporalidade e-PMG: Destinação.prazoDeGuarda (disposal.timePeriod)		

Código de identificação	**MDOC33 - Indicação de precedente qualificado**		
Rótulo	**moreqjus.processo.precedenteQualificado** **moreqjus.documento.precedenteQualificado**		
Definição	Indica se o documento ou o processo trata-se de precedente qualificado		
Objetivo	Identificar o documento ou o processo que deu origem à precedente qualificado, de observância obrigatória pela administração, pelo Poder Judiciário ou pela sociedade como orientador de atuação futura. O metadado tem o intuito de informar ao usuário e/ou sistema, de forma inequívoca, que o documento ou processo constitui precedente qualificado. O processo ou documento assim identificado é de guarda permanente conforme inc. VII do art. 30 da Resolução CNJ nº 324/2020..		
Aplica-se a	Processo/Dossiê	Volume	Documento
	O	NA	OA
Repetibilidade	Não repetível	Não repetível	Não repetível
Nota de aplicação	Aplicável no âmbito do GestãoDoc, deve ser unívoco e persistente. Os valores possíveis são: sim/não Exemplo: processo.precedenteQualificado: sim. Cabe anotação complementar, que pode ser registrada de forma estruturada em subelemento, conforme a seguir representado: · Moreqjus.processo.precedenteQualificado.numeroTema; e · Moreqjus.documento.predecenteQualificado.numeroTema.		
Exemplos	Processo identificado pela classe Incidente de Assunção de Competência (cód. 12087) ou Incidente de Resolução de Demandas Repetitivas (cód. 12085)		
Regra de preenchimento	Deve ser registrado de forma automática pelo GestãoDoc em classes processuais específicas (IRDR, ADI), quando proferido julgamento de mérito, e permitir anotação específica por usuário autorizado. Admite o estabelecimento de complementação.		
Requisito	RPC3.3.3; RPC3.3.12		
Equivalência			

Código de identificação	**MDOC34 - Localização**		
Rótulo	**moreqjus.documento.localização moreqjus.volume.localização moreqjus.processo.localização**		
Definição	Anotação em sistema do local de armazenamento de documento(s) físico ou virtual, caso não haja sua juntada no próprio sistema GestãoDoc		
Objetivo	Permitir a localização dos documentos em qualquer mídia. Monitorar o armazenamento de documentos.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	OA	F	OA
Repetibilidade	Não repetível	Não repetível	Não repetível
Nota de aplicação	Deve ser utilizado, obrigatoriamente, quando o documento é mantido em outra área de armazenamento, seja virtual ou física, incluindo a documentação digitalizada (Resolução CNJ nº 469/2022) e a documentação ou mídia digital que não puder ser anexada ao GestãoDoc (Resolução CNJ n.º 408/2021). Utilizado para documentos não digitais, para a parte não digital dos documentos híbridos e para os documentos digitais não capturados no GestãoDoc.		
Exemplos	Depósito 201, estante 8, prateleira 2; Caixa 3.456; PJe-Mídias.		
Regra de preenchimento	Os órgão devem estabelecer normas para o registro da localização dos documentos não digitais, de acordo com seu ambiente de guarda e armazenamento.		
Requisito	RPC3.6.3 / RPC3.6.4 / RPC3.6.7 / RCA4.1.24 / RCA4.6.2 / RFT5.3.3 / RAD6.4.3 / RPA7.1.1 / RPA7.1.2		
Equivalência	e-PMG: Localização(location)		

Código de identificação	**MDOC35 - Indicação de arquivamento**		
Rótulo	moreqjus.processo.arquivado moreqjus.documento.arquivado		
Definição	Indica a situação de encerramento da tramitação de um processo/dossiê/documento pelo arquivamento, que será considerado definitivo quando não necessitar de diligências do órgão produtor, de processamento ou de terceiros. Não deve ser utilizado para as situações em que se já se sabe aprioristicamente que o documento ou processo voltará a tramitar (v.g. arquivamento provisório).		
Objetivo	Identificar se o documento ou o processo está tramitando ou arquivado.		
Aplica-se a	Processo/Dossiê	Volume	Documento
	O	NA	OA
Repetibilidade	Não repetível	Não repetível	Não repetível
Nota de aplicação	Valores possíveis são: sim ou não. Exemplo: moreqjus.processo.arquivado: sim. Cabe anotação complementar nos metadados relativa aos eventos que transformam um status no outro: moreqjus.processo.arquivado.dataarquivamento e moreqjus.processo.arquivado.datadesarquivamento		
Exemplos	-		
Regra de preenchimento	Deve ser registrado de forma automática pelo GestãoDoc.		
Requisito	RPC 3.3.2; RPC 3.3.3, RPC 3.3.4, RPC3.3.12, RCA4.1.6		
Equivalência	-		

B1.2 Classe

Os metadados relativos à classe podem corresponder a quaisquer das classificações em níveis e subníveis existentes nas estruturas dos Planos de Classificação, como por exemplo classes e assuntos da área meio, e classes, assuntos, movimentos e documentos da área judicial (Tabelas Processuais Unificadas do Poder Judiciário), incluindo seus desdobramentos.

Os metadados previstos são:

- MCLA1 - Identificador da classe
- MCLA2 - Nome da classe
- MCLA3 - Código da classe
- MCLA4 - Subordinação da classe
- MCLA5 - Indicação de permissão de uso
- MCLA6 - Indicação de classe ativa/inativa
- MCLA7 - Prazo na idade corrente
- MCLA8 - Evento de contagem na idade corrente
- MCLA9 - Prazo na idade intermediária
- MCLA10 - Evento de contagem na idade intermediária
- MCLA11 - Destinação final
- MCLA12 - Sigilo associado à classe
- MCLA13 - Observação

Para os elementos de metadados referentes à identificação *de* **Classe** foi elaborada uma ficha individual que detalha cada elemento e apresenta as seguintes informações:

Código de identificação	
Rótulo	
Definição	
Objetivo	
Repetibilidade	
Nota de aplicação	
Exemplos	
Regra de preenchimento	
Requisito	
Equivalência	

- **Código de identificação e nome**: indicação do código e do nome atribuídos ao elemento.
- **Rótulo**: nome padrão que tem que ser utilizado para identificar o elemento a fim de facilitar a interoperabilidade de sistemas.
- **Definição**: indica qual informação deve ser registrada no elemento de metadado.
- **Objetivo**: a referência do que se pretende alcançar com a aplicação do elemento.
- **Obrigatoriedade**: indica a obrigatoriedade da aplicação do elemento. Os valores possíveis são: *obrigatório (O); obrigatório se aplicável (OA); facultativo (F); ou não se aplica (NA)*.
- **Repetibilidade**: indica se a informação pode ser registrada mais de uma vez – mais de um valor.
- **Nota de aplicação**: sugere formas de aplicação do elemento.
- **Exemplos**: apresenta alguns exemplos de aplicação que explicam o elemento.
- **Regra de preenchimento**: regra que especifica os valores, a codificação ou a lista de autoridades (lista de valores autorizados) convencionados para o preenchimento do elemento.
- **Requisito**: apresenta os requisitos relacionados com o elemento de metadado.
- **Equivalência**: referências para elementos equivalentes de outros esquemas de metadados.

Código de identificação	**MCLA1 - Identificador da classe**
Rótulo	**moreqjus.classe.id**
Definição	Identificador único atribuído pelo GestãoDoc à classe no ato de sua criação no sistema.
Objetivo	Identificar de forma unívoca a classe para que o GestãoDoc possa gerenciá-la.
Obrigatoriedade	O
Repetibilidade	Não repetível
Nota de aplicação	Refere-se às classes, subclasses, grupos e subgrupos.
Exemplos	--
Regra de preenchimento	Deve, preferencialmente, ser gerado de forma automática pelo GestãoDoc.
Requisito	RPC3.1.3 a RPC3.1.24 / RPC3.2.1 a RPC3.2.9 / RPC3.3.3 a RPC3.3.5 / RPC3.3.8 / RPC3.3.11 / RPC3.3.12 / RCA4.1.18 / RAD6.1.2 / RAD6.1.8 / RPA7.1.3 / RPA7.2.1/ RPA7.3.6 / RSE8.2.12 / RSE8.2.13 / RSE8.3.11 / RSE8.3.12 / RSE8.5.2 / RUS13.1.9
Equivalência	--

Código de identificação	**MCLA2 - Nome da classe**
Rótulo	**moreqjus.classe.nome**
Definição	Nome dos níveis dos planos de classificação e tabelas de temporalidade.
Objetivo	Registrar a denominação dos diversos níveis dos planos de classificação adotados.
Obrigatoriedade	O
Repetibilidade	Não repetível
Nota de aplicação	Refere-se às classes, subclasses, grupos e subgrupos, assuntos, movimentos e documentos utilizados como chave para a classificação de processos e documentos.
Exemplos	“Gestão de Pessoas”, “Direitos, obrigações e vantagens”, “Gestão Financeira”, “Participação em Órgãos Colegiados”. “Arrolamento Comum”, “Ação Civil Pública”, “Inventário e Partilha”, “Prestação de Alimentos”, “Petição Inicial” e “Acórdão”.
Regra de preenchimento	Registrar a denominação específica da classe, sem repetir a do nível hierárquico superior. No caso do processo judicial, observar o disposto na Resolução CNJ nº 46/2007.
	RPC3.1.3 a RPC3.1.24 / RPC3.2.1 a RPC3.2.9 / RPC3.3.3 a RPC3.3.5 / RPC3.3.8 / RPC3.3.11 / RPC3.3.12 / RCA4.1.18 / RAD6.1.2 / RAD6.1.8 / RPA7.1.3 / RPA7.2.1 / RPA7.3.6 / RSE8.2.12 / RSE8.2.13 / RSE8.3.11/ RSE8.3.12 / RSE8.5.2 / RUS13.1.9
Equivalência	--

Código de identificação	**MCLA3 - Código da classe**
Rótulo	**moreqjus.classe.codigo**
Definição	Código relativo a uma divisão dos planos de classificação e tabelas de temporalidade.
Objetivo	Registrar o código atribuído à classe respectiva.
Obrigatoriedade	O
Repetibilidade	Não repetível
Nota de aplicação	Refere-se às classes, subclasses, grupos e subgrupos, assuntos, movimentos e documentos utilizados como chave para a classificação de processos e documentos.
Exemplos	202 – Agravo de Instrumento 83 - Processo Cautelar Fiscal 10487 - Habitação 11977 - Alienação Parental
Regra de preenchimento	--
Requisito	RPC3.1.3 a RPC3.1.24 / RPC3.2.1 a RPC3.2.9 / RPC3.3.3 a RPC3.3.5 / RPC3.3.8 / RPC3.3.11 / RPC3.3.12 / RCA4.1.18 / RAD6.1.2 / RAD6.1.8 / RPA7.1.3 / RPA7.2.1 / RPA7.3.6 / RSE8.2.12 / RSE8.2.13 / RSE8.3.11 / RSE8.3.12 / RSE8.5.2 / RUS13.1.9
Equivalência	--

Código de identificação	**MCLA4 - Subordinação da classe**
Rótulo	**moreqjus.classe.subordinacao**
Definição	Subordinação da classe na hierarquia do plano de classificação e tabela de temporalidade.
Objetivo	Recuperar a relação hierárquica das diversas subdivisões dos planos de classificação.
Obrigatoriedade	O
Repetibilidade	Não repetível
Nota de aplicação	A obrigatoriedade não se aplica às classes de primeiro nível, mas aos níveis subordinados.
Exemplos	10110 – Direito Ambiental (Código hierárquico superior ao 10116 - Agrotóxico)
Regra de preenchimento	Registrar o código da classe imediatamente superior.
Requisito	RPC3.1.3 a RPC3.1.24 / RPC3.2.1 a RPC3.2.9 / RPC3.3.3 a RPC3.3.5/ RPC3.3.8 / RPC3.3.11 e R3.3.12 / RCA4.1.18 / RAD6.1.2 / RAD6.1.8 / RPA7.1.3 / RPA7.2.1 / RPA7.3.6 / RSE8.2.12 e RSE8.2.13 / RSE8.3.11 e RSE8.3.12 / RSE8.5.2 / RUS13.1.9
Equivalência	--

Código de identificação	**MCLA5 - Indicação de permissão de uso**
Rótulo	**moreqjus.classe.indicadorUso**
Definição	Indicação se a classe pode ser utilizada para classificar documentos ou se é apenas parte da estrutura hierárquica dos planos de classificação.
Objetivo	Apoiar o GestãoDoc para restringir o uso apenas das classes autorizadas para classificar documentos.
Obrigatoriedade	O
Repetibilidade	Não repetível
Nota de aplicação	Uma classe sem permissão de uso para classificar não pode ser subordinada a uma classe com permissão de uso.
Exemplos	--
Regra de preenchimento	Valores previstos: sim ou não.
Requisito	RPC3.1.3 a RPC3.1.24 / RPC3.2.1 a RPC3.2.9 / RPC3.3.3 a RPC3.3.5 / RPC3.3.8 / RPC3.3.11 e R3.3.12 / RCA4.1.18 / RAD6.1.2 / RAD6.1.8 / RPA7.1.3 / RPA7.2.1 / RPA7.3.6 / RSE8.2.12 e RSE8.2.13 / RSE8.3.11 e RSE8.3.12 / RSE8.5.2 / RUS13.1.9
Equivalência	--

Código de identificação	**MCLA6 - Indicação de classe ativa/inativa**
Rótulo	**moreqjus.classe.indicadorAtiva**
Definição	Indicação se a classe está ativa ou inativa para uso.
Objetivo	Apoiar o GestãoDoc para restringir o uso apenas das classes ativas na classificação de novos documentos.
Obrigatoriedade	O
Repetibilidade	Não repetível
Nota de aplicação	As classes inativas são aquelas que não são mais utilizadas, mas que não podem ser eliminadas devido ao fato de existirem documentos ou processos nela classificados anteriormente.
Exemplos	--
Regra de preenchimento	Valores previstos: ativa ou inativa; sim ou não.
Requisito	RPC3.1.3 a RPC3.1.24 / RPC3.2.1 a RPC3.2.9 / RPC3.3.3 a RPC3.3.5 / RPC3.3.8 / RPC3.3.11 e RPC3.3.12 / RCA4.1.18 / RAD6.1.2 / RAD6.1.8 / RPA7.1.3 / RPA7.2.1 / RPA7.3.6 / RSE8.2.12 / RSE8.2.13 / RSE8.3.11 / RSE8.3.12 / RSE8.5.2 / RUS13.1.9
Equivalência	--

Código de identificação	**MCLA7 - Prazo na idade corrente**
Rótulo	**moreqjus.classe.prazoCorrente**
Definição	Prazo de guarda previsto para a idade corrente, quando aplicável.
Objetivo	Apoiar o GestãoDoc na contagem do tempo de guarda do documento na idade corrente.
Obrigatoriedade	OA
Repetibilidade	Não repetível
Nota de aplicação	Esse elemento é utilizado pelo GestãoDoc em conjunto com o elemento Evento de contagem na idade corrente para identificar os documentos que já atingiram o prazo previsto. Para processos judiciais, não se aplica pois não há previsibilidade do prazo, uma vez que a fase corrente perdura da autuação à baixa definitiva do processo.
Exemplos	6 meses, 2 anos, 7 anos.
Regra de preenchimento	Preencher conforme o prazo previsto nas tabelas de temporalidade. No caso do prazo previsto nas tabelas de temporalidade e destinação de documentos ser “enquanto vigora”, o valor do elemento Prazo na idade corrente será 0 (zero), associado ao evento “fim da vigência do documento”.
Requisito	RPC3.1.1 / RPC3.1.3 a RPC3.1.24 / RPC3.2.1 a RPC3.2.9 / RPC3.3.3 a RPC3.3.5 / RPC3.3.8 / RPC3.3.11 / RPC3.3.12 / RCA4.1.18 / RAD6.1.2 / RAD6.1.8 / RPA7.1.3 / RPA7.2.1 / RPA7.3.6 / RSE8.2.12 / RSE8.2.13 / RSE8.3.11 / RSE8.3.12 / RSE8.5.2/ RUS13.1.9
Equivalência	--

Código de identificação	**MCLA8 - Evento de contagem na idade corrente**
Rótulo	**moreqjus.classe.eventoCorrente**
Definição	Evento que dispara o início da contagem do prazo de guarda na idade corrente.
Objetivo	Apoiar o GestãoDoc na contagem do tempo de guarda do documento ou processo na idade corrente.
Obrigatoriedade	OA
Repetibilidade	Não repetível
Nota de aplicação	Esse elemento é utilizado pelo GestãoDoc em conjunto com o elemento Prazo na idade corrente para identificar os documentos que já atingiram o prazo previsto.
Exemplos	Eventos: início da vigência, produção/registro do processo/dossiê administrativo.
Regra de preenchimento	Preencher conforme previsto na tabela de temporalidade e destinação de documentos. Quando o evento não for especificado, considera-se a produção/registro ou autuação do processo/dossiê.
Requisito	RPC3.1.1 / RPC3.1.3 a RPC3.1.24 / RPC3.2.1 a RPC3.2.9 / RPC3.3.3 a RPC3.3.5 / RPC3.3.8 / RPC3.3.11 / RPC3.3.12 / RCA4.1.18 / RAD6.1.2 / RAD6.1.8 / RPA7.1.3 / RPA7.2.1 / RPA7.3.6 / RSE8.2.12 / RSE8.2.13 / RSE8.3.11 / RSE8.3.12 / RSE8.5.2/ RUS13.1.9
Equivalência	--

Código de identificação	**MCLA9 - Prazo na idade intermediária**
Rótulo	**moreqjus.classe.prazoIntermediaria**
Definição	Prazo de guarda previsto para a idade intermediária.
Objetivo	Apoiar o GestãoDoc na contagem do tempo de guarda do documento na idade intermediária.
Obrigatoriedade	OA
Repetibilidade	Não repetível
Nota de aplicação	Esse elemento é utilizado pelo GestãoDoc em conjunto com o elemento Evento de contagem na idade intermediária para identificar os documentos que já atingiram o prazo previsto.
Exemplos	6 meses, 2 anos, 5 anos.
Regra de preenchimento	Preencher conforme o prazo previsto nas tabelas de temporalidade e destinação de documentos.
Requisito	RPC3.1.1 / RPC3.1.3 a RPC3.1.24 / RPC3.2.1 a RPC3.2.9 / RPC3.3.3 a RPC3.3.5 / RPC3.3.8 / RPC3.3.11 / RPC3.3.12 / RCA4.1.18 / RAD6.1.2 / RAD6.1.8 / RPA7.1.3 / RPA7.2.1 / RPA7.3.6 / RSE8.2.12 / RSE8.2.13 / RSE8.3.11 / RSE8.3.12 / RSE8.5.2/ RUS13.1.9
Equivalência	--

Código de identificação	**MCLA10 - Evento de contagem na idade intermediária**
Rótulo	**moreqjus.classe.eventoIntermediaria**
Definição	Evento que dispara o início da contagem do prazo de guarda na idade intermediária.
Objetivo	Apoiar o GestãoDoc na contagem do tempo de guarda do documento na idade intermediária.
Obrigatoriedade	OA
Repetibilidade	Não repetível
Nota de aplicação	Esse elemento é utilizado pelo GestãoDoc em conjunto com o elemento Prazo na idade intermediária para identificar os documentos e os processos que já atingiram o prazo previsto.
Exemplos	Eventos: aprovação de contas, fim da vigência do contrato, desligamento do servidor, conclusão do caso, baixa definitiva do processo judicial.
Regra de preenchimento	Preencher conforme previsto nas tabelas de temporalidade. Quando o evento não for especificado, considera-se a transferência como evento de início da contagem do prazo de guarda.
Requisito	RPC3.1.1 / RPC3.1.3 a RPC3.1.24 / RPC3.2.1 a RPC3.2.9 / RPC3.3.3 a RPC3.3.5 / RPC3.3.8 / RPC3.3.11 / RPC3.3.12 / RCA4.1.18 / RAD6.1.2 / RAD6.1.8 / RPA7.1.3 / RPA7.2.1 / RPA7.3.6 / RSE8.2.12 / RSE8.2.13 / RSE8.3.11 / RSE8.3.12 / RSE8.5.2a/ RUS13.1.9
Equivalência	--

Código de identificação	**MCLA11 - Destinação final**
Rótulo	**moreqjus.classe.destinacao**
Definição	Destinação final prevista para o documento: preservação ou eliminação.
Objetivo	Apoiar o GestãoDoc na produção das listagens de eliminação e de recolhimento.
Obrigatoriedade	O
Repetibilidade	Não repetível
Nota de aplicação	--
Exemplos	--
Regra de preenchimento	Preencher conforme previsto nas tabelas de temporalidade. Valores previstos: eliminação ou guarda permanente.
Requisito	RPC3.1.1 / RPC3.1.3 a RPC3.1.24 / RPC3.2.1 a RPC3.2.9 / RPC3.3.3 a RPC3.3.5 / RPC3.3.8 / RPC3.3.11 / RPC3.3.12 / RCA4.1.18 / RAD6.1.2 / RAD6.1.8 / RPA7.1.3 / RPA7.2.1 / RPA7.3.6 / RSE8.2.12 / RSE8.2.13 / RSE8.3.11 / RSE8.3.12 / RSE8.5.2 / RUS13.1.9
Equivalência	--

Código de identificação	**MCLA12 - Sigilo associado à classe**
Rótulo	**moreqjus.classe.sigilo**
Definição	Restrição de acesso aos documentos, aplicada de forma geral aos documentos de uma classe.
Objetivo	Automatizar a atribuição de restrição de acesso a documentos que possuam informação pessoal, sensível e outras previstas em legislação vigente.
Obrigatoriedade	OA
Repetibilidade	Não repetível
Nota de aplicação	Aplica-se a restrição de acesso aos documentos que possuam informação pessoal, sensível e outras previstas em legislação vigente. O valor previsto nesse elemento da classe deve ser herdado automaticamente pelo documento (elemento de identificação do documento – Níveis de acesso) no momento da classificação.
Exemplos	Informação pessoal (no caso da classe Apuração de responsabilidade e ação disciplinar). Segredo de justiça (no caso do Assunto “Adoção de Criança” - cód. 9974) Sigilo (no caso de aplicação do Código de Processo Penal – Pedido de Quebra de Sigilo de Dados e/ou Telefônico - Cód.310)
Regra de preenchimento	Utilizar os valores previstos para o elemento de identificação do documento – Níveis de acesso, excetuando-se os relativos à atribuição de grau de sigilo estabelecidos na Lei de Acesso à Informação - Lei 12.527 de 2011 (confidencial, reservado, secreto e ultrassecreto).
Requisito	RPC3.1.1 / RPC3.1.3 a RPC3.1.24 / RPC3.2.1 a RPC3.2.9 / RPC3.3.3 a RPC3.3.5 / RPC3.3.8 / RPC3.3.11 / RPC3.3.12 / RCA4.1.18 / RAD6.1.2 / RAD6.1.8 / RPA7.1.3 / RPA7.2.1 / RPA7.3.6 / RSE8.2.12 / RSE8.2.13 / RSE8.3.11 / RSE8.3.12 / RSE8.5.2 / RUS13.1.9
Equivalência	--

Código de identificação	**MCLA13 - Observação**
Rótulo	moreqjus.classe.observacao
Definição	Registra informações adicionais sobre a classe.
Objetivo	Registrar informações não previstas que podem ser relevantes para a gestão de documentos.
Obrigatoriedade	F
Repetibilidade	Não repetível
Nota de aplicação	--
Exemplos	Informações complementares tais como: previsão de conversão de suporte, legislação sobre os prazos de guarda.
Regra de preenchimento	--
Requisito	RPC3.1.1 / RPC3.1.3 a RPC3.1.24 / RPC3.2.1 a RPC3.2.9 / RPC3.3.3 a RPC3.3.5 / RPC3.3.8 / RPC3.3.11 / RPC3.3.12 / RCA4.1.18 / RAD6.1.2 / RAD6.1.8 / RPA7.1.3 / RPA7.2.1 / RPA7.3.6 / RSE8.2.12 / RSE8.2.13 / RSE8.3.11 / RSE8.3.12 / RSE8.5.2 / RUS13.1.9
Equivalência	--

B.1.3 Eventos

Estas informações referem-se ao controle do ciclo de vida e aos procedimentos de protocolo para controle dos documentos avulsos e processos.

Para os elementos de metadados relativos ao registro de **Eventos** (gestão do ciclo de vida, gestão do processo/dossiê, gerenciamento de classe e de preservação) foi elaborada uma ficha que especifica as informações a serem registradas sobre cada evento.

Código de identificação	
Rótulo	
Definição	
Obrigatoriedade	
Repetibilidade (Ocorrências)	
Regra de preenchimento	
Requisito	
Equivalência	

- **Código de identificação e nome**: indicação do código e do nome atribuídos ao elemento.
- **Rótulo:** nome padrão que tem que ser utilizado para identificar o elemento a fim de facilitar a interoperabilidade de sistemas.
- **Definição:** indica que informação deve ser registrada no elemento de metadado.
- **Obrigatoriedade:** indica a obrigatoriedade da aplicação do elemento. Os valores possíveis são: *obrigatório (O); obrigatório se aplicável (OA); facultativo (F); ou não se aplica (NA).*
- **Repetibilidade:** indica se a informação pode ser registrada mais de uma vez para um mesmo evento.
- **Regra de preenchimento:** regra que especifica os valores, a codificação ou a lista de autoridades (lista de valores autorizados) convencionados para o preenchimento do elemento.

- **Requisito:** apresenta os requisitos relacionados com o elemento de metadado.
- **Equivalência:** referências para elementos equivalentes de outros esquemas de metadados.

B.1.3.1 Eventos de gestão do ciclo de vida

Registra os eventos de captura, movimentação e controle do ciclo de vida do documento e processo/dossiê.

Os eventos de gestão do ciclo de vida poderão assumir estes ou outros valores:

ECV1	Captura	Descreve a captura do documento.
ECV2	Transferência – Envio	Registro do envio de transferência de documentos. Registrar no elemento Detalhe do evento informações complementares, tais como: método utilizado para o envio, localização, suporte, número do termo de transferência. Deve ser feito um registro para cada lote transferido.
ECV3	Transferência – Recebimento	Registro do recebimento da transferência de documentos. Registrar no elemento *Detalhe do evento* informações complementares, tais como: localização, suporte, identificador do ECV2 correspondente. Deve ser feito um registro para cada lote transferido.
ECV4	Recolhimento – Envio	Registro do envio de recolhimento de documentos. Registrar no elemento *Detalhe do evento* informações complementares, tais como: método utilizado para o envio, localização, suporte, número do termo de recolhimento.
ECV5	Eliminação	Registro do procedimento de eliminação. Registrar no elemento *Detalhe do evento* informações complementares, tais como: tipo de procedimento (fragmentação, desmagnetização, doação etc.), número do termo de eliminação, número do edital. Nota: a eliminação é precedida de avaliação feita fora do sistema, que subsidia a decisão de eliminação, mesmo que esta seja automática.
ECV6	Restrição de acesso	Registro do procedimento de classificação de sigilo e de marcação de outras hipóteses de sigilo e restrição de acesso. Quanto à classificação de sigilo, registrar no elemento *Detalhe do evento* informações complementares, tais como: grau de sigilo, fundamentação legal, data prevista para desclassificação. Quanto às demais hipóteses de sigilo, registrar no elemento *Detalhe do evento* informações complementares, tais como: tipo de restrição de acesso (informação pessoal, segredo de justiça, bancária, fiscal, propriedade industrial), previsão de prazo para cessação da restrição (quando for o caso), justificativa.
ECV7	Alteração da restrição de acesso	Registro do procedimento de alteração da restrição de acesso, que pode ser a remoção da restrição ou a reclassificação (no caso da classificação de sigilo). Quanto à desclassificação ou reclassificação de sigilo, registrar no elemento *Detalhe do evento* informações complementares, tais como: grau de sigilo, nova data prevista para desclassificação, motivação. Quanto à retirada das demais hipóteses de sigilo, registrar no elemento *Detalhe do evento* informações complementares, tais como: tipo de restrição de acesso (informação pessoal, segredo de justiça, bancária, fiscal, propriedade industrial), justificativa.

Cada evento deve ser registrado pelo seguinte conjunto de elementos de metadados:

- MECV1 - Identificador do evento
- MECV2 - Tipo de evento
- MECV3 - Identificador do processo/dossiê
- MECV4 - Identificador do documento
- MECV5 - Identificador do lote
- MECV6 - Data e hora do evento
- MECV7 - Agente responsável pelo evento
- MECV8 - Detalhes do evento

Código de identificação	**MECV1 - Identificador do evento**
Rótulo	moreqjus.eventoCv.id
Definição	Identificador do evento de ciclo de vida que está sendo registrado no GestãoDoc.
Obrigatoriedade	O
Repetibilidade	Não repetível
Regra de preenchimento	Deve ser registrado automaticamente pelo GestãoDoc.
Requisito	RPC3.1.16 / RPC3.1.18 / RPC3.4.3 / RPC3.4.5 / RPC3.4.6 /RCA4.1.6 / RAD8.4.7 / RSE8.5.2 / RSE8.5.3 / RSE8.5.5 / RSE8.5.10 / RSE8.5.12 / RAR9.2.1 / RAR9.2.2 / RAR9.2.3 / RAR9.2.4 / RAR9.2.5 / RPR10.2.6 / RPR10.3.1 / RPR10.3.6 / RSE11.3.3 / RSE11.3.8 / RSE11.4.4 / RSE11.4.5 / RSE11.6.2 / RSE11.7.1
Equivalência	--

Código de identificação	**MECV2 - Tipo de evento**
Rótulo	**moreqjus.eventoCv.tipo**
Definição	Identificação do tipo de evento de gestão do ciclo de vida.
Obrigatoriedade	O
Repetibilidade	Não repetível
Regra de preenchimento	Este elemento poderá assumir os valores a seguir indicados ou outros: · Captura · Transferência – Envio · Transferência – Recebimento · Recolhimento – Envio · Eliminação · Atribuição de restrição de acesso · Desclassificação de Sigilo · Reclassificação de Sigilo
Requisito	RPC3.1.16 / RPC3.1.18 / RPC3.4.3 / RPC3.4.5 / RPC3.4.6 /RCA4.1.6 / RAD8.4.7 / RSE8.5.2 / RSE8.5.3 / RSE8.5.5 / RSE8.5.10 / RSE8.5.12 / RAR9.2.1 / RAR9.2.2 / RAR9.2.3 / RAR9.2.4 / RAR9.2.5 / RPR10.2.6 / RPR10.3.1 / RPR10.3.6 / RSE11.3.3 / RSE11.3.8 / RSE11.4.4 / RSE11.4.5 / RSE11.6.2 / RSE11.7.1
Equivalência	--

Código de identificação	**MECV3 - Identificador do processo/dossiê**
Rótulo	**moreqjus.eventoCv.processoId**
Definição	Identificador do processo/dossiê que está sendo afetado pelo evento.
Obrigatoriedade	OA
Repetibilidade	Repetível
Regra de preenchimento	O código deve ser obtido no metadado MDOC3 Identificador do processo/dossiê.
Requisito	RPC3.1.16 / RPC3.1.18 / RPC3.4.3 / RPC3.4.5 / RPC3.4.6 /RCA4.1.6 / RAD8.4.7 / RSE8.5.2 / RSE8.5.3 / RSE8.5.5 / RSE8.5.10 / RSE8.5.12 / RAR9.2.1 / RAR9.2.2 / RAR9.2.3 / RAR9.2.4 / RAR9.2.5 / RPR10.2.6 / RPR10.3.1 / RPR10.3.6 / RSE11.3.3 / RSE11.3.8 / RSE11.4.4 / RSE11.4.5 / RSE11.6.2 / RSE11.7.1
Equivalência	--

Código de identificação	**MECV4 - Identificador do documento**
Rótulo	moreqjus.eventoCv.documentoId
Definição	Identificador do documento.
Obrigatoriedade	O
Repetibilidade	Repetível
Regra de preenchimento	O código deve ser obtido no metadado MDOC1 Identificador do documento. Obrigatório para eventos de transferência para identificar os documentos transferidos.
Requisito	RPC3.1.16 / RPC3.1.18 / RPC3.4.3 / RPC3.4.5 / RPC3.4.6 /RCA4.1.6 / RAD8.4.7 / RSE8.5.2 / RSE8.5.3 / RSE8.5.5 / RSE8.5.10 / RSE8.5.12 / RAR9.2.1 / RAR9.2.2 / RAR9.2.3 / RAR9.2.4 / RAR9.2.5 / RPR10.2.6 / RPR10.3.1 / RPR10.3.6 / RSE11.3.3 / RSE11.3.8 / RSE11.4.4 / RSE11.4.5 / RSE11.6.2 / RSE11.7.1
Equivalência	--

Código de identificação	**MECV5 - Identificador do lote**
Rótulo	**moreqjus.eventoCv.loteId**
Definição	Identificador do lote que está sendo afetado pelo evento.
Obrigatoriedade	O
Repetibilidade	Não repetível
Regra de preenchimento	O código pode ser gerado automaticamente no evento Transferência-envio, Transferência-recebimento, Recolhimento e Eliminação.
Requisito	RPC3.1.16 / RPC3.1.18 / RPC3.4.3 / RPC3.4.5 / RPC3.4.6 /RCA4.1.6 / RAD8.4.7 / RSE8.5.2 / RSE8.5.3 / RSE8.5.5 / RSE8.5.10 / RSE8.5.12 / RAR9.2.1 / RAR9.2.2 / RAR9.2.3 / RAR9.2.4 / RAR9.2.5 / RPR10.2.6 / RPR10.3.1 / RPR10.3.6 / RSE11.3.3 / RSE11.3.8 / RSE11.4.4 / RSE11.4.5 / RSE11.6.2 / RSE11.7.1
Equivalência	--

Código de identificação	**MECV6 - Data e hora do evento**
Rótulo	**moreqjus.eventoCv.dataHora**
Definição	Data e hora em que o evento foi realizado.
Obrigatoriedade	O
Repetibilidade	Não repetível
Regra de preenchimento	É recomendável seguir o padrão da ISO 8601:2019 – Data elements and interchange formats — Information interchange — Representation of dates and times.
Requisito	RPC3.1.16 / RPC3.1.18 / RPC3.4.3 / RPC3.4.5 / RPC3.4.6 /RCA4.1.6 / RAD8.4.7 / RSE8.5.2 / RSE8.5.3 / RSE8.5.5 / RSE8.5.10 / RSE8.5.12 / RAR9.2.1 / RAR9.2.2 / RAR9.2.3 / RAR9.2.4 / RAR9.2.5 / RPR10.2.6 / RPR10.3.1 / RPR10.3.6 / RSE11.3.3 / RSE11.3.8 / RSE11.4.4 / RSE11.4.5 / RSE11.6.2 / RSE11.7.1
Equivalência	--

Código de identificação	**MECV7 - Agente responsável pelo evento**
Rótulo	**moreqjus.eventoCv.agenteId**
Definição	Agente responsável pela realização do evento. Captura: responsável pela captura, produção ou registro; Transferência – envio: responsável pelo envio dos documentos para guarda intermediária; Transferência – recebimento: responsável pelo recebimento dos documentos para guarda intermediária; Recolhimento – envio: responsável pelo envio dos documentos para guarda permanente; Eliminação: responsável pela eliminação dos documentos; Restrição de acesso: responsável pela restrição de acesso; Alteração da restrição de acesso: responsável pela alteração da restrição de acesso.
Obrigatoriedade	O
Repetibilidade	Não repetível
Regra de preenchimento	O código deve ser obtido no metadado MAGE1 Identificador do agente.
Requisito	RPC3.1.16 / RPC3.1.18 / RPC3.4.3 / RPC3.4.5 / RPC3.4.6 /RCA4.1.6 / RAD8.4.7 / RSE8.5.2 / RSE8.5.3 / RSE8.5.5 / RSE8.5.10 / RSE8.5.12 / RAR9.2.1 / RAR9.2.2 / RAR9.2.3 / RAR9.2.4 / RAR9.2.5 / RPR10.2.6 / RPR10.3.1 / RPR10.3.6 / RSE11.3.3 / RSE11.3.8 / RSE11.4.4 / RSE11.4.5 / RSE11.6.2 / RSE11.7.1
Equivalência	--

Código de identificação	**MECV8 - Detalhes do evento**
Rótulo	moreqjus.eventoCv.detalhe
Definição	Registro de informações adicionais a respeito do evento de gestão do ciclo de vida.
Obrigatoriedade	OA
Repetibilidade	Não repetível
Regra de preenchimento	Podem ser registradas informações tais como identificador do método de transferência; termo de transferência; identificador do termo de recolhimento; identificador do edital; fundamentação legal da classificação; motivação da desclassificação; justificativas; suporte; localização.
Requisito	RPC3.1.16 / RPC3.1.18 / RPC3.4.3 / RPC3.4.5 / RPC3.4.6 /RCA4.1.6 / RAD8.4.7 / RSE8.5.2 / RSE8.5.3 / RSE8.5.5 / RSE8.5.10 / RSE8.5.12 / RAR9.2.1 / RAR9.2.2 / RAR9.2.3 / RAR9.2.4 / RAR9.2.5 / RPR10.2.6 / RPR10.3.1 / RPR10.3.6 / RSE11.3.3 / RSE11.3.8 / RSE11.4.4 / RSE11.4.5 / RSE11.6.2 / RSE11.7.1
Equivalência	--

B1.3.2 Eventos de gestão do processo/dossiê

Registra os eventos relacionados aos procedimentos de produção e registro realizados no GestãoDoc. Inclui também abertura, encerramento/baixa e reabertura de processos/dossiês.

No caso de processos judiciais, os eventos estão previstos na Tabela de Movimentos do Sistema de Gestão das Tabelas Processuais Unificadas do CNJ (SGT).

Os eventos de gestão de processo/dossiê poderão assumir estes ou outros valores:

EGP1	Abertura de processo/dossiê
EGP2	Encerramento/baixa de volume/processo/dossiê
EGP3	Reabertura processo/dossiê
EGP4	Juntada anexação
EGP5	Juntada apensação
EGP6	Desapensação
EGP7	Desentranhamento
EGP8	Desmembramento
EGP9	Tramitação – Envio
EGP10	Tramitação – Recebimento

Cada evento deve ser registrado pelo seguinte conjunto de elementos de metadados:

- MEGP1 - Identificador do evento
- MEGP2 - Tipo de evento
- MEGP3 - Identificador do processo/dossiê
- MEGP4 - Data e hora do evento
- MEGP5 - Agente responsável pelo evento
- MEGP6 - Identificador do documento

Código de identificação	**MEGP1 - Identificador do evento**
Rótulo	moreqjus.eventoProc.id
Definição	Identificador do evento de gestão de processo que está sendo registrado no GestãoDoc.
Obrigatoriedade	O
Repetibilidade	Não repetível
Regra de preenchimento	Deve ser registrado automaticamente pelo GestãoDoc.
Requisito	RCA4.1.6 / RAR9.2.1 / RPR10.2.6 / RPR10.3.1/ RPR10.3.6 / RSE11.3.3 / RSE11.3.8 / RSE11.4.4 / RSE11.4.5
Equivalência	--

Código de identificação	**MEGP2 - Tipo de evento**
Rótulo	moreqjus.eventoProc.tipo
Definição	Identificação do evento de gestão do processo.
Obrigatoriedade	O
Repetibilidade	Não repetível
Regra de preenchimento	Este elemento poderá assumir, por exemplo, os seguintes valores ou movimentos da Tabela de Movimentos Processuais Unificados: Abertura de processo/dossiê Encerramento de processo/dossiê Reabertura processo/dossiê Juntada anexação Juntada apensação Desapensação Desentranhamento Desmembramento Tramitação – Envio Tramitação – Recebimento
Requisito	RCA4.1.6 / RAD8.4.7 / RAR9.2.1 / RAR9.2.2 / RAR9.2.3 / RAR9.2.4 / RAR9.2.5 / RPR10.2.6 / RPR10.3.1/ RPR10.3.6 / RSE11.3.3 / RSE11.3.8 / RSE11.4.4 / RSE11.4.5 / RSE11.6.2 / RSE11.7.1
Equivalência	--

Código de identificação	**MEGP3 - Identificador do processo/dossiê**
Rótulo	moreqjus.eventoProc.processoId
Definição	Identificador do processo.
Repetibilidade	Não repetível
Obrigatoriedade	O
Regra de preenchimento	O código deve ser obtido no metadado MDOC3 Identificador do processo/dossiê.
Requisito	RCA4.1.6 / RAD8.4.7 / RAR9.2.1 / RAR9.2.2 / RAR9.2.3 / RAR9.2.4 / RAR9.2.5 / RPR10.2.6 / RPR10.3.1/ RPR10.3.6 / RSE11.3.3 / RSE11.3.8 / RSE11.4.4 / RSE11.4.5 / RSE11.6.2 / RSE11.7.1
Equivalência	--

Código de identificação	**MEGP4 - Data e hora do evento**
Rótulo	moreqjus.eventoProc.dataHora
Definição	Data e hora em que o evento foi realizado.
Obrigatoriedade	O
Repetibilidade	Não repetível
Regra de preenchimento	É recomendável seguir o padrão da ISO 8601:2019 – Data elements and interchange formats — Information interchange — Representation of dates and times.
Requisito	RCA4.1.6 / RAD8.4.7 / RAR9.2.1 / RAR9.2.2 / RAR9.2.3 / RAR9.2.4 / RAR9.2.5 / RPR10.2.6 / RPR10.3.1/ RPR10.3.6 / RSE11.3.3 / RSE11.3.8 / RSE11.4.4 / RSE11.4.5 / RSE11.6.2 / RSE11.7.1
Equivalência	--

Código de identificação	**MEGP5 - Agente responsável pelo evento**
Rótulo	**moreqjus.eventoProc.agenteId**
Definição	Agente responsável pela realização do evento.
Obrigatoriedade	O
Repetibilidade	Não repetível
Regra de preenchimento	O código deve ser obtido no metadado MAGE1 Identificador do agente.
Requisito	RCA4.1.6 / RAD8.4.7 / RAR9.2.1 / RAR9.2.2 / RAR9.2.3 / RAR9.2.4 / RAR9.2.5 / RPR10.2.6 / RPR10.3.1/ RPR10.3.6 / RSE11.3.3 / RSE11.3.8 / RSE11.4.4 / RSE11.4.5 / RSE11.6.2 / RSE11.7.1
Equivalência	--

Código de identificação	**MEGP6 - Identificador do documento**
Rótulo	**moreqjus.eventoProc.DocId**
Definição	Identificador do documento.
Obrigatoriedade	OA
Repetibilidade	Repetível
Regra de preenchimento	O código deve ser obtido no metadado MDOC2 - Identificador do documento.
Requisito	RCA4.1.6 / RAD8.4.7 / RAR9.2.1 / RAR9.2.2 / RAR9.2.5 / RPR10.2.6 / RPR10.3.1 / RPR10.3.6 / RSE11.3.3 / RSE11.3.8 / RSE11.4.4 / RSE11.4.5 / RSE11.7.1
Equivalência	--

B1.3.3 Eventos de gerenciamento da classe

Registram os eventos de gerenciamento dos planos de classificação.

Os eventos de gerenciamento da classe previstos são:

EGC1	Abertura de classe
EGC2	Desativação de classe
EGC3	Reativação de classe
EGC4	Mudança de nome de classe
EGC5	Deslocamento de classe
EGC6	Extinção de classe
EGC7	Alteração de prazo corrente
EGC8	Alteração de evento corrente
EGC9	Alteração de prazo intermediária
EGC10	Alteração de evento intermediária
EGC11	Alteração de destinação
EGC12	Alteração de sigilo associado à classe

Cada evento deve ser registrado pelo seguinte conjunto de elementos de metadados:

- MEGC1 - Identificador do evento
- MEGC2 - Tipo de evento
- MEGC3 - Identificador da classe afetada
- MEGC4 - Data e hora do evento
- MEGC5 - Agente responsável pelo evento
- MEGC6 - Valor anterior do atributo

Código de identificação	**MEGC1 - Identificador do evento**
Rótulo	moreqjus.eventoClasse.id
Definição	Identificador do evento de gerenciamento de classe que está sendo registrado no GestãoDoc.
Obrigatoriedade	O
Repetibilidade	Não repetível
Regra de preenchimento	Deve ser registrado automaticamente pelo GestãoDoc.
Requisito	RPC3.1.4 / RPC3.1.5 / RPC3.1.6 / RPC3.1.7 / RPC3.1.8 / RPC3.1.20 / RPC3.1.21 / RPC3.1.24 / RUS 13.1.9
Equivalência	--

Código de identificação	**MEGC2 -Tipo de evento**
Rótulo	moreqjus.eventoClasse.tipo
Definição	Identificação do tipo de evento de gerenciamento de classe.
Obrigatoriedade	O
Repetibilidade	Não repetível
Regra de preenchimento	Este elemento poderá assumir os seguintes valores: Abertura de classe Desativação de classe Reativação de classe Mudança de nome de classe Deslocamento de classe Extinção de classe Alteração de prazo corrente Alteração de evento corrente Alteração de prazo intermediária Alteração de evento intermediária Alteração de destinação Alteração de sigilo associado à classe
Requisito	RPC3.1.4 / RPC3.1.5 / RPC3.1.6 / RPC3.1.7 / RPC3.1.8 / RPC3.1.20 / RPC3.1.21 / RPC3.1.24
Equivalência	--

Código de identificação	**MEGC3 -Identificador da classe afetada**
Rótulo	**moreqjus.eventoClasse.classeId**
Definição	Identificador da classe afetada pelo evento de gerenciamento de classe que está sendo registrado.
Obrigatoriedade	O
Repetibilidade	Não repetível
Regra de preenchimento	O identificador deve ser obtido no elemento MCLA1 Identificador da classe
Requisito	RPC3.1.4 / RPC3.1.5 / RPC3.1.6 / RPC3.1.7 / RPC3.1.8 / RPC3.1.20 / RPC3.1.21 / RPC3.1.24
Equivalência	--

Código de identificação	**MEGC4 -Data e hora do evento**
Rótulo	**moreqjus.eventoClasse.dataHora**
Definição	Data e hora em que o evento foi realizado.
Obrigatoriedade	O
Repetibilidade	Não repetível
Regra de preenchimento	É recomendável seguir o padrão da ISO 8601:2019 – Data elements and interchange formats — Information interchange — Representation of dates and times.
Requisito	RPC3.1.4 / RPC3.1.5 / RPC3.1.6 / RPC3.1.7 / RPC3.1.8 / RPC3.1.20 / RPC3.1.21 / RPC3.1.24
Equivalência	--

Código de identificação	**MEGC5 -Agente responsável pelo evento**
Rótulo	**moreqjus.eventoClasse.agenteId**
Definição	Identificar o agente responsável pelo evento.
Obrigatoriedade	O
Repetibilidade	Não repetível
Regra de preenchimento	O identificador deve ser obtido no elemento MAGE1 Identificador do agente.
Requisito	RPC3.1.4 / RPC3.1.5 / RPC3.1.6 / RPC3.1.7 / RPC3.1.8 / RPC3.1.20 / RPC3.1.21 / RPC3.1.24
Equivalência	--

Código de identificação	**MEGC6 -Valor anterior do atributo**
Rótulo	**moreqjus.eventoClasse.valorAnterior**
Definição	Valor do elemento antes da realização do evento.
Objetivo	Possibilitar a recuperação histórica dos conteúdos alterados.
Obrigatoriedade	OA
Repetibilidade	Não repetível
Regra de preenchimento	Antes de realizar a alteração, copiar o valor do elemento específico de Identificação da classe que está sendo alterado (moreqjus.classe.nome, moreqjus.classe.codigo, moreqjus. classe.subordinacao, moreqjus.classe.indicadorUso, moreqjus.classe.indicadorAtiva, moreqjus.classe.prazoCorrente, moreqjus.classe.eventoCorrente, moreqjus.classe.prazoIntermediaria, moreqjus.classe.eventoIntermediaria, moreqjus.Classe.destinacao, moreqjus.classe.sigilo, moreqjus.classe.observacao). Obrigatórios para os eventos EGC7, EGC8, EGC9, EGC10, EGC11 e EGC12.
Requisito	RPC3.1.4 / RPC3.1.5 / RPC3.1.6 / RPC3.1.7 / RPC3.1.8 / RPC3.1.20 / RPC3.1.21 / RPC3.1.24
Equivalência	--

B1.3.4 Eventos de preservação

Os metadados indicados neste capítulo são os mais relevantes para a preservação dos componentes digitais. Trata-se de rol não exauriente, podendo ser previstos outros entendidos necessários pelos órgãos do Poder Judiciário.

Os eventos de preservação previstos são:

EPR1	Compressão	Registro da compressão ou descompressão de componentes digitais.
EPR2	Decifração	Registro da decifração de componentes digitais criptografados.
EPR3	Validação de assinatura digital	Registro da validação da assinatura digital de um documento, no momento da captura, por meio da conferência com o certificado digital.
EPR4	Cálculo *hash*	Registro do cálculo *hash* do arquivo, a ser armazenado no elemento de metadado do componente digital *moreqjus.componente.fixidade*, que serve para apoiar a verificação de fixidade ao longo do tempo.
EPR5	Verificação de fixidade[10]	Registro da verificação da fixidade do componente digital.
EPR6	Migração	Registro de procedimento de migração do componente digital.
EPR7	Replicação	Registro de procedimento de replicação do componente digital.
EPR8	Verificação de vírus	Registro de verificação de vírus no componente digital.
EPR9	Validação	Registro da validação do documento.

10. A verificação da fixidade é um evento de preservação que consiste em verificar a integridade da cadeia de bits que constitui um componente digital. É realizada por meio da comparação do resultado do cálculo *hash* com o valor armazenado no metadado *earq.componente.fixidade*. Não confundir com fixidez da forma documental, que diz respeito à manutenção da forma de um documento, ou seja, a garantia de que sua aparência ou apresentação documental permanece a mesma cada vez que o documento é manifestado, ou pode ser alterada segundo regras fixas (i.e., é dotado de variabilidade limitada). É importante notar que a perda da integridade dos bits não implica necessariamente a perda da integridade do documento conceitual, que só se dá quando há alteração na sua forma e conteúdo, de maneira lícita ou ilícita.

Cada evento deve ser registrado pelo seguinte conjunto de elementos de metadados:

- MEPR1 - Identificador do evento
- MEPR2 - Tipo de evento
- MEPR3 - Componente digital
- MEPR4 - Data e hora do evento
- MEPR5 - Agente responsável pelo evento
- MEPR6 - Resultado do evento
- MEPR7 - Detalhes do evento

Código de identificação	**MEPR1 - Identificador do evento**
Rótulo	**moreqjus.ePres.id**
Definição	Identificador do evento de preservação que está sendo registrado no GestãoDoc.
Obrigatoriedade	O
Repetibilidade	Não repetível
Regra de preenchimento	Deve ser registrado automaticamente pelo GestãoDoc.
Requisito	RCA4.1.6 / RSE8.3.2 / RAR9.2.1 / RAR9.2.2 / RAR9.2.3 / RAR9.2.4 / RAR9.2.5 / RPR10.2.6 / RPR10.3.1 / RPR10.3.6 / RSE11.3.3 / RSE11.3.8 / RSE11.4.4 / RSE11.4.5 / RSE11.6.2 / RSE11.7.1
Equivalência	--

Código de identificação	**MEPR2 - Tipo de evento**
Rótulo	**moreqjus.ePres.tipo**
Definição	Categoriza o tipo de evento de preservação.
Obrigatoriedade	O
Repetibilidade	Não repetível
Regra de preenchimento	Este elemento poderá assumir, no mínimo, os seguintes valores: Compressão Decifração Validação de assinatura digital Cálculo *hash* Verificação de fixidade Migração Replicação Verificação de vírus Validação
Requisito	RCA4.1.6 / RSE8.3.2 / RAR9.2.1 / RAR9.2.2 / RAR9.2.3 / RAR9.2.4 / RAR9.2.5 / RPR10.2.6 / RPR10.3.1 / RPR10.3.6 / RSE11.3.3 / RSE11.3.8 / RSE11.4.4 / RSE11.4.5 / RSE11.6.2 / RSE11.7.1
Equivalência	Premis: eventType

Código de identificação	**MEPR3 - Componente digital**
Rótulo	**moreqjus.ePres.componenteId**
Definição	Identificador do componente digital que está sendo afetado pelo evento de preservação registrado.
Obrigatoriedade	O
Repetibilidade	Repetível
Regra de preenchimento	O código deve ser obtido no metadado MCDI1 Identificador do componente digital
Requisito	RCA4.1.6 / RSE8.3.2 / RAR9.2.1 / RAR9.2.2 / RAR9.2.3 / RAR9.2.4 / RAR9.2.5 / RPR10.2.6 / RPR10.3.1 / RPR10.3.6 / RSE11.3.3 / RSE11.3.8 / RSE11.4.4 / RSE11.4.5 / RSE11.6.2 / RSE11.7.1
Equivalência	Premis: linkingObjectIdentifierValue

Código de identificação	**MEPR4 - Data e hora do evento**
Rótulo	**moreqjus.ePres.dataHora**
Definição	Data e hora em que o evento foi realizado, ou de seu início.
Obrigatoriedade	O
Repetibilidade	Não repetível
Regra de preenchimento	É recomendável seguir o padrão da ISO 8601:2019 – Data elements and interchange formats — Information interchange — Representation of dates and times.
Requisito	RCA4.1.6 / RSE8.3.2 / RAR9.2.1 / RAR9.2.2 / RAR9.2.3 / RAR9.2.4 / RAR9.2.5 / RPR10.2.6 / RPR10.3.1 / RPR10.3.6 / RSE11.3.3 / RSE11.3.8 / RSE11.4.4 / RSE11.4.5 / RSE11.6.2 / RSE11.7.1
Equivalência	Premis: eventDateTime

Código de identificação	**MEPR5 - Agente responsável pelo evento**
Rótulo	**moreqjus.ePres.agenteId**
Definição	Agente responsável pelo evento.
Obrigatoriedade	O
Repetibilidade	Repetível
Regra de preenchimento	O identificador deve ser obtido no metadado MAGE1 Identificador do agente
Requisito	RCA4.1.6 / RSE8.3.2 / RAR9.2.1 / RAR9.2.2 / RAR9.2.3 / RAR9.2.4 / RAR9.2.5 / RPR10.2.6 / RPR10.3.1 / RPR10.3.6 / RSE11.3.3 / RSE11.3.8 / RSE11.4.4 / RSE11.4.5 / RSE11.6.2 / RSE11.7.1
Equivalência	Premis: linkingAgentIdentifierValue

Código de identificação	**MEPR6 - Resultado do evento**
Rótulo	**moreqjus.ePres.Resultado**
Definição	Resultado do evento de preservação.
Obrigatoriedade	AO
Repetibilidade	Repetível
Exemplo	00 [código para registrar que a ação foi completada com sucesso]. CV-01 [código para registrar que o *checksum* foi validado].
Regra de preenchimento	Recomenda-se o uso de tabela com os resultados possíveis para padronização do preenchimento do elemento de metadado.
Requisito	RCA4.1.6 / RSE8.3.2 / RAR9.2.1 / RAR9.2.2 / RAR9.2.3 / RAR9.2.4 / RAR9.2.5 / RPR10.2.6 / RPR10.3.1 / RPR10.3.6 / RSE11.3.3 / RSE11.3.8 / RSE11.4.4 / RSE11.4.5 / RSE11.6.2 / RSE11.7.1
Equivalência	Premis: eventOutcome

Código de identificação	**MEPR7 - Detalhes do evento**
Rótulo	moreqjus.ePres.detalhe
Definição	Registro de informações adicionais a respeito do evento de preservação.
Nota de aplicação	Pode se registrar a metodologia e/ou tecnologia (software e hardware) utilizada no evento, bem como eventuais consequências no documento.
Obrigatoriedade	F
Repetibilidade	Repetível
Regra de preenchimento	--
Requisito	RCA4.1.6 / RSE8.3.2 / RAR9.2.1 / RAR9.2.2 / RAR9.2.3 / RAR9.2.4 / RAR9.2.5 / RPR10.2.6 / RPR10.3.1 / RPR10.3.6 / RSE11.3.3 / RSE11.3.8 / RSE11.4.4 / RSE11.4.5 / RSE11.6.2 / RSE11.7.1
Equivalência	Premis:eventDetailInformation

B1.4 Componente digital

Estas informações referem-se à identidade e às características do componente digital e possibilitam a identificação destes componentes no sistema de gestão arquivística de documentos, além de apoiar as ações de preservação de documentos digitais.

- MCDI1 - Identificador do componente digital
- MCDI2 - Nome original
- MCDI3 - Tamanho
- MCDI4 - Software de criação
- MCDI5 - Nível de composição
- MCDI6 - Inibidor
- MCDI7 - Formato de arquivo
- MCDI8 - Localização
- MCDI9 - Suporte
- MCDI10 - Dependência de software

- MCDI11 - Dependência de hardware
- MCDI12 - Outras dependências
- MCDI13 - Relação com outros componentes digitais
- MCDI14 - Fixidade
- MCDI15 - Assinatura digital

Para os elementos de metadados referentes a identificação *de* **Componente Digital** foi elaborada uma ficha individual que detalha cada elemento e apresenta as seguintes informações:

Código de identificação	
Rótulo	
Definição	
Objetivo	
Repetibilidade	
Nota de aplicação	
Exemplos	
Regra de preenchimento	
Requisito	
Equivalência	

- **Código de identificação e nome**: indicação do código e do nome atribuídos ao elemento.
- **Rótulo:** nome padrão que deve ser utilizado para identificar o elemento a fim de facilitar a interoperabilidade de sistemas.
- **Definição:** indica qual informação deve ser registrada no elemento de metadado.
- **Objetivo:** a referência do que se pretende alcançar com a aplicação do elemento.
- **Obrigatoriedade:** indica a obrigatoriedade da aplicação do elemento. Os valores possíveis são: *obrigatório (O); obrigatório se aplicável (OA); facultativo (F); ou não se aplica (NA).*
- **Repetibilidade:** indica se a informação pode ser registrada mais de uma vez.
- **Nota de aplicação:** sugere formas de aplicação do elemento.
- **Exemplos:** apresenta alguns exemplos de aplicação que explicam o elemento.
- **Regra de preenchimento:** regra que especifica os valores, a codificação ou a lista de autoridades (lista de valores autorizados) convencionados para o preenchimento do elemento.
- **Requisito:** os requisitos funcionais relacionados com o elemento de metadado.
- **Equivalência:** referências para elementos equivalentes de outros esquemas de metadados.

Código de identificação	**MCDI1 - Identificador do componente digital**
Rótulo	**moreqjus.componente.id**
Definição	Designação usada para identificar no GestãoDoc os componentes digitais que integram o documento.
Objetivo	Identificar de forma unívoca e persistente os componentes digitais dos documentos armazenados pelo GestãoDoc. Cada componente digital mantido no repositório tem que possuir um identificador único para relacioná-lo aos metadados descritivos e técnicos de forma que o GestãoDoc possa gerenciá-lo.
Obrigatoriedade	O
Repetibilidade	Não repetível
Nota de aplicação	O identificador do componente digital tem que ser único no âmbito do GestãoDoc.
Exemplos	IU24548 10.1016/S1057-2317(03)00016-X http://purl.oclc.org /OCLC/PURL/FAQ
Regra de preenchimento	Pode ser utilizado um identificador persistente, tal como DOI Handle System[11], mas isso não é obrigatório. Esta é uma decisão de implementação, e o tipo de identificador e a regra de formação deste devem estar claramente documentados.
Requisito	RCA4.1.5 / RCA4.1.20 / RCA4.1.26
Equivalência	Premis:ObjectIdentifierValue

11. DOI – Digital Object Identifier. Disponível em: https://www.doi.org. Acesso em: 16 out. 2022..

Código de identificação	**MCDI2 - Nome original**
Rótulo	**moreqjus.componente.nomeOriginal**
Definição	Nome original do arquivo referente ao componente digital no momento em que foi capturado no GestãoDoc, antes de ser renomeado com o identificador do GestãoDoc.
Objetivo	Possibilitar a identificação do componente digital por meio de seu nome original devido a razões diversas: o nome utilizado dentro do GestãoDoc pode não ser conhecido externamente; um produtor de arquivos pode procurar um documento pelo nome original do arquivo ou, ainda, o GestãoDoc pode necessitar reconstruir links originais com objetivo de acesso.
Obrigatoriedade	F
Repetibilidade	Não repetível
Nota de aplicação	Quando um GestãoDoc está importando documento de outro GestãoDoc, deve-se registrar o nome original do componente para verificação posterior.
Exemplos	0078NR.TIF
Regra de preenchimento	O conteúdo deve ser obtido automaticamente no momento da captura do documento para o GestãoDoc.
Requisito	RCA4.1.5 / RCA4.1.20 / RCA4.1.26
Equivalência	Premis:originalName

Código de identificação	**MCDI3 - Tamanho**
Rótulo	**moreqjus.componente.tamanho**
Definição	Informa o tamanho do componente digital em bytes.
Objetivo	Esta informação é útil para garantir a previsão de espaço de memória suficiente para mover ou processar arquivos, bem como para previsão de capacidade de armazenamento.
Obrigatoriedade	F
Repetibilidade	Não repetível
Nota de aplicação	O tamanho deve ser sempre indicado na mesma unidade (bytes), pois dessa forma fica dispensado o registro da unidade de medida. No caso de transferência desse metadado para outro sistema, é necessário que a outra parte esteja ciente da unidade de medida.
Exemplos	Tamanho: 345687
Regra de preenchimento	Deve ser obtido automaticamente pelo GestãoDoc.
Requisito	RCA4.1.5 / RCA4.1.20 / RCA4.1.26
Equivalência	Premis:size

Código de identificação	**MCDI4 - Software de criação**
Rótulo	**moreqjus.componente.softwareCriacao**
Definição	Informação a respeito do software utilizado para criar o componente digital.
Objetivo	Fornecer informações a respeito do software que criou o componente, para identificação de um software compatível para apresentação do documento ou para fins de conversão visando à preservação.
Obrigatoriedade	F
Repetibilidade	Não repetível
Nota de aplicação	Devem ser informados o nome do software, a versão e a data da criação do componente digital. Esse metadado deve ser registrado de forma estruturada, em três subelementos, conforme a seguir: · moreqjus.componente.SoftwareCriacaoNome · moreqjus.componente.SoftwareCriacaoVersao · moreqjus.componente.SoftwareCriacaoData
Exemplos	· moreqjus.componente.SoftwareCriacaoNome: MS Word · moreqjus.componente.SoftwareCriacaoVersao: 7 · moreqjus.componente.SoftwareCriacaoVersao: 2009-10-06
Regra de preenchimento	Pode ser extraído automaticamente do arquivo no momento da captura, uma vez que esse metadado é comumente registrado internamente no arquivo.
Requisito	Ver capítulo 10 (Preservação) RCA4.1.5 / RCA4.1.20 / RCA4.1.26
Equivalência	Premis:creatingApplicationName Premis:creatingApplicationVersion Premis:dateCreatedByApplication

Código de identificação	**MCDI5 - Nível de composição**
Rótulo	**moreqjus.componente.nivelComposicao**
Definição	Informação sobre se o componente digital está sujeito a um ou mais processos de compressão, criptografia ou empacotamento, bem como qual é esse nível.
Objetivo	Fornecer informações para orientar as intervenções necessárias para o acesso ao documento.
Obrigatoriedade	AO
Repetibilidade	Não repetível
Nota de aplicação	Nível de composição <0> (zero) indica que o componente digital não está sujeito a nenhum desses processos. Nível de composição <1> (um) ou maior indica que o componente digital foi submetido a um ou mais processos de compressão, criptografia ou empacotamento e que deve ser processado para que o documento possa ser acessado. Por exemplo, um arquivo A pode ser comprimido e gerar um arquivo B, que por sua vez é cifrado e gera um arquivo C. Para se ter acesso ao arquivo A é necessário decifrar o arquivo C e depois descomprimir o arquivo B. Ver descrição mais detalhada em Premis - Object characteristics and composition level: the “onion” model
Exemplos	0, 1, 2, ..., desconhecido
Regra de preenchimento	Zero, números inteiros positivos ou “desconhecido”.
Requisito	Ver capítulo 10 (Preservação) RCA4.1.1 / RCA4.1.2 / RCA4.1.5 / RCA4.1.6 / RCA4.1.12 / RCA4.1.13 / RCA4.1.14 / RCA4.1.20 / RCA4.1.26 / RAD6.2.1 / RAD6.2.2 / RAD6.2.4 / RAD6.2.8 / ROA7.3.15 / RSE8.3 / RPR10.2.8 / RPR10.3.6 / RSE11.3.1 / RSE11.3.3 / RSE11.3.8 / RIN14.1.1
Equivalência	Premis:CompositionLevel

Código de identificação	**MCDI6 - Inibidor**
Rótulo	moreqjus.componente.inibidor
Definição	Recursos que inibem o acesso, uso ou migração do componente digital.
Objetivo	Informar se um arquivo está criptografado, se tem proteção por senha, bem como as informações necessárias para sua decifração e acesso.
Obrigatoriedade	F
Repetibilidade	Não repetível
Nota de aplicação	Devem ser informados o tipo de inibidor, o alvo e a chave de acesso. Esse metadado deve ser registrado de forma estruturada, em três subelementos, conforme a seguir: Componente.InibidorTipo – refere-se ao método utilizado; Componente.InibidorAlvo – refere-se ao conteúdo ou à função protegida pelo inibidor; Componente.InibidorChave – refere-se à chave ou senha para decifração. A chave deve ser indicada, quando conhecida. No entanto, não é recomendável ser armazenada na forma de texto em um banco de dados não seguro.
Exemplos	Componente.InibidorTipo: DES Componente.InibidorAlvo: All content Componente.Inibidorchave: 65kgedr5
Regra de preenchimento	Quando um documento produzido externamente ao GestãoDoc tem um inibidor, é preciso que estas informações sejam fornecidas como metadados e enviadas juntamente com o documento capturado. Recomenda-se o uso de formas controladas para o subelemento “InibidorTipo”, preferencialmente a tabela sugerida no PREMIS Data dictionary: DES, PGP, Blowfish e Password Protection[12]. Quando o subelemento “InibidorAlvo” não é informado, assume-se que é todo o conteúdo do componente digital. Recomenda-se o uso de formas controladas para o subelemento “InibidorAlvo”, preferencialmente a tabela sugerida no PREMIS Data dictionary: All content, Function:play, Function:print[13].
Requisito	Ver capítulo 10 (Preservação) e 11 (Segurança) RPC3.2.4 / RCA4.2.2 / RCA4.1.2 / RCA4.1.5 / RCA4.1.6 / RCA4.1.13 / RCA4.1.14 / RCA4.1.20 / RCA4.1.26 / RSE11.3.1 / RSE11.3.2 / RSE11.3.3 / RSE11.3.4
Equivalência	Premis:inhibitorType Premis:inhibitorTarget Premis:inhibitorKey

12. Lista controlada pela Library of Congress, sugerida no PREMIS Data Dictionary. Disponível em: http://id.loc.gov/vocabulary/preservation/inhibitorType.html. Acesso em: 16 out. 2022...
13. Lista controlada pela Library of Congress, sugerida no PREMIS Data Dictionary. Disponível em: http://id.loc.gov/vocabulary/preservation/inhibitorType.html. Acesso em: 16 out. 2022...

Código de identificação	**MCDI7 - Formato de arquivo**
Rótulo	moreqjus.componente.formato
Definição	Identificação do formato de arquivo do componente digital.
Objetivo	O conhecimento do formato de arquivo do componente digital é essencial para o planejamento e a implementação de diversas ações de preservação como, por exemplo, a conversão devido à obsolescência do formato.
Obrigatoriedade	O
Repetibilidade	Não repetível
Nota de aplicação	Esse metadado deve ser registrado de forma estruturada, em dois subelementos, conforme a seguir: · moreqjus.componente.formatoNome · moreqjus.componente.formatoVersao Informações adicionais sobre o formato também podem ser registradas. Nos casos em que não for possível identificar o formato, este deve ser registrado como "desconhecido", e posteriormente identificado.
Exemplos	· moreqjus.componente.formatoNome: Adobe PDF/A-1A · moreqjus.componente.formatoVersao: 1.4
Regra de preenchimento	Recomenda-se o uso de formas controladas para a designação do formato, como bases de dados de registro de formato. Ex.: PRONOM[14], MIME[15]. Deve ser identificado automaticamente pelo GestãoDoc no momento da captura.
Requisito	RCA4.1.6 / RCA4.4.1 / RCA4.4.2 / RCA4.4.7 / RCA4.4.9 / RAD6.2.3 / RAD6.2.4 / RAD6.2.5 / RPA7.2.6 / RPA7.3.8 / RA7.3.9 / RPA7.3.12 / RCA4.1.5 / RCA4.1.20 / RCA4.1.26
Equivalência	Premis:formatName Premis:formatVersion

14. Serviço de base de dados de formatos de arquivo gerenciada pelo The National Archives (TNA), do Reino Unido. Disponível em: https://www.nationalarchives.gov.uk/PRONOM/Default.aspx. Acesso em: 16 out. 2022..
15. Lista de formatos digitais mais comuns na internet. Disponível em: https://www.iana.org/assignments/media-types/media-types.xhtml. Acesso em: 16 out. 2022..

Código de identificação	**MCDI8 - Localização**
Rótulo	moreqjus.componente.localizacao
Definição	Informações sobre a localização do componente digital.
Objetivo	As informações sobre localização são necessárias para encontrar o componente digital no sistema de armazenamento.
Obrigatoriedade	AO
Repetibilidade	Repetível
Nota de aplicação	Caso o GestãoDoc utilize um identificador como o handle, a localização estará implícita no identificador e não será necessário registrá-la novamente. Caso o GestãoDoc utilize uma única localização onde todos os componentes digitais são armazenados (um único sistema de arquivos), esta informação pode estar descrita na estrutura de configuração do GestãoDoc. Caso o GestãoDoc utilize um sistema de banco de dados para armazenar os componentes digitais, este item estará informado no próprio sistema. As operações de destinação do documento não necessariamente afetarão a sua localização. Por exemplo, um documento que será transferido para guarda intermediária, desde que o GestãoDoc tenha este suporte, poderá simplesmente ter a sua movimentação registrada para a unidade organizacional responsável pela guarda intermediária, sem que isso afete a localização do arquivo digital. Esse metadado deve ser registrado de forma estruturada, em dois subelementos, conforme a seguir: moreqjus.componente.localizacaoTipo moreqjus.componente.localizacaoValor
Exemplos	moreqjus.componente.localizacaoTipo: URI moreqjus.componente.localizacaoValor: https://www.gov.br/conarq/pt-br moreqjus.componente.localizacaoTipo: NTFS moreqjus.componente.localizacaoValor: C:\MyDocuments\Textos\Preservacao_digital moreqjus.componente.localizacaoTipo: URI moreqjus.componente.localizacaoValor: https://cnjjusbr.sharepoint.com/sites/ MoReq-Jus/Shared/Documents/MoReq-Jus.docx
Regra de preenchimento	De forma geral, a localização deve ser preenchida automaticamente pelo GestãoDoc.
Requisito	RPC3.6.3 / RCA4.1.24 / RFT5.3.1 / RFT5.3.2 / RTF5.3.3 / RPA7.2.21 / RAD8.4.3 / RAR9.1.18 / RPR10.3.8 / RPR10.3.2 / RPR10.3.4 / RPR10.3.6 / RPR10.3.7 / RSE11.2.8
Equivalência	Premis:contentLocationType Premis:contentLocationValue

Código de identificação	**MCDI9 - Suporte**
Rótulo	moreqjus.componente.suporte
Definição	Suporte físico no qual o componente digital está armazenado.
Objetivo	As informações sobre o suporte em que o componente digital está armazenado apoiam o monitoramento das ações de preservação necessárias, como, por exemplo, a atualização de suporte.
Obrigatoriedade	F
Repetibilidade	Não repetível
Nota de aplicação	Quanto ao suporte, devem ser registradas informações a respeito do tipo de suporte utilizado e sua vida útil. Os responsáveis pela preservação digital devem gerenciar a obsolescência das mídias de armazenamento. Em geral, esse monitoramento é realizado no nível do sistema de armazenamento, e não especificamente para cada item documental ou componente digital. Esta informação se aplica também a documentos que estão armazenados fora da estrutura de armazenamento do GestãoDoc, tais como provas de elevado volume digital mantidas em DVD´s. A informação é importante para auxiliar na recuperação do suporte, análise da obsolescência e rastreabilidade da cadeia de custódia.
Exemplos	Fita magnética, HD, CD-ROM, DVD.
Regra de preenchimento	O preenchimento da informação deve ser realizado na captura do documento.
Requisito	RFT5.3.1 / RFT5.3.2 / RFT5.3.3 / RPR10.1.1 / RPR10.1.2 / RPR10.1.3 / RPR10.1.4 / RPR10.1.5 / RSE11.2.8
Equivalência	Premis:storageMedium

Código de identificação	**MCDI10 - Dependência de *software***
Rótulo	**moreqjus.componente.sw**
Definição	Informações sobre o ambiente de software necessário para apresentar e/ou usar os componentes digitais, incluindo a aplicação e o sistema operacional.
Objetivo	Dar conhecimento do ambiente de software necessário para uso do recurso.
Obrigatoriedade	AO
Repetibilidade	Repetível
Nota de aplicação	Esse metadado deve ser registrado de forma estruturada, em quatro subelementos, conforme a seguir: moreqjus.componente.swNome moreqjus.componente.swVersao moreqjus.componente.swTipo moreqjus.componente.swDocumentacao
Exemplos	moreqjus.componente.swNome: Windows moreqjus.componente.swVersao: XP moreqjus.componente.swTipo: sistema operacional moreqjus.componente.swDocumentacao: manual do sistema moreqjus.componente.swNome: Word moreqjus.componente.swVersao: 7 moreqjus.componente.swTipo: aplicativo/visualizador
Regra de preenchimento	No caso de não haver uma versão formal do software, pode se indicar o ano em que foi lançado. Valores sugeridos para tipo de software: sistema operacional, aplicativo/visualizador, driver, biblioteca. Com relação à documentação, pode se indicar um identificador persistente que aponte para documentação do software, dentro ou fora do GestãoDoc.
Requisito	RCA4.1.2 / RCA4.1.6 / RCA4.4.2 / RAD6.2.5 / RPA7.3.9 / RPR10.2.7 / RPR10.3.2 / RPR10.3.8 / RUS13.1.1
Equivalência	Premis:swName Premis:swVersion Premis:swType Premis:swOtherInformation

Código de identificação	**MCDI11 - Dependência de *hardware***
Rótulo	**moreqjus.componente.hw**
Definição	Informações sobre os componentes de hardware necessários para operar o software referenciado em moreqjus.componente.sw, incluindo periféricos.
Objetivo	Dar conhecimento do ambiente de hardware necessário para uso do recurso.
Obrigatoriedade	AO
Repetibilidade	Repetível
Nota de aplicação	Esse metadado deve ser registrado de forma estruturada, em três subelementos, conforme a seguir: moreqjus.componente.hwNome moreqjus.componente.hwTipo moreqjus.componente.hwOutrasInformacoes
Exemplos	moreqjus.componente.hwNome: Intel x86 moreqjus.componente.hwTipo: processador moreqjus.componente.hwOutrasInformacoes: configuração mínima 60 Mhz moreqjus.componente.hwNome: RAM moreqjus.componente.hwTipo: memória moreqjus.componente.hwOutrasInformacoes: configuração mínima 64 Mb
Regra de preenchimento	Na informação sobre o nome do hardware, deve se registrar o fabricante, o modelo e a versão, quando pertinente. Valores sugeridos para tipos de hardware: processador, memória, dispositivos de entrada/saída, dispositivo de armazenamento. Outras informações podem incluir a configuração mínima recomendada ou documentação pertinente. Com relação à documentação, pode-se registrar um identificador persistente que aponte para documentação do hardware, dentro ou fora do GestãoDoc.
Requisito	Ver capítulo 10 (Preservação) / RPR10.3.8 / RUS13.1.1
Equivalência	Premis:hwName Premis:hwType Premis:hwOtherInformation

Código de identificação	**MCDI12 - Outras dependências**
Rótulo	**moreqjus.componente.outrasDependencias**
Definição	Informações sobre outras dependências, que não sejam as de software e hardware, necessárias para apresentar ou usar os documentos (por exemplo, DTD, XML Schema, fontes, folha de estilo).
Objetivo	Dar informação sobre outros tipos de dependências, além de software e hardware, necessárias para uso do recurso.
Obrigatoriedade	AO
Repetibilidade	Repetível
Nota de aplicação	Esse metadado deve ser registrado de forma estruturada, em dois subelementos, conforme a seguir: moreqjus.componente.outrasDependenciasTipo moreqjus.componente.outrasDependenciasId Em alguns casos o identificador do recurso já torna evidente o tipo do componente necessário.
Exemplos	moreqjus.componente.outrasDependenciasTipo: URI moreqjus.componente.outrasDependenciasId: https://wst.stf.jus.br/servico-intercomunicacao-2.2.2/intercomunicacao?wsdl
Regra de preenchimento	--
Requisito	Ver capítulo 10 (Preservação)
Equivalência	Premis:dependencyName Premis:dependencyIdentifierType Premis:dependencyIdentifierValue

Código de identificação	**MCDI13 - Relação com outros componentes digitais**
Rótulo	**moreqjus.componente.relacao**
Definição	Registro das relações de um componente digital com outros componentes digitais.
Objetivo	Tornar explícito o relacionamento entre componentes digitais para possibilitar o processamento e acesso aos documentos. Alguns documentos são formados por diversos componentes digitais relacionados. Estas relações são estruturais.
Obrigatoriedade	AO
Repetibilidade	Repetível
Nota de aplicação	As relações estruturais são fundamentais para apresentar o documento ao usuário. Devem ser registradas as seguintes informações para cada relacionamento: identificação dos objetos relacionados, tipo da relação (por exemplo, é parte de). Os órgãos devem estabelecer os tipos de relacionamentos mais relevantes, que deverão ser controlados nos metadados. Estas relações podem ser expressas das seguintes formas: tem parte de, é parte de (expressa as relações estruturais); tem fonte de (um componente digital é uma versão de outro componente, criado por uma transformação), é fonte de (um componente derivado de outro componente por um processo de transformação).
Exemplos	“relat_2009.pdf” é fonte de “relat_2009.zip”
Regra de preenchimento	--
Requisito	Ver capítulo 10 (Preservação) / RCA4.1.5
Equivalência	Premis:relationshiptype Premis:relationshipSubType Premis:relatedObjectIdentifier

Código de identificação	**MCDI14 - Fixidade**
Rótulo	**moreqjus.componente.fixidade**
Definição	Informações utilizadas para verificar se o componente digital sofreu mudanças não documentadas.
Objetivo	Verificar se o componente digital foi alterado de forma não documentada ou não autorizada, comprometendo sua autenticidade.
Obrigatoriedade	O
Repetibilidade	Não repetível
Nota de aplicação	Esse elemento registra informações do código *hash*[16] do componente digital, e de como este foi gerado, de forma a permitir a verificação da fixidade no futuro. Esse elemento não se refere à verificação da fixidade, que deve ser registrada no evento correspondente. Para se realizar a verificação da fixidade, um código hash deve ser previamente gerado e armazenado, para ser comparado a outro gerado posteriormente. Se os códigos coincidirem, significa que o objeto não foi alterado nesse intervalo de tempo. Esse metadado deve ser registrado de forma estruturada, em três subelementos, conforme a seguir: moreqjus.componente.fixidadeAlgoritimo moreqjus.componente.fixidadeCodigoHash moreqjus.componente.fixidadeOriginador Originador refere-se ao agente que fez o cálculo do código hash armazenado, que pode ser calculado pelo próprio GestãoDoc ou ter sido enviado junto com o documento.
Exemplos	moreqjus.componente.fixidadeAlgoritimo: MD5 moreqjus.componente.fixidadeCodigoHash: ed5f2ebd436f1cf88e5a39b3a257edf4a22be3c955a-c49es4a3 moreqjus.componente.fixidadeOriginador: MDS
Regra de preenchimento	Calculado e armazenado automaticamente pelo GestãoDoc. Recomenda-se o uso de formas controladas para a designação do algoritmo usado para gerar o código hash, preferencialmente a tabela sugerida no PREMIS Data Dictionary[17]. O originador deve ser representado por um identificador do agente que realizou o cálculo hash. Caso o originador seja um agente conhecido do GestãoDoc, pode se usar o Id do agente.
Requisito	Ver capítulo 10 (Preservação) / RPR10.2.2 / RSE11.4.9
Equivalência	Premis: messageDigestAlgorithm Premis: messageDigest Premis: messageDigestOriginator

16. Note que os termos "código hash" e "checksum" são comumente usados de forma intercambiável. No entanto, o termo "checksum" é mais corretamente utilizado para o produto de uma verificação de redundância cíclica (*cyclical redundancy check* - CRC), enquanto o termo "código hash" se refere ao resultado de uma função de hash criptográfica, que é ao que aqui se refere.
17. Lista controlada pela Library of Congress, sugerida no PREMIS Data Dictionary. Disponível em: http://id.loc.gov/vocabulary/preservation/cryptographicHashFunctions.html. Acesso em: 16 out. 2022.

Código de identificação	**MCDI15 - Assinatura digital**
Rótulo	**moreqjus.componente.assinatura**
Definição	Informações sobre a assinatura digital aplicada aos componentes digitais.
Objetivo	Usada para autenticar quem assinou o componente digital e/ou a informação contida nele. Também é usado para armazenar as informações relacionadas a essa assinatura de forma a apoiar validações posteriores.
Obrigatoriedade	AO
Repetibilidade	Repetível
Nota de aplicação	Esse metadado deve ser registrado de forma estruturada, em seis subelementos, conforme a seguir: moreqjus.componente.assinaturaCodificacao moreqjus.signatario moreqjus.componente.assinaturaMetodo moreqjus.componente.assinaturaValor moreqjus.componente.assinaturaRegrasValidacao moreqjus.componente.assinaturaChave A informação da codificação utilizada é essencial para se interpretar corretamente o valor da assinatura e a chave. O signatário é o indivíduo, instituição ou autoridade responsável por gerar a assinatura. Método refere-se aos algoritmos utilizados para criptografar e calcular o hash na geração da assinatura digital. Regras de validação são as operações que devem ser realizadas para validar a assinatura digital. Chave refere-se à chave pública do signatário necessária para validar a assinatura.
Exemplos	moreqjus.componente.assinaturaCodificacao: Base64 moreqjus.signatario: Ministério da Saúde moreqjus.componente.assinaturaMetodo: DSA-SHAI moreqjus.componente.assinaturaValor: da4f2ebd436f1cf88e5a39b3a257edf4a22be3c955ac49
Regra de preenchimento	Calculado e armazenado automaticamente pelo GestãoDoc. Recomenda-se o uso de formas controladas para a designação da codificação, preferencialmente a tabela sugerida no PREMIS Data Dictionary[18]. Caso o signatário seja um agente conhecido do GestãoDoc, pode se usar o Id do agente. Recomenda-se o uso de formas controladas para a designação do método, preferencialmente a tabela sugerida no PREMIS Data Dictionary[19]. As regras de validação podem incluir informações tais como: o método de codificação usado antes de calcular o resumo da mensagem ou se o objeto foi normalizado antes de assinar. Esse metadado pode apontar para um arquivo com a documentação dessas regras.
Requisito	RSE11.4.4 / RSE11.4.5

18. Lista controlada pela Library of Congress, sugerida no PREMIS Data Dictionary. Disponível em: http://id.loc.gov/vocabulary/preservation/cryptographicHashFunctions.html. Acesso em: 16 out. 2022.
19. Lista controlada pela Library of Congress, sugerida no PREMIS Data Dictionary. Disponível em: http://id.loc.gov/vocabulary/preservation/cryptographicHashFunctions.html. Acesso em: 16 out. 2022.

Equivalência	Premis: signatureEncoding Premis: signer Premis: signatureMethod Premis: signatureValue Premis: signatureValidationRules Premis: keyInformation

B1.5 Agente

Os metadados dessa seção identificam os agentes envolvidos na captura e no acesso aos documentos, bem como em todos os eventos de gestão do ciclo de vida, gestão de processos, gerenciamento do plano de classificação e de preservação.

Em geral, esses elementos são controlados pelo sistema de controle de acesso utilizado pelo GestãoDoc. Abaixo são apresentados apenas os elementos básicos de identificação do agente, necessários para representar a relação com os demais metadados.

- MAGE1 - Identificador do agente
- MAGE2 - Nome do agente
- MAGE3 - Status do agente

Para os elementos de metadados referentes à identificação *de* **Agente** foi elaborada uma ficha individual que detalha cada elemento e apresenta as seguintes informações:

Código de identificação	
Rótulo	
Definição	
Objetivo	
Repetibilidade	
Nota de aplicação	
Exemplos	
Regra de preenchimento	
Requisito	
Equivalência	

- **Código de identificação e nome**: indicação do código e do nome atribuídos ao elemento.
- **Rótulo:** nome padrão que deve ser utilizado para identificar o elemento a fim de facilitar a interoperabilidade de sistemas.
- **Definição:** indica qual informação deve ser registrada no elemento de metadado.
- **Objetivo:** a referência do que se pretende alcançar com a aplicação do elemento.
- **Obrigatoriedade:** indica a obrigatoriedade da aplicação do elemento. Os valores possíveis são: *obrigatório (O); obrigatório se aplicável (OA); facultativo (F); ou não se aplica (NA).*
- **Repetibilidade:** indica se a informação pode ser registrada mais de uma vez.
- **Nota de aplicação:** sugere formas de aplicação do elemento.
- **Exemplos:** apresenta alguns exemplos de aplicação que explicam o elemento.
- **Regra de preenchimento:** regra que especifica os valores, a codificação ou a lista de autoridades (lista de valores autorizados) convencionados para o preenchimento do elemento.
- **Requisito:** os requisitos funcionais relacionados com o elemento de metadado.
- **Equivalência:** referências para elementos equivalentes de outros esquemas de metadados.

Código de identificação	**MAGE1 - Identificador do agente**
Rótulo	moreqjus.agente.id
Definição	Código que identifica univocamente o agente no GestãoDoc.
Objetivo	Identificar univocamente o agente no GestãoDoc.
Obrigatoriedade	O
Repetibilidade	Não repetível
Nota de aplicação	Recomenda-se utilizar o código identificador já utilizado na instituição, tal como o número de matrícula, CPF, etc.
Exemplos	999.999.999-99 65418932
Regra de preenchimento	--
Requisito	RSE8.2.1 / RSE8.2.2
Equivalência	--

Código de identificação	**MAGE2 - Nome do agente**
Rótulo	**moreqjus.agente.nome**
Definição	Nome do agente que interage com o GestãoDoc.
Objetivo	Identificar o nome do agente.
Obrigatoriedade	O
Repetibilidade	Não repetível
Nota de aplicação	Um agente pode ser uma pessoa física, jurídica ou um sistema informatizado.
Exemplos	João da Silva Conselho Nacional de Justiça DEAJUD
Regra de preenchimento	--
Requisito	RSE8.2.1 / RSE8.2.2
Equivalência	--

Código de identificação	**MAGE3 - Status do agente**
Rótulo	moreqjus.agente.status
Definição	Indicação se o agente está ativo ou inativo.
Objetivo	Apoiar o GestãoDoc para permitir ações somente de agentes ativos.
Obrigatoriedade	O
Repetibilidade	Não repetível
Nota de aplicação	Este metadado refere-se ao status do agente no GestãoDoc e não à sua situação em outros contextos da organização.
Exemplos	--
Regra de preenchimento	Valores previstos: ativo ou inativo.
Requisito	--
Equivalência	--

ISBN 978-65-5972-119-1

CONSELHO
NACIONAL
DE JUSTIÇA