Conselho da Justiça Federal

Modelo de Requisitos

para Sistemas Informatizados de Gestão de Processos e Documentos da Justiça Federal

MoReq-Jus

Versão 1

Brasília, dezembro de 2007

Equipe técnica de elaboração do MoReq-Jus

Alexandre Libonati	Juiz Federal da Seção Judiciária do Rio de Janeiro
Eduardo César Weber	Diretor da Secretaria de Registros e Informações Processuais – Tribunal Regional Federal da 4ª Região
Jader Carlos Videira	Diretor da Divisão de Informática dos Juizados Especiais Federais – Tribunal Regional Federal da 3ª Região
Jany Rocha Wursch	Chefe da Seção de Integração com as Seções Judiciárias – Tribunal Regional Federal da 5ª Região
Lúcio Melre da Silva	Secretário de Tecnologia da Informação do Conselho da Justiça Federal
Luis Carlos de Freitas	Diretor da Subsecretaria de Informática da Seção Judiciária do Rio de Janeiro
Nádia Barbosa da Cruz Santana	Diretora da Divisão de Arquivo e Memória Institucional – Tribunal Regional Federal da 1ª Região
Neide Alves Dias De Sordi	Secretária de Pesquisa e Informação Jurídicas do Conselho da Justiça Federal
Patrícia Reis Longhi	Diretora-Geral da Seção Judiciária do Rio de Janeiro
Rita Helena dos Anjos	Coordenadora de Estudos e Pesquisas do Conselho da Justiça Federal

A equipe responsável pela elaboração do MoReq-Jus contou com o apoio de consultoria do Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPqD).

Conselho da Justiça Federal

Sumário

Apresentação 6

1 Introdução 11
- 1.1 Objetivos 13
- 1.2 Utilização 13
- 1.3 Organização do MoReq-Jus 14
- 1.4 Gestão de processos e documentos na Justiça Federal 15

2 Organização dos documentos institucionais: plano de classificação e manutenção dos documentos 30
- 2.1 Configuração e administração do plano de classificação no GestãoDoc 30
- 2.2 Classificação e metadados dos processos/dossiês 32
- 2.3 Gerenciamento dos processos/dossiês 33
- 2.4 Processos 35
- 2.5 Volumes: abertura, encerramento e metadados 36
- 2.6 Manutenção de documentos institucionais não-digitais e híbridos 37

3 Captura 39
- 3.1 Captura: procedimentos gerais 43
- 3.2 Captura em lote 47
- 3.3 Captura de mensagens de sistema de comunicação eletrônica 47
- 3.4 Formato de arquivo e estrutura dos documentos a serem capturados 48
- 3.5 Estrutura dos procedimentos de gestão 49

4 Armazenamento 51
- 4.1 Durabilidade 52
- 4.2 Capacidade 54
- 4.3 Efetividade de armazenamento 55

5 Preservação 56
- 5.1 Aspectos físicos 58
- 5.2 Aspectos lógicos 58
- 5.3 Aspectos gerais 59

6 Segurança 61
6.1 Cópias de segurança 64
6.2 Controle de acesso 65
6.3 Classificação da informação quanto ao grau de sigilo e restrição de acesso à informação sensível 68
6.4 Trilha de auditoria 69
6.5 Assinaturas digitais 71
6.6 Criptografia 74
6.7 Marcas d'água digitais 76
6.8 Acompanhamento de transferência 77
6.9 Autoproteção 78
6.10 Alteração, ocultação e exclusão de documentos institucionais 79

7 Tramitação e fluxo de trabalho 81
7.1 Controle do fluxo de trabalho 82
7.2 Controle de versões e do *status* do documento 84

8 Avaliação e destinação 85
8.1 Configuração dos instrumentos de classificação, temporalidade e destinação de documentos 87
8.2 Aplicação dos instrumentos de classificação, temporalidade e destinação de documentos 89
8.3 Exportação de documentos 90
8.4 Eliminação 92
8.5 Avaliação e destinação de documentos institucionais não-digitais e híbridos 93

9 Pesquisa, localização e apresentação de documentos 94
9.1 Recuperação de informação 94
9.2 Pesquisa e localização 94
9.3 Apresentação: texto, imagem, som e vídeo 96

10 Funções administrativas 99
10.1 Monitoração do sistema 99
10.2 Manutenção e evolução 99

11 Usabilidade 100

12 Interoperabilidade 103

13 Disponibilidade 104

14 Desempenho e escalabilidade 105

15 Glossário 107

16 Modelos de referência, legislação, regulamentações, normas e referências bibliográficas 113

16.1 Modelos de requisitos para sistemas informatizados de gestão arquivística de documentos 113

16.2 Legislação federal 113

16.3 Resoluções do Conselho Nacional de Arquivos — Conarq 114

16.4 Resoluções do Conselho da Justiça Federal — CJF 115

16.5 Normas 116

16.6 Referências bibliográficas 116

Apresentação

O Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos da Justiça Federal (MoReq-Jus) foi elaborado por um grupo de trabalho interdisciplinar, tendo como referência:

- O Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-ARQ), elaborado pela Câmara Técnica de Documentos Eletrônicos do Conselho Nacional de Arquivos (Conarq).
- O Modelo de Requisitos para Gestão de Arquivos Eletrónicos (MoReq), desenvolvido pelo Instituto dos Arquivos Nacionais/Torre do Tombo de Portugal. O MoReq português, por sua vez, teve como base o *Model Requirements for the Management of Electronic Records* (MoReq), elaborado pelo programa Intercâmbio de Dados entre Administrações (IDA) da Comissão Européia.

Os modelos mencionados têm como objetivos comuns fornecer requisitos para o desenvolvimento ou a avaliação de sistemas de gestão de documentos:

- Digitais — Os metadados e os próprios documentos são inseridos no sistema.
- Não-digitais — O sistema registra apenas os metadados dos documentos.
- Híbridos — Possibilita a gestão de documentos não-digitais e digitais.

A exemplo dos modelos mencionados, a existência de um programa de gestão de documentos na instituição é um dos requisitos para a utilização do MoReq-Jus, que se aplica aos sistemas de gestão de documentos relativos às atividades-meio e às atividades-fim da Justiça Federal.

Por se tratar de uma adaptação, na elaboração do MoReq-Jus, não se mencionou a fonte ou referência do texto, em sua maioria extraído do e-ARQ ou do MoReq.

A elaboração do MoReq-Jus foi uma iniciativa conjunta da Comissão Técnica Interdisciplinar para Gestão de Documentos da Justiça Federal (CT-GeD) e do Comitê Gestor do Sistema de Tecnologia da Informação e Comunicação da Justiça Federal (SIJUS). Representantes dessas duas comissões atuaram juntamente com um grupo de trabalho interdisciplinar, integrado por especialistas das áreas de Ciência da Informação, Tecnologia da Informação e Direito, que contou, ainda com o apoio de consultoria do CPqD.

O grupo de trabalho analisou os modelos e-ARQ e MoReq, comparando seus requisitos e definições com as peculiaridades dos sistemas de gestão de processos judiciais e de documentos administrativos do Conselho da Justiça Federal (CJF), dos Tribunais Regionais Federais (TRFs) e das Seções Judiciárias. A partir dessa análise, criaram-se as condições necessárias para a elaboração do MoReq-Jus.

As características peculiares dos sistemas da Justiça Federal inviabilizaram a utilização direta do e-ARQ. Foram necessárias extensões e adaptações que resultaram no MoReq-Jus.

A necessidade de se fazer adaptações ao e-ARQ já havia sido prevista naquele documento, no item 3 — Limites da Especificação, em decorrência da impossibilidade de o modelo abranger todos os requisitos necessários para qualquer órgão poder criar, manter e prover acesso a documentos digitais, como também das exigências legais e regulamentares distintas que devem ser levadas em conta na adoção desse modelo.

Assim, recomendou o Conarq que cada organização considerasse as suas atividades, os documentos que produz, bem assim o contexto de produção e manutenção dos documentos e, dependendo da situação, acrescentasse requisitos específicos ou assegurasse que os requisitos listados como facultativos ou altamente desejáveis pudessem ser classificados como obrigatórios. A decisão sobre a forma de adoção do e-ARQ foi, dessa forma, facultada a cada instituição.

A elaboração do MoReq-Jus decorreu da necessidade do CJF de estabelecer diretrizes e políticas que orientem a aquisição ou o desenvolvimento dos sistemas para a gestão de documentos na Justiça Federal, em cumprimento ao seu papel constitucional de órgão central do sistema Justiça Federal, conforme preconiza a Constituição.

A organização sistêmica da Justiça Federal visa manter a unidade da instituição, regionalizada, com a criação dos Tribunais Regionais Federais, para melhor atender ao jurisdicionado.

Sob esse enfoque, para a integração da Justiça Federal deve-se definir requisitos necessários aos sistemas que produzem, recebem, armazenam e possibilitam o acesso e a destinação dos processos e de outros documentos em suporte digital e não-digital.

Atualmente, as políticas que orientam a aquisição ou o desenvolvimento dos sistemas no âmbito da Justiça Federal são incipientes.

O processo judicial é o principal documento produzido pela Justiça Federal e sua gestão é realizada por diversos sistemas processuais. Em cada uma das cinco Regiões em que se organiza a Justiça Federal, existem, no mínimo, três sistemas processuais: um na primeira instância, um na segunda e outro para os Juizados Especiais Federais. A esses sistemas, somam-se vários outros, como o das varas de execução fiscal virtual, de pauta eletrônica, entre outros. Também para a gestão dos documentos e processos administrativos, diversos sistemas são utilizados com uma infinidade de denominações e características.

O estabelecimento de requisitos para sistemas de gestão de processos e documentos tornou-se mais premente com a publicação da Lei nº 11.419, de 2006, que dispõe sobre a informatização do processo judicial. Com sua publicação, o Brasil tornou-se um dos primeiros países do mundo a ter uma legislação que permite a adoção do processo eletrônico.

No entanto, essa norma é essencialmente procedimental, e os tribunais terão de estudar a melhor maneira de se adaptar à lei. O MoReq-Jus visa dar unidade a essa adaptação.

Uma das medidas já em curso é a adoção da infra-estrutura de chaves públicas da ICP-Brasil, que garante a aceitação do processo eletrônico por terceiros. Em complementaridade à adoção da certificação digital, outras medidas precisam ser implementadas para garantir a segurança e a preservação de longo prazo e, dessa forma, assegurar o direito à informação, albergado na Constituição Federal (CF) de 1988.

A CF, em seu art. 216, § 2º, estabelece que cabe à Administração Pública a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem. Assim, a sociedade delega à Justiça o dever de zelar por seus documentos e de propiciar o acesso a eles.

A Lei nº 8.159, 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.

O art. 3º da mencionada Lei conceitua gestão de documentos como o conjunto de procedimentos e operações técnicas que engloba a produção, a tramitação, o uso, a avaliação e o arquivamento em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente. Dessa forma, fica evidente que os sistemas de acompanhamento processual são também sistemas de gestão de documentos e que a gestão do documento permeia todo o andamento processual: da distribuição do processo — fase da produção do documento, passando por toda a tramitação — até sua destinação final, depois da baixa definitiva.

A gestão de documentos não é um problema exclusivamente arquivístico. Visa garantir a guarda e o acesso aos documentos em todos os seus estágios de vida. Portanto, envolve todos os atores e unidades da instituição e precisa atender às demandas de todos.

Para o cumprimento dessa atribuição, o Conselho da Justiça Federal aprovou resoluções que estabelecem o Programa de Gestão Documental da Justiça Federal e outras que contemplam aspectos da gestão documental. Esse programa inclui a gestão de documentos administrativos e das ações judiciais transitadas em julgado e definitivamente arquivadas da instituição.

A política de gestão de processos e documentos, para garantir a segurança dos processos e outros documentos em meio digital, precisa incluir questões

relativas à segurança e à preservação da informação, considerando as peculiaridades dos documentos em suporte digital[1]:

- Fragilidade intrínseca do armazenamento digital (degradação física do suporte).
- Rápida obsolescência da tecnologia digital: *hardware*, *software* e formatos.
- Necessidade de tratamento adequado das entidades integrantes do documento digital: objeto físico (suporte), lógico (*software* e formatos) e conceitual (conteúdo).
- Complexidade e custos da preservação digital.
- Complexidade dos controles para garantir a autenticidade, a confidencialidade, a integridade e a disponibilidade desses documentos.

Há mais de uma década, os grandes institutos de pesquisas europeus e americanos vêm-se preocupando com a preservação digital, em decorrência da incapacidade dos atuais sistemas eletrônicos de informação em assegurar a preservação dos documentos em longo prazo.

A Unesco publicou a Carta de Preservação do Patrimônio Digital – um alerta sobre a possibilidade de desaparecimento do legado digital – e sugere que os Estados membros adotem um conjunto de medidas para salvaguardar esse patrimônio. Essa Carta tem o objetivo de conscientizar e ampliar a discussão sobre a instabilidade do legado digital, que se encontra em perigo de perda e de falta de confiabilidade. Manifesta ainda a necessidade de se estabelecer políticas, estratégias e ações que garantam a preservação de longo prazo e o acesso contínuo aos documentos digitais.

No Brasil, o Conarq, além do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos — e-ARQ Brasil, estabelecido pela Resolução nº 25, de 27 de abril de 2007, elaborou também a Carta para a Preservação do Patrimônio Arquivístico Digital Brasileiro, bem como as resoluções nº 20, de 16 de julho de 2004, sobre a inserção de documentos arquivísticos digitais nos programas de gestão de documentos e a nº 24, de 3 de agosto de 2006, sobre transferência e recolhimento de documentos arquivísticos digitais.

A preocupação mundial decorre da possibilidade de estarmos prestes a viver uma nova Idade Média — uma Era Negra em que muito do que sabemos agora, muito do que está codificado e escrito eletronicamente poderá se perder para sempre.

Alguns exemplos de perda de documentos em suporte digital, nas últimas décadas, justificam essa preocupação, principalmente com a confiabilidade e

1 Conselho Nacional de Arquivo. Carta para a Preservação do Patrimônio Arquivístico Digital, 2004. Disponível em: <http://www.conarq.arquivonacional.gov.br/Media/publicacoes/cartapreservpatrimarqdigitalconarq2004.pdf> . Acesso em: 21 jun. 2007.

durabilidade das mídias digitais. Pesquisas indicam que a vida média de uma mídia óptica é de 30 anos, mas o seu equipamento de leitura estará obsoleto em 10 anos[2]. Esses resultados fortalecem a necessidade do estabelecimento de uma política institucional para a preservação digital.

Além dos problemas relativos à obsolescência dos *softwares, hardwares* e da fragilidade das mídias, ainda temos a questão dos ambientes tecnológicos da Justiça Federal, em contínua alteração e crescente complexidade.

Esse cenário de incertezas se completa com a atual indisponibilidade dos arquivos de documentos e processos eletrônicos para as unidades arquivísticas, a fim de garantir a gestão e o acesso contínuo aos conteúdos e funcionalidades; com a não-participação de profissionais da área de Informação no processo de gestão de processos e documentos digitais; com a falta de funcionalidades de gestão arquivística nos sistemas processuais, de forma a evitar perda ou adulteração de documentos; com o grande número de sistemas em *softwares* proprietários, dificultando a migração dos documentos, por falta de acesso aos códigos-fontes e documentação insuficiente.

A definição de padrões de metadados, de controles de autenticidade e integridade de mídias e de normas e procedimentos para assegurar a acessibilidade, a autenticidade e a integridade dos documentos digitais deve compor uma política de preservação de longo prazo desse patrimônio digital.

Os processos eletrônicos dos Juizados Especiais Federais, das varas de execução fiscal e outros documentos em formato digital já representam um grande volume de documentos, a reclamar o estabelecimento de uma política de gestão da informação digital.

Espera-se que o MoReq-Jus venha a se constituir em uma ferramenta para promoção da padronização na gestão da documentação digital e não-digital, de forma a garantir que o patrimônio documental da Justiça Federal seja produzido e mantido de forma confiável, íntegra, autêntica e acessível.

Nesse sentido, o grupo de trabalho responsável pela elaboração do MoReq-Jus proporá ao CJF a constituição de uma metodologia de avaliação dos sistemas informatizados implantados na Justiça Federal para sua certificação quanto ao grau de aderência ao modelo.

Conselho da Justiça Federal
Brasília, setembro de 2007

2 INNARELLI, Humberto Celeste. Documentos digitais e sua fragilidade em relação ao suporte. In: *II Simpósio Internacional de Bibliotecas Digitais*. IBICT, Unicamp, 2004. Disponível em: <http://libdigi.unicamp.br/document/?view=8397>. Acesso em: 21 jun. 2007.

1 Introdução

O Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos da Justiça Federal (MoReq-Jus) estabelece condições a serem cumpridas na produção, tramitação, guarda, armazenamento, preservação, arquivamento ou no recebimento de documentos, pelos sistemas de gestão de processos e documentos digitais, não-digitais ou híbridos, a fim de garantir a sua confiabilidade e autenticidade, assim como o seu acesso.

O MoReq-Jus estabelece processos e 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 simultaneamente os documentos e processos digitais, não-digitais e híbridos. Para os documentos não-digitais o sistema registra apenas as referências a esses documentos e as operações de produção, tramitação, guarda, armazenamento, preservação, arquivamento e recebimento. No caso dos sistemas de documentos digitais, registra os documentos e as operações mencionadas.

A produção de documentos digitais levou à criação de sistemas de gerenciamento de documentos. Entretanto, para assegurar que documentos digitais sejam confiáveis e autênticos e que possam ser preservados com essas características, é fundamental que esses sistemas incorporem os conceitos arquivísticos e suas implicações no gerenciamento dos documentos digitais.

Para o bom entendimento desse Modelo de Requisitos, alguns conceitos que nortearam o trabalho foram relacionados a seguir. Outras definições operacionais foram incluídas no Capítulo 15, Glossário.

Sistema de Informação

Conjunto organizado de políticas, procedimentos, pessoas, equipamentos e programas computacionais que produzem, processam, armazenam e provêem acesso à informação proveniente de fontes internas e externas para apoiar o desempenho das atividades da Justiça Federal.

Gestão de Documentos

Conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento dos documentos em fase corrente e intermediária, visando sua eliminação ou seu recolhimento para a guarda permanente.

Sistema de Gestão de Documentos

Conjunto de procedimentos e operações técnicas, cuja interação permite a eficiência e a eficácia da gestão de processos e documentos.

Gerenciamento Eletrônico de Documentos (GED)

Conjunto de tecnologias utilizadas para organização da informação não-estruturada da Justiça Federal, que pode ser dividido nas seguintes funcionalidades: captura, gerenciamento, armazenamento e distribuição. Entende-se por informação não-estruturada: mensagem de correio eletrônico, arquivo de texto, imagem ou som, planilhas etc.

O GED engloba tecnologias de digitalização, automação de fluxos de trabalho (*workflow*), processamento de formulários, indexação, entre outras.

Sistema Informatizado de Gestão de Processos e Documentos (GestãoDoc)

Sistema mais abrangente que o GED, 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 operações como: produção do documento, controle da 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 confiáveis, íntegros e autênticos.

No caso dos documentos digitais, um GestãoDoc deve abranger todos os tipos de documentos digitais da instituição, atendendo a padronização da plataforma tecnológica da Justiça Federal.

A partir dessas definições podemos fazer as seguintes considerações:

- Um sistema de informação abarca todas as fontes de informação existentes na Justiça Federal, incluindo o sistema de gestão de processos judiciais e administrativos e documentos, a biblioteca, o centro de documentação, o serviço de comunicação, entre outros.
- O GestãoDoc mantém a organicidade dos documentos e a inter-relação destes com as atividades da instituição.
- A concepção de um GestãoDoc, por ser um sistema de gestão de processos e documentos, tem de dar-se a partir da implementação de uma política arquivística na instituição.

- O ciclo de vida dos documentos refere-se às sucessivas etapas pelas quais passam: produção, tramitação, uso, avaliação, arquivamento e destinação (guarda permanente, devolução às partes ou eliminação).

Requisitos 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[3].
- Gestão dos documentos a partir de sua classificação para manter a 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 entre documentos digitais e documentos não-digitais.
- Armazenamento seguro para garantir a integridade dos documentos.
- Avaliação e seleção dos documentos para recolhimento e preservação daqueles considerados de valor permanente.
- Aplicação de critérios de classificação e guarda.
- Exportação dos documentos para transferência e recolhimento.
- Instrumentos para gestão de estratégias de preservação dos documentos.

As especificações dos requisitos funcionais e não-funcionais de sistemas e dos metadados a serem implementados nos diferentes tipos de GestãoDoc existentes na Justiça Federal não estão incluídas neste documento. Serão detalhadas para cada sistema específico.

1.1 Objetivos

O MoReq-Jus tem por objetivo fornecer especificações técnicas e funcionais, para orientar a aquisição, o detalhamento e o desenvolvimento de sistemas de gestão de processos e documentos no âmbito da Justiça Federal. Também tem por objetivo estabelecer critérios para certificação do grau de aderência ao modelo.

1.2 Utilização

O MoReq-Jus é especialmente dirigido a:

3 Um documento institucional digital pode ser constituído por vários componentes digitais, por exemplo, um relatório acompanhado de planilhas, fotografias ou plantas, armazenados em diversos arquivos digitais. Além disso, há de se considerar a relação orgânica dos documentos institucionais.

- Potenciais usuários de um GestãoDoc — Na elaboração de um edital de licitação para a apresentação de propostas de fornecimento de *software*.
- Usuários de um GestãoDoc — Como base para auditoria ou inspeção do GestãoDoc existente.
- Fornecedores e desenvolvedores de sistemas — Como guia no desenvolvimento de um GestãoDoc em conformidade com os requisitos exigidos.
- Profissionais e provedores de serviços de gestão de documentos — Com vistas a orientar a execução desses serviços a partir de uma abordagem arquivística.
- Potenciais usuários de serviços externos de gestão de documentos — Como guia para a especificação dos serviços a serem adquiridos.

1.3 Organização do MoReq-Jus

O MoReq-Jus descreve o modelo de requisitos necessários para o desenvolvimento de um GestãoDoc.

O capítulo inicial apresenta a gestão de processos e documentos na Justiça Federal, a política arquivística e os instrumentos utilizados na gestão de processos e documentos.

Os demais capítulos apresentam os aspectos da funcionalidade, o glossário e as referências normativas e bibliográficas.

Os aspectos da funcionalidade estão divididos em:

- Organização dos documentos (plano de classificação)
- Captura
- Armazenamento
- Preservação
- Segurança
- Tramitação
- Destinação
- Recuperação da informação
- Funções administrativas
- Usabilidade
- Interoperabilidade
- Disponibilidade
- Desempenho

Cada capítulo compreende um texto preliminar que apresenta o assunto e a relação dos requisitos correspondentes ao capítulo. Os requisitos são apresentados em quadros numerados com o enunciado correspondente e a classificação dos níveis de obrigatoriedade.

Níveis 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 se ignorar um determinado item, mas a totalidade das implicações deve ser cuidadosamente examinada antes da escolha de uma proposta diferente.

Com relação aos requisitos considerados desejáveis, deve ser observado que uma implementação que não inclui determinado item desejável deve estar preparada para interoperar com outra que o inclui, mesmo com o não-atendimento pleno da funcionalidade. De forma inversa, uma implementação que inclui um item desejável deve estar preparada para interoperar com outra implementação que não o inclui.

1.4 Gestão de processos e documentos na Justiça Federal

O processo de informatização da Justiça Federal, iniciado na década de 80, foi sensivelmente acelerado a partir de 2002, com a implantação dos Juizados Especiais Federais, determinada pela Lei nº 10.259, de 2001. Essa Lei trouxe flexibilidades processuais que possibilitaram a mudança de suportes de registro das informações. Os documentos gerados no decorrer das atividades da Justiça Federal, até então em meio não-digital, passam a ser registrados também em formato digital.

Essas mudanças decorreram das características do documento digital, que deixa de ser apenas entidade física e torna-se também entidade lógica, e conceitual, trazendo a necessidade de adequação nas políticas de segurança e de preservação de documentos da instituição.

Os documentos digitais e as alterações na legislação processual trouxeram uma série de vantagens na produção, transmissão, armazenamento e acesso aos documentos, mas, por sua vez, provocaram novos desafios. A facilidade de acesso pode acarretar intervenções não-autorizadas, adulteração ou perda dos documentos.

Também os sistemas de gerenciamento passam a ser utilizados para os documentos não-digitais e digitais.

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

Para conferir essa capacidade, os documentos precisam ser confiáveis, autênticos, acessíveis, compreensíveis e preserváveis, o que só é possível com a implantação de um programa de gestão de processos e documentos.

Os documentos institucionais, segundo a Teoria das Três Idades, quanto ao seu ciclo de vida, são classificados em correntes, intermediários e permanentes.

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 à eficácia administrativa com relação à recuperação da informação disponível, à tomada de decisões e ao cumprimento da missão institucional da Justiça Federal.

1.4.1 Definição da política arquivística

O Programa de Gestão de Documentos da Justiça Federal (JusArq), instituído pela Resolução CJF nº 217, de 1999, define o conjunto de procedimentos e operações técnicas que compreendem a gestão de documentos na instituição. As principais características são apresentadas a seguir:

- Estabelece as unidades arquivísticas como responsáveis pela avaliação documental, organização do acervo arquivístico da instituição e pelo acesso aos documentos sob sua guarda, entre outras ações do Programa de Gestão de Documentos.
- Classifica os documentos da administração judiciária, para fins de arquivamento, em correntes, intermediários e permanentes.
- Institui o Plano de Classificação e Tabela de Temporalidade da Documentação da Administração Judiciária Federal (PCTT), que delimita o conjunto de documentos permanentes, de valor histórico, probatório e informativo, a serem definitivamente preservados.
- Estabelece o conceito de documentos essenciais, que devem ser encaminhados para guarda permanente nas unidades de arquivo imediatamente após sua produção, e a integração entre o sistema de protocolo e controle de tramitação dos documentos administrativos e judiciais e a unidade de arquivo.
- Promove a constituição de comissões e grupos permanentes de avaliação documental.
- Estabelece que a guarda do documento, independentemente do suporte físico (papel ou eletrônico), deve garantir sua autoria, integridade e tempestividade.
- Define os assuntos, as classes processuais e os prazos de guarda, com base na natureza do provimento jurisdicional.
- Faculta ao magistrado a formulação de proposta fundamentada de guarda definitiva de processo em que atue.

- Determina que a eliminação de processos judiciais transitados em julgado deve ser precedida por publicação de Edital de Eliminação, e autoriza às partes interessadas nos processos a serem eliminados a requisição dos autos para guarda particular.
- Determina a observância aos critérios de preservação ambiental, preferencialmente por meio da reciclagem dos documentos a serem descartados.
- Instituiu a responsabilidade da Comissão Técnica Interdisciplinar para Gestão de Documentos da Justiça Federal pela coordenação do Programa de Gestão de Documentos da Justiça Federal e pela atualização dos seus instrumentos.
- Define os documentos de guarda permanente, que devem ser recolhidos, imediatamente após sua publicação, às unidades arquivísticas, os responsáveis por sua gestão e estabelece a preservação de amostras representativas do universo dos julgados.

1.4.2 Instrumentos utilizados na gestão de processos e documentos

Os instrumentos sistematizam a gestão dos documentos produzidos e recebidos pela Justiça Federal no exercício de suas atividades, com vistas a uniformizar o tratamento da documentação, agilizando a recuperação da informação.

Gestão de documentos e processos administrativos ~~da Justiça Federal~~

O Plano de Classificação e a Tabela de Temporalidade da Documentação da Administração Judiciária Federal (PCTT) determinam a temporalidade e a destinação dos documentos da administração judiciária, como: pautas de julgamento, livros de sentenças, alvarás, mandados de intimação e previstos na Lei nº 5.010, de 1966. O PCTT foi aprovado pela Resolução CJF nº 217, de 1999, e complementado pela Resolução CJF nº 393, de 2004.

Com base no PCTT, um GestãoDoc deve automatizar a informação e emitir relatórios periódicos dos documentos que deverão ser transferidos ao arquivo permanente ou eliminados.

Gestão de processos judiciais

A classificação por assunto dos processos judiciais é feita com base na Tabela Única de Assuntos da Justiça Federal (TUA), aprovada pela Resolução CJF nº 317, de 2003.

A TUA é utilizada na classificação da petição inicial, organizada por ramos do Direito e estruturada em três ou quatro níveis. O pedido, com as suas especificações e os seus fundamentos jurídicos, é analisado para definir os assuntos a serem registrados.

Além de possibilitar a gestão dos documentos e processos judiciais, a TUA tem como objetivos:

- Facilitar a recuperação e maximizar o uso da informação processual, atingindo níveis crescentes de acessibilidade para usuários internos e externos.
- Melhorar a compreensão do andamento processual pelo jurisdicionado.
- Aprimorar o controle de prevenção e a distribuição processual por competências em razão da matéria.
- Possibilitar o aproveitamento, nas instâncias superiores, das informações processuais inseridas nos sistemas de 1ª Instância.
- Padronizar nacionalmente o cadastramento das matérias e ações discutidas nos processos.
- Facilitar o intercâmbio da informação entre sistemas e bases de dados, possibilitando uma integração mais abrangente para a implantação de sistemas de âmbito nacional, que contribuirão para a celeridade processual.
- Atingir maior uniformidade no tratamento da informação, visando à geração de análises estatísticas confiáveis para comparação do desempenho entre as instituições.
- Racionalizar o fluxo do processo.

A classificação segundo os procedimentos previstos na legislação processual é realizada de acordo com a Tabela Única de Classes da Justiça Federal (TUC), instituída pela Resolução CJF nº 328, de 2003.

A política de gestão das ações judiciais transitadas em julgado e arquivadas na Justiça Federal estabelece a temporalidade e a destinação dos autos findos. Os critérios legais de temporalidade são estabelecidos com base na natureza do provimento jurisdicional demandado e o efetivamente obtido para maior segurança na atribuição dos prazos legais. Também garante a preservação de conjuntos amostrais semelhantes nos diversos acervos da Justiça Federal. Essa política de gestão foi aprovada pelas Resoluções CJF ns. 359 e 393, de 2004.

1.4.3 Manual de gestão de documentos

O Programa de Gestão de Documentos da Justiça Federal está consolidado em dois manuais. O Manual de Procedimentos do Programa de Gestão Documental da Justiça Federal[4] e o Manual de Gestão de Autos Findos[5]. Esses instrumentos são utilizados em treinamentos realizados pelo Centro de Estudos Judiciários para a formação de multiplicadores em Gestão

4 Manual de Procedimentos do Programa de Gestão Documental da Justiça Federal, CJF, Brasília, 2001. 59 p. Disponível em: <http://www.jf.gov.br/portal/gestaodocumental/documentos/MANUAL%20DE%20PROCEDIMENTOS.pdf>. Acesso em: 29 abr. 2007.

5 Manual de Gestão de Autos Findos do Programa de Gestão Documental da Justiça Federal. Brasília, 2005. 36 p. Disponível em: <http://daleth.cjf.gov.br/Download/Manual%20Gestão%20Documental_21.doc>. Acesso em: 29 abr. 2007.

Documental. Os manuais descrevem a política de gestão e as rotinas para a implantação do Programa.

1.4.4 Vocabulário controlado e Tesauro

As unidades de arquivo, bibliotecas e órgãos de jurisprudência da Justiça Federal utilizam, no processo de indexação de documentos, o Tesauro Jurídico da Justiça Federal, elaborado pelo Centro de Estudos Judiciários do Conselho da Justiça Federal. O Tesauro Jurídico da Justiça Federal inclui a terminologia do Direito nas áreas de competência da Justiça Federal.

As categorias e subcategorias dessa obra correspondem às classificações e divisões dos textos legais pertinentes, com a adoção da terminologia usualmente empregada pelos magistrados, selecionada dos acórdãos incluídos nas bases de dados de jurisprudência dos Tribunais Regionais Federais.

A consulta ao Tesauro Jurídico da Justiça Federal está disponível em: <http://daleth.cjf.gov.br/sd4cgi/om_isapi.dll?clientID=107038&infobase=thesaurus&softpage=Browse_Frame_Pg>.

A página do Programa de Gestão Documental — no Portal da Justiça Federal — apresenta os manuais, as normas e os instrumentos mencionados para a orientação aos servidores envolvidos no processo de gestão de documentos e processos administrativos e judiciais. Está disponível em: <http://www.jf.gov.br/portal/gestaodocumental/index.html>.

1.4.5 Designação de responsabilidades

A designação de responsabilidades é um dos fatores que garantem 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 no programa de gestão.

As responsabilidades devem ser distribuídas a todos os magistrados e servidores de acordo com a função e a hierarquia de cada um e devem envolver as seguintes categorias:

- Colegiado do Conselho da Justiça Federal — autoridade máxima responsável pela aprovação dos requisitos estabelecidos neste documento, pela Política de Segurança da Informação e pelo Programa de Gestão de Documentos.
- Presidentes dos TRFs, corregedores, diretores de foro e magistrados — reais responsáveis pela viabilidade da política e normas aprovadas pelo Colegiado. Caberá a eles apoiar integralmente a implantação dos requisitos estabelecidos neste documento e da política de gestão, alocando recursos humanos, materiais e financeiros e promovendo o envolvimento de todos no programa de gestão de processos e documentos.

- Comitê Gestor do Sistema de Tecnologia da Informação e Comunicação da Justiça Federal (SIJUS) — tem como competência, nos termos da Resolução CJF n. 380, de 2004, elaborar, submeter ao Colegiado do CJF, acompanhar e avaliar a implantação da política de Tecnologia da Informação e Comunicação da Justiça Federal, de forma a garantir a uniformidade, a compatibilidade e a integração dos dados e soluções e a uniformização dos procedimentos e processos judiciais ou administrativos em nível nacional.
- Comissão Técnica Interdisciplinar para Gestão de Documentos da Justiça Federal — conforme estabelecem as Resoluções CJF n. 217, de 1999, e n. 359, de 2004, cabe-lhe a coordenação do Programa e a proposição de normas, manuais, instrumentos e treinamentos de servidores para a sua implantação.
- Comissões Permanentes de Avaliação Documental nos Tribunais Regionais Federais e Grupos Permanentes de Avaliação de Documentos nas Seções Judiciárias — instituídas pelos arts. 4º e 5º da Resolução CJF n. 217, de 1999, têm a competência de aplicar os procedimentos do Programa de Gestão Documental; proceder à avaliação casuística dos processos definidos como passíveis de eliminação, com vistas a selecionar aqueles que, pela sua peculiaridade, devem ser preservados permanentemente; e analisar propostas de guarda definitiva de documentos feitas por magistrados bem como pronunciar-se acerca do seu acolhimento.
- Profissionais de arquivo — responsáveis pela implantação do programa de gestão documental e pela avaliação e controle dos trabalhos executados no âmbito de suas instituições. Além disso, o profissional de arquivo é responsável também pela disseminação das técnicas e cultura arquivísticas.
- Gerentes de unidades organizacionais ou grupos de trabalho — responsáveis por garantir que os membros de sua equipe produzam e mantenham documentos como parte de suas tarefas, de acordo com o programa de gestão de processos e documentos.
- Usuários — 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.
- Gestores dos sistemas de informação e de tecnologia da informação — responsáveis pelo projeto, desenvolvimento e manutenção de sistemas de informação nos quais os documentos digitais e não-digitais são gerados e usados, e pela operacionalização dos sistemas de computação e de comunicação.

1.4.6 Exigências a serem cumpridas pelo programa de gestão de processos e documentos

O programa de gestão de processos e documentos terá de atender a uma série de exigências, tanto em relação ao documento institucional como ao seu próprio funcionamento.

O documento institucional deve:

- Refletir corretamente o que foi comunicado, decidido ou implementado;
- Conter os metadados necessários para documentar a ação.
- Servir de suporte às atividades.
- Revelar as atividades realizadas.

O programa de gestão de processos e documentos deve:

- Contemplar o ciclo de vida dos documentos.
- Garantir a acessibilidade aos documentos.
- Manter os documentos em ambiente seguro.
- Reter os documentos somente pelo período estabelecido nos instrumentos de classificação, temporalidade e destinação da política de gestão documental da Justiça Federal.
- Implementar estratégias de preservação dos documentos desde sua produção e pelo tempo que houver sido definido; e
- Garantir as qualidades de um documento institucional: organicidade, unicidade, confiabilidade, integridade, autenticidade, não-repúdio, tempestividade e confidencialidade.

A cada uma das mencionadas qualidades do documento institucional, corresponde novo conjunto de exigências a serem cumpridas pelo programa de gestão, conforme especificado a seguir:

- **Organicidade** — O documento institucional caracteriza-se por sua contextualização, que reflete suas funções e atividades. Os documentos institucionais apresentam um conjunto de relações que devem ser mantidas, com o registro da seqüência das atividades realizadas por meio da aplicação dos critérios de classificação.
- **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, permite-se a utilização de referências lógicas para a individualização dos documentos digitais. Nessa hipótese, deve ser garantida a localização única do documento.
- **Confiabilidade** — O documento é dotado de todos os elementos exigidos pela organização e pelo sistema jurídico-administrativo a que pertence, de forma a produzir conseqüências no mundo administrativo e jurídico. É criado por usuário autorizado, e todos os seus procedimentos de criação

foram bem controlados. Pode-se garantir de forma indubitável 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 se de tratar de original ou cópia. O documento autêntico deve manter a mesma forma do momento de sua produção e ter a garantia de sua autoria.

  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 identificação única e unívoca do autor.

- **Tempestividade** — O documento institucional deve ter garantida a hora legal do momento de sua produção, alteração e registros dos eventos de sua tramitação.

  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 pelo mesmo, 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 definir estratégias de armazenamento e preservação, bem como regras para a transmissão dos documentos. Os mecanismos de assinatura e preservação do documento deverão respeitar a legislação vigente, de modo a ter garantida sua identificação e permitir-lhe o acesso.

1.4.7 Metodologia do programa de gestão

A metodologia de planejamento e implantação de um programa de gestão de processos e documentos estabelece oito passos, não necessariamente seqüenciais, podendo ser desenvolvidos em diferentes estágios, interativa, parcial ou gradualmente, de acordo com as necessidades da instituição. A metodologia prevê ainda ciclos de aplicação, e as tarefas previstas do passo "c" ao passo "h" devem ser realizadas periodicamente.

É importante destacar que este programa de gestão não se restringe a documentos digitais. É necessário prever a manutenção de documentos em outros suportes, como papel, fitas de vídeo ou de áudio, etc. Há de se considerar, portanto, o caráter híbrido dos documentos a serem geridos e a necessidade de preservação da integridade e da usabilidade dos documentos digitais e não-digitais.

Os oito passos referidos são:

a. Levantamento preliminar

Consiste em identificar e registrar atos normativos, legislação, regimento e regulamentos.

O objetivo deste primeiro passo é gerar o conhecimento necessário sobre a missão, a estrutura organizacional e o contexto jurídico-administrativo no qual a instituição opera, de forma a poder-se identificar as exigências para produzir e manter documentos.

Esta etapa de levantamento, já realizada na Justiça Federal, é fundamental para a definição de quais documentos devem ser produzidos e capturados, de acordo com as normas estabelecidas no programa de gestão documental.

b. Análise das funções, das atividades desenvolvidas e dos documentos produzidos

Consiste em identificar, documentar e classificar cada função e atividade, bem como identificar e documentar os fluxos de trabalho e os documentos produzidos.

O objetivo é desenvolver um modelo conceitual sobre o que a instituição faz e como faz, demonstrando como os processos e documentos se relacionam com a missão e as atividades.

Na Justiça Federal, o levantamento da produção documental subsidiou a definição dos procedimentos de produção, captura, controle, armazenamento, acesso e destinação dos documentos.

Com a ampliação da produção de documentos digitais, é desejável que o levantamento seja atualizado. Essa definição é particularmente importante em ambientes digitais, em que os documentos só poderão ser capturados e mantidos se o sistema tiver sido projetado para tal.

Os produtos resultantes deste passo devem incluir:

- Esquema de classificação das funções e atividades.
- Mapa dos fluxos de trabalho que mostre quando e quais documentos são produzidos ou recebidos como resultado das atividades desenvolvidas.

A análise das funções e atividades fornece a base para desenvolver ferramentas de gestão de documentos, que devem incluir:

- Critérios de classificação para contextualizar os documentos produzidos e recebidos.
- Instrumentos de classificação, temporalidade e destinação para estabelecer os prazos de guarda e as ações de destinação dos documentos.
- Tesauro e vocabulário controlado para identificar e indexar documentos de uma atividade específica.

c. Identificação das exigências a serem cumpridas para a produção de documentos

Consiste em identificar que documentos devem ser produzidos, determinar a forma documental que melhor satisfaça cada atividade desempenhada e definir quem está autorizado a produzir cada documento. Essas exigências devem tomar por base a legislação vigente, as normas internas, a necessidade de se manter documentos em suporte digital e não-digital concomitantemente e ainda os riscos decorrentes da falta de registro de uma atividade em um tipo de documento.

O objetivo deste passo é assegurar que somente os documentos realmente necessários sejam produzidos, que sua produção seja obrigatória e que o seja de forma completa e correta.

Os produtos resultantes deste passo podem incluir:

- Lista das exigências a serem cumpridas para a produção e a manutenção de documentos.
- Relatório de avaliação dos riscos decorrentes da falta de registro de uma atividade em documento.
- Documento formal, regulamentando as exigências a serem cumpridas para a produção e a manutenção de documentos, especificando que documentos devem ser produzidos, a forma documental que devem apresentar e a relação dos níveis de permissão de acesso.

Na Justiça Federal, a produção de documentos processuais é definida pelos Códigos Processuais e Provimentos das Corregedorias. Os documentos administrativos a serem produzidos foram definidos pelo PCTT.

d. Avaliação dos sistemas existentes

Consiste em identificar e avaliar o sistema de gestão de processos e documentos, bem como outros sistemas de informação e comunicação existentes.

O objetivo deste passo é identificar as lacunas entre as exigências para a produção e manutenção de processos e documentos e o desempenho do sistema de gestão de processos e documentos, bem como dos sistemas de informação e comunicação existentes. Isso fornecerá a base para o desenvolvimento de novos sistemas ou alterações nos sistemas vigentes de forma a atender às exigências, identificadas e acordadas nos passos anteriores.

Os produtos resultantes deste passo podem ser:

- Inventário do sistema de gestão de processos e documentos, bem como dos demais sistemas de informação e comunicação existentes.
- Relatório sobre o sistema de gestão de processos e documentos e sistemas de informação existentes, avaliando até que ponto atendem às exigências a serem cumpridas para a produção e manutenção de documentos.
- Relatório sobre a avaliação da integração entre os documentos digitais e os não-digitais constantes de um dossiê híbrido.

e. Identificação das estratégias para satisfazer as exigências a serem cumpridas para a produção de documentos

Consiste em determinar as estratégias (padrões, procedimentos, práticas e ferramentas) que levem ao cumprimento das exigências para a produção de documentos. O objetivo deste passo é avaliar o potencial de cada estratégia para alcançar o resultado desejado e o risco, em caso de falha.

A escolha das estratégias deve considerar:

- A natureza da instituição, incluindo sua missão e história.
- Os tipos de atividades desenvolvidas.
- A forma como as atividades são conduzidas.
- O ambiente tecnológico existente.
- As tendências tecnológicas.
- A cultura institucional e
- A inclusão das funcionalidades do sistema anterior.

Os produtos resultantes deste passo podem incluir:

- Lista das estratégias selecionadas para satisfazer as exigências para a produção de documentos.

- Documento a ser encaminhado à administração, recomendando a elaboração de um projeto de gestão de documentos e relacionando as estratégias a serem adotadas, com as devidas justificativas.

f. Projeto e implementação do sistema de gestão de processos e documentos

Consiste em projetar um sistema de gestão que incorpore as estratégias selecionadas no passo anterior, que atenda às exigências identificadas e documentadas no passo "c" e que corrija quaisquer deficiências identificadas no passo "d", redesenhando os procedimentos e os sistemas de informação e comunicação existentes, implementando-os e integrando-os ao sistema de gestão de processos e documentos.

O projeto de um sistema de gestão de processos e documentos visa:

- Projetar mudanças ou adaptações para sistemas, nos processos e práticas correntes.
- Determinar como incorporar essas mudanças ou adaptações para melhorar a gestão dos processos e documentos na instituição.
- Adaptar ou adotar soluções tecnológicas, considerando, o quanto possível, um plano estratégico de evolução para minimizar os efeitos da obsolescência tecnológica.

Para alcançar esses objetivos, o projeto e a implementação de um sistema de gestão de processos e documentos devem ter como base uma metodologia de desenvolvimento de sistemas que inclua:

- Organização dos processos envolvidos.
- Especificações detalhadas dos componentes tecnológicos, como *software* e *hardware*, considerando que o sistema deve ser modular, evolutivo e expansível. Uma metodologia de especificação de requisitos do *software* deve ser adotada para representar as diferentes visões do sistema, como, por exemplo, casos de uso.
- Metodologia de gestão de projetos, envolvendo planejamento:
  - das atividades (escopo), incluindo as responsabilidades (recursos humanos) e o cronograma (tempo).
  - dos custos.
  - das aquisições.
  - dos riscos.
  - da integração.
  - da qualidade.
  - da comunicação.
- Plano de segurança da informação (física e lógica) e de contingência.
- Metodologia e procedimentos de auditoria.

- *Design* do *software*, com diagramas representando a arquitetura e os componentes do sistema, a integração e a interoperabilidade entre os sistemas.
- Implementação dos componentes de *software*, pela construção e aquisição.
- Documentação técnica do sistema voltada a usuários.
- Testes do sistema.
- Plano de implantação do sistema, inclusive com previsão de treinamento de pessoal.
- Detalhamento das revisões periódicas do projeto, em conformidade com o plano estratégico de evolução e com as mudanças na tecnologia e no mercado.

g. Implantação do sistema de gestão de processos e documentos

Consiste em colocar em produção o objeto do projeto e da implementação por meio de:

- Procedimentos de carga de dados, conversão de dados e migração de sistemas.
- Homologação do sistema, mediante sua validação por parte dos usuários e da área de tecnologia de informação (TI), para autorizar a operação do sistema no ambiente de produção.
- Projeto piloto — entrada em produção do sistema em uma área de abrangência menor.
- Dimensionamento de ambiente computacional (*hardware*, *software* e comunicação de dados) para dar suporte ao sistema de gestão de processos e documentos.
- Instalação dos componentes.
- Parametrização do sistema para adaptá-lo a necessidades específicas.
- Treinamento de pessoal.
- Operação assistida.
- Integração do sistema com os procedimentos e os demais sistemas de informação e comunicação existentes.
- Suporte e manutenção do sistema.

A implantação de um sistema de gestão de processos e documentos é um empreendimento complexo. Ela deve ser planejada de modo a minimizar a necessidade de interrupções das atividades na instituição. O processo de implantação deverá contar com documentação prévia, detalhando os passos previstos, bem como gerar relatórios das ações realizadas e de problemas encontrados.

Os produtos resultantes deste passo podem incluir:

- Regulamentação das políticas, diretrizes e procedimentos por meio de normas e manuais.
- Material de treinamento.
- Documentação dos processos de conversão e migração dos sistemas.
- Relatórios sobre avaliação de desempenho do sistema.

h. Monitoramento e ajustes

Consiste em recolher, de forma sistemática, informação sobre o desempenho do sistema de gestão de processos e documentos.

O desempenho é medido ao avaliar se os documentos são produzidos e organizados de acordo com as necessidades da instituição e se estão relacionados apropriadamente aos processos dos quais fazem parte.

O objetivo deste passo é medir o desempenho do sistema, detectar possíveis deficiências e fazer os ajustes necessários.

Este passo envolve:

- Planejamento e aplicação de testes de avaliação de desempenho.
- Entrevistas com a administração, equipe e outros parceiros.
- Aplicação de questionários para medir o desempenho do sistema.
- Observação, análise, avaliação da correção e auditoria das informações e dos procedimentos implementados.

A análise de informações quantitativas providas pelo monitoramento tem por objetivo a avaliação concreta dos benefícios da automação trazida pelo sistema. Outro objetivo importante do monitoramento constante é a minimização de riscos nas atividades do programa de gestão.

Constatações de insuficiência de desempenho do sistema, em face da demanda das informações gerenciadas, poderão indicar a necessidade de incremento no *hardware* (*upgrades*), reconfigurações no ambiente do sistema e evolução do *software*, na forma de versões otimizadas.

Os produtos resultantes deste passo podem incluir:

- Desenvolvimento e aplicação de uma metodologia para avaliar objetivamente o sistema de gestão de processos e documentos.
- Documentação do desempenho desse sistema.
- Relatório para a administração com conclusões e recomendações.

1.4.8 Suspensão ou extinção do GestãoDoc

Quando um GestãoDoc é suspenso ou extinto, ele deve tonar-se acessível para consulta, e novos documentos não devem ser incluídos. Quanto aos documentos já inseridos, poderão ser removidos de acordo com as diretrizes de destinação ou transferidos para outros sistemas.

O processo de suspensão ou extinção do GestãoDoc deve ser documentado, incluindo planos de conversão ou mapeamento dos dados, pois essas informações detalhadas serão necessárias à verificação de autenticidade, integridade e manutenção da acessibilidade dos documentos contidos no sistema suspenso ou extinto.

2 Organização dos documentos institucionais: plano de classificação e manutenção dos documentos

Os documentos institucionais podem ser agregados em processos/dossiês, de forma estruturada. Essa estrutura reflete as funções e atividades da organização, representadas no plano de classificação.

A Justiça Federal organiza seus documentos institucionais em documentos e processos: judiciais e administrativos.

O plano de classificação dos processos judiciais concretiza-se por meio da TUC e da TUA. Já os documentos administrativos são classificados pelo PCTT, incluindo os da atividade administrativa forense.

2.1 Configuração e administração do plano de classificação no GestãoDoc

Os requisitos desta seção referem-se às funcionalidades do sistema para apoiar a configuração do plano de classificação dentro do GestãoDoc — como desenhar um plano de classificação em um GestãoDoc.

REF.	REQUISITO	OBRIG.
RPC2.1.1	Incluir e ser compatível com os instrumentos de classificação da política de gestão documental da Justiça Federal.	O
RPC2.1.2	Garantir a criação de classes, subclasses, grupos e subgrupos nos níveis do plano de classificação de acordo com o método de codificação adotado.	O
RPC2.1.3	Permitir a usuários autorizados o acréscimo de novas classes de acordo com as alterações do sistema de classificação de documentos e processos da Justiça Federal.	O
RPC2.1.4	Registrar as datas de: abertura de uma nova classe, reclassificação, movimentação e modificação da classe no respectivo metadado.	O
RPC2.1.5	Registrar a mudança de nome de uma classe já existente no respectivo metadado.	O

REF.	REQUISITO	OBRIG.
RPC2.1.6	Permitir o deslocamento de uma classe inteira, incluindo as subclasses, grupo, subgrupos e os documentos ali classificados, para um outro ponto do plano de classificação. Nesse caso, é necessário fazer o registro do deslocamento nos metadados do plano de classificação.	O
RPC2.1.7	Permitir que o gestor do sistema torne inativa e inacessível aos demais usuários uma classe em que não serão mais classificados documentos.	O
RPC2.1.8	Impedir a eliminação de uma classe ativa ou inativa.	O
RPC2.1.9	Permitir a associação de metadados às classes e restringir a inclusão e alteração desses mesmos metadados somente a usuários autorizados.	O
RPC2.1.10	Disponibilizar pelo menos dois mecanismos de atribuição de identificadores às classes do plano de classificação, prevendo a possibilidade de se utilizar ambos, separadamente ou em conjunto, na mesma aplicação: ▪ Atribuição de um código numérico ou alfanumérico. ▪ Atribuição de um termo que identifique cada classe.	O
RPC2.1.11	Prever atributos associados aos instrumentos de classificação e indexação de assunto de modo a não permitir classificações genéricas. *Com exceção do usuário autorizado, em algumas classes não é permitido incluir documentos. Nesses casos os documentos devem ser classificados apenas nos níveis subordinados.* *Na TUA os processos devem ser classificados nos níveis 3 ou 4 e quando se tratar de assunto novo os usuários autorizados, apenas provisoriamente, podem utilizar o nível 2.* *No PCTT nenhum documento/processo administrativo pode ser classificado no Assunto Principal (primeiro nível). Em caso de assunto não existente, utilizar o assunto secundário hierárquico.*	O

REF.	REQUISITO	OBRIG.
RPC2.1.12	Utilizar o termo completo para identificar uma classe. *Entende-se por termo completo toda a hierarquia referente àquela classe.* *TUA:* *01.14.05.02 — Habilitação, Registro Cadastral e Julgamento da Licitação — Licitações — Licitações e Contratos — Administrativo.* *PCTT:* *23.405.01-A — Requisição de servidor (solicitação, prorrogação, etc.) — Requisição de pessoal. Cessão — Movimentação de pessoal — Quadros, tabelas e política de pessoal — Administração e desenvolvimento de pessoas.*	O
RPC2.1.13	Assegurar que os termos completos, que identificam cada classe, sejam únicos no plano de classificação.	O
RPC2.1.14	Importar e exportar total ou parcialmente um plano de classificação.	D
RPC2.1.15	Prover funcionalidades com vistas à elaboração de relatórios para apoiar a gestão do plano de classificação, incluindo a capacidade de gerar relatório: ▪ Completo do plano de classificação. ▪ Parcial do plano de classificação a partir de um ponto determinado na hierarquia. ▪ Dos documentos ou processos/dossiês classificados em uma ou mais classes do plano de classificação. ▪ De documentos classificados por unidade administrativa.	O

2.2 Classificação e metadados dos processos/dossiês

Os requisitos desta seção referem-se à formação e classificação de processos/dossiês e à associação de metadados.

REF.	REQUISITO	OBRIG.
RPC2.2.1	Permitir a classificação dos processos/dossiês somente nas classes autorizadas. *Ver RPC2.1.11*	O

REF.	REQUISITO	OBRIG.
RPC2.2.2	Permitir a classificação de um número ilimitado de processos/dossiês dentro de uma classe.	O
RPC2.2.3	Utilizar o termo completo da classe para identificar um processo/dossiê, tal como especificado em RPC2.1.12.	O
RPC2.2.4	Permitir a associação de metadados aos processos/dossiês e restringir a inclusão e alteração desses mesmos metadados somente a usuários autorizados.	O
RPC2.2.5	Associar os metadados dos processos/dossiês conforme estabelecido nos elementos de metadados.	O
RPC2.2.6	Permitir que um novo processo/dossiê herde, da classe na qual foi classificado, determinados metadados predefinidos. *Exemplos desta herança são: temporalidade prevista e restrição de acesso.*	O
RPC2.2.7	Relacionar os metadados herdados de forma que uma alteração no metadado de uma classe seja automaticamente incorporada ao processo/dossiê que herdou esse metadado.	D
RPC2.2.8	Permitir a alteração conjunta de um determinado metadado em um grupo de processos/dossiês previamente selecionado.	O

2.3 Gerenciamento dos processos/dossiês

Os requisitos desta seção referem-se ao gerenciamento dos documentos institucionais no que diz respeito a controles de abertura e encerramento de processos/dossiês e seus respectivos volumes e inclusão de novos documentos nesses processos/dossiês e respectivos volumes, bem como procedimentos de reclassificação.

REF.	REQUISITO	OBRIG.
RPC2.3.1	Registrar automaticamente a data de abertura e de encerramento ou baixa do processo/dossiê. *Essas datas são parâmetros para aplicação dos prazos de guarda e destinação do processo/dossiê.*	O
RPC2.3.2	Permitir que um processo/dossiê seja encerrado, reaberto ou baixado mediante procedimentos regulamentares.	O

REF.	REQUISITO	OBRIG.
RPC2.3.3	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
RPC2.3.4	Manter o registro de suas posições anteriores à reclassificação, quando um processo/dossiê é reclassificado, de forma a obter-se um histórico.	O
RPC2.3.5	Permitir que o usuário autorizado introduza as razões para a reclassificação, quando um processo/dossiê ou documento é reclassificado.	O
RPC2.3.6	Permitir a geração de referências cruzadas para processos/dossiês afins.	O
RPC2.3.7	Registrar múltiplas entradas para um documento digital em mais de um processo/dossiê.	O
RPC2.3.8	Impedir a eliminação de um 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. *A eliminação será devidamente registrada em trilha de auditoria.*	O
RPC2.3.9	Impedir o acréscimo de novos documentos a processos/dossiês já encerrados. *Para receber novos documentos, os processos/dossiês encerrados deverão ser reabertos.*	O
RPC2.3.10	Permitir a consulta aos processos/dossiês já encerrados.	O
RPC2.3.11	Garantir a integridade da relação hierárquica entre classe, processo/dossiê, volume e documento em todos os momentos, independentemente de atividades de manutenção, ações do usuário ou falha de componentes do sistema. *Em hipótese alguma poderá ocorrer uma situação em que qualquer ação do usuário ou falha do sistema dê origem a uma inconsistência na base de dados do GestãoDoc.*	O
RPC2.3.12	Oferecer ferramentas para a realização de operações em lote, tais como: abertura e encerramento de processos/dossiês e seus respectivos volumes, reclassificação, citação/intimação, sentença/decisão/despacho, etc.	O

2.4 Processos

A formação e manutenção de processos na Justiça Federal apresentam 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 (ex.: 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.

O detalhamento dessas regras está previsto em legislação e demais normas específicas, que deverão ser respeitadas pelos órgãos, de acordo com seu âmbito de atuação.

REF.	REQUISITO	OBRIG.
RPC2.4.1	Prever a formação/autuação de processos conforme estabelecido nas leis e regulamentações vigentes.	O
RPC2.4.2	Prever que as peças integrantes do processo recebam paginação contextualizada de acordo com cada processo relacionado. *Uma mesma contestação juntada a vários processos tem numeração diferente de acordo com a numeração de cada processo.*	O
RPC2.4.3	Prever procedimentos para reunião de processos por apensação. Nos processos judiciais, a apensação 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 05 da TUMP (apensado o processo) e seu complemento obrigatório (número do processo).*	O
RPC2.4.4	Prever procedimentos para desapensação. Nos processos judiciais, via de regra, a desapensação 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 06 da TUMP (desapensado o processo) e seu complemento obrigatório (número do processo).*	O

REF.	REQUISITO	OBRIG.
RPC2.4.5	Prever procedimentos para desentranhamento de 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/atributo 15.01 da TUMP (cancelamento de juntada — desentranhamento) e seu complemento obrigatório (especificar documento).*	O
RPC2.4.6	Prever procedimentos para desmembramento de um processo judicial ou administrativo em dois ou mais processos. Nos processos judiciais, sempre ocorre por decisão judicial, como no exemplo do art. 46, parágrafo único, do CPC ou do art. 80, CPP. *Esse procedimento deverá ser registrado nos metadados do processo.*	O
RPC2.4.7	Prever procedimentos para a anexação de documentos organizados em volumes próprios a um determinado processo. *Esse procedimento deverá ser registrado nos metadados do processo.*	O

2.5 Volumes: abertura, encerramento e metadados

Em alguns casos os processos/dossiês são compartimentados em volumes ou partes, de acordo com convenções predeterminadas. Essa divisão não está baseada no conteúdo intelectual dos processos/dossiês, mas em outros critérios, como a dimensão, o número de documentos, períodos de tempo etc. Essa prática tem como objetivo facilitar o gerenciamento físico dos processos/dossiês.

Os requisitos desta seção referem-se à utilização de volumes para subdividir processos/dossiês.

REF.	REQUISITO	OBRIG.
RPC2.5.1	Gerenciar volumes para subdividir processos/dossiês, distinguindo entre processos/dossiês e volumes.	O
RPC2.5.2	Permitir a associação de metadados aos volumes e restringir a inclusão e a alteração desses mesmos metadados somente a usuários autorizados.	O

REF.	REQUISITO	OBRIG.
RPC2.5.3	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
RPC2.5.4	Permitir a abertura de volumes a qualquer processo/dossiê que não esteja encerrado.	O
RPC2.5.5	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
RPC2.5.6	Impedir a reabertura de um volume já encerrado para acréscimo de documentos.	O
RPC2.5.7	Assegurar que um volume somente conterá documentos. Não é permitido que contenha outro volume ou um outro processo/dossiê.	O
RPC2.5.8	Permitir que um volume seja encerrado por meio de procedimentos regulamentares.	O

2.6 Manutenção de documentos institucionais não-digitais e híbridos

A Justiça Federal possui documentos e processos digitais e não-digitais. Esses últimos podem estar registrados em papel ou outros suportes, tais como fitas de vídeo, de áudio etc. Um GestãoDoc deve registrar os documentos ou processos/dossiês não-digitais e digitais utilizando o mesmo plano de classificação e deve ainda possibilitar a gestão de documentos ou processos/dossiês híbridos, formados por uma parte digital e uma parte não-digital.

REF.	REQUISITO	OBRIG.
RPC2.6.1	Capturar documentos ou processos/dossiês não-digitais e gerenciá-los como os digitais. *Para conceito de captura veja capítulo 3.*	O

REF.	REQUISITO	OBRIG.
RPC2.6.2	Gerenciar as partes dos documentos ou processos/dossiês híbridos, associando-as ao mesmo número identificador, atribuído pelo sistema, e título, além de indicar que se trata de um documento institucional híbrido.	O
RPC2.6.3	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
RPC2.6.4	Possuir mecanismos para acompanhar a movimentação do documento, processo/dossiê não-digital, de forma que se evidencie ao usuário a localização atual.	O
RPC2.6.5	Oferecer ao usuário funcionalidades para solicitar vista, carga ou desarquivamento de um documento e/ou processo não-digital.	O
RPC2.6.6	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.	O
RPC2.6.7	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
RPC2.6.8	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. *(Conforme resolução do CJF)*	O
RPC2.6.9	Registrar na trilha de auditoria todas as alterações efetuadas nos metadados dos documentos ou processos/dossiês não-digitais ou híbridos.	O

3 Captura

A captura é a incorporação de um documento/processo ao GestãoDoc, quando passará a seguir as rotinas de tramitação. Uma vez capturado, o documento será incluído no fluxo de trabalho.

Tradicionalmente, nos sistemas de gestão de processos e documentos em papel, a captura é feita no momento em que o documento é registrado, classificado e identificado. Para o processo judicial é o momento da autuação.

Em um GestãoDoc, o documento tanto pode ser produzido diretamente dentro do sistema e então capturado automaticamente no momento do registro, como pode ser produzido fora do sistema, capturado e registrado posteriormente.

A política de gestão de processos e documentos da Justiça Federal é única para documentos não-digitais, digitais e híbridos, assim, os GestãoDocs terão de capturar todos os documentos pertinentes independentemente do suporte.

Além do código de classificação, descritores, número de protocolo e número de registro, a captura pode prever a introdução de outros metadados, a saber: data e hora da criação, da transmissão e do recebimento do documento; nome do autor, do originador, do digitador e do destinatário, entre outros. Esses metadados podem ser registrados em vários níveis de detalhe, dependendo das necessidades geradas pelos procedimentos da Justiça Federal e do seu contexto jurídico-administrativo.

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

A captura tem como pré-requisito 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.
- A destinação final do documento: guarda permanente ou passível de eliminação.

A captura consiste nas ações de:

- Protocolo
- Autuação
- Classificação
- Indexação
- Atribuição de restrição de acesso
- Arquivamento

Protocolo

As atividades de protocolo são constituídas pelo conjunto de operações que visam ao controle de entrada dos documentos produzidos e recebidos que tramitam na Justiça Federal, assegurando sua localização, recuperação e acesso.

Após o recebimento dos documentos, o serviço de protocolo identifica se o documento é processual ou administrativo/forense, atribuindo-lhe número e data de entrada, anotando o código de classificação e, de acordo com essa identificação, seleciona o sistema onde tramitará ou será autuado.

Autuação

- **Registro do processo judicial**

  Consiste em formalizar a captura do documento judicial dentro do sistema de gestão de processos e documentos, por meio da atribuição de um número identificador e de uma descrição informativa.

  O registro tem por objetivo demonstrar que o documento foi produzido ou recebido e capturado pelo sistema de gestão de processos e documentos, bem como facilitar sua recuperação.

  Os documentos judiciais são de dois tipos:

  - Vinculados diretamente ao processo (petição inicial, certidão de trânsito em julgado, recurso etc.).
  - Relacionados a atividades administrativas forenses (diário eletrônico, pauta de julgamentos, estatísticas etc.).

  Os documentos serão numerados pelo sistema de Numeração Única de Processos, conforme requisitos estabelecidos pelas Resoluções do Conselho da Justiça Federal.

  Além de numerados, os documentos serão classificados de acordo com as tabelas processuais do CJF.

- **Registro de documentos e processos administrativos**

  As atividades dos protocolos administrativos, independentemente de serem centralizados ou descentralizados, visam ao registro do documento institucional por captura dos dados informacionais dos documentos recebidos, tais como: o número original, o assunto do PCTT, a data da produção, a data do registro, o conteúdo etc., com a finalidade de informar, de forma rápida e precisa, a sua situação e localização.

  Os documentos produzidos no âmbito da instituição (memorandos, pareceres, requisições etc.) serão numerados, classificados e encaminhados com base no PCTT.

  Os documentos pertinentes às atividades administrativas forenses devem receber um número atribuído pelo sistema e classificação de acordo com a classe 90 do PCTT.

Classificação

É o ato ou efeito de analisar e identificar o conteúdo dos documentos e processos judiciais e de selecionar a classe (tipologia documental) à qual pertencem para fins de arranjo e de recuperação da informação. Essa classificação é feita a partir de planos ou esquemas de classificação aprovados pelo Conselho da Justiça Federal.

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

A classificação deve se basear no plano de classificação e envolve os seguintes passos:

- Identificar a ação que o documento registra.
- Localizar a ação ou atividade no plano de classificação.
- Comparar a atividade com a estrutura organizacional para verificar se é apropriada à unidade que gerou o documento.
- Aplicar a classificação ao documento.

Na Justiça Federal, os documentos e processos administrativos são classificados com base no Plano de Classificação e Tabela de Temporalidade — PCTT, para fins de armazenamento e atribuição de prazos de guarda e de destinação.

Os processos judiciais são classificados pela Tabela Única de Classes — TUC, que lhes assegura a reunião pela tipologia documental.

Indexação

A indexação de assuntos envolve duas etapas principais:

- 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.

Na Justiça Federal, os processos judiciais são indexados pela Tabela Única de Assuntos — TUA.

Atribuição de restrição de acesso

Os documentos também devem ser analisados com relação às precauções de segurança — se são considerados ostensivos ou sigilosos. Para os documentos sigilosos, a legislação estabelece diferentes graus a serem atribuídos 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 pela Justiça Federal e envolve os seguintes passos:

- Identificar a ação ou atividade que o documento registra.
- Identificar a unidade administrativa à qual o documento pertence.
- Verificar a precaução de segurança e o grau de sigilo.
- Atribuir o grau de sigilo e as restrições de acesso ao documento.
- Registrar o grau de sigilo e as restrições de acesso no sistema de gestão de processos e documentos.

Os requisitos de segurança são apresentados no Capítulo 6.

Arquivamento

O arquivamento de documentos e processos em fase corrente é a guarda dos documentos não-digitais ou mídias digitais no local estabelecido, de acordo com a sua classificação.

Os métodos de arquivamento devem ser associados ao Plano de Classificação, de acordo com a especificidade de cada tipo documental, visando facilitar o arquivamento, a busca e a recuperação do documento.

A escolha de um método ideal de arquivamento deve ser determinada pela natureza dos documentos e pela estrutura da organização. Esses métodos podem ser:

- Direto (alfabético, geográfico) — Busca o documento no local arquivado, sem intervenção de instrumentos de pesquisas.
- Indireto (por assuntos, numérico) — Necessita de consultas a guias ou instrumentos de pesquisa para a localização do documento.

A operação de arquivamento dos documentos digitais se diferencia do arquivamento dos documentos não-digitais porque nesses últimos a operação

é ao mesmo tempo lógica e física, como, por exemplo, arquivar um relatório na pasta.

3.1 Captura: procedimentos gerais

REF.	REQUISITO	OBRIG.
RCA3.1.1	A captura deve garantir a execução das funções relacionadas a seguir, de acordo com o sistema de classificação da Justiça Federal: ▪ 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 ou critérios de guarda. ▪ Controlar e validar a introdução de metadados.	O
RCA3.1.2	Capturar documentos digitais das seguintes formas: ▪ Documento individual produzido em arquivo digital fora do GestãoDoc. ▪ Documento individual produzido em *workflow* integrado ao GestãoDoc. ▪ Documentos em lote.	O
RCA3.1.3	Automatizar a produção de documentos por meio da exibição de formulários e modelos predefinidos pelo programa de gestão de processos e documentos.	D
RCA3.1.4	Automatizar a produção de petições eletrônicas por meio da exibição de formulários e modelos predefinidos.	O
RCA3.1.5	Aceitar o conteúdo do documento, bem como as informações que definem sua apresentação.	O
RCA3.1.6	Os documentos associados a vários objetos digitais devem ser desassociados e capturados individualmente.	O

REF.	REQUISITO	OBRIG.
RCA3.1.7	Permitir a inserção de todos os metadados, obrigatórios e optativos, definidos em sua configuração e garantir que se mantenham associados ao documento. São exemplos de metadados: ▪ Nome do arquivo digital. ▪ Número identificador atribuído pelo sistema. ▪ Data e hora de produção e captura. ▪ Data e hora de transmissão e recebimento. ▪ Título ou descrição abreviada. ▪ Formato (gênero / espécie / tipo). ▪ Usuário cadastrador. ▪ Unidade responsável pela execução da ação. ▪ Indicação de anotação. ▪ Restrição de acesso. ▪ Registro das migrações e data em que ocorreram. ▪ Números das páginas inicial e final do documento. ▪ Tamanho do documento. ▪ *Checksum*. ▪ *Software* (nome e versão) sob o qual o documento foi produzido ou no qual foi capturado. ▪ Máscaras de formatação (*template*) necessárias para interpretar a estrutura do documento. ▪ Classificação de acordo com os instrumentos de classificação, temporalidade e destinação da política de gestão documental da Justiça Federal.	O
RCA3.1.8	Permitir a inserção dos metadados obrigatórios, previstos em legislação específica da Justiça Federal, no momento da captura de documentos e processos/dossiês.	O
RCA3.1.9	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
RCA3.1.10	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

REF.	REQUISITO	OBRIG.
RCA3.1.11	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
RCA3.1.12	Utilizar o sistema de classificação e indexação de assuntos da Justiça Federal para apoiar a atribuição do metadado assunto/descritor.	O
RCA3.1.13	Utilizar o tesauro ou vocabulário controlado para apoiar a atribuição do metadado assunto/descritor.	D
RCA3.1.14	Garantir que os metadados associados a um documento sejam alterados somente por usuários autorizados.	O
RCA3.1.15	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
RCA3.1.16	Garantir a visualização do 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
RCA3.1.17	Garantir a inserção de outros metadados após a captura. *Por exemplo, data e hora de alteração e mudança de suporte.*	O
RCA3.1.18	Permitir ao usuário o registro de todas as versões de documento enquanto não for dada publicidade.	D
RCA3.1.19	Registrar a versão final do documento institucional após ter sido dada publicidade ou assinado digitalmente.	O

REF.	REQUISITO	OBRIG.
RCA3.1.20	Prestar assistência aos usuários no que diz respeito à 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 dossiês que contenham documentos institucionais relacionados. ▪ Indicar classificações possíveis a partir dos metadados já inseridos, como, por exemplo, classe de apelação criminal quando se tratar de processo criminal e com apelação recebida ou pauta de julgamento. ▪ Indicar classificações possíveis a partir do conteúdo do documento.	D
RCA3.1.21	Permitir que um usuário disponibilize documentos a outro usuário para complementar o processo de captura, no caso dos procedimentos dessa captura serem executados por vários usuários.	O
RCA3.1.22	No caso de documentos ou processos/dossiês 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
RCA3.1.23	Emitir um aviso caso o usuário tente registrar um documento não-digital aparentemente igual a outro que já tenha sido registrado no mesmo processo/dossiê.	O
RCA3.1.24	Impedir a reinserção de documentos digitais que forem detectados como idênticos.	O
RCA3.1.25	Permitir a captura dos documentos não-digitais e/ou híbridos.	O
RCA3.1.26	Acrescentar aos metadados dos documentos não-digitais informações sobre sua localização.	O

3.2 Captura em lote

REF.	REQUISITO	OBRIG.
RCA3.2.1	Proporcionar a captura em lote de documentos gerados por outros sistemas. Esse procedimento tem que: ▪ 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 documento 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

3.3 Captura de mensagens de sistema de comunicação eletrônica

O sistema de comunicação eletrônica é utilizado para criar, transmitir e receber mensagens eletrônicas e outros documentos digitais por meio de redes de computadores. As características do sistema de comunicação eletrônica podem dificultar seu gerenciamento. Assim, um GestãoDoc deve permitir controles de gestão para dotar os usuários da capacidade de capturar apenas mensagens e anexos previamente selecionados.

Esse procedimento requer que os usuários avaliem a pertinência e a importância dos itens, bem como o risco de não os capturar.

REF.	REQUISITO	OBRIG.
RCA3.3.1	Permitir a captura de mensagens de sistema de comunicação eletrônica após a seleção de quais serão objeto de registro.	O
RCA3.3.2	Assegurar a captura dos metadados referentes à mensagem de sistema de comunicação eletrônica, de tal forma que a confiabilidade e a autenticidade estejam garantidas.	O

3.4 Formato de arquivo e estrutura dos documentos a serem capturados

Os órgãos da Justiça Federal precisarão realizar a captura de uma gama diversificada de documentos com formatos de arquivo e estruturas diferentes. Os requisitos técnicos para a captura variarão de acordo com a complexidade dos documentos. Em alguns ambientes não é possível identificar antecipadamente todas os formatos de arquivo e estruturas possíveis dos documentos, já que alguns são recebidos de fontes externas.

Documentos automodificáveis

Alguns documentos aparentam ter seus conteúdos alterados sem intervenção do usuário. Um exemplo é 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. Entretanto o documento lógico não se modifica, apenas sua exibição (documento conceitual) sofre alterações conforme o *software* utilizado para visualizá-lo.

Outros documentos podem conter um código que os modifique realmente. É o caso de 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. Caso isso não seja possível, os documentos devem ser armazenados em formatos que desativem o código automodificador ou visualizados por meio de *software* que não desencadeie a alteração. Por exemplo, uma planilha de cálculo que contenha "macros" deve ser convertida para um formato estável, como o PDF, antes de ser capturada no GestãoDoc.

Quando não for possível converter os documentos automodificáveis para formato estável ou visualizá-los por meio de *software* que não desencadeie a alteração, a captura desses documentos no GestãoDoc deve ser acompanhada do registro das informações relativas às funções automodificadoras nos metadados.

REF.	REQUISITO	OBRIG.
RCA3.4.1	Possuir a capacidade de capturar documentos nos formatos previamente definidos como padrão para a Justiça Federal.	O

REF.	REQUISITO	OBRIG.
RCA3.4.2	Capturar, entre outros, os seguintes documentos: ▪ Informações de outros aplicativos: contabilidade, folha de pagamento, desenho assistido por computador (CAD). ▪ Documentos em papel digitalizados por meio de escâner. ▪ Documentos sonoros. ▪ Videoclipes. ▪ Diagramas e mapas digitais. ▪ Dados estruturados.	D
RCA3.4.3	Capturar documentos que se apresentam com as seguintes estruturas: ▪ Simples: texto, imagens, mensagens sistema de comunicação eletrônica, slides digitais, som e vídeo. ▪ Composta: mensagens de sistema de comunicação eletrônica com anexos, páginas Web e publicações eletrônicas.	D
RCA3.4.4	Permitir que um documento composto seja capturado de qualquer uma das duas formas seguintes: ▪ Único documento de arquivo composto. ▪ Série de documentos de arquivo simples relacionados, um para cada componente do documento composto.	O
RCA3.4.5	Incluir novos formatos e arquivos à medida que forem adotados pela Justiça Federal.	O
RCA3.4.6	Armazenar em formato que desative o código automodificador quando da captura de documento automodificável.	O

3.5 Estrutura dos procedimentos de gestão

A gestão de processos e documentos digitais prevê o estabelecimento de três domínios dentro do ambiente eletrônico.

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

As regras estabelecidas pelo sistema de gestão de processos e documentos definem em que espaços os documentos podem ser:

- Produzidos, recebidos, alterados, capturados (registrados, classificados, indexados e arquivados ou encaminhados), armazenados e eliminados.

- O espaço no qual os metadados são incluídos.
- Os direitos de acesso em cada espaço e a maneira pela qual os documentos tramitam dentro e fora da Justiça Federal.

Uma vez capturados, os documentos e seus metadados devem ser mantidos em versão definitiva e protegidos contra alterações deliberadas ou acidentais.

REF.	REQUISITO	OBRIG.
RCA3.5.1	Reconhecer três domínios para o controle dos procedimentos de gestão: espaço individual, espaço de grupo e espaço geral.	O
RCA3.5.2	Operacionalizar as regras estabelecidas pelo sistema de gestão de processos e documentos nos três espaços.	O
RCA3.5.3	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 6.10 — Alteração e exclusão de documentos institucionais.	O
RCA3.5.4	Emitir um aviso, ao se tentar capturar um documento cujos dados estruturados estejam incompletos e impedir quando estiverem inconsistentes.	O

4 Armazenamento

As considerações e as ações relativas ao armazenamento dos documentos institucionais não-digitais e digitais permeiam todo seu ciclo de vida. Esse armazenamento deve garantir a integridade e o acesso aos documentos.

Os documentos, independentemente do formato, requerem um armazenamento criterioso desde o momento de sua criação, para garantir sua preservação de longo prazo.

Num cenário híbrido que envolve ao mesmo tempo documentos institucionais não-digitais e digitais, deve-se atentar para requisitos de armazenamento que atendam igualmente às necessidades desses dois tipos de documentos.

As condições de armazenamento devem considerar o volume e as propriedades físicas dos documentos. Devem ser projetadas também em razão da proteção contra o acesso não-autorizado e perdas por destruição, furto e sinistro.

No caso dos documentos institucionais digitais, a Justiça Federal deve dispor de políticas e diretrizes para conversão, migração ou acesso a esses documentos de maneira a garantir sua autenticidade, acessibilidade e utilização. Os procedimentos de conversão e migração devem detalhar as mudanças ocorridas nos sistemas e nos formatos dos documentos. (Ver Capítulo 5, especificamente voltado à preservação)

Os fatores importantes na seleção das opções de armazenamento são:

- Volume e estimativa de crescimento dos documentos — Fator que deve ser considerado para se avaliar a capacidade de armazenamento — capacidade dos dispositivos de armazenamento e no caso de documentos não-digitais, áreas de depósito, tipos e quantidade de estante.
- Segurança dos documentos — As instalações de armazenamento (depósitos, arquivos, computadores) devem prever limitação de acesso aos documentos, como, por exemplo, controle das áreas de armazenamento e sistemas de detecção de entradas não-autorizadas. 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 GestãoDoc. (Ver Capítulo 6, Segurança)
- Características físicas do suporte e do ambiente — Fatores como tipo de suporte, peso, grau de contaminação do documento e do ambiente, temperatura e umidade influenciarão na adequação das condições de armazenamento. Nesse sentido, devem ser adotados procedimentos — como o controle e verificação do tempo de vida útil e da estabilidade dos suportes — para prevenir quaisquer 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 (tais como isótopos radioativos, toxinas e mofo) e infestação de insetos e microorganismos. Os documentos digitais devem passar periodicamente pela troca de suporte — transferência de informações contidas num suporte para outro. Essa técnica é conhecida por rejuvenescimento (*refreshing*).

- Freqüência de uso — O uso mais ou menos freqüente dos documentos deve ser considerado na seleção das opções de armazenamento. No caso dos documentos não-digitais, as opções envolverão acondicionamento (pastas suspensas, caixas entre outros) 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 e outros) em diferentes graus de disponibilidade e velocidade.
- Custo relativo das opções de armazenamento dos documentos — Além do custo dos dispositivos de armazenamento, deve ser considerado o dos equipamentos para sua manipulação e de *software* de controle.

Os documentos digitais são armazenados em dispositivos de armazenamento eletrônicos, magnéticos e ópticos. Do ponto de vista tecnológico, distinguem-se três tipos de memória, em ordem decrescente de preço e velocidade de acesso: primária, secundária e terciária.

As memórias secundária e terciária são adequadas para armazenamento.

Os equipamentos devem adequar-se às características das operações — *on-line* ou *off-line*. Operações *on-line* só podem ser realizadas por meio 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.

4.1 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.

REF.	REQUISITO	OBRIG.
RAR4.1.1	Utilizar dispositivos e padrões estáveis no mercado. *Utilizar preferencialmente padrões abertos de armazenamento (como exemplo: ISO 9660:1988 — definição do formato de sistema de arquivos para CD-Rom).* *A escolha dos dispositivos de armazenamento deve contemplar padrões estáveis de mercado e fornecedores consolidados.*	O
RAR4.1.2	Avaliar periodicamente a escolha de dispositivos sempre que a evolução tecnológica indicar mudanças importantes.	O
RAR4.1.3	Efetuar migrações preventivas sempre que se tornar patente ou previsível a obsolescência do padrão corrente.	O
RAR4.1.4	Manter o registro de MTBF (*Mean Time Between Failures*)[6] para as memórias secundárias, bem como as datas de sua aquisição.	D
RAR4.1.5	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 RAR4.1.4 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.*	D
RAR4.1.6	Manter estatísticas da durabilidade efetivamente observada das memórias secundária e terciária.	D
RAR4.1.7	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.*	D

6 *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.

REF.	REQUISITO	OBRIG.
RAR4.1.8	Quando se proceder à eliminação de documentos, as memórias de suporte devem ser devidamente "sanitizadas", isto é, ter suas informações efetivamente indisponibilizadas. 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

4.2 Capacidade

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

REF.	REQUISITO	OBRIG.
RAR4.2.1	Possuir capacidade de armazenamento suficiente para a acomodação de todos os documentos, metadados e suas cópias de segurança.	O
RAR4.2.2	Utilizar dispositivos com maior capacidade unitária de armazenamento, a fim de reduzir a sobrecarga operacional.	D
RAR4.2.3	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
RAR4.2.4	Permitir ao administrador a configuração dos limites de capacidade de armazenamento dos diversos dispositivos.	D
RAR4.2.5	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

REF.	REQUISITO	OBRIG.
RAR4.2.6	Informar automaticamente ao administrador quando os dispositivos de armazenamento *on-line* atingirem níveis de alerta e níveis críticos de ocupação.	O
RAR4.2.7	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
RAR4.2.8	Permitir a definição de outras estatísticas referentes à capacidade de armazenamento de acordo com as necessidades específicas da Justiça Federal.	D

4.3 Efetividade de armazenamento

REF.	REQUISITO	OBRIG.
RAR4.3.1	Os dispositivos de armazenamento devem suportar métodos de detecção de erros para leitura e escrita de dados e prover mecanismos automáticos de aviso ao administrador do sistema.	O
RAR4.3.2	Utilizar técnicas de restauração de dados em caso de falhas.	O
RAR4.3.3	Utilizar mecanismos de proteção que previnam alterações indevidas e mantenham a integridade dos dados armazenados.	O
RAR4.3.4	Prever a utilização de técnicas para garantir maior confiabilidade e desempenho. *As técnicas recomendadas incluem redundância e paralelismo.*	D
RAR4.3.5	A integridade dos dispositivos de armazenamento deve ser periodicamente verificada.	O

5 Preservação

Os documentos institucionais devem-se manter acessíveis e utilizáveis por todo o tempo que se fizer necessário, com vistas a garantir sua longevidade, funcionalidade e disponibilidade. Deverão ser asseguradas as características dos documentos — tais como: autenticidade, integridade e acessibilidade — pela adoção de estratégias institucionais e técnicas proativas de criação e de preservação, que garantam sua perenidade. Essas estratégias são estabelecidas por uma política de preservação. As razões para preservação de um determinado documento normalmente estão associadas a seu valor probatório e informativo.

Tradicionalmente a preservação de documentos institucionais se concentra na obtenção da estabilidade do suporte da informação. Nos documentos não-digitais, o conteúdo e o suporte estão intrinsecamente ligados, assim, a manutenção do suporte garante a preservação do documento. De forma distinta, nos documentos digitais o foco da preservação é a manutenção do acesso, que pode exigir mudança de suporte e formatos, bem como a atualização do ambiente tecnológico. A fragilidade do suporte digital e a obsolescência tecnológica de *hardware*, *software* e formato exigem essas intervenções periódicas.

As estratégias de preservação de documentos institucionais podem ser divididas em gerais e específicas da tecnologia digital.

As primeiras incluem monitoramento e controle ambiental das instalações, restrições de acesso, cuidados no manuseio de equipamentos e material de acervo.

Já as estratégias voltadas para tecnologia digital compreendem cuidados quanto à durabilidade das mídias e à atualização da base tecnológica.

O problema da durabilidade das mídias pode ser contornado mediante cópias periódicas para novas mídias (*refreshing*).

Por outro lado, cuidados com a atualização da base tecnológica exigem planejamento e estratégias mais complexas, envolvendo mudanças de *software* e de *hardware*. O desafio a ser enfrentado é vencer a obsolescência tecnológica.

As mudanças em *software* — incluindo sistemas operacionais, sistemas de gerenciamento de banco de dados e aplicativos como editores de texto, planilhas eletrônicas, editores de imagem, entre outros — costumam ser bastante freqüentes. Os *softwares* podem ser simplesmente descontinuados, substituídos por outros equivalentes ou superiores, ou ainda ter sua versão atualizada para correção de *bugs* ou acréscimo de novas funcionalidades. É importante notar que os fornecedores de *software* deixam de prestar suporte a versões mais antigas de seus produtos.

Os formatos também sofrem alterações, muitas vezes em função de mudanças ocorridas nos programas aos quais estão associados. Novos programas podem ser compatíveis com os formatos antigos, mas também podem apresentar incorreções durante operações de leitura e escrita de dados nesses formatos.

Algumas técnicas comumente utilizadas para evitar os riscos provenientes da obsolescência tecnológica são:

- **Preservação da tecnologia** — Evita a necessidade imediata de implementação de novos sistemas. Porém, as necessidades de manutenção e integração com outros sistemas podem apresentar problemas ao longo do tempo. A preservação do *hardware*, em especial, é uma alternativa cara, mesmo nas situações em que o *hardware* é compartilhado entre mais de um usuário. Além disso, essa alternativa não é exeqüível a longo prazo, uma vez que o *hardware* pode ser danificado de forma irreversível, ficando completamente indisponível.
- **Emulação** — É a simulação de um determinado *hardware* ou *software* por meio de *software*. Permite que um computador moderno, possivelmente mais barato e de fácil manutenção, possa executar programas antigos desenvolvidos originalmente para outra plataforma. Para evitar possíveis perdas de informação e funcionalidades, deve ser realizada com bastante rigor. A probabilidade de ocorrência de perdas de informações e funcionalidades aumenta à medida que são utilizadas diversas camadas de emulação, como resultado da aplicação dessa técnica repetidas vezes.
- **Conversão de dados** — É empregada quando os formatos se tornam obsoletos. Os dados em formatos antigos são convertidos para novos formatos, apoiados em *hardware* e *software* mais atuais. Esse processo não está isento de problemas, podendo resultar em perdas de informações e funcionalidades. A conversão de dados também pode ser utilizada para reduzir a quantidade de formatos utilizados e, conseqüentemente, de sistemas a serem mantidos e gerenciados, de modo a facilitar as ações de preservação.
- **Migração** — A migração para novos sistemas é realizada no caso de obsolescência de elementos — *hardware*, *software* e formatos. Envolve, inclusive, a conversão de dados. Pode abranger uma grande quantidade desses elementos e, dessa forma, apresentar uma maior complexidade para ser planejada e executada. Apesar disso, mostra-se como uma alternativa interessante para o acompanhamento das mudanças decorrentes da evolução tecnológica. A migração, assim como a emulação e a conversão de dados, apresenta riscos quanto à integridade e à funcionalidade dos documentos institucionais digitais, por isso, deve ser realizada de modo criterioso e sistemático.

Embora os problemas de degradação dos suportes e obsolescência tecnológica possam ser contornados com conhecimento técnico e utilização de técnicas de preservação, sua execução pode ser muito dispendiosa. Por

isso, as preocupações com preservação devem existir desde a concepção do GestãoDoc e a escolha de sua base tecnológica. De uma forma geral, recomenda-se a utilização de suportes de alta qualidade e que tenham uma vida útil prevista adequada para os 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.

As estratégias e os procedimentos de preservação devem ser bem definidos, documentados e periodicamente revisados. É importante destacar que as ações de preservação são contínuas e devem ser implementadas desde a produção dos documentos até sua destinação final.

Qualquer que seja a estratégia de preservação adotada, há de se documentar os procedimentos e as estruturas de metadados.

Nesta seção, não se pretende apresentar procedimentos de preservação preestabelecidos ou argumentar em favor de uma técnica específica. Os requisitos foram organizados em aspectos físicos, lógicos e gerais.

É atribuição do Conselho da Justiça Federal a definição e o acompanhamento da implementação da política de preservação de documentos institucionais da Justiça Federal.

5.1 Aspectos físicos

REF.	REQUISITO	OBRIG.
RPR5.1.1	Os suportes de armazenamento devem ser acondicionados, manipulados e utilizados em condições ambientais compatíveis com sua vida útil prevista e/ou pretendida, dentro das especificações técnicas de seu fabricante e de entidades isentas e com base em estatísticas de utilização.	O
RPR5.1.2	Permitir ao administrador especificar a vida útil prevista/pretendida dos suportes.	O
RPR5.1.3	Permitir o controle da vida útil dos suportes para auxiliar no processo de rejuvenescimento.	O
RPR5.1.4	Informar automaticamente quais são os suportes que se encontram próximos do fim de sua vida útil.	O

5.2 Aspectos lógicos

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

REF.	REQUISITO	OBRIG.
RPR5.2.1	Manter cópias de segurança que devem ser guardadas em ambientes adequados segundo a política de segurança da informação da Justiça Federal. *O armazenamento das cópias de segurança deve ser realizado em local diferente de onde se encontra a informação original.* *As informações mantidas em mídia terciária devem ser duplicadas e armazenadas em locais diferentes.*	O
RPR5.2.2	Possuir funcionalidades para a verificação periódica dos dados armazenados, visando detecção, reparação e informação de possíveis erros. *Nesse caso, recomenda-se a utilização de um checksum robusto, que permita a constatação da integridade dos dados e seja seguro quanto a fraudes.*	O
RPR5.2.3	Permitir ao administrador a reparação dos dados armazenados que apresentarem erros.	O
RPR5.2.4	Manter um histórico dos resultados da verificação periódica dos dados armazenados.	O
RPR5.2.5	Efetivar ações de preservação sempre que verificada obsolescência tecnológica ou quando favoreça a padronização da plataforma tecnológica da Justiça Federal.	O
RPR5.2.6	Suportar a transferência em bloco de documentos e metadados para outros sistemas.	O

5.3 Aspectos gerais

REF.	REQUISITO	OBRIG.
RPR5.3.1	Registrar as operações de preservação realizadas em trilhas de auditoria.	O
RPR5.3.2	Utilizar suportes de armazenamento, recursos de *hardware* e de *software* que sejam estáveis no mercado e amplamente disponíveis e que contribuam para a padronização e uniformização da plataforma tecnológica da Justiça Federal.	D
RPR5.3.3	As modificações em um GestãoDoc e em sua base tecnológica devem ser verificadas em um 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

REF.	REQUISITO	OBRIG.
RPR5.3.4	Utilizar normas amplamente aceitas, descritas em especificações abertas e disponíveis publicamente, no que refere a estruturas para codificação, armazenamento e banco de dados.	D
RPR5.3.5	Evitar a utilização de estruturas proprietárias, para codificação, armazenamento ou banco de dados.	D
RPR5.3.6	Nos caso em que se utilize estruturas proprietárias, para codificação, armazenamento ou banco de dados, elas devem estar plenamente documentadas (incluindo o motivo para a utilização dessas estruturas proprietárias) e essa documentação, disponível para o administrador.	O
RPR5.3.7	Gerir metadados relativos à preservação dos documentos e seus respectivos componentes.	O

6 Segurança

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 característica de acesso aos dados, manutenção de trilhas de auditoria e de rotinas de cópias de segurança.

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

Problemas de segurança não são resolvidos apenas com tecnologia, já que envolvem características do comportamento humano. Por isso o GestãoDoc deve ser projetado, desenvolvido e mantido em consonância com a Política de Segurança de Informação da Justiça Federal.

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.

Os documentos também devem ser analisados em relação à confidencialidade: ostensivos, reservados, sigilosos etc. Regras, normas e legislação[7] estabelecem diferentes razões para o sigilo e também diferentes graus a serem atribuídos a cada documento e as autoridades competentes para fazê-lo. (Ver Capítulo 3, Captura — Atribuição de restrição de acesso)

Um sistema de gestão de processos e documentos 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

7 Lei nº 8.159, de 8 de janeiro de 1991; Lei nº 11.111, de 5 de maio de 2005; Decreto nº 4.553 de 27 de dezembro de 2002 e Decreto nº 5.301, de 9 de dezembro de 2004.

informações processuais, consulta e arquivamento, conforme estabelecido pela Resolução CJF nº 507, de 2006.

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

Uso e rastreamento

O uso dos documentos pelos usuários deve ser registrado pelo sistema nos seus respectivos metadados. A gestão desse uso 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 da Justiça Federal.

Trilha de auditoria

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, 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 da Justiça Federal 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 pela Justiça Federal, 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.

Cópias de segurança

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 da Justiça Federal.

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 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 restauração posterior das mesmas, 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 da Justiça Federal. O procedimento de cópias de segurança não pode ser confundido com uma estratégia de preservação de longo prazo.

Segurança da infra-estrutura

A natureza das medidas de segurança da infra-estrutura de instalações do acervo digital diz respeito a requisitos operacionais e não é muito diferente daquela do acervo não-digital. Essas medidas devem considerar os seguintes aspectos:

- As salas reservadas a computadores servidores, equipamentos de rede e ao armazenamento dos documentos digitais devem ter temperatura ambiente e umidade relativa do ar controladas, fornecimento estável de energia elétrica e aterramento. Deve haver controle contínuo para verificar se essas condições são atendidas.
- Equipamentos contra incêndio devem ser providos em toda área de instalação e estar de acordo com as normas de segurança estabelecidas.
- A substituição dos equipamentos contra incêndio deve seguir uma rotina de verificação e ocorrer antes do final da vida útil a eles prevista.

- Instalações adequadas de pára-raios, com procedimentos de manutenção periódica, seguindo a legislação e normas técnicas já estabelecidas.
- A área reservada à instalação do GestãoDoc deverá ser restrita e com controle de acesso físico, com o objetivo de controlar o acesso às informações.
- As salas de infra-estrutura de tecnologia da informação são de utilização exclusiva de pessoal autorizado e devem possuir controle eletrônico de acesso.

Os requisitos de identificação, autenticação de usuário e trilhas de auditoria devem integrar qualquer GestãoDoc. Políticas de segurança da informação específicas poderão definir o rigor, maior ou menor, do tratamento dos demais requisitos. Atenção especial deve ser dada, nesse aspecto, às normais internacionais ISO 17799 e 27001.

No que diz respeito ao controle de acesso, esta 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.

Quanto à utilização da tecnologia de criptografia, tanto para sigilo quanto para autenticação, o rigor dos requisitos está sujeito às normas do ICP-Brasil e à política de segurança da informação da Justiça Federal. 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. Nesses casos, o não-repúdio é garantido pela MP 2.200-2, de 2001, utilizando certificados digitais emitidos no âmbito da ICP-Brasil.

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.

6.1 Cópias de segurança

As cópias de segurança têm por objetivo prevenir a perda de informações, e garantir a disponibilidade do sistema. Os procedimentos de *backup* devem ser feitos regularmente e, pelo menos uma cópia deve ser armazenada remotamente (*off-site*).

Podem-se distinguir vários tipos de informações necessários ao funcionamento de um GestãoDoc. Essas informações compreendem os documentos digitais, metadados e informações de controle associadas às camadas de *software* relacionadas ao GestãoDoc (sistema operacional, gerenciador de bancos de dados, *software* aplicativo). Todas essas informações devem ser incluídas nos procedimentos de cópias de segurança.

REF.	REQUISITO	OBRIG.
RSE6.1.1	Cumprir a política de segurança da informação da Justiça Federal.	O
RSE6.1.2	Possibilitar o acompanhamento das ações efetivadas de *backup* e *restore.*	D

6.2 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.

Identificação e autenticação de usuários

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.

REF.	REQUISITO	OBRIG.
RSE6.2.1	Implementar o controle de acesso, mantendo pelo menos os seguintes atributos dos usuários, de acordo com a política de segurança da informação da Justiça Federal: ▪ Identificador do usuário. ▪ Autorizações de acesso. ▪ Credenciais de autenticação. *Senha, chave criptográfica e biometria são exemplos de credenciais de autenticação.*	O
RSE6.2.2	Utilizar, para efeito de autenticação, um sistema de gerenciamento de identidade externo .	D
RSE6.2.3	Exigir que o usuário esteja devidamente identificado e autenticado antes que este inicie qualquer operação no sistema.	O

REF.	REQUISITO	OBRIG.
RSE6.2.4	Garantir que os valores dos atributos de segurança e controle de acesso, associados ao usuário estejam dentro de conjuntos de valores válidos.	O
RSE6.2.5	Garantir que as tecnologias de credenciais de autenticação só possam ser modificadas pelo administrador, em conformidade com a política de segurança da informação da Justiça Federal.	O
RSE6.2.6	Permitir avaliação periódica dos direitos de acesso dos usuários do sistema.	O

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.

REF.	REQUISITO	OBRIG.
RSE6.2.7	Permitir o acesso a funções administrativas do sistema somente a usuários autorizados e sob controle rigoroso do gestor.	O
RSE6.2.8	Fornecer uma das seguintes respostas (estabelecidas durante a configuração) se o usuário solicitar o acesso ou pesquisa em um documento institucional, volume ou processo/dossiê específicos aos quais não tenha o direito de acesso: ▪ Mostrar determinados dados cadastrais do documento ou processo. ▪ Demonstrar a existência do processo/dossiê ou documento mas não seu conteúdo (exemplo: informações pessoais). ▪ Não mostrar qualquer informação constante do documento, nem indicar sua existência (exemplo: quebra de sigilo telefônico).	O
RSE6.2.9	Garantir que somente o gestor seja capaz de criar, alterar, remover ou revogar as permissões associadas a perfis de usuários, grupos de usuários ou usuários individuais.	O
RSE6.2.10	Implementar imediatamente alterações ou revogações dos atributos de segurança de usuários e de documentos digitais.	D
RSE6.2.11	Oferecer ferramentas de aumento de produtividade ao gestor, tais como: 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

REF.	REQUISITO	OBRIG.
RSE6.2.12	Quando um GestãoDoc controlar o acesso por grupos de usuários, perfis de usuários e usuários individuais obedecer a uma hierarquia de permissões preestabelecida na política de segurança da informação da Justiça Federal.	O

Controle de acesso por papéis de usuários

Papéis são funções ou cargos com responsabilidades e autoridades bem definidas.

Operações são tarefas executadas sobre os documentos e os processos/dossiês.

Atribuições de usuários são as associações entre usuários e papéis. Um usuário pode estar associado a um ou mais papéis e vice-versa.

Permissões são garantias aprovadas para realização de operações sobre documentos institucionais.

REF.	REQUISITO	OBRIG.
RSE6.2.13	Utilizar os seguintes atributos do usuário ao implementar a política de controle de acesso por perfis de usuários sobre documentos: ▪ Identificação do usuário. ▪ Perfis associados ao usuário.	O
RSE6.2.14	Utilizar os seguintes atributos dos documentos ao implementar a política de controle de acesso por perfis: ▪ Identificação do documento. ▪ Operações permitidas para os vários perfis de usuários, sobre as unidades a que pertence o documento.	O
RSE6.2.15	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
RSE6.2.16	Impedir que um usuário assuma perfis com direitos conflitantes. Em caso de conflito, prevalece o perfil mais restritivo.	O
RSE6.2.17	Permitir a criação de hierarquias de perfis e o conceito de herança de permissões entre eles.	O

6.3 Classificação da informação quanto ao grau de sigilo e restrição de acesso à informação sensível

Os requisitos descritos nesta seção referem-se ao acesso aos processos/dossiês e documentos com base na classificação do grau de sigilo bem como restrição de acesso à informação sensível.

De acordo com a Resolução CJF nº 507, de 2006, nos processos judiciais a informação sensível é tratada de duas formas:

- Considera-se em segredo de justiça a investigação, o processo, os dados e as informações determinadas pela autoridade judicial competente para o feito, em 1º e 2º graus, nos termos da legislação aplicável à matéria.
- Considera-se sigilosa, quando determinada pela autoridade judicial competente, toda a informação, documento, elemento ou feito que, por sua natureza ou quando a preservação de direitos individuais e o interesse público o exigirem deva ser de conhecimento restrito e, portanto, requeira medidas especiais para segurança de seu conteúdo. O caráter sigiloso poderá ser atribuído ao processo ou às partes. Quando atribuído ao processo, a consulta ao sistema será restrita a pessoas autorizadas, a critério da autoridade judicial.

REF.	REQUISITO	OBRIG.
RSE6.3.1	Aceitar a definição de graus de sigilo e de perfis de usuários de acordo com as necessidades da Justiça Federal.	O
RSE6.3.2	Implementar a classificação de grau de sigilo baseando-se nos seguintes atributos de segurança para documentos e para usuários: ▪ Grau de sigilo do documento. ▪ Credencial de segurança do usuário.	O
RSE6.3.3	Recusar o acesso de usuários a documentos que possuam um grau de sigilo superior à sua credencial de segurança.	O
RSE6.3.4	Garantir que os documentos sem atribuição de grau de sigilo, importados a partir de fontes externas ao GestãoDoc, estejam sujeitos às políticas de controle de acesso e de sigilo.	O
RSE6.3.5	Manter a marcação de sigilo original durante a importação de documentos marcados com graus de sigilo, a partir de fontes externas ao GestãoDoc.	O
RSE6.3.6	Garantir a não-ambigüidade na associação entre as marcações de grau de sigilo e os outros atributos de segurança (permissões) do documento importado.	D

REF.	REQUISITO	OBRIG.
RSE6.3.7	Garantir que nos casos em que grau de sigilo e atributos de segurança incidam sobre um mesmo documento, o critério de acesso seja o de maior restrição.	O
RSE6.3.8	Permitir que o usuário autorizado seja capaz de alterar o grau de sigilo de todos os documentos institucionais de um processo/dossiê ou documento, em caso de erro ou reavaliação.	O
RSE6.3.9	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
RSE6.3.10	Permitir somente ao gestor a possibilidade de alterar a configuração dos valores predefinidos (*default*) para os atributos de segurança e marcações de graus de sigilo, quando necessário e apropriado.	O
RSE6.3.11	Permitir somente aos usuários autorizados realizar as ações: criar, alterar, conceder ou revogar credenciais de segurança aos usuários.	O
RSE6.3.12	Prover mecanismos de proteção que permitam cópias de segurança de documentos confidenciais, preservando a inviolabilidade da informação. *Tais cópias poderão migrar para sites remotos, fora do controle do GestãoDoc. Por isso, os mecanismos citados deverão lançar mão de técnicas de criptografia.*	O

6.4 Trilha de auditoria

A trilha de auditoria consiste num 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 digitais e informa sobre a sua autenticidade.

REF.	REQUISITO	OBRIG.
RSE6.4.1	Assegurar 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

REF.	REQUISITO	OBRIG.
RSE6.4.2	Registrar na trilha de auditoria as informações: ▪ Data e hora da captura de todos os documentos. ▪ Responsável pela captura. ▪ Alteração do grau de sigilo de um documento ou de um processo/dossiê, registrando as modificações efetuadas. ▪ Qualquer alteração nos instrumentos de classificação, temporalidade e destinação da política de gestão documental da Justiça Federal. ▪ Qualquer ação de reavaliação de documentos. ▪ Qualquer alteração nos metadados associados a processos/dossiês ou documentos. ▪ Data e hora de produção, aditamento e exclusão de metadados. ▪ Usuário, data e hora de acesso ou tentativa de acesso a documentos e ao GestãoDoc. ▪ Tentativas de acesso negado a qualquer documento. ▪ Ações de exclusão de qualquer documento e seus metadados. ▪ 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.). ▪ Todos os eventos de administração de manutenção das trilhas de auditoria (alarmes, cópias, configuração de parâmetros etc.).	O
RSE6.4.3	Registrar, em cada evento auditado, informações sobre a identidade do usuário.	O
RSE6.4.4	Permitir a leitura das trilhas de auditoria apenas ao administrador e ao auditor.	O
RSE6.4.5	Possuir mecanismos para a realização de buscas nos eventos das trilhas de auditoria.	O
RSE6.4.6	Impedir qualquer modificação de conteúdo da trilha de auditoria.	O
RSE6.4.7	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

REF.	REQUISITO	OBRIG.
RSE6.4.8	Gerar um alarme, para os administradores, se o tamanho da trilha de auditoria exceder um limite preestabelecido.	O
RSE6.4.9	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 mal sucedida), conforme especificado pela política de segurança da informação da Justiça Federal. ▪ Ocorrência de vários *logins* simultâneos do mesmo usuário em locais (computadores) diferentes. ▪ *Login* do usuário fora do horário autorizado, após *logoff* no período normal.	D
RSE6.4.10	Fornecer relatórios, em ordem cronológica, sobre as ações que afetam processos/dossiês e documentos.	O
RSE6.4.11	Garantir que somente administradores sejam capazes de configurar o conjunto de eventos auditáveis e seus atributos.	O
RSE6.4.12	Documentar em trilha de auditoria as configurações do GestãoDoc que redefinam o conjunto de eventos auditáveis.	O

6.5 Assinaturas digitais

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 e o certificado digital correspondente, utilizados na assinatura.

Descrição do processo de assinatura digital

Para assinar digitalmente um arquivo, aplica-se inicialmente uma função matemática ao conteúdo do arquivo, obtendo-se um resumo criptográfico (*hash*) desse arquivo. A função *hash* garante a integridade de um documento na medida em que qualquer alteração no conteúdo desse documento altera o resultado da função *hash* aplicada sobre o mesmo.

O *hash* é então criptografado com a chave privada do signatário.

A criptografia de chave pública ou assimétrica permite verificar a autoria de um documento assinado digitalmente, uma vez que só é possível decifrar as informações, cifradas com determinada chave privada, utilizando-se a chave pública correspondente. Os pares de chaves são únicos. A chave privada é de posse e responsabilidade exclusiva de seu proprietário.

Os certificados digitais são documentos digitais que certificam a posse de um determinado par de chaves por um indivíduo ou instituição.

O signatário de um documento, ao calcular o *hash* gera uma espécie de "impressão digital" do conteúdo do documento.

Ao criptografar o *hash* com sua chave privada, junta-se a sua própria "impressão digital" ao *"pacote"* composto nesse momento de original mais assinatura digital (*hash* criptografado).

Finalmente, o certificado digital do signatário é agregado ao pacote. Agregar o certificado ao pacote possibilita a divulgação da chave pública do signatário e a imediata verificação da validade do certificado e da integridade do documento. Assim, um arquivo assinado digitalmente geralmente compõe-se de:

- Original.
- Assinatura digital (*hash* criptografado — assinado).
- Certificado do signatário.

O receptor do "pacote", inicialmente desempacota o certificado e utiliza as funções de PKI (*Public Key Infrastructure*) para fazer a verificação da validade do certificado e da cadeia de certificação. Validado o certificado, extrai-se a chave pública deste, aplicando-a à assinatura.

Só será possível decifrar a assinatura se a chave pública for correspondente à chave privada utilizada para a assinatura. Uma vez que a operação criptográfica se concretize estará estabelecida a autoria da assinatura e obtém-se o *hash* do documento.

Em seguida, aplica-se a função *hash* ao original e compara-se com o *hash* assinado. Dessa forma, é estabelecida a integridade do documento.

Toda operação descrita acima é feita de forma automática e transparente para o usuário, pelos assinadores digitais (que também fazem a verificação). Esses aplicativos emitem avisos caso ocorra falha na validação do documento ou certificado.

Não-repúdio e validade legal

O não-repúdio é determinado pela relação do titular de um certificado e a autoridade certificadora, responsável por garantir:

- A identidade do titular do certificado.
- Que o titular do certificado gerou seu próprio par de chaves.
- Que o titular se compromete pela segurança e inviolabilidade da chave privada.

No Brasil, com o advento da ICP-Brasil e da MP nº 2.200-2, de 2001, foi estabelecida a validade legal de documentos assinados digitalmente, utilizando-se certificados digitais emitidos dentro da cadeia de certificação da ICP-Brasil.

A ICP-Brasil fiscaliza e audita o processo de emissão digital das autoridades certificadoras integrantes a fim de garantir a total confiabilidade do processo de certificação. Assim, dá respaldo à determinação legal de integridade, autenticidade e não-repúdio dos arquivos assinados digitalmente.

Autoridade Certificadora da Justiça (AC-JUS) e sua cadeia de certificação

A AC-JUS foi instituída com intuito de criar regras específicas tanto para emissão de certificados como para o leiaute interno dos certificados (informações que contém). A AC-JUS, a exemplo da AC-Raiz e AC-SRF, não emite certificados para usuários. Credencia ACs, chamadas "subseqüentes", para que, seguindo as regras específicas da AC-JUS realize a emissão dos certificados aos usuários.

Os certificados emitidos na cadeia de certificação da AC-JUS recebem a marca Cert-JUS. Os certificados Cert-JUS são de uso exclusivo de servidores públicos, e ao utilizá-los o titular se identifica como servidor de determinada instituição pública. Na cadeia de certificação foram definidos os perfis de certificado:

- Cert-JUS Institucional — Utilização exclusiva de servidores do Poder Judiciário.
- Cert-JUS Poder Público — Utilização dos servidores de órgãos externos ao Poder Judiciário.
- Cert-JUS Equipamento Servidor — Destinado a aplicações e equipamentos servidores de órgãos públicos.
- Cert-JUS Código Seguro — Destinado à assinatura de código fonte de programas.

REF.	REQUISITO	OBRIG.
RSE6.5.1	Garantir a origem e a integridade dos documentos com assinatura digital.	O
RSE6.5.2	Utilizar o padrão ICP-Brasil quando houver necessidade de emprego de assinatura digital.	O
RSE6.5.3	Verificar a validade da assinatura digital no momento da captura do documento, e caso não esteja válida, recusar a captura.	O
RSE6.5.4	No processo de verificação da assinatura digital, registrar nos metadados do documento: ▪ Validade da assinatura verificada. ▪ Autoridade certificadora do certificado digital. ▪ Data e hora em que a verificação ocorreu.	O

REF.	REQUISITO	OBRIG.
RSE6.5.5	Armazenar juntamente com o documento as informações de certificação: ▪ Assinatura digital. ▪ Certificado digital (cadeia de certificação) usado na verificação da assinatura.	O
RSE6.5.6	Receber atualizações tecnológicas quanto à plataforma criptográfica de assinatura digital.	O
RSE6.5.7	Acessar relógios e carimbador de tempo oficiais para o seu próprio uso.	O

6.6 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 subsiste, mas de forma ininteligível. O processo inverso é decriptografar ou decifrar: recuperar a informação original, passível de interpretação e modificação.

A criptografia objetiva controlar o acesso à informação e não aos arquivos, de modo que o furto do arquivo não implica furto da informação.

Criptografia simétrica e assimétrica

A criptografia baseia-se em chaves ou senhas, informações externas ao arquivo. Quando uma mesma chave serve para criptografar ("fechar") e para decriptografar ("abrir") o arquivo, tem-se **criptografia simétrica**.

Criptografia assimétrica, por sua vez, conta com um par de chaves: uma para fechar e outra para abrir. Curioso (e importante) é que são chaves alternáveis: um arquivo fechado com uma pode ser aberto com a outra chave do par e vice-versa. Porém, não se pode fechar e depois abrir com a mesma chave.

Aplicabilidade

Criptografia simétrica é especialmente indicada quando um mesmo agente (usuário ou sistema) cripta e decripta a informação. É muito usada em bancos de dados. A ênfase é segurança em armazenamento e recuperação da informação.

Criptografia assimétrica prevê um agente emissor e um agente receptor, geralmente em sistemas distintos. A ênfase é a transmissão segura da informação. É base para as assinaturas e certificações digitais citadas no item anterior.

Na criptografia assimétrica, as chaves constituintes do par são designadas por chave privada (resguardada pelo usuário) e chave pública (de conhecimento público). O mecanismo de criptografia de chaves públicas, complementado pela infra-estrutura administrativa da ICP-Brasil, equaciona a questão de transmitir dados, de modo seguro, por meio inseguro (internet).

Utilização de criptografia num GestãoDoc

Num GestãoDoc, o armazenamento e a recuperação de informações sigilosas (aí incluídos *backups* e *restores*) utilizará a criptografia simétrica. Já na comunicação, identificação de usuários e em sessões *Web*, será utilizada a criptografia assimétrica, em consonância com a ICP-Brasil.

A desvinculação entre as aplicações de criptografia torna o modelo mais ágil: por um lado, a dinâmica envolvida na criptografia externa fica sob responsabilidade da ICP-Brasil, sem necessidade de duplicação e atualização de informação dentro do GestãoDoc. Em particular, o GestãoDoc não terá a preocupação com aspectos como temporalidade de senhas públicas, listas de certificados ou a obsolescência tecnológica de *hardwares* e *softwares.*

Por outro lado, a utilização de criptografia simétrica no gerenciamento interno da informação, além da simplicidade conceitual, possibilita mais autonomia nos processos de controle do GestãoDoc. Por exemplo: cópias de segurança e *backups* passam a contar com mecanismos de proteção criptográfica com funcionamento independente do estado tecnológico da criptografia do mundo externo.

Uma conexão importante entre os "dois mundos" acontece no momento da captura de documentos. Aí compreendida a fase de autenticação, que valer-se-á da força conferida pela certificação digital. Uma vez, porém, assimilado ao GestãoDoc, a autenticidade passa a ser preservada com auxílio da garantia de integridade e sigilo apoiados nos controles internos do sistema. Inversamente, sempre que informações devem sair do GestãoDoc, endereçadas a agentes remotos, entra novamente em cena a criptografia assimétrica.

O quadro a seguir resume esquematicamente o exposto:

TECNOLOGIA DE CRIPTOGRAFIA	CLASSE DE ACESSO	FUNCIONALIDADE NO GESTÃODOC	PADRONIZAÇÃO
Simétrica	Interno	Armazenamento e recuperação	Interna ao GestãoDoc
Assimétrica	Externo	Sessões Web	ICP-Brasil

RSE6.6.1	Utilizar a criptografia no armazenamento e na transmissão de documentos digitais sigilosos.	O
RSE6.6.2	Limitar o acesso aos documentos cifrados àqueles usuários portadores da chave de decifração.	O
RSE6.6.3	Registrar os seguintes metadados sobre um documento cifrado: ▪ Indicação se está cifrado ou não. ▪ Algoritmos usados na cifração.	O
RSE6.6.4	Permitir a captura de documentos cifrados.	D
RSE6.6.5	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. ▪ Motivo da alteração.	O
RSE6.6.6	Nos casos de aplicação do item anterior, prover mecanismos para convivência temporária de dois sistemas de criptografia distintos. *O objetivo é viabilizar a transição para o novo sistema sem indisponibilizar a operação do GestãoDoc.*	O
RSE6.6.7	Impedir a abertura (*disclosure*) de senhas, bem como a remoção de criptografia de documentos, 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 de custódia de senhas, externos ao GestãoDoc.*	O
RSE6.6.8	Possuir uma arquitetura capaz de receber atualizações tecnológicas quanto à plataforma criptográfica.	O

6.7 Marcas d'água digitais

Marcas d'água servem para marcar uma imagem digital com informação sobre 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 ou de uma chave protegida. Tecnologias semelhantes podem ser aplicadas a sons e a imagens em movimento digitalizadas.

O GestãoDoc deve manter, recuperar e assimilar novas tecnologias de marcas d'água.

REF.	REQUISITO	OBRIG.
RSE6.7.1	Recuperar informação contida em marcas d'água digitais, mediante anuência do usuário autorizado.	O
RSE6.7.2	Armazenar documentos institucionais digitais que contenham marcas d'água digitais, assim como informação de apoio relacionada à marca d'água.	O
RSE6.7.3	Possuir uma arquitetura capaz de receber atualizações tecnológicas quanto à plataforma de geração e de detecção de marca d'água digital.	O

6.8 Acompanhamento de transferência

Durante seu ciclo de vida, os documentos institucionais e seus respectivos metadados podem ser transferidos de uma mídia de suporte, ou de um local, para outro, à medida que sua utilização decresce e/ou se modifica. Essa transferência pode ser interna, (por exemplo, um deslocamento de armazenamento *on-line* para *off-line*), como externa, podendo trazer deslocamento para outra instituição (por exemplo, em casos de alteração de competência).

É necessário um recurso de acompanhamento, a fim de se registrar a mudança de local, tanto para facilitar o acesso como para cumprir requisitos regulamentares.

REF.	REQUISITO	OBRIG.
RSE6.8.1	Manter, para cada documento ou cada processo/dossiê, o histórico das movimentações e transferências de mídia sofridas por aquele documento ou processo/dossiê.	O
RSE6.8.2	Monitorar e registrar informações acerca do local atual e da transferência de processos/dossiês digitais e não-digitais.	O

REF.	REQUISITO	OBRIG.
RSE6.8.3	Registrar metadados que incluam: ▪ Número identificador dos documentos atribuído pelo sistema. ▪ Localização atual e também as localizações anteriores, definidas pelo usuário. ▪ Data e hora de envio/transferência. ▪ Data e hora da recepção no novo local. ▪ Destinatário. ▪ Usuário responsável pela transferência. ▪ Método de transferência.	O

6.9 Autoproteção

Num ambiente digital, a autoproteção consiste na capacidade do sistema de computação de verificar a integridade de programas e de dados de controle como uma medida de proteção inicial. As técnicas de autoproteção aumentam a confiança no funcionamento correto dos programas de computador.

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.

REF.	REQUISITO	OBRIG.
RSE6.9.1	Negar a efetivação da captura sem a verificação de vírus ou código malicioso.	O
RSE6.9.2	Possuir dispositivos e procedimentos que reduzam as possibilidades de erros, falhas e descontinuidades no seu funcionamento que causem danos ou perdas aos documentos institucionais digitais.	D
RSE6.9.3	Entrar em modo de manutenção, no qual a possibilidade de restaurar o sistema para um estado seguro é oferecida, após falha ou descontinuidade do sistema, quando a recuperação automática não for possível. *Na restauração ao estado seguro, um GestãoDoc deve recuperar informações no maior nível tecnicamente viável.*	O

REF.	REQUISITO	OBRIG.
RSE6.9.4	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
RSE6.9.5	Preservar um estado seguro de funcionamento, interrompendo completamente a interação com usuários, quando quaisquer dos seguintes erros ocorrerem: ▪ Falha de comunicação entre cliente e servidor. ▪ Perda de integridade das informações de controle de acesso. ▪ Impossibilidade de registro em trilha de auditoria.	O
RSE6.9.6	Permitir ao gestor a definição do limite de tentativas de acesso. Quando esse valor for atingido, o acesso deve ser bloqueado.	O

6.10 Alteração, ocultação e exclusão de documentos institucionais

Os documentos institucionais completos não podem, em regra, ser alterados e excluídos, exceto no término do seu ciclo de vida num GestãoDoc. No entanto, os usuários autorizados podem precisar retificar operações, para corrigir erros de usuário (por exemplo, documentos juntados indevidamente a um processo/dossiê). Para cumprir requisitos jurídicos, usuários autorizados podem precisar ocultar informação sensível sem afetar o documento correspondente.

REF.	REQUISITO	OBRIG.
RSE6.10.1	Permitir a anulação da operação em caso de erro do usuário, de acordo com as normas vigentes. Essa anulação tem que ser registrada nos metadados. *Exemplos:* ▪ *Após a distribuição do processo judicial, o ato não poderá ser anulado. A correção se dará pelo lançamento de evento baixa definitiva por erro de distribuição.* ▪ *No caso de documento juntado a processo errado, a ação adequada é o desentranhamento.*	O

REF.	REQUISITO	OBRIG.
RSE6.10.2	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 no programa de gestão documental da Justiça Federal.*	O
RSE6.10.3	Permitir aos usuários autorizados a retificação dos metadados, com registro inclusive, na trilha de auditoria.	O
RSE6.10.4	Permitir a ocultação de dados ou partes do documento para visualização ou consulta em casos de sigilo/segredo de justiça. As formas de ocultação devem compreender: ▪ Omissão de páginas de um documento. ▪ Adição de retângulos opacos para ocultar nomes ou palavras sensíveis. ▪ Outros recursos necessários para formatos de vídeo ou de áudio.	D
RSE6.10.5	Quando uma cópia truncada é produzida, registrar essa ação nos metadados do documento, incluindo, pelo menos, a data, a hora, o motivo, e a pessoa que a produziu.	O

7 Tramitação e fluxo de trabalho

Os requisitos desta seção tratam apenas dos casos em que um GestãoDoc inclui recursos de automação de fluxo de trabalho (*workflow*). Abrangem funções para controle do fluxo de trabalho e atribuição de metadados para registro da tramitação dos documentos, incluindo o *status* do documento (minuta ou via original).

Os recursos de um GestãoDoc para controle do fluxo de trabalho podem compreender:

- Tramitação de um documento antes de seu registro/captura.
- Tramitação posterior a seu registro/captura.

As tecnologias de fluxo de trabalho gerenciam o registro de eventos e as movimentações de documentos digitais ou não-digitais sob o controle automatizado de um programa. São geralmente usadas para:

- Gestão de processos ou de tarefas, tais como registro e destinação de documentos e processos/dossiês.
- Verificação e aprovação de documentos ou processos/dossiês antes do registro.
- Encaminhamento de documentos ou processos/dossiês de forma controlada, de um usuário para outro, com a identificação das ações a serem realizadas, tais como: verificar documento, marcar audiência, vista ao Ministério Público.
- Comunicações aos usuários internos e externos sobre a disponibilidade de um documento, a saber: as processuais (citação, intimação) e as administrativas (contatos com fornecedores, autorização para pagamentos).
- Distribuição de documentos ou processos/dossiês.
- Publicação de documentos ou processos/dossiês.

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. No caso de o participante ser um indivíduo, a tarefa é direcionada a determinado usuário com identificação específica. No caso de o participante ser um grupo de trabalho, a tarefa é direcionada para o grupo (formado por vários usuários, cada um com sua identificação no sistema). A tarefa tem de ser distribuída entre os usuários do grupo, e o documento, após ser cumprido por um membro do grupo, 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.

7.1 Controle do fluxo de trabalho

REF.	REQUISITO	OBRIG.
RTF7.1.1	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
RTF7.1.2	Possuir capacidade, sem limitações, para estabelecer o número necessário de trâmites nos fluxos de trabalho.	O
RTF7.1.3	Disponibilizar uma função para avisar a um participante do fluxo que um documento lhe foi enviado, especificando a ação necessária.	O
RTF7.1.4	Permitir a utilização de qualquer sistema de comunicação eletrônica para que um usuário possa informar outros usuários sobre documentos que requeiram sua atenção.	D
RTF7.1.5	Permitir que fluxos de trabalho pré-programados sejam definidos, alterados e mantidos exclusivamente pelo gestor.	O
RTF7.1.6	Possibilitar que tarefas e ações sejam redistribuídas, quando necessário, em um fluxo de trabalho, a um usuário ou grupo diferente do que havia sido previsto. *Um usuário pode precisar enviar um documento a outro usuário, em função do conteúdo daquele ou em razão de eventual afastamento do usuário responsável.*	O
RTF7.1.7	Registrar na trilha de auditoria todas as alterações ocorridas nesse fluxo.	O
RTF7.1.8	Registrar a tramitação de todos os documentos a fim de que os usuários possam conhecer a situação de cada um deles no processo.	O
RTF7.1.9	Efetuar a gestão dos documentos em filas de espera que possam ser examinadas e controladas pelo gestor.	O
RTF7.1.10	Permitir que os usuários visualizem a fila de espera do trabalho a eles destinado e que selecionem os itens a trabalhar.	O

REF.	REQUISITO	OBRIG.
RTF7.1.11	Fornecer fluxos condicionais de acordo com os dados de entrada do usuário ou os dados do sistema. *Os fluxos que remetem o documento a um dos participantes dependem de uma condição determinada por um deles. Por exemplo, um fluxo pode levar um documento a um participante ou outro, conforme os dados de entrada do participante anterior; ou a definição do fluxo pode depender de um valor calculado pelo sistema.*	D
RTF7.1.12	Fornecer um histórico de movimentação dos documentos. *O histórico de movimentação corresponde a um conjunto de metadados de datas de entrada e saída; nomes de responsáveis; titulo do documento, providências, etc.*	O
RTF7.1.13	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
RTF7.1.14	Incluir processamento condicional, permitindo que um fluxo de trabalho seja suspenso para aguardar a chegada de um documento e prossiga, como definido pelo próprio fluxo, quando o documento é recebido.	O
RTF7.1.15	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
RTF7.1.16	Reconhecer indivíduos e grupos de trabalho como participantes.	O
RTF7.1.17	Prever a forma de distribuição dos documentos entre os membros do grupo, sempre que o participante for um grupo de trabalho.	O
RTF7.1.18	Permitir que a captura de documentos desencadeie automaticamente fluxos de trabalho.	O
RTF7.1.19	Fornecer meios de elaboração de relatórios completos para permitir que gestores monitorem a tramitação dos documentos e o desempenho dos participantes.	O
RTF7.1.20	Registrar a tramitação de um documento em seus metadados. Os metadados referentes à tramitação devem registrar, dentre outros, data e hora de envio e de recebimento e identificação dos usuários.	O

REF.	REQUISITO	OBRIG.
RTF7.1.21	Manter versões dos fluxos alterados e estabelecer vínculos entre os documentos já processados ou em processamento nos fluxos alterados.	O
RTF7.1.22	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

7.2 Controle de versões e do *status* do documento

Um GestãoDoc tem de ser capaz de estabelecer — pelo seu recurso de fluxo de trabalho — o *status* do documento: minuta ou via original. No caso dos documentos digitais, esse *status* é estabelecido de acordo com o fluxo do documento no GestãoDoc. Assim, por exemplo:

- O documento é uma minuta enquanto estiver no espaço individual ou do grupo.
- Um documento transmitido do espaço individual ou do grupo, para o espaço geral, onde não poderá mais ser alterado, e daí para fora da instituição, será sempre recebido como um original.
- Um documento enviado do espaço individual ao grupo, para fins de comentários, é uma minuta, que deverá ter seu número de versões devidamente controlado.
- Quando um usuário autorizado recupera um documento do espaço geral e o armazena em seu espaço, ele cria uma nova minuta.

REF.	REQUISITO	OBRIG.
RTF7.2.1	Registrar o *status* de transmissão do documento: minuta ou via original.	O
RTF7.2.2	Controlar as diversas versões de um documento em produção.	O
RTF7.2.3	Manter o identificador único do documento e registrar, em metadados específicos, o controle de versões.	O

8 Avaliação e destinação

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.

A avaliação é o processo de análise dos documentos e visa estabelecer os prazos de guarda e a destinação, de acordo com os valores primário e secundário que lhes são atribuídos. Os prazos de guarda e as ações de destinação devem estar formalizados nos instrumentos de classificação, temporalidade e destinação da política de gestão documental da Justiça Federal.

Os prazos de guarda referem-se ao tempo necessário para o arquivamento dos documentos nas fases corrente e intermediária, visando atender exclusivamente às necessidades da administração que os gerou, com base em estimativas de utilização. Nesse sentido, nenhum documento deve ser conservado por tempo maior que o necessário.

A aplicação dos critérios de avaliação é feita com suporte na teoria das três idades e efetiva-se, primeiramente, nos arquivos correntes, a fim de se distinguirem os documentos de valor eventual (de eliminação sumária) daqueles de valor probatório e/ou informativo.

Deve-se evitar a transferência para os arquivos intermediários de documentos que não tenham sido anteriormente avaliados, pois as atividades de avaliação e seleção nesses arquivos são extremamente onerosas do ponto de vista técnico e gerencial.

A destinação dos documentos é efetivada após a atividade de seleção, que consiste na separação dos documentos de valor permanente daqueles passíveis de eliminação, mediante critérios e técnicas estabelecidos nos instrumentos de classificação, temporalidade e destinação.

A complexidade e a abrangência de conhecimentos exigidos pelo processo de avaliação, que implica o estabelecimento de critérios de valor, requerem a constituição de comissões ou grupos multidisciplinares permanentes de avaliação documental, conforme estabelecem as Resoluções CJF nº. 217, de 1999, e 359, de 2004.

Um GestãoDoc deve identificar, sempre que possível, a temporalidade e a destinação prevista para o documento no momento da captura e do registro, de acordo com os prazos e as ações definidas nos instrumentos de classificação, temporalidade e destinação da Justiça Federal. Essa informação deve ser registrada em um metadado associado ao documento.

O sistema de gestão de documentos deve também ter capacidade de identificar aqueles que já cumpriram sua temporalidade para que se implemente a destinação prevista. No caso de um GestãoDoc, esse sistema

deverá ser capaz de listar os documentos que tenham cumprido o prazo definido nos instrumentos de classificação, temporalidade e destinação.

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 um determinado período, no arquivo corrente do órgão que os gerou.
- Eliminação física.
- Transferência.
- Recolhimento à unidade de arquivo.

Um documento incluído automaticamente em um relatório de eliminação gerado por um GestãoDoc, em razão dos critérios estabelecidos, precisa ser individualmente avaliado pela Comissão de Avaliação da instituição antes de ser efetivamente eliminado. Em razão das suas peculiaridades, um documento pode ser considerado de valor permanente.

Um GestãoDoc deve ser capaz de permitir a preservação de conjuntos amostrais representativos dos documentos eliminados segundo os critérios previamente estabelecidos.

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, do edital de ciência de eliminação e do termo de eliminação, de acordo com a legislação vigente, e deve obedecer aos seguintes princípios:

- A eliminação deverá sempre ser autorizada pelas comissões de avaliação e pelos grupos de trabalho com base no programa de gestão documental da Justiça Federal.
- A eliminação deverá ser realizada de forma a impossibilitar a recuperação posterior de qualquer informação confidencial contida nos documentos eliminados, como, por exemplo, dados de identificação pessoal ou assinatura.
- Todas as cópias dos documentos eliminados, inclusive cópias de segurança e cópias de preservação, independentemente do suporte, deverão ser destruídas.

Transferência

Transferência é a passagem de documentos do arquivo corrente para o arquivo intermediário, sob a guarda da unidade de arquivo do órgão, onde aguardarão o cumprimento dos prazos de guarda e a destinação final.

Recolhimento

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

Em alguns casos — especificados no Programa de Gestão de Documentos da Justiça Federal — como sentenças, acórdãos, atos normativos etc., o recolhimento do documento ocorre no ato da sua publicidade.

Os procedimentos de transferência e 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 no que diz respeito a:

- Compatibilidade de suporte e formato, de acordo com as normas previstas pelo programa de gestão documental da Justiça Federal.
- 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 unidade de arquivo do órgão.
- Informações sobre as migrações realizadas no órgão produtor.

Os requisitos desta seção referem-se aos procedimentos de avaliação e destinação dos documentos gerenciados pelo GestãoDoc.

8.1 Configuração dos instrumentos de classificação, temporalidade e destinação de documentos

Estes requisitos referem-se à criação e manutenção dos instrumentos de classificação, temporalidade e destinação da política de gestão documental da Justiça Federal em um GestãoDoc.

REF.	REQUISITO	OBRIG.
RAD8.1.1	Prover funcionalidades para definição e manutenção de todos os instrumentos de classificação, temporalidade e destinação da política de gestão documental da Justiça Federal.	O
RAD8.1.2	Associar automaticamente a um documento, processo/dossiê administrativo a classificação, a temporalidade e a destinação previstas no PCTT.	O

REF.	REQUISITO	OBRIG.
RAD8.1.3	Associar automaticamente a um processo judicial a classificação de guarda permanente, de acordo com as normas do CJF.	O
RAD8.1.4	Associar automaticamente a um processo judicial passível de eliminação, os critérios definidos pelo fluxo para seleção das ações judiciais da Justiça Federal, definido pelas normas do CJF.	D
RAD8.1.5	Prever a transferência da gestão de documentos e processos/dossiês para a unidade de arquivo.	O
RAD8.1.6	Prever a iniciação automática da contagem dos prazos de guarda referenciados nos instrumentos de classificação, temporalidade e destinação da política de gestão documental da Justiça Federal a partir do último arquivamento. *Acontecimentos específicos não-detectáveis automaticamente pelo sistema devem ser informados ao GestãoDoc por usuário autorizado como, por exemplo, "6 anos após julgamento pelo Tribunal de Contas da União" conforme PCTT.*	O
RAD8.1.7	Limitar ao gestor a definição e a manutenção (alteração, inclusão e exclusão) dos instrumentos de classificação, temporalidade e destinação da política de gestão documental da Justiça Federal.	O
RAD8.1.8	Permitir que um gestor altere o prazo, destinação ou classificação prevista em algum item dos instrumentos de classificação, temporalidade e destinação da política de gestão documental da Justiça Federal e garantir que a alteração tenha efeito em todos os documentos ou processos/dossiês associados àquele item. *As alterações nos instrumentos de classificação, temporalidade e destinação da política de gestão documental da Justiça Federal só poderão ser feitas após o resultado de um processo de reavaliação realizado pelo CJF.*	O
RAD8.1.9	Manter o histórico das alterações realizadas nos instrumentos de classificação, temporalidade e destinação da política de gestão documental da Justiça Federal.	O
RAD8.1.10	Importar e exportar total ou parcialmente um instrumento de classificação, temporalidade e destinação da política de gestão documental da Justiça Federal.	O

REF.	REQUISITO	OBRIG.
RAD8.1.11	Prover funcionalidades para a elaboração de relatórios que apóiem a gestão dos instrumentos de classificação, temporalidade e destinação da política de gestão documental da Justiça Federal, incluindo a capacidade de: ▪ Gerar relatório completo do instrumento de classificação, temporalidade e destinação de documentos. ▪ Gerar relatório parcial do instrumento de classificação, temporalidade e destinação de documentos a partir de um ponto determinado na hierarquia do plano de classificação. ▪ Gerar relatório dos documentos ou processos/dossiês aos quais está atribuído um determinado prazo de guarda. ▪ Identificar as inconsistências existentes entre os instrumentos de classificação, temporalidade e destinação de documentos e o plano de classificação.	O

8.2 Aplicação dos instrumentos de classificação, temporalidade e destinação de documentos

Estes requisitos referem-se à aplicação dos instrumentos de classificação, temporalidade e destinação de documentos: procedimentos de controle e verificação dos prazos e da destinação prevista, antes de se proceder às ações de destinação propriamente ditas.

REF.	REQUISITO	OBRIG.
RAD8.2.1	Prover funcionalidades para informar o usuário autorizado sobre os documentos ou processos/dossiês que já cumpriram ou estão para cumprir o prazo de guarda previsto.	O
RAD8.2.2	Pedir confirmação antes de realizar os procedimentos de destinação (emissão de relatórios, editais, etc.), conforme normas do CJF.	O
RAD8.2.3	Restringir as funcionalidades de destinação a usuários autorizados da unidade de arquivo.	O
RAD8.2.4	Quando um usuário autorizado reclassifica documentos ou processos/dossiês de uma classe ou assunto para outro, adotar automaticamente a temporalidade e a destinação vigentes na nova classe ou assunto.	O

REF.	REQUISITO	OBRIG.
RAD8.2.5	Os documentos previamente definidos pelo Programa de Gestão Documental como de guarda permanente (sentenças, inteiro teor de acórdão, etc.) deverão ter sua guarda garantida.	O
RAD8.2.6	Quando um documento digital — não previamente definido pelo Programa de Gestão Documental como de guarda permanente — estiver associado a mais de um dossiê ou processo, e tiver prazos de guarda diferentes associados a ele, esse prazo deverá ser o mais abrangente. *Quando um documento digital estiver associado a mais de um dossiê ou processo, o GestãoDoc deverá criar um registro para cada referência desse documento. Cada registro estará vinculado ao mesmo objeto digital.* *No momento da eliminação, o objeto digital não poderá ser eliminado sem antes ter ocorrido a verficação da temporalidade de todas as referências associadas a ele. O objeto digital só poderá ser eliminado quando os prazos de guarda de todas as referências tiverem sido cumpridos. Antes disso, só se pode fazer a eliminação de cada registro individualmente.*	O

8.3 Exportação de documentos

Um GestãoDoc deve ter capacidade de exportar documentos, processos/dossiês para apoiar a ação de transferência de documentos, ou ainda para realizar uma migração ou enviar uma cópia para outro local ou sistema.

É absolutamente necessário que as ações sejam executadas de maneira controlada, havendo registro nos metadados e na trilha de auditoria e verificação dos documentos relacionados.

REF.	REQUISITO	OBRIG.
RAD8.3.1	Exportar documentos e processos/dossiês digitais e seus metadados para outro sistema, dentro ou fora do órgão.	O

REF.	REQUISITO	OBRIG.
RAD8.3.2	Exportar um documento e processo/dossiê ou grupo de documentos e processos/dossiês numa seqüência 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 exportados como uma unidade. ▪ 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
RAD8.3.3	Exportar 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 pela Justiça Federal.	O
RAD8.3.4	Exportar todos os tipos de documentos que estiver apto a capturar.	D
RAD8.3.5	Produzir um relatório detalhado sobre qualquer falha que ocorra durante uma exportação. O relatório tem de identificar os documentos e processos/dossiês que tenham originado erros de processamento ou cuja exportação não tenha sido bem sucedida.	O
RAD8.3.6	Conservar todos os documentos e processos/dossiês digitais que tiverem sido exportados, pelo menos até que tenham sido importados no sistema destinatário com êxito.	O
RAD8.3.7	Manter metadados relativos a documentos e processos/dossiês exportados.	O
RAD8.3.8	Possibilitar a ordenação dos documentos e processos/dossiês digitais a serem exportados de acordo com elementos de metadados selecionados pelo usuário.	D
RAD8.3.9	Exigir do usuário autorizado, ao exportar documentos e processos/dossiês híbridos, a confirmação de que a parte não-digital dos mesmos documentos e processos/dossiês tenha sido recebida adequadamente antes de confirmar a exportação da parte sob forma digital.	O

REF.	REQUISITO	OBRIG.
RAD8.3.10	Permitir que documentos sejam exportados mais de uma vez. *Exemplo: O magistrado determina a remessa de processo eletrônico para o Superior Tribunal de Justiça (STJ) e também para o Ministério Público Federal (MPF).*	O

8.4 Eliminação

A eliminação de documentos institucionais deve ser realizada de acordo com o previsto nos instrumentos de classificação, temporalidade e destinação de documentos, após a avaliação dos documentos e de acordo com a regulamentação do CJF.

Os procedimentos para eliminação de documentos institucionais em um GestãoDoc têm de ser executados de forma controlada, fazendo-se registro nos metadados e trilha de auditoria.

REF.	REQUISITO	OBRIG.
RAD8.4.1	Restringir a função de eliminação de documentos ou processos/dossiês a usuários autorizados.	O
RAD8.4.2	Solicitar confirmação da eliminação a um usuário autorizado antes que qualquer ação seja tomada com relação ao documento e processo/dossiê.	O
RAD8.4.3	Avisar o usuário autorizado quando um documento ou processo/dossiê passível de eliminação encontrar-se relacionado a outro documento ou processo/dossiê.	O
RAD8.4.4	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.	O
RAD8.4.5	Quando um documento tiver várias referências armazenadas no sistema, garantir que todas essas referências sejam verificadas antes de eliminar o objeto digital. *Ver RAD8.2.6*	O
RAD8.4.6	Produzir um relatório detalhando qualquer falha que ocorra durante uma eliminação. O relatório deverá identificar os documentos cuja eliminação não tenha sido bem sucedida.	O
RAD8.4.7	Quando eliminar documentos ou processos/dossiês híbridos, exigir do usuário autorizado a confirmação de que a parte não-digital dos mesmos tenha sido eliminada também antes de confirmar a eliminação da parte sob forma digital.	O

REF.	REQUISITO	OBRIG.
RAD8.4.8	Gerar relatório com os documentos e processos/dossiês: ▪ Passíveis de eliminação (edital). ▪ Selecionados para guarda permanente pela aplicação do plano amostral. ▪ Definitivamente eliminados (termo de eliminação).	O
RAD8.4.9	Manter metadados relativos a documentos e processos/dossiês eliminados.	O

8.5 Avaliação e destinação de documentos institucionais não-digitais e híbridos

Os documentos institucionais não-digitais e os híbridos gerenciados pelo GestãoDoc devem ter os procedimentos de avaliação e destinação controlados pelo GestãoDoc, assim como os documentos digitais.

REF.	REQUISITO	OBRIG.
RAD8.5.1	Aplicar os mesmos instrumentos de classificação, temporalidade e destinação da política de gestão documental da Justiça Federal para os documentos não-digitais, digitais ou híbridos.	O
RAD8.5.2	Alertar ao usuário autorizado sobre a existência e localização de uma parte não-digital associada a um documento híbrido que esteja destinado a ser exportado, transferido ou eliminado.	O
RAD8.5.3	Permitir a exportação de metadados de documentos e processos/dossiês não-digitais.	O
RAD8.5.4	Permitir ao usuário autorizado uma nova classificação do processo/dossiê e documentos para fins específicos de destinação, sem alteração de sua classificação original.	O

9 Pesquisa, localização e apresentação de documentos

Um sistema de gestão de documentos deve prever funções de recuperação e acesso aos documentos institucionais e às informações neles contidas, de forma a satisfazer a condução das atividades e os requisitos relativos à transparência do órgão. A recuperação inclui a pesquisa, a localização e a apresentação dos documentos.

Em um GestãoDoc a apresentação dos documentos consiste em exibi-los por meio de um ou mais dispositivos de apresentação, tais como monitor de vídeo, impressora, caixa de som, etc. No âmbito do sistema de gestão de documentos, a pesquisa é feita a partir de bases de dados e produtos decorrentes. Já em um GestãoDoc a pesquisa é flexibilizada por parâmetros predefinidos, selecionados dentre as informações coletadas no momento do registro do documento e dentre os metadados a ele associados.

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

9.1 Recuperação de informação

REF.	REQUISITO	OBRIG.
RPL9.1.1	Fornecer facilidades para pesquisa, localização e apresentação dos documentos.	O
RPL9.1.2	Fornecer interface de pesquisa, localização e apresentação opcionais via um ambiente *Web*.	D
RPL9.1.3	Prever a navegação gráfica do plano de classificação, a navegação direta de uma classe ou assunto, para os documentos institucionais criados nessa classe ou assunto, e a seleção, recuperação e apresentação direta dos documentos institucionais e de seus conteúdos por meio desse mecanismo.	D
RPL9.1.4	Restringir a recuperação de informações de documentos e processos/dossiês sigilosos e em segredo de justiça aos usuários que possuam credencial de segurança adequada.	O

9.2 Pesquisa e localização

A pesquisa é o processo de identificação de documentos institucionais por meio de parâmetros definidos pelo usuário com o objetivo de confirmar,

localizar e recuperar esses documentos, bem como seus respectivos metadados.

REF.	REQUISITO	OBRIG.
RPL9.2.1	Fornecer uma série de funções que atuem sobre os metadados relacionados com os diversos níveis de agregação (documento, unidade de arquivamento e classe) 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, quer individualmente quer reunidos em grupo.	O
RPL9.2.2	Permitir a pesquisa regional de forma integrada, apresentando todos os documentos e processos/dossiês, sejam eles digitais, híbridos ou não-digitais, que satisfaçam aos parâmetros da pesquisa.	O
RPL9.2.3	Permitir a pesquisa nacional de forma integrada, apresentando todos os documentos e processos/dossiês, sejam eles digitais, híbridos ou não-digitais, que satisfaçam aos parâmetros da pesquisa.	D
RPL9.2.4	Permitir que todos os metadados de gestão de um documento ou processo/dossiê sejam pesquisados. *O usuário deve ser informado quando a pesquisa não obtiver resultado.*	O
RPL9.2.5	Permitir que os conteúdos sob a forma de texto dos documentos sejam pesquisados. *O usuário deve ser informado quando a pesquisa não obtiver resultado.*	D
RPL9.2.6	Permitir que um documento ou processo/dossiê seja recuperado por meio de todas as formas de identificação implementadas, incluindo no mínimo: ▪ Identificador ▪ Título ou descrição abreviada ▪ Datas ▪ Unidade de origem/destino ▪ Signatário/redator/parte/advogado/magistrado/interessado ▪ Classificação de acordo com os instrumentos de classificação	O
RPL9.2.7	Fornecer uma interface que possibilite a pesquisa combinada de metadados e de conteúdo do documento por meio dos operadores lógicos: “E”, “OU” e “NÃO”.	D

REF.	REQUISITO	OBRIG.
RPL9.2.8	Permitir que os termos utilizados na pesquisa sejam qualificados, especificando-se um metadado ou o conteúdo do documento como fonte de busca.	D
RPL9.2.9	Permitir a utilização de caracteres coringa e busca fonética para a pesquisa de metadados.	D
RPL9.2.10	Permitir que os usuários possam refinar as pesquisas já realizadas.	D
RPL9.2.11	Quando o órgão utilizar tesauros ou vocabulário controlado, realizar pesquisa dos documentos e processos/dossiês por meio da navegação destes instrumentos.	D
RPL9.2.12	Permitir a pesquisa previamente parametrizada, de acordo com o perfil ou necessidade do usuário.	O
RPL9.2.13	Permitir a pesquisa e recuperação de uma unidade de arquivamento e exibir a lista de todos os documentos que o compõem.	O

9.3 Apresentação: texto, imagem, som e vídeo

Um GestãoDoc pode conter documentos institucionais com formatos e estruturas os mais diversos e deve ter capacidade para apresentá-los ao usuário sem adulterá-los, utilizando-se adequadamente de suportes tecnológicos para texto, imagem, som e vídeo.

O sistema deverá informar os programas (*software*) adicionais necessários e a configuração adequada, como, por exemplo, *plug-in*, configuração de navegador.

REF.	REQUISITO	OBRIG.
RPL9.3.1	Apresentar o resultado da pesquisa como uma lista de documentos e processos/dossiês digitais, não-digitais ou híbridos que cumpram os parâmetros daquela.	O
RPL9.3.2	Após apresentar o resultado da pesquisa, além de informar a quantidade de itens recuperados, deve-se permitir ao usuário as seguintes opções: ▪ Acessar os documentos e processos/dossiês resultantes da pesquisa. ▪ Redefinir os parâmetros de pesquisa e fazer nova consulta.	O

REF.	REQUISITO	OBRIG.
RPL9.3.3	Permitir que os documentos e processos/dossiês apresentados em uma lista de resultados sejam selecionados e, em seguida, abertos.	D
RPL9.3.4	Permitir ao gestor a configuração de pesquisas, possibilitando as seguintes parametrizações: ▪ Determinação do número máximo de itens recuperáveis em uma pesquisa. ▪ Definição dos metadados que devem ser exibidos nas listas de resultados de pesquisa.	D
RPL9.3.5	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. ▪ Armazenamento dos resultados de uma pesquisa.	D
RPL9.3.6	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. ▪ De uma classe para as unidades de arquivamento a ela relacionadas.	D
RPL9.3.7	Apresentar o conteúdo de todos os tipos de documentos institucionais digitais capturados, preservando as características e os formatos.	O
RPL9.3.8	Reproduzir os documentos capturados, preservando o formato produzido pelas aplicações geradoras.	O
RPL9.3.9	Permitir que todos os documentos de um processo/dossiê sejam impressos ou armazenados em uma única operação, na seqüência determinada pelo usuário.	O

REF.	REQUISITO	OBRIG.
RPL9.3.10	Apresentar os documentos institucionais em formatos padronizados para publicação digital e interoperabilidade, além do formato nativo. *No que se refere à interoperabilidade com outros sistemas, ver Capítulo 12, Interoperabilidade.*	O
RPL9.3.11	Realizar pesquisa e exibição de documentos e processos/dossiês simultaneamente para diversos usuários.	O
RPL9.3.12	Permitir ao gestor determinar que vias ou cópias em papel de documentos, processos/dossiês e quais metadados podem ser reproduzidos.	D
RPL9.3.13	Permitir ao gestor o estabelecimento de permissões para armazenamento e reprodução de documentos, processos/dossiês.	O

10 Funções administrativas

10.1 Monitoração do sistema

REF.	REQUISITO	OBRIG.
RFA10.1.1	Permitir que o gestor, de maneira controlada e sem esforço excessivo, recupere, identifique, visualize e reconfigure os parâmetros do sistema e os atributos dos perfis dos usuários.	O
RFA10.1.2	Fornecer ao gestor relatórios flexíveis para o gerenciamento dos volumes e itens e sua utilização, que apresentem no mínimo: ▪ Quantidade de processos/dossiês, volumes e itens a partir de parâmetros ou atributos definidos (tempo, classe, unidade administrativa etc.). ▪ Estatísticas de operações relativas a processos/dossiês, volumes e itens. ▪ Relatórios de operações por usuário.	O
RFA10.1.3	Prover documentação cobrindo aspectos de administração do sistema. A documentação deve incluir todas as informações necessárias para o correto gerenciamento do sistema.	O

10.2 Manutenção e evolução

REF.	REQUISITO	OBRIG.
RFA10.2.1	Possuir documentação de implementação.	O
RFA10.2.2	Ser aderente à normatização do CJF nos aspectos de processo de desenvolvimento de *software*.	O
RFA10.2.3	Possuir um ambiente de homologação para avaliação de novas versões de *software*, que permita testes: ▪ Funcionais ▪ De preservação da integridade do acervo digital	O

11 Usabilidade

O projeto de um sistema de *software* com boa usabilidade[8] exige preocupação com a facilidade de utilização. A objetividade de apresentação de informações pelo sistema deve possibilitar a realização segura e eficiente das tarefas, ao mesmo tempo em que oferece interação agradável com o usuário.

Boa parte do sucesso de um sistema depende de sua aceitação. Um sistema desenvolvido objetivando facilidade de utilização tem mais chance de satisfazer os usuários. Além disso, exigirá menores custos de manutenção, treinamento e suporte.

REF.	REQUISITO	OBRIG.
RUS11.1.1	Possuir documentação completa, clara, inteligível e organizada para utilização do *software*.	O
RUS11.1.2	Possuir sistema de ajuda on-line.	O
RUS11.1.3	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
RUS11.1.4	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
RUS11.1.5	Toda mensagem de erro produzida deve ser clara e significativa, de modo a permitir ao usuário corrigir ou cancelar a operação.	O
RUS11.1.6	A interface deve seguir padrões preestabelecidos e consolidados como boas práticas de projeto gráfico, validados cientificamente. *Normas ou regras de interface podem ser relativas à utilização de padrão de identidade visual (ligado à "marca" da instituição ou alguma legislação específica da Justiça Federal), bem como a utilização de guias de estilo para implementação e verificação da padronização da interface, desde que não interfira nos princípios básicos da ergonomia cognitiva.*	O

[8] O conceito de usabilidade é tratado pela norma ISO/IEC 9126:1991 Information technology — *Software product evaluation*: quality characteristics and guidelines for their use.

REF.	REQUISITO	OBRIG.
RUS11.1.7	Utilização de um conjunto simples e consistente de regras de interface, privilegiando a facilidade de aprendizado de operação pelos seus usuários. *A utilização de um conjunto de regras consistentes 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
RUS11.1.8	A interface de visualização dos documentos institucionais deve fornecer o recurso de arrastar e soltar, se apropriado no ambiente operacional do GestãoDoc.	D
RUS11.1.9	Permitir que a estrutura de classes, assuntos e processos/dossiês seja visualizada em diferentes formas de apresentação.	D
RUS11.1.10	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. ▪ Avisos sonoros, incluindo tom e volume.	D
RUS11.1.11	Utilizar barras de ferramentas, permitindo ao usuário a possibilidade de configuração e de habilitar/desabilitar esse tipo de recurso. Porém, de forma a não infringir a recomendação de utilização de um conjunto simples e consistente de regras de interface.	D
RUS11.1.12	Permitir a utilização de janelas, sua movimentação, redimensionamento e gravação das modificações da aparência, possibilitando a personalização por perfil de usuário dentro de parâmetros ergonômicos.	D

REF.	REQUISITO	OBRIG.
RUS11.1.13	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. ▪ Valores predefinidos por um administrador (para campos de metadados como, por exemplo, o nome da organização que está utilizando o sistema).	D
RUS11.1.14	A interface tem de possibilitar a utilização às pessoas portadoras de necessidades especiais, de modo a atender o Decreto 5.296, de 2004.	O
RUS11.1.15	A interação deve permitir a interface com leitores de telas para portadores de deficiências visuais.	O
RUS11.1.16	A utilização não tem de tornar obrigatório o uso de aparelho selecionador específico (*mouse*, por exemplo).	O
RUS11.1.17	Permitir a realização de transações ou tarefas mais freqüentemente executadas com um pequeno número de iterações (cliques de *mouse*, por exemplo) e sem mudanças excessivas de contexto.	D
RUS11.1.18	Integração com o sistema de comunicação eletrônica da organização, de forma a permitir a geração de mensagens com possibilidade de manipular documentos digitais, sem necessidade de sair do GestãoDoc.	D
RUS11.1.19	No caso de integração com o sistema de comunicação eletrônica, deve ser possível fazer referências a documentos institucionais sem necessidade de envio de cópias adicionais.	D
RUS11.1.20	Possuir integração com o sistema padrão de edição de documentos.	D
RUS11.1.21	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
RUS11.1.22	Restringir o acesso às funcionalidades administrativas impossibilitando sua visualização ao usuário.	O

12 Interoperabilidade

A adoção de regras e padrões de comunicação já consolidados permite a consulta entre sistemas heterogêneos, sem que o usuário perceba as operações envolvidas, convergindo para uma relação sinérgica entre as partes.

Esta seção estabelece requisitos mínimos para que um GestãoDoc possa interoperar com outros sistemas de informação, inclusive sistemas legados, respeitando normas de segurança de acordo com padrões abertos de interoperabilidade.

Por interoperabilidade, entende-se: "Intercâmbio coerente de informações e serviços entre sistemas. A interoperabilidade deve possibilitar a substituição de qualquer componente ou produto usado nos pontos de interligação por outro de especificação similar, sem comprometimento das funcionalidades do sistema"[9]. Isto se faz mediante a utilização de regras e padrões de comunicação.

O GestãoDoc deverá adotar o padrão de interoperabilidade regulamentado pelo CJF.

REF.	REQUISITO	OBRIG.
RIN12.1.1	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 da Justiça Federal.*	O
RIN12.1.2	Interoperar com outros sistemas por intermédio de padrões abertos de interoperabilidade que deverão ser regulamentados pelo CJF.	O
RIN12.1.3	Aplicar os requisitos de segurança descritos neste documento para execução das operações de interoperabilidade. *Isso é fundamental para que as operações, feitas em ambiente com interoperabilidade, não afetem a integridade dos documentos e impossibilitem acessos não autorizados.*	O

9 <https://www.governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-de-interoperabilidade>. Acesso em: 20 jul 2007.

13 Disponibilidade

Requisitos de disponibilidade descrevem as exigências mínimas sobre prontidão de atendimento de um sistema.

Os requisitos de disponibilidade devem ser especificados pelo administrador do GestãoDoc de acordo com o nível de serviço a ser fornecido. Por exemplo, os períodos previstos de atendimento ("8x5" indica 8 horas por dia útil, "24x7" indica atendimento contínuo), bem como 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.

REF.	REQUISITO	OBRIG.
RDI13.1.1	Garantir disponibilidade de operação durante o período definido pela instituição, ressalvadas as falhas causadas por problemas de infra-estrutura.	O

14 Desempenho e escalabilidade

Os requisitos de desempenho enfocam a eficiência no atendimento às requisições de usuários, de acordo com suas expectativas quanto aos tempos de resposta. O tempo de resposta tanto é influenciado por requisitos de qualidade do *software* quanto por fatores externos, como, por exemplo, infra-estrutura 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 mesmo 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 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 infra-estrutura de informação olhando para a relação entre o capital investido e os níveis de performance obtidos.

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

REF.	REQUISITO	OBRIG.
RDE14.1.1	Manter estatísticas dos tempos de atendimento, discriminados por tipo de operação.	D
RDE14.1.2	Ser expansível até comportar um número máximo preestabelecido de usuários simultâneos, provendo continuidade efetiva de serviços.	O
RDE14.1.3	Manter registros de atualização de versão de infra-estrutura e do próprio sistema.	O
RDE14.1.4	Permitir adaptação a instituições de estruturas similares, mas de diferentes tamanhos.	D

REF.	REQUISITO	OBRIG.
RDE14.1.5	Fornecer evidências do grau de escalabilidade ao longo do tempo, mantendo avaliações quantitativas de: ▪ Número máximo de *sites* remotos suportados com desempenho adequado. ▪ 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. ▪ Expectativa de crescimento das bases de dados. ▪ Expectativa de crescimento do número de estações.	D

15 Glossário

Administrador	Responsável por manter o ambiente operacional do sistema.
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	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.
Avaliação de documentos	A passagem dos documentos de uma idade para outra é definida por meio do processo de avaliação, que considera a freqüência de uso dos documentos por seus produtores e a identificação de seus valores primário e secundário. No caso dos documentos que cumpriram valor primário, mas não apresentam valor secundário, estes serão eliminados. Já aqueles que não são mais necessários às atividades rotineiras do órgão que os criou, mas apresentam valor secundário, serão destinados à guarda permanente.
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.
Captura	Incorporação de documento ao sistema.

Checksum	Valor calculado a partir dos dados, para comprovação de integridade.
Ciclo de vida dos documentos	As sucessivas etapas pelas quais os documentos passam: produção, tramitação, uso, avaliação, arquivamento e destinação (guarda permanente ou eliminação).
Classe	Primeira divisão de um plano de classificação ou de um código de classificação.
Código de classificação	Conjunto de símbolos, normalmente letras e/ou números, derivado de um plano de classificação.
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	Separação de processos que estavam apensados. Nos processos judiciais, via de regra, 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.
Documento institucional	Documento produzido e recebido pelo Poder Judiciário Federal no exercício de suas funções. (Lei n. 8.159, de 1991, art. 20)
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.
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, *stress* 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.
Gestão de documentos	Conjunto de procedimentos e operações técnicas que engloba a produção, a tramitação, a utilização, a avaliação e o arquivamento em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente. (Lei nº 8.159, de 1991, art. 3)
Gestor	Responsável pelo gerenciamento das regras de negócio do sistema. Cabe ao gestor, entre outras atividades, a criação de usuários e atribuição de privilégios.
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.
Minuta	Versão preliminar de documento sujeita à aprovação.
Plano de classificação	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.
Processo	Conjunto de documentos oficialmente reunidos no decurso de uma ação administrativa ou judicial, que constitui uma unidade.
Rejuvenescimento	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.
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 freqüentes. 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 e judicial. Também chamado "movimentação ou trâmite".
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	▪ 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. ▪ GestãoDoc Aquele que é cadastrado no sistema. Aquele 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 de sua utilidade para fins diferentes daqueles para os quais foram originalmente produzidos, como, por exemplo, provas judiciais e administrativas e pesquisas acadêmicas.

Versão	Estado de um documento em determinada fase de sua elaboração.
Via original	Primeiro documento completo e efetivo.

16 Modelos de referência, legislação, regulamentações, normas e referências bibliográficas

16.1 Modelos de requisitos para sistemas informatizados de gestão arquivística de documentos

- CONSELHO NACIONAL DE ARQUIVOS — Câmara Técnica De Documentos Eletrônicos (Brasil). *Modelo de Requisitos para Sistemas Informatizados de gestão Arquivística de Documentos*. 2006. Versão 1. Disponível em: <http://www.conarq.arquivonacional.gov.br/Media/publicacoes/earqbrasilv1.pdf>. Acesso em: 18 set 2007.
- INSTITUTO DOS ARQUIVOS NACIONAIS/TORRE DO TOMBO, E INSTITUTO DE INFORMÁTICA (Portugal). Modelo de Requisitos para a Gestão de Arquivos Electrónicos. In: *Recomendações para a gestão de documentos de arquivo electrónicos*. Lisboa: O Instituto, 2002. v. 2. Disponível em: <http://www.iantt.pt/downloads/SIADE_Caderno1.pdf>. Acesso em: 8 set 2007.
- THE NATIONAL ARCHIVES OF ENGLAND, WALES AND THE UNITED KINGDOM. *Requirements for electronic records management systems*: 1: Functional requirements — 2002 revision: final revision. Kew:The Archives, 2002. Disponível em: <http://www.nationalarchives.gov.uk/documents/requirementsfinal.pdf>. Acesso em: 8 set 2007.

16.2 Legislação federal

Um GestãoDoc deve cumprir a legislação e regulamentações vigentes, em especial as relacionadas a seguir:

- **Lei nº 5.010, de 30 de maio de 1966**, que organiza a Justiça Federal de primeira instância, e dá outras providências.
- **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.

- **Lei nº 10.259, de 12 de julho de 2001**, que dispõe sobre a instituição dos Juizados Especiais Cíveis e Criminais, no âmbito da Justiça Federal.
- **Lei nº 11.111, de 5 de maio de 2005**, que regulamenta a parte final do disposto no inc. XXXIII do *caput* do art. 5º da Constituição Federal e dá outras providências.
- **Lei nº 11.280, de 16 de fevereiro de 2006**, que altera os arts. 112, 114, 154, 219, 253, 305, 322, 338, 489 e 555 da Lei nº 5.869, de 11 de janeiro de 1973 — Código de Processo Civil, relativos à incompetência relativa, meios eletrônicos, prescrição, distribuição por dependência, exceção de incompetência, revelia, carta precatória e rogatória, ação rescisória e vista dos autos; e revoga o art. 194 da Lei n. 10.406, de 10 de janeiro de 2002 — Código Civil.
- **Lei nº 11.419, de 19 de dezembro de 2006**, que dispõe sobre a informatização do processo judicial.
- **Decreto nº 4.553, de 27 de dezembro de 2002**, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.
- **Decreto nº 5.296, de 2 de dezembro de 2004**, que regulamenta as Leis ns 10.048, de 8 de novembro de 2000, que dá prioridade de atendimento às pessoas que especifica, e 10.098, de 19 de dezembro de 2000, que estabelece normas gerais e critérios básicos para a promoção da acessibilidade das pessoas portadoras de deficiência ou com mobilidade reduzida, e dá outras providências.
- **Decreto nº 5.301, de 9 de dezembro de 2004**, que Regulamenta o disposto na Medida Provisória nº 228, de 9 de dezembro de 2004, que dispõe sobre a ressalva prevista na parte final do disposto no inc. XXXIII do art. 5º da Constituição, e dá outras providências.
- **MP nº 2.200-2, de 24 de agosto de 2001**, que institui a Infra-Estrutura de Chaves Públicas Brasileira — ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

16.3 Resoluções do Conselho Nacional de Arquivos — Conarq

- **Resolução nº 14, de 24 de outubro de 2001**, que aprova a versão revisada e ampliada da Resolução do Conarq nº 4, de 28 de março de 1996, que dispõe sobre o Código de Classificação de Documentos de Arquivo para a Administração Pública: Atividades-Meio, a ser adotado como modelo para os arquivos correntes dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR), e os prazos de guarda e a destinação de documentos estabelecidos na Tabela Básica de

Temporalidade e Destinação de Documentos de Arquivo Relativos às Atividades-Meio da Administração Pública.

- **Resolução nº 20, de 16 de julho de 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.
- **Resolução nº 24, de 3 de agosto de 2006**, que estabelece diretrizes para a transferência e recolhimento de documentos arquivísticos digitais para instituições arquivísticas públicas.
- **Resolução nº 25, de 27 de abril de 2007**, que 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.

16.4 Resoluções do Conselho da Justiça Federal — CJF

- **Resolução nº 217, de 22 de dezembro de 1999**, que disciplina o Programa de Gestão de Documentos da Administração Judiciária de 1° e 2° graus.
- **Resolução nº 317, de 26 de maio de 2003**, que institui a Tabela Única de Assuntos no âmbito do Conselho e da Justiça Federal de 1º e 2º graus.
- **Resolução nº 328, de 28 de agosto de 2003**, que institui tabelas de classes e de movimentação processual a serem uniformizadas no âmbito do Conselho e da Justiça Federal de 1º e 2º graus.
- **Resolução nº 341, de 5 de dezembro de 2003**, que trata da prorrogação do prazo estabelecido para implantação da tabela única de assuntos.
- **Resolução nº 342, de 5 de dezembro de 2003**, que dispõe sobre o prazo para conclusão dos trabalhos e implantação das tabelas de classes e de movimentação processual.
- **Resolução nº 359, de 29 de março de 2004**, que estabeleceu a política de gestão das ações judiciais transitadas em julgado e arquivadas na Justiça Federal.
- **Resolução nº 380, de 5 de julho de 2004**, que dispõe sobre a organização das atividades de Tecnologia da Informação e Comunicação em forma de sistema.
- **Resolução nº 393, de 20 de setembro de 2004**, que altera as Resoluções ns 217, de 22 de dezembro de 1999, que disciplina o Programa de Gestão de Documentos da Administração Judiciária da Justiça Federal de primeiro e segundo graus, e 359, de 29 de março de 2004, que estabelece a política de gestão das ações judiciais transitadas em julgado e arquivadas na Justiça Federal de 1° e 2° graus e dá outras providências.

- **Resolução nº 471, 5 de outubro de 2005**, que aprova a Tabela Única de Movimentação Processual da Justiça Federal — TUMP e dá outras providências.
- **Resolução nº 507, de 31 de maio de 2006**, que estabelece diretrizes para o tratamento de processos e investigações sigilosas ou que tramitem em segredo de justiça, no âmbito na Justiça Federal de 1° e 2° graus.

16.5 Normas

- ISO 9660:1988 — Information processing — Volume and file structure of CD-ROM for information interchange.
- ISO 14721:2003 — Space data and information transfer systems — Open archival information system (OAIS) — Reference model.
- ISO 15408 — Common Criteria 2.X.
- ISO/IEC 9126:1991 Information technology — Software product evaluation: quality characteristics and guidelines for their use.
- ISO/IEC 17799:2005 — Information technology — Security techniques — Code of practice for information security management.
- ISO/IEC 27001:2005 — Information technology — Security techniques — Information security management systems — Requirements.
- AS ISO 15489.1 — Australian Standard Records Management. Part 1: General, 2002.
- AS ISO 15489-2 — Australian Standard Records Management. Part 2: Guidelines, 2002.

16.6 Referências bibliográficas

ARELLANO, Miguel Ángel Márdero. Preservação Digital. In: *Seminário de Gestão da Informação Jurídica em Espaços Digitais*, Supremo Tribunal Federal, Brasília. 2007. Disponível em: <www.stf.gov.br/sijed/Palestras/17.pdf>. Acesso em: 9 set 2007.

ARELLANO, Miguel Ángel Márdero, ANDRADE, Ricardo Sodré. Preservação digital e os profissionais da informação. DataGramaZero — *Revista de Ciência da Informação* — v.7 n.5 out/06. Disponível em: <http://www.dgz.org.br/out06/Art_05.htm>. Acesso em: 9 set 2007.

ARQUIVO NACIONAL (Brasil). *Dicionário Brasileiro de Terminologia Arquivística*. Rio de Janeiro: Arquivo Nacional, 2005.

CONSELHO INTERNACIONAL DE ARQUIVOS. Comitê de arquivos correntes em ambiente electrônico. *Documentos de arquivo electrônicos*: manual para arquivistas. ICA, Estudo nº 16. 2005. Disponível em: <http://www.ica.org/en/node/30273>. Acesso em: 8 set 2007.

CONSELHO NACIONAL DE ARQUIVOS. *Carta para a Preservação do Patrimônio Arquivístico Digital*, 2004. Disponível em: <http://www.conarq.arquivonacional.gov.br/Media/publicacoes/cartapreservpatrimarqdigitalconarq2004.pdf>. Acesso em: 21 jun 2007.

INNARELLI Humberto Celeste. Documentos digitais e sua fragilidade em relação ao suporte. In: *II Simpósio Internacional de Bibliotecas Digitais*. IBICT, Unicamp, 2004. Disponível em: <http://libdigi.unicamp.br/document/?view=8397>. Acesso em: 21 jun 2007.

Manual de Gestão de Autos Findos do Programa de Gestão Documental da Justiça Federal. Brasília, 2005. 36 p. Disponível em: <http://daleth.cjf.gov.br/Download/Manual%20Gestão%20Documental_21.doc>. Acesso em: 29 abr 2007.

Manual de Procedimentos do Programa de Gestão Documental da Justiça Federal, CJF, Brasília, 2001. 59 p. Disponível em: <http://www.jf.gov.br/portal/gestaodocumental/documentos/MANUAL%20DE%20PROCEDIMENTOS.pdf>. Acesso em: 29 abr 2007.

NATIONAL LIBRARY OF AUSTRALIA — NLA. *Guidelines for the preservation of digital heritage*. Paris: UNESCO, 2003. 177p. Disponível em: <http://unesdoc.unesco.org/images/0013/001300/130071e.pdf>. Acesso em: 6 set 2007.

ROCHA, Cláudia Lacombe. *Gestão e preservação de documentos arquivísticos digitais*. GED RIO, 1, 2006, Rio de Janeiro. Anais. Rio de Janeiro: Centro Nacional de Gerenciamento da Informação, 2006.

RONDINELLI, Rosely Cury. *Gerenciamento arquivístico de documentos eletrônicos*: uma abordagem teórica da diplomática arquivística contemporânea. Rio de Janeiro: Editora FGV, 2002. 160 p.

SANTOS, Vanderlei Batista dos. *Gestão de documentos eletrônicos:* uma visão arquivística. Brasília: ABARQ, 2002. 140p.

THOMAZ, Kátia P. *Gestão e preservação de documentos eletrônicos de arquivo*: revisão de literatura: parte 1. Arquivística.net, v. 2, n. 1, 2006. Disponível em: <http://www.arquivistica.net>. Acesso em: 8 set 2007.

THOMAZ, Kátia P. *Gestão e preservação de documentos eletrônicos de arquivo*: revisão de literatura: parte 2. Arquivística.net, v. 2, n. 1, 2006. Disponível em: <http://www.arquivistica.net/>. Acesso em: 08 set 2007.

UNESCO. División de la Sociedad de la Información. *Directrices para la preservación del patrimonio digital*. Preparado por la Biblioteca Nacional de Australia. Canberra: Biblioteca Nacional de Austrália, 2002. 176p. Disponível em: <http://unesdoc.unesco.org/ulis/cgibin/ulis.pl?database=ged&req=2&by=3&sc

1=1&look=new&sc2=1&text_p=inc&text=Directrices+para+la+preservaci%F3n+del+patrimonio+digital&submit=GO>. Acesso em: 8 ago 2006.