
Câmara Técnica de Documentos Eletrônicos

MODELO DE REQUISITOS PARA
SISTEMAS INFORMATIZADOS DE
GESTÃO ARQUIVÍSTICA DE DOCUMENTOS

# e-ARQ Brasil

2009
dezembro
Versão 1.1

# EQUIPE TÉCNICA DE ELABORAÇÃO DO E-ARQ BRASIL

## Equipe de redação da Câmara Técnica de Documentos Eletrônicos

Claudia Lacombe Rocha – Arquivo Nacional
Margareth da Silva – Arquivo Nacional
Rosely Curi Rondinelli – Fundação Casa de Rui Barbosa

## Equipe de sistematização dos metadados da Câmara Técnica de Documentos Eletrônicos

Brenda Couto de Brito Rocco – Arquivo Nacional
Carlos Augusto Silva Ditadi – Arquivo Nacional
Claudia Lacombe Rocha – Arquivo Nacional
Luiz Fernando Sayão – Comissão Nacional de Energia Nuclear
Margareth da Silva – Arquivo Nacional
Neire do Rossio Martins – Universidade Estadual de Campinas
Rosely Curi Rondinelli – Fundação Casa de Rui Barbosa

## Integrantes da Câmara Técnica de Documentos Eletrônicos que participaram deste trabalho

Ana Pavani – PUC-RJ – até setembro de 2004
Brenda Couto de Brito Rocco – Arquivo Nacional – a partir de maio de 2007
Carlos Augusto Silva Ditadi – Arquivo Nacional
Carlos Henrique Marcondes – Universidade Federal Fluminense – a partir de maio de 2007
Carmen Tereza Coelho Moreno – Biblioteca Nacional – até julho de 2005
Claudia Lacombe Rocha – Arquivo Nacional
Cláudio Muniz Machado Cavalcanti – Ministério do Planejamento, Orçamento e Gestão – a partir de fevereiro de 2008
Ednylton Franzosi – Ministério do Planejamento, Orçamento e Gestão – de março de 2005 até fevereiro de 2008
Gladys Machado Pereira Santos Lima – Marinha do Brasil – de abril de 2006 a junho de 2007
Humberto Innarelli – Universidade Estadual de Campinas
João Alberto de Oliveira Lima – Senado Federal – a partir de julho de 2008
Luiz Fernando Sayão – Comissão Nacional de Energia Nuclear
Marcos de Oliveira Matos – Marinha do Brasil – até julho de 2004
Margareth da Silva – Arquivo Nacional
Maria Izabel de Oliveira – Arquivo Nacional
Maria Rosangela da Cunha – Marinha do Brasil – até agosto de 2008
Neire do Rossio Martins – Universidade Estadual de Campinas
Paulo Roberto Ferreira Passos – Presidência da Republica – até maio de 2005
Rosely Curi Rondinelli – Fundação Casa de Rui Barbosa
Sergio Dagnino Falcão – Câmara dos Deputados
Vanderlei Batista dos Santos – Câmara dos Deputados

## Colaboradores

Ana Celeste Indolfo – Arquivo Nacional
Elisabeth Maçulo – Arquivo Nacional
Eugênio Pacelli – Casa Civil da Presidência da República
José Márcio Batista Rangel – Arquivo Nacional
Nilmar Saísse – Analista de Sistemas
Rodolfo de Sousa Nascimento – Arquivo Nacional
Vera Lúcia Hess de Mello Lopes – Arquivo Nacional

Contribuições às consultas públicas

Adriana Lampert Berwanger, Carmem Célia Vieira dos Santos, Eliane de Mello Miranda, Emiliano Medeiros, Fátima Lúcia Gazen de Mesquita, Leonice Geni Röpke, Luciana Baggio Bortolotto, Marcelo Bernardes, Norma Helena Kunrath e Vanessa Berwanger Sandri (Ministério Público do Rio Grande do Sul); Albano Oliveira, Aurora Freixo, Pablo Soledade, Ricardo Andrade e Tarsio Cavalcante (Grupo de Estudos sobre Cultura, Representação e Informação Digital/Instituto de Ciência da Informação da Universidade Federal da Bahia); Alraune Reinke da Paz, Andresa de Moraes e Castro e Sebastiana Coelho Costa (Secretaria de Arquivo do Senado Federal); Claudia Martinez Bandeira Oliveira; Jackson Guterres dos Santos; Jairo Fonseca; Kathya S. O. Campelo Bezerra; Katia de Pádua Thomaz; Luiz Fernando Duarte de Almeida; Marcelo Breganhola; Nelson da Silva e Ricardo Felipe Custódio (Laboratório de Segurança em Computação da Rede Nacional de Ensino e Pesquisa – LabSEC/RNP); Nicir Maria Gomes Chaves; Patricia Dias de Rossi; Sônia Reimão; Vilma Jesus de Oliveira, Ana Cátia Ferreira Viana, Danielle da Silva Rocha, Fabianne Gonçalves e Ivonete Pereira Tavares (Centro de Documentação e Histórico da Aeronáutica e Museu Aeroespacial/Comando da Aeronáutica/Ministério da Defesa).

O Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPqD) apoiou o Arquivo Nacional na redação dos requisitos de segurança, armazenamento, preservação, funções administrativas e técnicas, usabilidade, interoperabilidade, disponibilidade, desempenho e escalabilidade.

Revisão

Alba Gisele Gouget – Arquivo Nacional
Mariana Simões – Arquivo Nacional

# Sumário

# Introdução

Neste documento, é apresentado um Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-ARQ Brasil), elaborado no âmbito da Câmara Técnica de Documentos Eletrônicos (CTDE) do Conselho Nacional de Arquivos. No período de 2004 a 2006, foram redigidas a Parte I e a seção "Aspectos de funcionalidades" da Parte II e, entre 2007 e 2009, foi elaborado o esquema de metadados, que complementa a Parte II.

Este trabalho foi desenvolvido considerando a existência de um importante legado de documentos em formato digital, que vem sendo tratado por especialistas de diversas áreas, entre as quais arquivologia e tecnologia da informação. Esses especialistas conceituam o documento arquivístico e o documento arquivístico digital para poder analisar e propor soluções que enfrentem os desafios trazidos por este formato.

Inicialmente, é importante explicitar as definições de documento arquivístico e documento arquivístico digital estabelecidas pela CTDE. Essas definições, assim como outros conceitos aqui utilizados, encontram-se no glossário.

| O que é documento arquivístico? |
| --- |
| É um documento produzido e/ou recebido e mantido por pessoa física ou jurídica, no decorrer das suas atividades, qualquer que seja o suporte, e dotado de organicidade. |
| O que é documento digital? |
| É a informação registrada, codificada em dígitos binários e acessível por meio de sistema computacional. |
| O que é documento arquivístico digital? |
| É um documento digital que é tratado e gerenciado como um documento arquivístico, ou seja, incorporado ao sistema de arquivos. |
| O que é documento arquivístico convencional? |
| É um documento arquivístico não digital. |

Em seguida, devem ser considerados os fundamentos da diplomática,[1] da arquivologia, especialmente da gestão de documentos, e da tecnologia da informação para fornecer um conjunto de requisitos que seja amplo, rigoroso e de qualidade.

[1] Disciplina que tem como objeto o estudo da estrutura formal e da confiabilidade e autenticidade dos documentos.

### O que é e-ARQ Brasil?

É uma especificação de requisitos a serem cumpridos pela organização produtora/recebedora de documentos, pelo sistema de gestão arquivística e pelos próprios documentos, a fim de garantir sua confiabilidade e autenticidade, assim como sua acessibilidade.

Além disso, o e-ARQ Brasil pode ser usado para orientar a identificação de documentos arquivísticos digitais.

O e-ARQ Brasil estabelece requisitos mínimos para um Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD), independentemente da plataforma tecnológica em que for desenvolvido e/ou implantado.

O SIGAD deve ser capaz de gerenciar, simultaneamente, os documentos digitais e os convencionais. No caso dos documentos convencionais, o sistema registra apenas as referências sobre os documentos e, para os documentos digitais, a captura, o armazenamento e o acesso são feitos por meio do SIGAD.

Os requisitos dirigem-se a todos que fazem uso de sistemas informatizados como parte do seu trabalho rotineiro de produzir, receber, armazenar e acessar documentos arquivísticos. Um SIGAD inclui um sistema de protocolo informatizado, entre outras funções da gestão arquivística de documentos.

O e-ARQ Brasil especifica todas as atividades e operações técnicas da gestão arquivística de documentos, desde a produção, tramitação, utilização e arquivamento até a sua destinação final. Todas essas atividades poderão ser desempenhadas pelo SIGAD, o qual, tendo sido desenvolvido em conformidade com os requisitos aqui apresentados, conferirá credibilidade à produção e à manutenção de documentos arquivísticos.

### O que é SIGAD?

É um conjunto de procedimentos e operações técnicas, característico do sistema de gestão arquivística de documentos, processado por computador. Pode compreender um *software* particular, um determinado número de *software*s integrados, adquiridos ou desenvolvidos por encomenda, ou uma combinação destes.

O sucesso do SIGAD dependerá, fundamentalmente, da implementação prévia de um programa de gestão arquivística de documentos.

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

Nesse sentido, é importante estabelecer a diferença entre sistema de informação, gestão arquivística de documentos, sistema de gestão arquivística de documentos, gerenciamento eletrônico de documentos (GED) e sistema informatizado de gestão arquivística de documentos (SIGAD).

### Sistema de informação

Conjunto organizado de políticas, procedimentos, pessoas, equipamentos e programas computacionais que produzem, processam, armazenam e proveem acesso à informação proveniente de fontes internas e externas para apoiar o desempenho das atividades de um órgão ou entidade.

### Gestão arquivística 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 recolhimento para guarda permanente.

### Sistema de gestão arquivística de documentos

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

### Gerenciamento eletrônico de documentos (GED)

Conjunto de tecnologias utilizadas para organização da informação não estruturada de um órgão ou entidade, que pode ser dividido nas seguintes funcionalidades: captura, gerenciamento, armazenamento e distribuição. Entende-se por informação não estruturada aquela que não está armazenada em banco de dados, como mensagem de correio eletrônico, arquivo de texto, imagem ou som, planilhas etc.

O GED pode englobar tecnologias de digitalização, automação de fluxos de trabalho (*workflow*), processamento de formulários, indexação, gestão de documentos, repositórios, entre outras.

A literatura sobre GED distingue, geralmente, as seguintes funcionalidades: captura (ou entrada), armazenamento, apresentação (ou saída) e gerenciamento, e cita as tecnologias de digitalização, automação de fluxos de trabalho (*workflow*) etc. como possibilidades, não como componentes obrigatórios.

### Sistema informatizado de gestão arquivística de documentos (SIGAD)

É um conjunto de procedimentos e operações técnicas que visam o controle do ciclo de vida dos documentos, desde a produção até a destinação final, seguindo os princípios da gestão arquivística de documentos e apoiado em um sistema informatizado.

Um SIGAD tem que ser capaz de manter a relação orgânica entre os documentos e de garantir a confiabilidade, a autenticidade e o acesso, ao longo do tempo, aos documentos arquivísticos, ou seja, seu valor como fonte de prova das atividades do órgão produtor.

O SIGAD é aplicável em sistemas híbridos, isto é, que utilizam documentos digitais e documentos convencionais.

Um SIGAD inclui operações como: captura de documentos, 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 arquivísticos digitais e não digitais confiáveis e autênticos.

No caso dos documentos digitais, um SIGAD deve abranger todos os tipos de documentos arquivísticos digitais do órgão ou entidade, ou seja, textos, imagens fixas e em movimento, gravações sonoras, mensagens de correio eletrônico, páginas *web*, bases de dados.

Com base nestas definições, podemos tecer as seguintes considerações:

- Um sistema de informação abarca todas as fontes de informação existentes no órgão ou entidade, incluindo o sistema de gestão arquivística de documentos, biblioteca, centro de documentação, serviço de comunicação, entre outros;
- Um GED trata os documentos de maneira compartimentada, enquanto o SIGAD parte de uma concepção orgânica, qual seja, a de que os documentos possuem uma inter-relação que reflete as atividades da instituição que os criou. Além disso, diferentemente do SIGAD, o GED nem sempre incorpora o conceito arquivístico de ciclo de vida[2] dos documentos;
- Um SIGAD é um sistema informatizado de gestão arquivística de documentos e, como tal, sua concepção tem que se dar a partir da implementação de uma política arquivística no órgão ou entidade.

### Requisitos arquivísticos que caracterizam um SIGAD

- captura, armazenamento, indexação e recuperação de todos os tipos de documentos arquivísticos;
- captura, armazenamento, indexação e recuperação de todos os componentes digitais do documento arquivístico como uma unidade complexa;[3]
- gestão dos documentos a partir do plano de classificação para manter a relação orgânica entre os documentos;
- implementação de metadados associados aos documentos para descrever os contextos desses mesmos documentos (jurídico-administrativo, de proveniência, de procedimentos, documental e tecnológico);[4]

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

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

[4] Ver Glossário.

- integração entre documentos digitais e convencionais;
- foco na manutenção da autenticidade dos documentos;
- avaliação e seleção dos documentos para recolhimento e preservação daqueles considerados de valor permanente;
- aplicação de tabela de temporalidade e destinação de documentos;
- transferência e recolhimento dos documentos por meio de uma função de exportação;
- gestão de preservação dos documentos.

A especificação dos requisitos e dos metadados a serem implementados em um SIGAD será tratada na Parte II deste documento.

# 1 OBJETIVOS

- Orientar a implantação da gestão arquivística de documentos arquivísticos digitais e não digitais;
- Fornecer especificações técnicas e funcionais, além de metadados, para orientar a aquisição e/ou a especificação e desenvolvimento de sistemas informatizados de gestão arquivística de documentos.

# 2 ÂMBITO E UTILIZAÇÃO

O e-ARQ Brasil deve ser utilizado para desenvolver um sistema informatizado ou para avaliar um já existente, cuja atividade principal seja a gestão arquivística de documentos.

O e-ARQ Brasil é aplicável aos sistemas que produzem e mantêm somente documentos digitais e aos que compreendem documentos digitais e convencionais. Com relação aos documentos convencionais, o sistema inclui apenas o registro das referências nos metadados, já no caso dos documentos digitais, o sistema inclui os próprios documentos.

Desde que a organização estabeleça um programa de gestão arquivística de documentos, o e-ARQ Brasil é aplicável aos setores público e privado de qualquer esfera e âmbito de atuação, servindo para diferentes tipos de documentos arquivísticos. Destina-se, igualmente, aos documentos relativos às atividades-meio e às atividades-fim de um órgão ou entidade e não se restringe a um ramo de atividade específica. Pode ser adotado como padrão ou norma pela administração pública federal, estadual, municipal, dos poderes Executivo, Legislativo e Judiciário,

a fim de uniformizar o desenvolvimento e aquisição de sistemas que visam produzir e manter documentos arquivísticos em formato digital.

O e-ARQ Brasil é especialmente dirigido a:

- fornecedores e programadores: para orientar o desenvolvimento de um SIGAD em conformidade com os requisitos exigidos;
- profissionais da gestão arquivística de documentos: para orientar a execução desses serviços a partir de uma abordagem arquivística;
- usuários de um SIGAD: como base para auditoria ou inspeção do SIGAD instalado;
- potenciais usuários de um SIGAD: como apoio na elaboração de edital para apresentação de propostas de fornecimento de *software*;
- potenciais compradores de serviços externos de gestão de documentos: como material auxiliar para a especificação dos serviços a serem comprados;
- organizações de formação: como um documento de referência para a formação em gestão arquivística de documentos;
- instituições acadêmicas: como recurso de ensino.

Todo o conteúdo deste documento está em consonância com a política do Conselho Nacional de Arquivos, que verifica a proteção especial dos documentos de arquivo e, particularmente, a preservação do patrimônio arquivístico digital. As orientações, políticas e especificações contidas neste documento estão alinhadas com a necessidade de garantir que os documentos arquivísticos digitais sejam produzidos e mantidos de forma confiável, autêntica, e permaneçam acessíveis.

O conteúdo deste documento é de domínio público, não havendo restrições à sua reprodução nem à utilização das informações nele contidas. A reprodução pode ser feita em qualquer suporte, sem necessidade de autorização específica, desde que sejam mencionados os créditos ao Conselho Nacional de Arquivos. O uso do material, no todo ou em parte, com fins depreciativos será objeto de tratamento jurídico por parte do Conselho Nacional de Arquivos, vinculado ao Arquivo Nacional, órgão da Casa Civil da Presidência da República, detentor dos direitos autorais.

É proibida a utilização do todo ou de parte do conteúdo deste documento para fins comerciais.

## 3 LIMITES DA ESPECIFICAÇÃO

O e-ARQ Brasil compreende uma extensa variedade de requisitos para diferentes esferas de atuação, ramos de atividade e tipos de documentos. No entanto, o e-ARQ Brasil sozinho não abrange todos os requisitos necessários para qualquer órgão ou entidade poder criar, manter e dar acesso a documentos digitais. As organizações possuem exigências legais e regulamentares distintas que devem ser levadas em conta ao se adotar este modelo. Cada organização deve considerar as suas atividades, os documentos que produz, bem como o contexto de produção e manutenção do documento e, dependendo da situação, acrescentar requisitos

específicos e/ou assegurar que os requisitos listados aqui como facultativos ou altamente desejáveis possam ser classificados como obrigatórios. Além disso, o sucesso da implementação depende de uma série de decisões, que vão exigir a adoção de uma política arquivística abrangente que não se limita, pura e simplesmente, a selecionar um *software* ou adaptar um já existente.

O e-ARQ Brasil, ainda que discorra sobre vários aspectos da gestão arquivística de documentos, deixa a critério de cada organização ou grupo de organizações a decisão de como adotá-lo, se de forma modular ou completa. Por último, cabe ressaltar que o presente documento foi elaborado para profissionais das áreas de administração, de arquivo e de tecnologia da informação, requerendo a interação entre eles para que a implementação seja bem-sucedida.

# 4 NORMAS E OUTRAS ORIENTAÇÕES DE REFERÊNCIA

## 4.1 Normas

a) Sobre especificação de requisitos de segurança funcional:

- ISO 15408 – Common criteria 2.x., 2005

b) Sobre gestão de documentos:

- AS ISO 15489.1 – Australian standard records management. Part 1: general, 2002
- AS ISO 15489-2 – Australian standard records management. Part 2: guidelines, 2002

c) Sobre preservação:

- ISO 14721 – Reference model for an open archival information system (OAIS), 2003

d) Sobre metadados:

- ISO 23081-1 – Information and documentation – Records management processes – Metadata for records – Part 1: Principles, 2006
- ISO 15836 – Dublin core metadata element set, 2003

## 4.2 Resoluções do Conselho Nacional de Arquivos

- Resolução do CONARQ n. 14, de 24 de outubro de 2001

  Aprova a versão revisada e ampliada da Resolução do CONARQ n. 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 do CONARQ n. 20, de 16 de julho de 2004

  Dispõe sobre a inserção dos documentos digitais em programas de gestão arquivística de documentos dos órgãos e entidades integrantes do Sistema Nacional de Arquivos.

## 4.3 Modelos de requisitos para sistemas informatizados de gestão arquivística de documentos

- Design criteria standard for electronic records management *software* applications: DOD 5015.2-STD, 2002
- MoReq – Modelo de requisitos para a gestão de arquivos electrónicos, 2002
- Requirements for electronic records management systems: Functional requirements, United Kingdom, 2002

## 4.4 Padrões, modelos e esquemas de metadados

- e-Government Metadata Standard – e-GMS, United Kingdom, v. 3.0, 2004
- Metainformação para Interoperabilidade de Portugal – MIP, Lisboa, 2006
- MoReq 2 – Model requirements for the management of electronic records update and extension, 2007
- Padrão de Metadados do Governo Eletrônico – e-PMG, Brasil (minuta)
- PREMIS Data Dictionary for Preservation Metadata – version 2

## 4.5 Orientações para gestão e preservação de documentos digitais

- Directrices para la preservación del patrimonio digital, 2002
- Documentos de arquivo electrónico: manual para arquivistas, ICA, Estudo n. 16, 2005
- Electronic Records Management Initiative. Disponível em: <http://www.archives.gov/records-mgmt/initiatives/erm-overview.html>
- INTERPARES Project. Disponível em: <http://www.interpares.org>
- Management, appraisal and preservation of electronic records guidelines. Disponível em: <http://www.nationalarchives.gov.uk/electronicrecords/advice/guidelines.htm>

# 5 ORGANIZAÇÃO DA ESPECIFICAÇÃO

O e-ARQ Brasil está dividido em duas partes. A Parte I, *Gestão arquivística de documentos*, pretende fornecer um arcabouço para que cada órgão ou entidade possa desenvolver um programa de gestão arquivística de documentos, e a Parte 2, *Especificação de requisitos para sistemas informatizados de gestão arquivística de documentos*, descreve os requisitos necessários para desenvolver o SIGAD.

A Parte I contém sete capítulos e trata da política arquivística, do planejamento e da implantação do programa de gestão arquivística de documentos, dos procedimentos e controles do SIGAD e dos instrumentos utilizados na gestão de documentos.

A Parte II está organizada em *Aspectos de funcionalidade*, *Metadados*, *Glossário* e *Referências*. Os Aspectos de funcionalidade contêm catorze capítulos, divididos em seções, e tratam de organização de documentos (incluindo o plano de classificação), produção, tramitação, captura, destinação, recuperação da informação, segurança, armazenamento, preservação, funções administrativas e técnicas, e requisitos adicionais. Cada seção compreende um preâmbulo e a relação dos requisitos correspondentes àquela seção. Os requisitos são apresentados em quadros numerados com o enunciado correspondente e a classificação dos níveis de obrigatoriedade. O esquema de Metadados apresenta elementos relacionados a quatro tipos de entidades: documento, classe, agente e componente digital.

### Obrigatoriedade dos requisitos

Os requisitos foram classificados em obrigatórios, altamente desejáveis e facultativos, de acordo com o grau maior ou menor de exigência para que o SIGAD possa desempenhar suas funções.

No e-ARQ Brasil, os requisitos foram considerados:

- obrigatórios quando indicados pela frase: “O SIGAD tem que...”
- altamente desejáveis quando indicados pela frase: “O SIGAD deve...”
- facultativos quando indicados pela frase: “O SIGAD pode...”

Cada requisito numerado é classificado como:

| | | |
|---|---|---|
| (O) | = obrigatório = | “O SIGAD tem que ...” |
| (AD) | = altamente desejável = | “O SIGAD deve ...” |
| (F) | = facultativo = | “O SIGAD pode ...” |

TEM = o requisito é imprescindível.

DEVE = podem existir razões válidas em circunstâncias particulares para ignorar um determinado item, mas a totalidade das implicações deve ser cuidadosamente examinada antes de se escolher uma proposta diferente.

PODE = o requisito é opcional.

Tanto para os requisitos considerados altamente desejáveis como para os requisitos facultativos, é preciso observar que uma implementação que não inclua determinado item altamente desejável ou facultativo deve estar preparada para interoperar com uma outra implementação que inclui o item, mesmo tendo funcionalidade reduzida. De forma inversa, uma implementação que inclua um item altamente desejável ou facultativo deve estar preparada para interoperar com uma outra implementação que não inclui o item.

## Obrigatoriedade dos metadados

Os metadados apresentados neste documento também foram classificados de acordo com o grau maior ou menor de exigência para apoiar as funcionalidades do SIGAD.

Cada elemento de metadado é classificado como:

(O) = obrigatório

(OA) = obrigatório, se aplicável

(F) = facultativo

Obrigatório = o elemento deve, obrigatoriamente, estar presente.

Obrigatório, se aplicável = o elemento pode ser aplicável ou não, porém, se aplicável, sua presença é obrigatória.

Facultativo = os elementos facultativos estão relacionados à implementação do sistema e cabe à instituição decidir ou não pelo seu uso. O grau facultativo pode tornar-se obrigatório para determinada instituição, dependendo de suas necessidades específicas.

# Parte I
# Gestão arquivística de documentos

## 1 CONSIDERAÇÕES INICIAIS

Após a Segunda Guerra Mundial, a tecnologia do computador extrapolou os limites do uso militar, e começou uma expansão pelas instituições públicas e privadas dos países do capitalismo central. Até a década de 1970, o uso do computador era limitado aos especialistas devido à necessidade do domínio de estruturas complexas de *hardware* (componentes físicos do sistema computacional) e de *software* (programas). Eram os tempos do CPD – Centro de Processamento de Dados, cujos profissionais atuavam completamente separados do restante da instituição.

Os anos 80 trouxeram duas grandes novidades: os computadores pessoais e as redes de trabalho. Os primeiros marcaram o início da descentralização das atividades informatizadas. O desenvolvimento de programas amigáveis e os custos baixos / a redução dos custos da tecnologia levaram à disseminação do uso dos microcomputadores. Essa disseminação foi potencializada com o advento da tecnologia de rede, que evoluiu, rapidamente, das redes locais (*local area network* – LAN) para as metropolitanas, nacionais e globais, sendo a *Internet* a maior delas.

O avanço das tecnologias de informação e comunicação (TIC), a partir dos anos 90, muda radicalmente os mecanismos de registro e comunicação da informação nas instituições públicas e privadas. Os documentos produzidos no decorrer das atividades dessas instituições, até então em meio convencional, assumem novas características, isto é, passam a ser gerados em ambientes eletrônicos, armazenados em suportes magnéticos e ópticos, em formato digital, e deixam de ser apenas entidades físicas para se tornarem entidades lógicas. Além disso, o gerenciamento dos documentos, tanto os digitais como os convencionais, começa a ser feito por meio de um sistema informatizado conhecido como gerenciamento eletrônico de documentos (GED).

Os documentos digitais trouxeram uma série de vantagens no que se refere à produção, transmissão, armazenamento e acesso que, por sua vez, acarretaram alguns problemas. A simplicidade de criação e transmissão de documentos traz como consequência a informalidade na linguagem, nos procedimentos administrativos, bem como o esvaziamento das posições hierárquicas. A facilidade de acesso acarreta, às vezes, intervenções não autorizadas que podem resultar na adulteração ou perda dos documentos. A rápida obsolescência tecnológica (*software*, *hardware* e formatos) e a degradação das mídias digitais dificultam a preservação de longo prazo dos documentos e sua acessibilidade contínua. Estes e outros problemas requerem a adoção de medidas preventivas para minimizá-los.

Considerando-se que os documentos arquivísticos se constituem, primeiramente, em instrumentos fundamentais para a tomada de decisão e para a prestação de contas de órgãos ou entidades, e, num segundo momento, em fontes de prova, garantia de direitos aos cidadãos e testemunhos de ação, faz-se necessária a adoção de procedimentos rigorosos de controle para garantir a confiabilidade e a

autenticidade desses documentos, bem como o acesso contínuo a eles. Isso só é possível com a implantação de um programa de gestão arquivística de documentos.

Com a difusão dos documentos digitais, a gestão arquivística de documentos tornou-se o principal foco de estudo da comunidade arquivística internacional. Nos últimos anos, projetos desenvolvidos nos Estados Unidos, Canadá, Europa e Austrália resultaram na revisão de conceitos arquivísticos, na definição de diretrizes de gestão e na especificação de requisitos funcionais e metadados para sistemas de gestão arquivística de documentos.

A gestão arquivística compreende a responsabilidade dos órgãos produtores e das instituições arquivísticas[5] em assegurar que a documentação produzida seja o registro fiel das suas atividades e que os documentos permanentes sejam devidamente recolhidos às instituições arquivísticas.

A partir da década de 1950, o conceito de gestão arquivística de documentos foi estabelecido nos Estados Unidos com o objetivo de racionalizar a produção documental, facilitar o acesso aos documentos e regular sua eliminação ou guarda permanente.

No Brasil, a gestão arquivística de documentos ganhou amparo legal a partir da lei n. 8.159, de 8 de janeiro de 1991, a Lei de Arquivos, e do decreto n. 4.073, de 3 de janeiro de 2002, que regulamenta a gestão de documentos na administração pública federal.

O Conselho Nacional de Arquivos, criado pela lei n. 8.159, de 1991, tem por finalidade definir a política nacional de arquivos públicos e privados, e exercer orientação normativa, visando a gestão documental e a proteção especial aos documentos de arquivo.[6] É um órgão colegiado, vinculado ao Arquivo Nacional, composto por plenário, câmaras técnicas, câmaras setoriais e comissões especiais. Do plenário participam o diretor-geral do Arquivo Nacional, representantes dos poderes Executivo, Legislativo e Judiciário federais, do Arquivo Nacional, dos arquivos públicos estaduais e do Distrito Federal, dos arquivos municipais, das instituições mantenedoras de curso superior de arquivologia, das associações de arquivistas e das instituições profissionais que atuam nas áreas de ensino, pesquisa, preservação ou acesso a fontes documentais.

O Sistema Nacional de Arquivos (SINAR) tem o CONARQ como órgão central e é composto pelo Arquivo Nacional, pelos arquivos dos poderes Executivo, Legislativo e Judiciário federais, e pelos arquivos estaduais, do Distrito Federal e municipais. Podem ainda integrar o SINAR as pessoas físicas e jurídicas de direito privado, detentoras de arquivos, mediante acordo com o CONARQ. O SINAR tem por finalidade implementar a política nacional de arquivos públicos e privados, em conformidade com as diretrizes e normas emanadas pelo CONARQ, promovendo a gestão, a preservação e o acesso às informações e aos documentos na esfera de competência dos integrantes do SINAR.[7]

[5] Entende-se por instituição arquivística aquela que tem como finalidade a guarda, preservação, acesso e divulgação de documentos arquivísticos, ainda que integrando bibliotecas, museus e centros de documentação.

[6] Conforme art. 1º do decreto n. 4.073, de 3 de janeiro de 2002.

[7] Conforme arts. n. 10 a 13 do decreto n. 4.073, de 3 de janeiro de 2002.

Foi, portanto, no âmbito do CONARQ, que a Câmara Técnica de Documentos Eletrônicos (CTDE) redigiu e elaborou o "Modelo de requisitos para sistemas informatizados de gestão arquivística de documentos – e-ARQ Brasil".

## 2 O QUE É GESTÃO ARQUIVÍSTICA DE DOCUMENTOS?

Os documentos produzidos e recebidos no decorrer das atividades de um órgão ou entidade, independentemente do suporte em que se apresentam, registram suas políticas, funções, procedimentos e decisões. Nesse sentido, constituem-se em documentos arquivísticos, que conferem aos órgãos e entidades a capacidade de:

- conduzir as atividades de forma transparente, possibilitando a governança e o controle social das informações;
- apoiar e documentar a elaboração de políticas e o processo de tomada de decisão;
- possibilitar a continuidade das atividades em caso de sinistro;
- fornecer evidência em caso de litígio;
- proteger os interesses do órgão ou entidade e os direitos dos funcionários e dos usuários ou clientes;
- assegurar e documentar as atividades de pesquisa, desenvolvimento e inovação, bem como a pesquisa histórica;
- manter a memória corporativa e coletiva.

Para que tenham essa capacidade, os documentos arquivísticos precisam ser confiáveis, autênticos, acessíveis e compreensíveis, o que só é possível por meio da implantação de um programa de gestão arquivística de documentos, que permitirá a sua preservação.

A Câmara Técnica de Documentos Eletrônicos (CTDE) define gestão arquivística de documentos[8] como o conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento de documentos arquivísticos em fase corrente e intermediária, visando sua eliminação ou recolhimento para guarda permanente.

No bojo do conceito de gestão arquivística de documentos, está a teoria de que os documentos passam por três idades, a saber:

- corrente: os documentos que estão em curso, isto é, tramitando ou que foram arquivados, mas são objeto de consultas frequentes; eles são conservados nos locais onde foram produzidos sob a responsabilidade do órgão produtor;
- intermediária: os documentos que não são mais de uso corrente, mas que, por ainda conservarem algum interesse administrativo, aguardam, no

[8] Entende-se gestão arquivística de documentos como sinônimo de gestão de documentos, ressaltando a característica arquivística desta gestão para diferenciá-la de outros tipos de gerenciamento de documentos.

arquivo intermediário, o cumprimento do prazo estabelecido em tabela de temporalidade e destinação, para serem eliminados ou recolhidos ao arquivo permanente;

- permanente: os documentos que devem ser definitivamente preservados em razão de seu valor histórico, probatório ou informativo.

A passagem dos documentos de uma idade para outra é definida pelo processo de avaliação, que leva em conta a frequência de uso dos documentos por seus produtores e a identificação de seu valor primário e secundário. O valor primário é atribuído aos documentos considerando sua utilidade administrativa imediata, isto é, as razões pelas quais esses documentos foram produzidos. Já o 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. A propósito, lembramos que, segundo Rousseau e Couture, "Enquanto todos os documentos têm um valor primário que dura mais ou menos tempo conforme o caso, nem todos têm ou adquirem necessariamente um valor secundário".[9] Os documentos que cumpriram valor primário, mas não apresentam valor secundário serão eliminados. Já aqueles que não são mais necessários às atividades rotineiras do órgão ou entidade que os criou, mas apresentam valor secundário, serão destinados a guarda permanente.

O "Código de classificação de documentos de arquivo para a administração pública: atividades-meio" e a "Tabela básica de temporalidade e destinação de documentos de arquivo relativos às atividades-meio da administração pública", aprovados pelo CONARQ,[10] são instrumentos fundamentais para a implementação da gestão arquivística de documentos.

Além de aprovar e publicar esses instrumentos, regulamentando a classificação e avaliação de documentos, o CONARQ regulamentou também, em suas resoluções, os procedimentos de eliminação, transferência e recolhimento de documentos.[11]

Os órgãos e entidades devem estabelecer, documentar, instituir e manter políticas, procedimentos e práticas para a gestão arquivística de documentos, com base nas diretrizes estabelecidas pelo CONARQ.

A gestão arquivística de documentos compreende:

- definição da política arquivística;
- designação de responsabilidades;
- planejamento do programa de gestão;
- implantação do programa de gestão.

---

[9] ROUSSEAU, Jean-Yves; COUTURE, Carol. *Os fundamentos da disciplina arquivística*. Lisboa: Publicações D. Quixote, 1994, p. 118.

[10] Resolução do CONARQ n. 14, de 24 de outubro de 2001.

[11] Resolução do CONARQ n. 1, de 18 de outubro de 1995; Resolução do CONARQ n. 2, de 18 de outubro de 1995; Resolução do CONARQ n. 5, de 30 de setembro de 1996; Resolução do CONARQ n. 7, de 20 de maio de 1997; Resolução do CONARQ n. 20, de 16 de julho de 2004; Resolução do CONARQ n. 21, de 4 de agosto de 2004; Resolução do CONARQ n. 24, de 3 de agosto de 2006.

No final do século XX, a necessidade da implantação de programas de gestão arquivística de documentos foi reforçada pela produção crescente de documentos arquivísticos exclusivamente em formato digital – textos, mensagens de correio eletrônico, bases de dados, planilhas, imagens, gravações sonoras, material gráfico, páginas da *web* etc.

O documento digital apresenta especificidades que podem comprometer sua autenticidade, uma vez que é suscetível à degradação física dos seus suportes, à obsolescência tecnológica de *hardware*, *software* e de formatos, e a intervenções não autorizadas, que podem ocasionar adulteração e destruição. Somente com procedimentos de gestão arquivística é possível assegurar a autenticidade dos documentos arquivísticos digitais.

## 3 DEFINIÇÃO DA POLÍTICA ARQUIVÍSTICA

Órgãos e entidades devem definir uma política de gestão arquivística de documentos que tenha por objetivo produzir, manter e preservar documentos confiáveis, autênticos, acessíveis e compreensíveis, de maneira a apoiar suas funções e atividades.

Essa política é iniciada com uma declaração oficial de intenções que especifica, de forma resumida, como será realizada a gestão no órgão ou entidade. A declaração pode incluir as linhas gerais do programa de gestão, bem como os procedimentos necessários para que essas intenções sejam alcançadas. Deve também ser comunicada e implementada em todos os níveis dos órgãos e entidades. No entanto, uma declaração por si só não garante uma boa gestão arquivística de documentos. Para a política ser bem-sucedida, são fundamentais o apoio da direção superior e a alocação dos recursos necessários para sua implementação. Além disso, é necessária a formação de um grupo de trabalho ligado aos níveis mais altos da hierarquia do órgão ou entidade, com a designação de um responsável pelo cumprimento da política e pela implementação do programa de gestão arquivística.

A política de gestão arquivística de documentos deve ser formulada com base na análise do perfil institucional, isto é, de seu contexto jurídico-administrativo, estrutura organizacional, missão, competências, funções e atividades, de forma que os documentos produzidos sejam os mais adequados, completos e necessários. Além disso, deve estar articulada às demais políticas informacionais existentes no órgão ou entidade, tais como políticas de sistemas e de segurança da informação.

É fundamental que todos os funcionários estejam envolvidos na política de gestão arquivística de documentos a ser implantada na instituição. Para tanto, deve ser feito um trabalho de conscientização sobre a relevância dessa gestão e sobre o papel de cada um na produção e manutenção de documentos confiáveis e autênticos.

A política de gestão arquivística de documentos deve explicitar as responsabilidades e designar as autoridades envolvidas no programa de gestão, de forma que, por exemplo, quando for identificada a necessidade de produzir e capturar documentos, esteja claro quem é o responsável por essas ações.

## 4 DESIGNAÇÃO DE RESPONSABILIDADES

A designação de responsabilidades é um dos fatores que garantem o êxito da gestão arquivística de 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 funcionários de acordo com a função e a posição hierárquica de cada um e envolver as seguintes categorias:

- Direção superior: é a autoridade máxima responsável pela viabilidade da política de gestão arquivística de documentos. A ela caberá apoiar, integralmente, a implantação dessa política, alocando recursos humanos, materiais e financeiros, e promovendo o envolvimento de todos no programa de gestão arquivística.
- Profissionais de arquivo: são os responsáveis pelo planejamento e implantação do programa de gestão arquivística, assim como pela avaliação e controle dos trabalhos executados no âmbito do programa. Além disso, os profissionais de arquivo são responsáveis também pela disseminação das técnicas e da cultura arquivística.
- Gerentes de unidades ou grupos de trabalho: são os responsáveis por garantir que os membros de suas equipes produzam e mantenham documentos como parte de suas tarefas, de acordo com o programa de gestão arquivística de documentos.
- Usuários finais: são os responsáveis, em todos os níveis, pela produção e uso dos documentos arquivísticos em suas atividades rotineiras, conforme estabelecido pelo programa de gestão.
- Gestores dos sistemas de informação e de tecnologia da informação: são as equipes responsáveis pelo projeto, desenvolvimento e manutenção de sistemas de informação nos quais os documentos arquivísticos digitais são gerados e usados, e pela operacionalização dos sistemas de computação e de comunicação.

## 5 PLANEJAMENTO E IMPLANTAÇÃO DO PROGRAMA DE GESTÃO ARQUIVÍSTICA DE DOCUMENTOS

O programa de gestão arquivística de documentos deve ter como base a política arquivística e a designação de responsabilidades definidas anteriormente, além do contexto jurídico-administrativo, de forma que esteja de acordo com a missão institucional e a legislação vigente.

O planejamento envolve o levantamento e a análise da realidade institucional, o estabelecimento das diretrizes e procedimentos a serem cumpridos pelo órgão ou entidade, o desenho do sistema de gestão arquivística de documentos e a elaboração de instrumentos e manuais.

No planejamento do programa de gestão, algumas tarefas fundamentais devem ser cumpridas:

- levantamento da estrutura organizacional e das atividades desempenhadas;
- levantamento da produção documental, diferenciando os documentos arquivísticos dos não arquivísticos;
- levantamento, caso existam, dos sistemas utilizados, internamente, para tratamento de documentos e informações;
- definição, a partir do levantamento da produção documental, dos tipos de documentos que devem ser mantidos e produzidos, e das informações devem conter;
- definição e/ou aperfeiçoamento da forma desses documentos;
- análise e revisão do fluxo dos documentos;
- elaboração e/ou revisão do plano de classificação e da tabela de temporalidade e destinação;
- definição dos metadados a serem criados no momento da produção do documento e ao longo do seu ciclo de vida;
- definição e/ou aperfeiçoamento dos procedimentos de protocolo e de arquivamento dos documentos;
- definição e/ou aperfeiçoamento dos procedimentos para acesso, uso e transmissão dos documentos;
- definição do ambiente tecnológico que compreende os sistemas (*hardware* e *software*), formatos, padrões e protocolos que darão sustentação aos procedimentos de gestão e preservação de documentos, integrando, quando possível, os sistemas legados;
- definição da infraestrutura para armazenamento dos documentos convencionais, que compreende espaço físico, mobiliário e acessórios;
- definição das equipes de trabalho de arquivo e de tecnologia de informação;
- definição de programas de capacitação de pessoal;
- elaboração e/ou revisão de manuais e instruções normativas.
- definição dos meios de divulgação e de capacitação de pessoal;
- definição do plano de ação do programa de gestão, com seus objetivos, metas e estratégias de implantação, divulgação e acompanhamento, visando a melhoria contínua.

A implantação do programa de gestão arquivística de documentos envolve a execução e o acompanhamento de ações e projetos, efetuados simultaneamente. Deve atender aos objetivos definidos no planejamento do programa no que se refere à capacitação de pessoal, implantação de sistemas de gestão arquivística, integração com os sistemas de informação existentes e os processos administrativos do órgão ou entidade. Essa etapa pode incluir a suspensão de atividades e procedimentos vigentes que forem considerados inadequados.

A execução propriamente dita significa pôr em prática os planos de ação e os projetos aprovados.

O acompanhamento da implantação ocorre por meio de relatórios, sumários, gráficos, reuniões e entrevistas, entre outros. O acompanhamento percorre todo o processo de implantação e pode implicar em revisão e correções operacionais e estratégicas.

A revisão deve gerar decisões, providências e medidas de aperfeiçoamento do próximo ciclo do planejamento da gestão arquivística de documentos.

## 5.1 Exigências a serem cumpridas pelo programa de gestão arquivística de documentos

O programa de gestão arquivística de documentos terá que atender a uma série de exigências, tanto em relação ao documento arquivístico como ao seu próprio funcionamento:

O documento arquivístico deve:

- refletir corretamente o que foi comunicado, decidido ou a ação implementada;
- conter os metadados necessários para documentar a ação;
- ser capaz de apoiar as atividades;
- prestar contas das atividades realizadas.

O programa de gestão arquivística de documentos deve:

- contemplar o ciclo de vida dos documentos;
- garantir a acessibilidade dos documentos;
- manter os documentos em ambiente seguro;
- reter os documentos somente pelo período estabelecido na tabela de temporalidade e destinação;
- implementar estratégias de preservação dos documentos desde a sua produção e pelo tempo que for necessário;
- garantir as seguintes qualidades do documento arquivístico: organicidade, unicidade, confiabilidade, autenticidade e acessibilidade.

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

a) Organicidade

O documento arquivístico se caracteriza pela organicidade, ou seja, pelas relações que mantém com os demais documentos do órgão ou entidade e que refletem suas funções e atividades. Os documentos arquivísticos não são coletados artificialmente, mas estão ligados uns aos outros por um elo que se materializa no plano de classificação, que os contextualiza no conjunto ao qual pertencem. Os documentos arquivísticos apresentam um conjunto de relações que devem ser mantidas.

*Exigência*: Os procedimentos de gestão arquivística devem registrar e manter as relações entre os documentos e a sequência das atividades realizadas, por meio da aplicação de um plano de classificação.

### b) Unicidade

O documento arquivístico 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.

*Exigência*: O programa de gestão arquivística deve prever a identificação de cada documento individualmente, sem perder de vista o conjunto de relações que o envolve.

### c) Confiabilidade[12]

Um documento arquivístico confiável é aquele que tem a capacidade de sustentar os fatos que atesta. A confiabilidade está relacionada ao momento em que o documento é produzido e à veracidade do seu conteúdo. Para tanto, há que ser dotado de completeza[13] e ter seus procedimentos de produção bem controlados. Dificilmente, pode-se assegurar a veracidade do conteúdo de um documento; ela é inferida da completeza e dos procedimentos de produção. A confiabilidade é uma questão de grau, ou seja, um documento pode ser mais ou menos confiável.

*Exigência*: Para garantir a confiabilidade, o programa de gestão arquivística dos órgãos e entidades deve assegurar que os documentos arquivísticos sejam produzidos no momento em que ocorre a ação, ou imediatamente após, por pessoas diretamente envolvidas na condução das atividades e devidamente autorizadas; e com o grau de completeza requerido tanto pelo próprio órgão ou entidade como pelo sistema jurídico.

### d) Autenticidade

Um documento arquivístico autêntico é aquele que é o que diz ser, independentemente de se tratar de minuta, original ou cópia, e que é livre de adulterações ou qualquer outro tipo de corrupção. Enquanto a confiabilidade está relacionada ao momento da produção, a autenticidade está ligada à transmissão do documento e à sua preservação e custódia. Um documento autêntico é aquele que se mantém da mesma forma como foi produzido e, portanto, apresenta o mesmo grau de confiabilidade que tinha no momento de sua produção. Assim, um documento não completamente confiável, mas transmitido e preservado sem adulteração ou qualquer outro tipo de corrupção, é autêntico.

---

[12] *Confiabilidade* é sinônimo de fidedignidade, tradução do termo em inglês *reliability*. *"Reliability is conferred to records by the controls exercised on the creation and by the completeness of their form."* DURANTI, Luciana. The InterPARES Project. In: *Authentic records in the electronic age*. Vancouver: University of British Columbia, 2000, p. 12, nota 2.

[13] *Completeza* se refere à presença, no documento arquivístico, de todos os elementos intrínsecos e extrínsecos exigidos pela organização produtora e pelo sistema jurídico-administrativo ao qual pertence, de maneira que esse mesmo documento possa ser capaz de gerar consequências (ver *Glossário*).

*Exigência*: Para assegurar a autenticidade dos documentos arquivísticos, o programa de gestão arquivística tem que garantir sua identidade[14] e integridade.[15] Para tanto, deve implementar e documentar políticas e procedimentos que controlem a transmissão, manutenção, avaliação, destinação e preservação dos documentos, garantindo que eles estejam protegidos contra acréscimo, supressão, alteração, uso e ocultação indevidos.

e) Acessibilidade

Um documento arquivístico acessível é aquele que pode ser localizado, recuperado, apresentado e interpretado.

*Exigência*: para assegurar a acessibilidade, o programa de gestão arquivística deve garantir a transmissão de documentos para outros sistemas sem perda de informação e de funcionalidade. O sistema deve ser capaz de recuperar qualquer documento, a qualquer tempo, e de apresentá-lo com a mesma forma que tinha no momento de sua produção.

## 5.2 Metodologia do programa de gestão

A metodologia do planejamento e da implantação de um programa de gestão arquivística de documentos estabelece oito passos que não são lineares, isto é, podem ser desenvolvidos em diferentes estágios, interativa, parcial ou gradualmente, de acordo com as necessidades do órgão ou entidade. A metodologia estabelece, ainda, ciclos de aplicação, sendo que as tarefas previstas para os passos C a H devem ser realizadas periodicamente.

Os oito passos citados acima são:

a) Levantamento preliminar

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

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

O levantamento preliminar também implica numa apreciação geral dos pontos fortes e fracos das práticas de gestão de documentos existentes no órgão ou entidade. Essa apreciação será a base para a definição do escopo do programa de gestão.

Este passo é fundamental para a definição de quais documentos devem ser produzidos e capturados, bem como para a elaboração do plano de classificação e da tabela de temporalidade e destinação, que devem ter como base as funções e atividades desenvolvidas pelo órgão ou entidade.

[14] Refere-se a atributos que caracterizam o documento arquivístico e o distinguem dos demais. Esses atributos se constituem nos elementos intrínsecos da forma documental e nas anotações.

[15] Refere-se ao estado dos documentos que se encontram completos e não sofreram nenhum tipo de corrupção ou alteração não autorizada nem documentada.

### b) Análise das funções, das atividades desenvolvidas e dos documentos produzidos

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

O objetivo deste passo é desenvolver um modelo conceitual sobre o que o órgão ou entidade faz e como faz, demonstrando como os documentos se relacionam com sua missão e suas atividades. O modelo subsidiará a definição dos procedimentos de produção, captura, controle, armazenamento, acesso e destinação dos documentos. Essa definição é particularmente importante em ambientes eletrônicos, onde os documentos adequados não são capturados e mantidos se o sistema não for projetado para isso.

Os produtos resultantes deste passo podem incluir:

- esquema de classificação das funções e atividades;
- mapa dos fluxos de trabalho que mostre quais e quando os documentos são produzidos ou recebidos como resultado das atividades desenvolvidas pelo órgão.

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

- tesauro e vocabulário controlado para identificar e indexar documentos de uma atividade específica;
- código de classificação para contextualizar os documentos produzidos e recebidos;
- tabela de temporalidade e destinação que define os prazos de guarda e as ações de destinação dos documentos.

### 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 função ou atividade desempenhada e definir quem está autorizado a produzir cada documento. Essas exigências devem tomar por base a legislação vigente, as normas internas e os riscos decorrentes da falta de registro de uma atividade em documento arquivístico.

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

Os produtos resultantes deste passo podem incluir:

- lista das exigências a serem cumpridas para a produção e manutenção de documentos;
- relatório de avaliação dos riscos decorrentes da falta de registro de uma atividade em documento arquivístico;

- documento formal, regulamentando as exigências a serem cumpridas para a produção e manutenção de documentos, ou seja, definindo quais documentos devem ser produzidos, que forma documental devem apresentar e os níveis de permissão de acesso.

### d) Avaliação dos sistemas existentes

Consiste em identificar e avaliar o sistema de gestão arquivística de documentos e outros sistemas de informação e comunicação existentes no órgão ou entidade.

O objetivo deste passo é identificar as lacunas entre as exigências para a produção e manutenção de documentos e o desempenho do sistema de gestão arquivística de documentos e dos sistemas de informação e comunicação existentes. Isso fornecerá a base para o desenvolvimento de novos sistemas ou para 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 arquivística de documentos e dos sistemas de informação e comunicação existentes no órgão ou entidade;
- relatório sobre o sistema de gestão arquivística de documentos e os sistemas de informação existentes, avaliando até que ponto atendem às exigências a serem cumpridas para a produção e manutenção de documentos arquivísticos.

### e) Identificação das estratégias para satisfazer as exigências a serem cumpridas para a produção de documentos arquivísticos

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

A escolha das estratégias deve levar em conta:

- a natureza do órgão ou entidade, 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.

Os produtos resultantes deste passo podem incluir:

- lista das estratégias selecionadas de modo a satisfazer as exigências para produção dos documentos arquivísticos;
- documento a ser encaminhado à administração recomendando a elaboração de um projeto de gestão arquivística de documentos e relacionando as estratégias a serem adotadas, com as devidas justificativas.

f) Projeto do sistema de gestão arquivística de documentos

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

O projeto de um sistema de gestão arquivística de documentos objetiva:

- planejar mudanças ou adaptações para sistemas informatizados, processos e práticas correntes;
- determinar como incorporar essas mudanças ou adaptações para melhorar a gestão dos documentos arquivísticos no órgão ou entidade;
- adaptar ou adotar soluções tecnológicas, considerando, na medida do possível/o máximo possível, um plano estratégico de evolução que vise minimizar os efeitos da obsolescência tecnológica.

Para alcançar esses objetivos, o projeto de um sistema de gestão arquivística de documentos deve incluir:

- definição de tarefas, responsabilidades e cronograma;
- diagramas representando a arquitetura e os componentes do sistema;
- modelos representando visões diferentes do sistema, tais como processos, fluxos de dados e entidades de dados;
- especificações detalhadas para construir ou adquirir componentes tecnológicos como *software* e *hardware*, considerando que o sistema deve ser modular, evolutivo e expansível;
- plano de segurança da informação (física e lógica) e de contingência;
- metodologia e procedimentos de auditoria;
- planos mostrando como o projeto integrará os sistemas e os processos existentes;
- previsão de treinamento de pessoal;
- planos de teste;
- plano de implementação do sistema;
- detalhamento das revisões periódicas do projeto, em conformidade com o plano estratégico de evolução e com as mudanças na tecnologia e no mercado.

g) Implementação do sistema de gestão arquivística de documentos

Consiste na execução do projeto por meio de:

- treinamento de pessoal;
- introdução do sistema de gestão arquivística de documentos ou adaptação do já existente;

- integração do sistema de gestão arquivística de documentos com os procedimentos e os sistemas de informação e comunicação existentes.

A implementação de um sistema de gestão arquivística de documentos é um empreendimento complexo, que deve ser realizado com o mínimo de interrupção das atividades do órgão ou entidade e envolve riscos e a necessidade de prestação de contas. Esses riscos podem ser minimizados com o planejamento cuidadoso e a documentação dos processos de implementação.

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 de gestão arquivística de documentos.

h) Monitoramento e ajustes

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

Verifica-se o desempenho avaliando se os documentos estão sendo produzidos e organizados de acordo com as necessidades do órgão ou entidade e se estão relacionados, apropriadamente, aos processos dos quais fazem parte.

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

Este passo envolve:

- entrevistas com a administração, equipe e outros parceiros;
- aplicação de questionários para medir o desempenho do sistema de gestão arquivística de documentos;
- exame da documentação (manuais de procedimentos, material de treinamento) desenvolvida durante a implementação do sistema de gestão arquivística de documentos;
- observação, análise e auditoria das informações e dos procedimentos implementados.

O monitoramento garantirá o retorno contínuo dos investimentos no programa de gestão arquivística de documentos, além de fornecer informação objetiva sobre a capacidade do órgão ou entidade em produzir e gerenciar documentos arquivísticos apropriados, assegurando o seu armazenamento de maneira segura.

O monitoramento minimizará o grau de exposição a riscos por falha do sistema de gestão arquivística de documentos. Além disso, antecipará a identificação de mudanças significativas nas exigências para a produção e manutenção de documentos arquivísticos, bem como a necessidade de um novo ciclo de desenvolvimento do programa de gestão.

Os produtos resultantes deste passo podem incluir:

- desenvolvimento e aplicação de uma metodologia para avaliar, objetivamente, o sistema de gestão arquivística de documentos;
- documentação do desempenho do sistema de gestão arquivística de documentos;
- relatório para a administração, com conclusões e recomendações.

## 5.3 Suspensão ou extinção do SIGAD

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

O processo de suspensão ou extinção de SIGAD deve ser documentado, inclusive os planos de conversão ou mapeamento dos dados, pois essas informações detalhadas serão necessárias à verificação de autenticidade e manutenção da acessibilidade dos documentos inseridos no sistema suspenso ou extinto.

# 6 PROCEDIMENTOS E OPERAÇÕES TÉCNICAS DO SISTEMA DE GESTÃO ARQUIVÍSTICA DE DOCUMENTOS DIGITAIS E CONVENCIONAIS

## 6.1 Captura

A captura consiste em declarar um documento como um documento arquivístico, incorporando-o ao sistema de gestão arquivística por meio das seguintes ações:

- registro;
- classificação;
- indexação;
- atribuição de restrição de acesso;
- arquivamento.

Os objetivos da captura são:

- identificar o documento como documento arquivístico;
- demonstrar a relação orgânica dos documentos.

Captura é a incorporação de um documento ao sistema de gestão arquivística, quando ele passa a seguir as rotinas de tramitação e arquivamento. Uma vez capturado, o documento pode ser incluído num fluxo de trabalho e, posteriormente, arquivado, ou ser, imediatamente, arquivado em uma pasta, no caso de documentos em papel, ou diretório, no caso de documentos digitais.

Tradicionalmente, nos sistemas de gestão arquivística de documentos em papel, a captura é feita no momento em que o documento é registrado, classificado e/ou identificado.

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

Além do código de classificação, descritores, número de protocolo e número de registro, a captura pode prever a introdução de outros metadados, tais como data e hora de produção, da transmissão e do recebimento do documento; nome do autor, do originador, do redator e do destinatário, entre outros. Esses metadados podem ser registrados em vários níveis de detalhamento, dependendo das necessidades geradas pelos procedimentos do órgão ou entidade e do seu contexto jurídico-administrativo.

Os metadados são essenciais para identificar o documento arquivístico de maneira inequívoca e mostrar sua relação com os outros documentos.

A captura tem como pré-requisito a definição de:

- quais documentos (produzidos e recebidos) serão capturados pelo sistema de gestão arquivística de documentos;
- quem deve ter acesso a esses documentos e em que níveis;
- por quanto tempo serão retidos.

As decisões sobre captura e retenção devem ser consideradas no momento da concepção do sistema de gestão arquivística de documentos. A decisão referente a quais documentos devem ser capturados e por quanto tempo devem ser mantidos requer que se levem em conta os seguintes fatores: legislação vigente, exigências quanto à transparência e ao exercício das atividades do órgão ou entidade, e o grau de risco que correm caso não capturem documentos arquivísticos.

Entre os documentos que exigem captura estão aqueles que:

- responsabilizam uma organização ou indivíduo por uma ação;
- documentam uma obrigação ou responsabilidade;
- estão relacionados à prestação de contas do órgão ou entidade.

### *6.1.1 Registro*

O registro consiste em formalizar a captura do documento dentro do sistema de gestão arquivística por meio da atribuição de um número identificador e de uma descrição informativa. Em um SIGAD, essa descrição informativa corresponde à atribuição de metadados.

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

Os documentos podem ser registrados em níveis diferentes dentro de um sistema de gestão arquivística de documentos, ou seja, além do número identificador

atribuído pelo sistema, o documento pode receber também um número único do processo/dossiê a que pertence.

As atividades de protocolo são constituídas pelo conjunto de operações que visam o controle dos documentos produzidos e recebidos que tramitam no órgão ou entidade, assegurando sua localização, recuperação e acesso. Após o recebimento dos documentos, o serviço de protocolo faz o registro, atribuindo-lhes número e data de entrada, anotando o código de classificação e o assunto, e procedendo à distribuição dos documentos nas unidades destinatárias.

Na administração pública, em determinados casos, documentos formam processos, os quais devem ser autuados por uma unidade protocolizadora. Um processo é o documento ou conjunto de documentos que exige um estudo mais detalhado ou procedimentos como despachos, pareceres técnicos, anexos ou, ainda, instruções para pagamento de despesas. No procedimento de autuação, a unidade protocolizadora faz o registro do processo, atribuindo-lhe um número único. Esse número é formado a partir de parâmetros estabelecidos por normas que garantam sua unicidade e integridade.

Nesse sentido, devem ser seguidas as recomendações e normas específicas existentes para a utilização dos serviços de protocolo nas diversas esferas e âmbitos da administração pública, que regulamentam o registro, autuação e outros procedimentos relativos aos processos e demais documentos oficiais.

O registro inclui os seguintes metadados obrigatórios:

- número identificador atribuído pelo sistema;
- data e hora do registro;
- título ou descrição abreviada: palavra, frase ou grupo de caracteres que nomeiam um documento arquivístico;
- produtor: nome da pessoa física ou jurídica responsável pela produção do documento arquivístico;
- autor: nome da pessoa física com autoridade e capacidade para emitir o documento ou em nome da qual ou sob cujo comando o documento é emitido;
- redator: nome da pessoa física responsável pela redação do documento;
- originador: identificação da pessoa física ou jurídica designada no endereço eletrônico ou *log in* em que o documento é gerado ou enviado.

O registro pode incluir informações descritivas mais detalhadas a respeito do documento em questão e de outros a ele relacionados, tais como:

- data de produção;
- data e hora de transmissão e recebimento;
- destinatário (com identificação do cargo): organização ou pessoa para quem o documento foi dirigido;
- espécie documental: divisão de gênero documental que reúne tipos de documentos por seu formato. São exemplos de espécies documentais ata, carta, decreto, memorando, ofício, planta, relatório;

- classificação de acordo com o código de classificação;[16]
- associações a documentos diferentes que podem estar relacionados pelo fato de registrarem a mesma atividade ou se referirem à mesma pessoa ou situação;
- formato, *software* e versão em que o documento foi produzido ou capturado;
- máscaras de formatação (*template*) necessárias para apresentar o documento;
- restrição de acesso;[17]
- descritor: palavra ou grupo de palavras que, em indexação e tesauro, designam um conceito ou assunto preciso, excluindo outros sentidos e significados;
- prazos de guarda;[18]
- documentos anexos.

### *6.1.2 Classificação*

Classificação é o ato ou efeito de analisar e identificar o conteúdo dos documentos arquivísticos e de selecionar a classe sob a qual serão recuperados. Essa classificação é feita a partir de um plano de classificação elaborado pelo órgão ou entidade e que pode incluir ou não a atribuição de código aos documentos.

A classificação determina o agrupamento de documentos em unidades menores (processos e dossiês) e o agrupamento destas em unidades maiores, formando o arquivo do órgão ou entidade. Para isso, deve tomar por base o conteúdo do documento, que reflete a atividade que o gerou e determina o uso da informação nele contida. A classificação também define a organização física dos documentos, constituindo-se em referencial básico para sua recuperação.

Os objetivos da classificação são:

- estabelecer a relação orgânica dos documentos arquivísticos;
- assegurar que os documentos sejam identificados de forma consistente ao longo do tempo;
- auxiliar a recuperação de todos os documentos arquivísticos relacionados a 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 ou atividade registrada no/pelo documento;
- 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 as normas/regras de classificação ao documento.

[16] Ver 6.1.2 – *Classificação*.

[17] Ver 6.1.4 – *Atribuição de restrição de acesso*.

[18] Ver 6.2 – *Avaliação, temporalidade e destinação*.

### *6.1.3 Indexação*

Indexação é a atribuição de termos à descrição do documento, utilizando vocabulário controlado e/ou lista de descritores, tesauro e o próprio plano de classificação.

A seleção dos termos para indexação é feita, normalmente, com base em:

- tipologia documental: divisão de espécie documental que reúne documentos por suas características comuns no que diz respeito à fórmula diplomática, natureza de conteúdo ou técnica de registro. São exemplos de tipos documentais: atestado de frequência de pessoal, atestado de saúde ocupacional, alvará de licença para construção, alvará de habite-se;
- título ou cabeçalho do documento;
- assunto do documento: palavras-chave ou termos compostos que representem corretamente o conteúdo do documento;
- datas associadas com as transações registradas no documento;
- documentação anexada.

A indexação tem como objetivo ampliar as possibilidades de busca e facilitar a recuperação dos documentos, e pode ser feita de forma manual ou automática.

### *6.1.4 Atribuição de restrição de acesso*

Os documentos também devem ser analisados com relação às precauções de segurança, ou seja, se são considerados ostensivos ou sigilosos. No caso dos sigilosos, a legislação estabelece graus de sigilo a serem atribuídos a cada documento.

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

A atribuição de restrições deve ser feita no momento da captura, com base no esquema de classificação de segurança e sigilo elaborado pelo órgão ou entidade, e envolve os seguintes passos:

- identificar a ação ou atividade que o documento registra;
- identificar a unidade administrativa à qual o documento pertence;
- verificar as precauções 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 arquivística de documentos.

### *6.1.5 Arquivamento*

Arquivar é a técnica de colocar e conservar numa mesma ordem, devidamente classificados de acordo com o plano de classificação, todos os documentos de um órgão ou entidade, utilizando métodos adequados, de forma que fiquem protegidos e sejam facilmente localizados e manuseados.

No sistema de gestão arquivística de documentos em papel, o documento é arquivado quando colocado, em uma pasta ou arquivo que contém um título, juntamente com outros a ele relacionados e ordenados conforme critérios previamente estipulados. Esse agrupamento conecta o documento a outros sobre o mesmo assunto, função ou atividade.

Um sistema de gestão arquivística de documentos em papel deve controlar os títulos das pastas. Colocar um documento em uma pasta é um processo consciente de determinar sua classificação e arquivá-lo em uma sequência predefinida. Os documentos arquivados na pasta podem ser datados e numerados sequencialmente, como medida de segurança. As condições de acesso e a destinação podem ser controladas por mecanismos predefinidos.

Um sistema de gestão arquivística de documentos digitais deverá também controlar os títulos das pastas ou diretórios nos quais os documentos foram armazenados procurando fazer as conexões existentes entre os vários objetos digitais a partir de uma codificação identificadora única. Os documentos digitais arquivados em repositórios organizados podem ser datados e numerados seqüencialmente como medida de segurança. As condições de acesso e a destinação podem ser controladas por mecanismos predefinidos.

A operação de arquivamento dos documentos digitais se diferencia do arquivamento dos documentos convencionais porque nestes o arquivamento é ao mesmo tempo uma operação lógica e física, como, por exemplo, arquivar um relatório na pasta Relatórios. No documento digital, como suporte e conteúdo são entidades separadas e o documento é constituído por um objeto físico (suporte), lógico (*software* e formato) e conceitual (apresentação), a operação de arquivar significa armazenar o objeto digital, mantendo sua identificação única e os ponteiros para outros objetos digitais.

## 6.2 Avaliação, temporalidade e destinação

A avaliação é uma atividade vital em um programa de gestão arquivística de documentos, pois permite racionalizar o acúmulo de documentos nas fases corrente e intermediária, facilitando a constituição dos arquivos permanentes.

A avaliação é o processo de análise dos documentos arquivísticos, visando estabelecer os prazos de guarda e a destinação, de acordo com os valores primário e secundário[19] que lhes são atribuídos. Os prazos de guarda e as ações de destinação deverão estar formalizados na tabela de temporalidade e destinação do órgão ou entidade.

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, baseado em estimativas de uso. Nesse sentido, nenhum documento deve ser conservado por tempo maior que o necessário.

A aplicação dos critérios de avaliação é feita com base na teoria das três idades e efetiva-se, primeiramente, nos arquivos correntes, a fim de se distinguirem os

[19] Ver Capítulo 2 da Parte I, *O que é gestão arquivística de documentos?*

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 na tabela de temporalidade e destinação.

A complexidade e a abrangência dos conhecimentos exigidos pelo processo de avaliação, que implica no estabelecimento de critérios de valor, requerem a participação de pessoas das diversas áreas profissionais do órgão ou entidade, conforme legislação vigente.

O sistema de gestão arquivística de documentos, particularmente no caso de um SIGAD, deve identificar a temporalidade e a destinação previstas para o documento no momento da captura e do registro, de acordo com os prazos e ações estabelecidos na tabela de temporalidade e destinação do órgão ou entidade. Essa informação deve ser registrada em um metadado associado ao documento.

O sistema de gestão arquivística de documentos também deve poder identificar os documentos que já cumpriram sua temporalidade, para implementar a destinação prevista. Se for um SIGAD, esse sistema deve ser capaz de listar os documentos que tenham cumprido o prazo previsto na tabela de temporalidade e destinação.

As determinações sobre a destinação devem ser aplicadas aos documentos, de forma sistemática, no curso das atividades rotineiras do órgão ou entidade. Essas determinações não podem ser implementadas em documentos que estejam com pendências, sob litígio ou investigação.

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

- retenção dos documentos, por um determinado período, no arquivo corrente do órgão ou entidade que os gerou;
- eliminação física;
- transferência;
- recolhimento para instituição arquivística.

### Eliminação

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

A eliminação deve ser precedida da elaboração da 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 deve sempre ser autorizada pela autoridade arquivística na sua esfera de competência;

- os documentos arquivísticos que estiverem pendentes, sob litígio ou investigação não podem ser destruídos;
- a eliminação deve 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, devem ser destruídas.

### Transferência

Transferência é a passagem de documentos do arquivo corrente para o arquivo intermediário, onde aguardarão o cumprimento dos prazos de guarda e a destinação final. Ao serem transferidos, os documentos devem ser acompanhados de listagem de transferência.

A transferência pode ser realizada de duas formas:

- transferência para uma área de armazenamento apropriada sob controle do órgão ou entidade que produziu o documento;
- transferência para uma instituição arquivística, que ficará responsável pela custódia do documento.

Quando os documentos transferidos ficam sob custódia de um órgão ou entidade diferente do que os produziu, a organização responsável pela custódia tem a obrigação de mantê-los e gerenciá-los de forma adequada, garantindo sua destinação final, preservação e acesso. Todas essas obrigações devem estar formalizadas em um contrato firmado entre o órgão ou entidade que produziu os documentos e o responsável por sua custódia.

### Recolhimento

Recolhimento é a entrada de documentos em arquivos permanentes de acordo com a jurisdição arquivística a que pertencem. Os documentos a serem recolhidos devem ser acompanhados de instrumentos que permitam sua identificação e controle, segundo a legislação vigente.[20]

Os procedimentos de transferência e recolhimento de arquivos digitais para instituição arquivística que impliquem na transposição desses documentos de um SIGAD para outro sistema informatizado devem adotar providências no que diz respeito a:

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

[20] Lei n. 8.159, de 8 de janeiro de 1991, e Resolução do CONARQ n. 2 do CONARQ, de 1995.

## 6.3 Pesquisa, localização e apresentação dos documentos

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

Em um SIGAD, a apresentação dos documentos consiste em exibi-los por meio de um ou mais dispositivos de apresentação, como monitor de vídeo, impressora, caixa de som etc. No âmbito do sistema de gestão arquivística de documentos, a pesquisa é feita utilizando-se instrumentos de busca, como guias, inventários, catálogos, repertórios e índices. Já em um SIGAD, a pesquisa se faz por meio de parâmetros predefinidos, selecionados entre as informações coletadas no momento do registro do documento e entre os metadados a ele associados.

Todos os recursos de pesquisa, localização e apresentação de documentos têm que ser submetidos a controles de acesso e segurança, que serão especificados a seguir.

## 6.4 Segurança: controle de acesso, trilhas de auditoria e cópias de segurança

O sistema de gestão arquivística deve prever controles de acesso e procedimentos de segurança que garantam a integridade dos documentos. Entre esses procedimentos, podem-se destacar o uso de controles técnicos e programáticos, diferenciando tipos de documentos, perfis de usuários e características de acesso aos dados, e a manutenção de trilhas de auditoria e de rotinas de cópias de segurança.

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

### Controle de acesso

O sistema de gestão arquivística precisa limitar ou autorizar o acesso a documentos por usuário e/ou grupos de usuários.

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 com relação às precauções de segurança, ou seja, se são considerados ostensivos ou sigilosos. No caso dos documentos sigilosos,[21] existem regras, normas e legislação[22] que estabelecem diferentes razões e graus de sigilo a serem atribuídos a cada documento, além de

[21] Lei n. 8.159/1991.

[22] Decreto n. 4.553, de 27 de dezembro de 2002, decreto n. 5.301, de 9 de dezembro de 2004, e lei n. 11.111, de 5 de maio de 2005.

definirem as autoridades competentes para fazê-lo (ver seção 6.1.4 – *Atribuição de restrição de acesso*).

Os documentos relativos ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, como, por exemplo, dossiês funcionais e prontuários médicos, estão sujeitos a restrições de acesso, conforme legislação específica.

Um sistema de gestão arquivística deve impedir que usuários não autorizados tenham acesso aos documentos classificados como sigilosos, isto é, submetidos às categorias de sigilo previstas em lei, bem como àqueles tidos como originalmente sigilosos. O acesso aos metadados dos documentos sigilosos depende de regulamentação interna do órgão ou entidade.

O monitoramento e mapeamento das permissões de acesso devem ser um processo contínuo em todos os sistemas de gestão arquivística 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, do que cada um pode acessar;
- identificação da precaução de segurança e da categoria de sigilo dos documentos;
- garantia de que somente os indivíduos autorizados tenham acesso aos documentos classificados e aos originalmente sigilosos;
- registro de todos os acessos, tentativas de acesso e uso dos documentos (visualização, impressão, transmissão e cópia para a área de transferência), com identificação de usuário, data, hora e, se possível, 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 e uso indevidos aos documentos. O grau de controle de acesso e o detalhamento do registro na trilha de auditoria dependem da natureza do órgão ou entidade e dos documentos produzidos.

### Trilha de auditoria

A trilha de auditoria é o conjunto de informações registradas que permite o rastreamento de intervenções ou tentativas de intervenção no documento arquivístico digital ou no SIGAD.

A trilha de auditoria deve registrar o movimento e o uso dos documentos arquivísticos dentro de um SIGAD (captura, registro, classificação, indexação, arquivamento, armazenamento, recuperação da informação, acesso e uso, preservação e destinação), informando quem operou, a data e a hora, e as ações realizadas. A trilha de auditoria tem o objetivo de fornecer informações sobre o

cumprimento das políticas e regras da gestão arquivística de documentos do órgão ou entidade, e serve para:

- identificar os autores de cada operação realizada nos documentos;
- prevenir a perda de documentos;
- monitorar todas as operações realizadas no SIGAD;
- garantir a segurança e a integridade do SIGAD.

No caso de procedimentos que exijam prazo a ser cumprido pelo órgão ou entidade, devem ser implementadas ações de rastreamento, de forma a:

- determinar os passos a serem dados em resposta às atividades ou ações registradas no documento;
- atribuir a uma pessoa a responsabilidade por cada ação;
- registrar a data em que uma ação deve ser executada e a data em que ocorreu.

### Cópias de segurança

O SIGAD deve prever controles para proporcionar a salvaguarda regular dos documentos arquivísticos e dos seus metadados. Deve também poder recuperá-los rapidamente em caso de perda devido a sinistro, falhas no sistema, contingência, quebra de segurança ou degradação do suporte. Esses mecanismos devem seguir a política de segurança da informação do órgão ou entidade.

Em sistemas de gestão arquivística de documentos convencionais, pode-se prever a reprodução de documentos em outros suportes como medida de segurança, como, por exemplo, pelos processos de microfilmagem e digitalização.

Nos sistemas de gestão arquivística de documentos digitais, o SIGAD deve prover meios de realização de cópias de segurança (becape, do inglês *backup*). Esse processo consiste na realização de cópias periódicas das informações com o propósito de restauração posterior, em caso de perda devido a falhas de *software*, *hardware* ou mesmo de acidentes. O processo reverso ao *backup* é a restauração (*restore*), que consiste em recuperar as informações para o ambiente de produção do SIGAD em um estado consistente.

Como o objetivo é restaurar o sistema em caso de falhas, as informações não são armazenadas por períodos muito longos (normalmente, até um ano). Dessa forma, o procedimento de cópias de segurança não pode ser confundido com uma estratégia de preservação de longo prazo.

### Segurança da infraestrutura

A natureza das medidas de segurança da infraestrutura de instalações do acervo digital diz respeito a requisitos operacionais e não é muito diferente daquela do acervo convencional. 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, e fornecimento estável de energia elétrica.

Deve haver controle contínuo para verificar se essas condições estão sendo atendidas;

- equipamentos contra incêndio devem estar presentes em toda a área de instalação e de acordo com as normas de segurança estabelecidas;
- os equipamentos contra incêndio devem ser verificados periodicamente e substituídos antes do término da vida útil prevista;
- o órgão ou entidade tem que prever instalações adequadas de para-raios, com procedimentos de manutenção periódica, seguindo a legislação e as normas técnicas estabelecidas;
- a área reservada à instalação do SIGAD deve ser compartimentada, com o objetivo de controlar o acesso às informações;
- as salas de computadores servidores são de uso exclusivo de pessoal autorizado e devem ter controle eletrônico de acesso;
- para acesso a áreas de segurança, identificações e credenciais de segurança têm de estar de acordo com as atribuições individuais e as regras de segurança do órgão ou entidade.

## 6.5 Armazenamento

As considerações e ações relativas ao armazenamento dos documentos arquivísticos convencionais e digitais permeiam todo o seu ciclo de vida. Esse armazenamento deve garantir a autenticidade e o acesso aos documentos pelo tempo estipulado na tabela de temporalidade e destinação.

Documentos de valor permanente, independentemente do formato, requerem um armazenamento criterioso desde o momento da sua produção, para garantir sua preservação no longo prazo.

Num cenário híbrido, isto é, que envolve ao mesmo tempo documentos arquivísticos convencionais e digitais, devem-se considerar requisitos de armazenamento que atendam igualmente às necessidades desses dois tipos de documentos.

As condições de armazenamento têm de levar em conta o volume e as propriedades físicas dos documentos. Devem ser projetadas considerando também a proteção contra acesso não autorizado e perdas por destruição, furto e sinistro.

No caso dos documentos arquivísticos digitais, os órgãos e entidades devem dispor de políticas e diretrizes para conversão ou migração desses 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 seção 6.6 – *Preservação*).

Os fatores mais importantes para a seleção das opções de armazenamento são:

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

- segurança dos documentos: as instalações de armazenamento (depósitos, arquivos, computadores) deverão prever a limitação de acesso aos documentos, como, por exemplo, o controle das áreas de armazenamento e sistemas de detecção de entrada não autorizada. O depósito deve estar localizado em área que não seja de risco. No caso de documentos digitais, devem ser previstos procedimentos que previnam a perda de documentos por falha do SIGAD (ver seção 6.4 – *Segurança*: cópias de segurança e segurança da infraestrutura);
- características físicas do suporte e do ambiente: fatores como tipo de suporte, peso, grau de contaminação do documento e do ambiente, temperatura e umidade influenciam a adequação das condições de armazenamento. Nesse sentido, devem ser adotados procedimentos – como controle e verificação do tempo de vida útil e da estabilidade dos suportes – para prevenir danos aos documentos. É importante que os meios de acondicionamento sejam robustos e adequados ao formato e à quantidade de documentos. As áreas de depósito devem ter amplitude adequada, estabilidade de temperatura e de níveis de umidade, proteção contra sinistro, contaminação (isótopos radioativos, toxinas, mofo) e infestação de insetos ou micro-organismos. Os documentos digitais devem passar, periodicamente, pela troca de suporte, isto é, as informações contidas num suporte devem ser transferidas para outro. Essa técnica é denominada atualização (*refreshing*).
- frequência de uso: o uso mais ou menos frequente dos documentos deve ser levado em conta na seleção das opções de armazenamento. No caso dos documentos convencionais, as opções envolvem acondicionamento (pastas suspensas, caixas) e localização dos depósitos (próximos ou distantes da área de trabalho). Já em relação aos documentos digitais, as opções podem envolver armazenamento *on-line* (acesso imediato) ou *off-line*, nas chamadas "mídias removíveis" de armazenamento (disco óptico, fita magnética), em diferentes graus de disponibilidade e velocidade.
- custo relativo das opções de armazenamento dos documentos: além do custo dos dispositivos de armazenamento, devem ser considerados, para sua manipulação, os valores dos equipamentos e do *software* de controle. Pelo previsível alto custo, pode-se considerar a possibilidade de terceirização do armazenamento. Nesse caso, porém, surgem outros problemas, como garantias legais sobre a custódia, restrições de acesso e capacidade tecnológica. Recursos como o uso de criptografia podem impedir o acesso não autorizado, assim como a utilização de *checksum*[23] permite rastrear eventuais comprometimentos de conteúdo.

Os documentos digitais são armazenados em dispositivos eletrônicos, magnéticos e ópticos. É interessante notar que, do ponto de vista tecnológico, distinguem-se três tipos de memória, em ordem decrescente de preço e velocidade de acesso:

- memória primária;
- memória secundária;
- memória terciária.

[23] Valor calculado a partir dos dados que permite verificar se houve alteração.

A memória primária é essencial a qualquer sistema computacional. É nela que *software* e dados são armazenados durante a execução. Representantes típicas dessa classe são as memórias RAM (*random access memory*), memórias extremamente rápidas. Seu conteúdo é de natureza dinâmica, volátil, e permanece registrado apenas durante a execução do *software*.

A memória secundária apresenta volume maior de armazenamento que a primária, sendo, por outro lado, mais lenta. Não é volátil. São exemplos os discos rígidos magnéticos (*hard disk*, HD), que podem ser usados isoladamente ou combinados em *disk arrays.* Diversas tecnologias permitem, com o uso de *disk arrays,* obter maior desempenho e confiabilidade do que seria possível com discos isolados.

A 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 com a perda de dados é superior ao preço das mídias que fisicamente os contêm.

As memórias secundária e terciária são adequadas ao armazenamento.

## 6.6 Preservação

Os documentos arquivísticos têm de se manter acessíveis e utilizáveis pelo tempo que for necessário, garantindo-se sua longevidade, funcionalidade e acesso contínuo. Devem ser asseguradas as características dos documentos, tais como autenticidade e acessibilidade, pela adoção de estratégias institucionais e técnicas proativas de produção e preservação que garantam sua perenidade. Essas estratégias são estabelecidas por uma política de preservação.

Tradicionalmente, a preservação de documentos arquivísticos concentra-se na obtenção da estabilidade do suporte da informação. Nos documentos convencionais, conteúdo e suporte estão intrinsecamente ligados, de modo que a manutenção do suporte garante a preservação do documento. Por outro lado, nos documentos digitais, o foco da preservação é a manutenção do acesso, que pode implicar mudança de suporte e formato, bem como atualização do ambiente tecnológico. A fragilidade do suporte digital e a obsolescência tecnológica de *hardware*, *software* e formato exigem intervenções periódicas.

As estratégias de preservação de documentos arquivísticos devem ser selecionadas com base em sua capacidade de manter as características desses documentos e na avaliação custo-benefício. Podem incluir monitoramento e controle ambiental, restrições de acesso, cuidados no manuseio direto e obtenção de suportes e materiais mais duráveis (papel, tinta, disco óptico, fita magnética).

No caso específico dos documentos digitais, essas estratégias incluem a prevenção da obsolescência tecnológica e de danos físicos ao suporte, por meio de procedimentos de migração, como atualização (*refreshing*) e conversão.[24]

[24] Ver *Glossário*.

Outras técnicas utilizadas na preservação de documentos digitais são emulação, encapsulamento e preservação da tecnologia. A adoção de formatos digitais abertos configura-se, adicionalmente, como medida de preservação recomendável e necessária.

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

O desenvolvimento de novas tecnologias pode tornar disponíveis outros procedimentos para preservar documentos digitais por longos períodos.

As estratégias de preservação de documentos digitais e dos respectivos metadados devem ser formuladas e integradas ao SIGAD desde a fase de elaboração do projeto do sistema. Só assim será possível garantir o uso e o acesso aos documentos digitais durante todo o período previsto para sua guarda.

## 7 INSTRUMENTOS UTILIZADOS NA GESTÃO ARQUIVÍSTICA DE DOCUMENTOS

É necessário o desenvolvimento de uma série de instrumentos para apoiar os procedimentos e operações técnicas de gestão arquivística de documentos.

### Instrumentos principais

- plano de classificação, codificado ou não, baseado nas funções e atividades do órgão ou entidade;
- tabela de temporalidade e destinação;
- manual de gestão arquivística de documentos;
- esquema de classificação referente à segurança e ao acesso aos documentos.

### Instrumentos adicionais

- glossário;
- vocabulário controlado;
- tesauro.

Outros instrumentos que não são específicos da gestão arquivística de documentos, mas podem apoiar as operações de gestão:

- relatório de análise do contexto jurídico-administrativo do órgão ou entidade;
- relatório dos riscos que envolvem as atividades desenvolvidas pelo órgão ou entidade;
- plano de contingência e plano de prevenção contra desastres;
- estrutura organizacional e delegação de competências do órgão ou entidade;
- registro dos funcionários e das permissões de acesso aos sistemas do órgão ou entidade.

## 7.1 Plano de classificação e código de classificação

Um plano de classificação é um 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.[25]

A estruturação de um plano de classificação pode ser facilitada pela utilização de códigos (numéricos ou alfanuméricos) para designar as classes, constituindo um código de classificação.

O código de classificação de documentos é um instrumento de trabalho utilizado para classificar todo e qualquer documento produzido ou recebido por um órgão ou entidade no exercício de suas funções e atividades.

A classificação é utilizada para agrupar os documentos a fim de contextualizá-los, agilizar sua recuperação e facilitar tanto as tarefas de destinação (eliminação ou recolhimento dos documentos) como as de acesso.

O número de níveis de classificação varia de acordo com o órgão ou entidade e envolve os seguintes fatores:

- natureza das atividades desenvolvidas;
- tamanho do órgão ou entidade;
- complexidade da estrutura organizacional;
- tecnologia utilizada.

## 7.2 Tabela de temporalidade e destinação

A tabela de temporalidade e destinação é um instrumento arquivístico que determina prazos de guarda tendo em vista a transferência, recolhimento e eliminação de documentos.

A elaboração da tabela de temporalidade e destinação deve envolver a autoridade administrativa, o arquivista ou o responsável pela guarda de documentos, os profissionais das áreas jurídicas e financeiras, além de profissionais ligados ao campo de conhecimento de que tratam os documentos objeto da avaliação e outros que se façam necessários.

No setor público, a aplicação da tabela de temporalidade e destinação deve estar condicionada à sua aprovação pela instituição arquivística pública em sua específica esfera de competência.

A tabela de temporalidade e destinação deve contemplar as atividades-meio e as atividades-fim. Sua estrutura básica deve apresentar os seguintes itens:

- identificador de classe;
- prazos de guarda nas fases corrente e intermediária;
- destinação final (eliminação ou guarda permanente);
- observações necessárias a sua aplicação.

[25] Cf. *Dicionário Brasileiro de Terminologia Arquivística*, p. 132.

Deve-se elaborar um índice alfabético para agilizar a localização dos assuntos no plano ou código e na tabela.

A definição dos prazos de guarda no sistema de gestão arquivística de documentos de um órgão ou entidade tem por finalidade:

- conservar os documentos necessários ao cumprimento de obrigações legais e de prestação de contas;
- conservar os documentos importantes para a memória corporativa;
- eliminar os documentos que não são mais necessários;
- atender às necessidades e interesses de pessoas ou instituições externas ao órgão ou entidade por meio das seguintes ações:
    - identificação dos interesses legítimos de terceiros na preservação dos documentos arquivísticos. Os interessados podem ser pessoas e organizações afetadas pelas ações ou decisões do órgão ou entidade ou que precisam dos seus documentos arquivísticos para cumprir suas funções como auditores, entidades investigativas, autoridades arquivísticas ou pesquisadores;
    - identificação e avaliação dos ganhos legais, financeiros, políticos, sociais e outros que o órgão ou entidade possa ter na preservação dos documentos arquivísticos para servir aos interesses da pesquisa e da sociedade como um todo;
    - cumprimento dos regulamentos da autoridade arquivística, na sua esfera de competência.

O prazo de guarda estabelecido para a fase corrente corresponde ao período em que o documento é frequentemente consultado, exigindo sua permanência junto às unidades organizacionais.

O prazo de guarda estabelecido para a fase intermediária corresponde ao período em que o documento ainda é necessário à administração, porém com uso pouco frequente, podendo, então, ser transferido para depósitos em outro local, embora permaneça à disposição do órgão produtor.

## *7.3 Manual de gestão arquivística de documentos*

O órgão ou entidade deve elaborar um manual com o objetivo de estabelecer procedimentos regulares no tocante à produção, tramitação, arquivamento e destinação dos documentos arquivísticos, de acordo com as normas e a legislação vigente. Esse manual deve contemplar todos os tipos de documentos necessários à condução das atividades do órgão ou entidade, independentemente do suporte, incluindo atividades-meio e atividades-fim.

O manual pode compreender os seguintes pontos:

- definição e identificação de todos os documentos arquivísticos produzidos e identificação e separação dos documentos não arquivísticos, como documentos pessoais, cópias extras, publicações, entre outros;
- classificação dos documentos de acordo com a atividade desenvolvida;

- classificação dos documentos quanto a segurança e sigilo, e sua desclassificação;
- estabelecimento da forma documental no que diz respeito a logomarca, título, numeração, local, data, origem, destinatário, assunto, anexos, normas de redação, formas de tratamento, assinatura, regras de digitação, rubrica, autenticação (selo, carimbo, carimbo de tempo, assinatura digital) etc.;
- procedimentos para captura, registro, autuação, recebimento, tramitação, distribuição, expedição e reprodução dos documentos;
- procedimentos para implementação do plano de classificação, da tabela de temporalidade e destinação e da destinação dos documentos.

## 7.4 Esquema de classificação de acesso e segurança

O esquema de classificação de acesso e segurança é a definição das categorias de usuários e das permissões de acesso e uso do sistema de gestão arquivística para produção, leitura, atualização e eliminação dos documentos.

O órgão ou entidade deve controlar quem está autorizado a acessar os documentos arquivísticos e em que circunstâncias esse acesso é permitido, dado que os documentos podem conter informação pessoal, comercial ou operacionalmente sensível. É igualmente necessário aplicar as restrições de acesso a usuários externos, de acordo com a legislação vigente.

## 7.5 Glossário

Glossário é um vocabulário afeito a uma área específica do conhecimento, que envolve definições conceituais, dispostas em ordem alfabética. Num glossário, os termos não guardam relações entre si.

Um glossário pode estar anexo ao plano de classificação e à tabela de temporalidade e destinação, bem como ao manual de gestão.

## 7.6 Vocabulário controlado e tesauro

A indexação dos documentos pode ser limitada à terminologia estabelecida no plano de classificação ou a outros controles adequados à complexidade dos documentos do órgão ou entidade, como tesauro ou vocabulário controlado.

Vocabulário controlado é um conjunto normalizado de termos que serve para indexação e recuperação da informação. Permite controlar a terminologia utilizada na indexação, estabelecendo os termos aceitos pelo órgão ou entidade e controlando o uso de sinônimos, homônimos, abreviaturas e acrônimos. O significado dos termos não é definido, mas apenas algumas associações entre eles, como, por exemplo, a relação entre sinônimos.

Tesauro é uma lista controlada de termos ligados por meio de relações semânticas, hierárquicas, associativas ou de equivalência que cobre uma área específica do conhecimento. Em um tesauro, o significado do termo e as relações hierárquicas com outros termos são explicitados.

# Parte II

# Especificação de requisitos para sistemas informatizados de gestão arquivística de documentos (SIGAD)

## Aspectos de funcionalidade

### 1 ORGANIZAÇÃO DOS DOCUMENTOS ARQUIVÍSTICOS: PLANO DE CLASSIFICAÇÃO E MANUTENÇÃO DOS DOCUMENTOS

A organização dos documentos arquivísticos é feita com base num plano ou código de classificação. Tal instrumento constitui-se no núcleo central de qualquer SIGAD. Por meio dele, são estabelecidas a hierarquia e a relação orgânica dos documentos, devidamente demonstradas na forma como eles são organizados em unidades de arquivamento.[26]

Os documentos produzidos ou recebidos no decorrer das atividades do órgão ou entidade são acumulados em unidades de arquivamento e organizados, de forma hierárquica, em classes,[27] de acordo com um plano de classificação.[28] Como não há, necessariamente, o agrupamento físico dos documentos digitais, eles são reunidos em unidades lógicas de arquivamento por meio de metadados, como, por exemplo, número identificador, título e código.

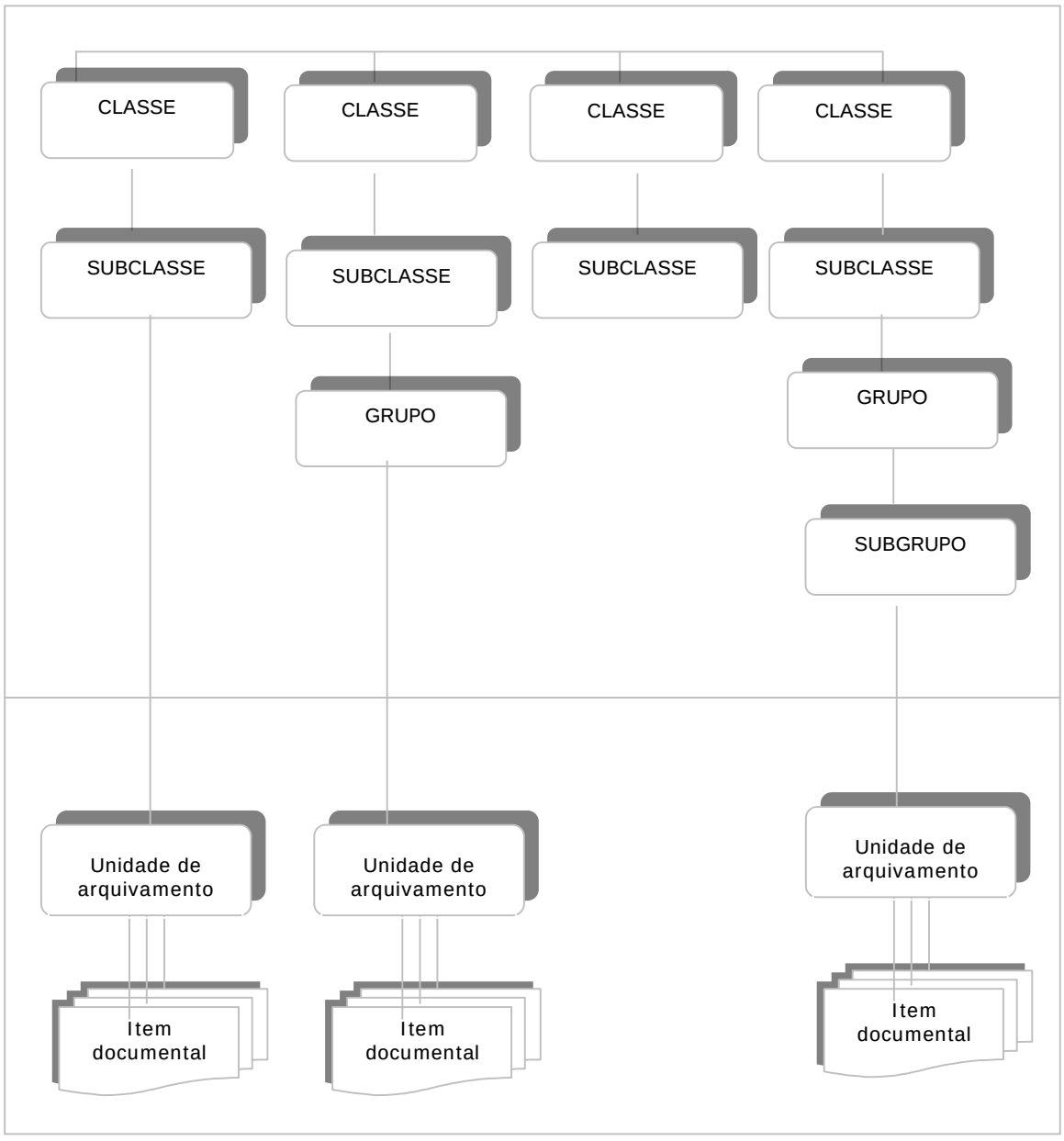
As atividades de gestão de documentos, como controle de temporalidade e destinação, são feitas com base nas unidades de arquivamento. Dessa forma, no momento do arquivamento, os documentos devem ser inseridos em uma unidade de arquivamento, que está subordinada, hierarquicamente, ao plano de classificação. O diagrama a seguir exemplifica esta organização hierárquica dos documentos.

[26] Unidade de arquivamento é o documento considerado para fins de classificação, arranjo, armazenamento e notação. Uma unidade de arquivamento pode ser um dossiê, processo ou pasta em que estejam reunidos documentos sob o mesmo código de classificação, como, por exemplo, as folhas de ponto de determinado ano, relatórios de atividades de um período específico ou atas de reunião.

[27] Daqui em diante, nesta seção, deve-se entender *classe* como um termo genérico que inclui os demais níveis do plano de classificação, isto é, subclasse, grupo e subgrupo.

[28] A Resolução do CONARQ n. 14, de 28 de outubro de 2001, aprova a versão revisada e ampliada da Resolução do CONARQ n. 4, de 28 de março de 1996, que dispõe sobre a classificação, temporalidade e destinação de documentos de arquivo relativos às atividades-meio da administração pública. Esse instrumento também orienta a elaboração de código de classificação e tabela de temporalidade e destinação de documentos para as atividades finalísticas.

## Diagrama de organização dos documentos



## 1.1 Configuração e administração do plano de classificação no SIGAD

Os requisitos desta seção referem-se às funcionalidades do sistema para apoiar a configuração do plano de classificação no SIGAD, ou seja, como desenhar um plano de classificação em um SIGAD.

| Referência | Requisito | Obrig[29] |
|---|---|---|
| 1.1.1 | Um SIGAD tem que incluir e ser compatível com o plano de classificação do órgão ou entidade.<br><br>*O plano de classificação dos integrantes do SINAR deve estar de acordo com a legislação e ser aprovado pela instituição arquivística na esfera de competência específica.* | O |
| 1.1.2 | Um SIGAD tem que garantir a criação de classes, subclasses, grupos e subgrupos nos níveis do plano de classificação de acordo com o método de codificação adotado.<br><br>*Por exemplo, quando se adotar o método decimal para codificação, cada classe pode ter no máximo dez subordinações, e assim sucessivamente.* | O |
| 1.1.3 | Um SIGAD tem que permitir a usuários autorizados acrescentar novas classes sempre que necessário. | O |
| 1.1.4 | Um SIGAD tem que registrar a data de abertura de uma nova classe no respectivo metadado. | O |
| 1.1.5 | Um SIGAD tem que registrar a mudança de nome de uma classe já existente no respectivo metadado. | O |
| 1.1.6 | Um SIGAD tem que permitir o deslocamento de uma classe inteira, incluídas as subclasses, grupo, subgrupos e documentos nela classificados, para outro ponto do plano de classificação. Nesse caso, é necessário fazer o registro do deslocamento nos metadados do plano de classificação. | O |
| 1.1.7 | Um SIGAD deve permitir que usuários autorizados tornem inativa uma classe em que não sejam mais classificados documentos. | AD |
| 1.1.8 | Um SIGAD tem que permitir que um usuário autorizado apague uma classe inativa.<br><br>*Só pode ser apagada uma classe que não tenha documentos nela classificados*. | O |

[29] O campo *obrigatoriedade* apresenta a seguinte classificação: *O – obrigatório; AD – altamente desejável; F – facultativo.*

| Referência | Requisito | Obrig[29] |
|---|---|---|
| 1.1.9 | Um SIGAD tem que impedir a eliminação de uma classe que tenha documentos nela classificados. Essa eliminação pode ocorrer a partir do momento em que todos os documentos ali classificados tenham sido recolhidos ou eliminados, e seus metadados apagados, ou que esses documentos tenham sido reclassificados. | O |
| 1.1.10 | Um SIGAD tem que permitir a associação de metadados às classes, conforme estabelecido no padrão de metadados, e deve restringir a inclusão e alteração desses mesmos metadados somente a usuários autorizados. | O |
| 1.1.11 | Um SIGAD tem que disponibilizar pelo menos dois mecanismos de atribuição de identificadores a classes do plano de classificação, prevendo a possibilidade de se utilizar ambos, separadamente ou em conjunto, na mesma aplicação:<br>• atribuição de um código numérico ou alfanumérico;<br>• atribuição de um termo que identifique cada classe. | O |
| 1.1.12 | Um SIGAD deve prever um atributo associado às classes para registrar a permissão de uso daquela classe para classificar um documento.<br>*Em algumas classes, não é permitido incluir documentos. Nesse caso, os documentos devem ser classificados apenas nos níveis subordinados.*<br>*Por exemplo, no código de classificação previsto na Resolução do CONARQ n. 14:*<br>*Não é permitido classificar documentos no grupo 021 (ADMINISTRAÇÃO GERAL:PESSOAL:RECRUTAMENTO E SELEÇÃO). Os documentos de recrutamento e seleção devem ser classificados nos subgrupos 021.1 (ADMINISTRAÇÃO GERAL:PESSOAL: RECRUTAMENTO E SELEÇÃO: CANDIDATOS A CARGO E EMPREGO PÚBLICOS) e 021.2 (ADMINISTRAÇÃO GERAL:PESSOAL: RECRUTAMENTO E SELEÇÃO:EXAMES DE SELEÇÃO).* | AD |
| 1.1.13 | Um SIGAD tem que utilizar o termo completo para identificar uma classe.<br>*Entende-se por termo completo toda a hierarquia referente àquela classe. Por exemplo:*<br>*MATERIAL:AQUISIÇÃO:MATERIAL PERMANENTE:COMPRA*<br>*MATERIAL:AQUISIÇÃO:MATERIAL DE CONSUMO:COMPRA* | O |
| 1.1.14 | Um SIGAD tem que assegurar que os termos completos, que identificam cada classe, sejam únicos no plano de classificação. | O |
| 1.1.15 | Um SIGAD pode prever pesquisa e navegação na estrutura do plano de classificação por meio de uma interface gráfica. | F |

| Referência | Requisito | Obrig[29] |
|---|---|---|
| 1.1.16 | Um SIGAD deve ser capaz de importar e exportar, total ou parcialmente, um plano de classificação.<br>*Ver item 12 - Interoperabilidade* | AD |
| 1.1.17 | Um SIGAD tem que prover funcionalidades para elaboração de relatórios de apoio à gestão do plano de classificação, incluindo a capacidade de:<br>• gerar relatório completo do plano de classificação;<br>• gerar relatório parcial do plano de classificação a partir de um ponto determinado na hierarquia;<br>• gerar relatório dos documentos ou dossiês/processos classificados em uma ou mais classes do plano de classificação;<br>• gerar relatório de documentos classificados por unidade administrativa. | O |
| 1.1.18 | Um SIGAD deve possibilitar a consulta ao plano de classificação a partir de qualquer atributo ou combinação de atributos, e gerar relatório com os resultados obtidos. | AD |

## 1.2 Classificação e metadados das unidades de arquivamento

Os requisitos desta seção referem-se à formação, classificação e reclassificação das unidades de arquivamento (dossiês/processos e pastas) e à associação de metadados.

| Referência | Requisito | Obrig |
|---|---|---|
| 1.1.19 | Um SIGAD tem que permitir a classificação das unidades de arquivamento somente nas classes autorizadas.<br>*Ver requisito 1.1.12* | O |
| 1.1.20 | Um SIGAD tem que permitir a classificação de um número ilimitado de unidades de arquivamento dentro de uma classe. | O |
| 1.1.21 | Um SIGAD tem que utilizar o termo completo da classe para identificar uma unidade de arquivamento, tal como especificado no item 1.1.13. | O |
| 1.1.22 | Um SIGAD tem que permitir a associação de metadados às unidades de arquivamento e deve restringir a inclusão e alteração desses metadados a usuários autorizados. | O |
| 1.1.23 | Um SIGAD tem que associar os metadados das unidades de arquivamento conforme estabelecido no padrão de metadados. | O |

| Referência | Requisito | Obrig |
|---|---|---|
| 1.1.24 | Um SIGAD tem que permitir que uma nova unidade de arquivamento herde, da classe em que foi classificada, alguns metadados predefinidos.<br>*Exemplos desta herança são prazos de guarda previstos na*<br>*tabela de temporalidade e destinação e restrição de acesso.* | O |
| 1.1.25 | Um SIGAD deve relacionar os metadados herdados de forma que uma alteração no metadado de uma classe seja automaticamente incorporada à unidade de arquivamento que herdou esse metadado. | AD |
| 1.1.26 | Um SIGAD pode permitir a alteração conjunta de um determinado metadado em um grupo de unidades de arquivamento previamente selecionado. | F |
| 1.1.27 | Um SIGAD tem que permitir que uma unidade de arquivamento e seus respectivos volumes e/ou documentos sejam reclassificados por um usuário autorizado e que todos os documentos já inseridos permaneçam nas unidades de arquivamento e nos volumes que estão sendo transferidos, mantendo a relação entre documentos, volumes e unidades de arquivamento. | O |
| 1.1.28 | Quando uma unidade de arquivamento ou documento é reclassificado, um SIGAD deve manter o registro de suas posições anteriores à reclassificação, de forma a manter um histórico. | AD |
| 1.1.29 | Quando uma unidade de arquivamento ou documento é reclassificado, um SIGAD deve permitir que o administrador introduza as razões para a reclassificação. | AD |
| 1.1.30 | Um SIGAD pode permitir que os usuários criem referências cruzadas para unidades de arquivamento afins. | F |

## 1.3 Gerenciamento dos dossiês/processos

Os requisitos desta seção referem-se ao gerenciamento dos documentos arquivísticos no que diz respeito a controles de abertura e encerramento de dossiês/processos e seus respectivos volumes, e à inclusão de novos documentos nesses dossiês/processos e seus volumes ou nas pastas virtuais.

| Referência | Requisito | Obrig |
|---|---|---|
| 1.1.31 | Um SIGAD tem que registrar nos metadados as datas de abertura e de encerramento do dossiê/processo.<br>*Essa data pode servir de parâmetro para aplicação dos prazos de guarda e destinação do dossiê/processo.* | O |

| Referência | Requisito | Obrig |
|---|---|---|
| 1.1.32 | Um SIGAD tem que permitir que um dossiê/processo seja encerrado por meio de procedimentos regulamentares e somente por usuários autorizados. | O |
| 1.1.33 | Um SIGAD tem que permitir a consulta aos dossiês/processos já encerrados por usuários autorizados. | O |
| 1.1.34 | Um SIGAD tem que impedir o acréscimo de novos documentos a dossiês/processos já encerrados.<br><br>Dossiês/*processos encerrados devem ser reabertos para receber novos documentos*. | O |
| 1.1.35 | Um SIGAD deve ser capaz de registrar múltiplas entradas para um documento digital (objeto digital) em mais de um dossiê/processo ou pasta, sem a duplicação física desse documento.<br><br>*Quando um documento digital estiver associado a mais de um dossiê ou processo, o SIGAD deve criar um registro para cada referência desse documento. Cada registro estará vinculado ao mesmo objeto digital.* | AD |
| 1.1.36 | Um SIGAD tem que impedir sempre a eliminação de uma unidade de arquivamento digital ou de qualquer parte de seu conteúdo, a não ser quando estiver de acordo com a tabela de temporalidade e destinação de documentos.<br><br>*A eliminação será devidamente registrada em trilha de auditoria.* | O |
| 1.1.37 | Um SIGAD tem que garantir sempre a integridade da relação hierárquica entre classe, dossiê/processo, volume e documento, e entre classe, pasta e documento, independentemente de atividades de manutenção, ações do usuário ou falha de componentes do sistema.<br><br>*Em hipótese alguma pode o SIGAD permitir que uma ação do usuário ou falha do sistema dê origem a inconsistência em sua base de dados.* | O |

## 1.4 Requisitos adicionais para o gerenciamento de processos

A formação e manutenção de processos no setor público obedecem a regras específicas, que os diferenciam dos dossiês e apoiam a preservação de sua autenticidade. O detalhamento dessas regras está previsto em normas e legislação específica, que deverão ser respeitadas pelo órgão ou entidade, de acordo com sua esfera e âmbito de atuação.

Esta seção inclui requisitos específicos para a gestão dos processos, aplicáveis caso o SIGAD capture esse tipo de documento.

| Referência | Requisito | Obrig |
|---|---|---|
| 1.1.38 | Um SIGAD tem que prever a formação/autuação de processos,[30] por usuário autorizado conforme estabelecido em legislação específica. | O |
| 1.1.39 | Um SIGAD deve prever funcionalidades para apoiar a pesquisa sobre a existência de processo relativo à mesma ação ou interessado. | AD |
| 1.1.40 | Um SIGAD tem que prever que os documentos integrantes do processo digital recebam numeração sequencial sem falhas, não se admitindo que documentos diferentes recebam a mesma numeração. | O |
| 1.1.41 | Um SIGAD tem que controlar a renumeração dos documentos integrantes de um processo digital.<br><br>*Este requisito tem por objetivo impedir a exclusão não autorizada de documentos de um processo.*<br><br>*Casos especiais que autorizem a renumeração devem obedecer à legislação específica na devida esfera e âmbito de competência.* | O |
| 1.1.42 | Um SIGAD tem que prever procedimentos para juntada de processos segundo a legislação específica na devida esfera e âmbito de competência. A juntada pode ser por *anexação*[31] ou *apensação*.[32]<br><br>Este procedimento deve ser registrado nos metadados do processo. | O |
| 1.1.43 | Um SIGAD tem que prever procedimentos para desapensação de processos segundo a legislação específica na devida esfera e âmbito de competência.<br><br>Esse procedimento deve ser registrado nos metadados do processo. | O |
| 1.1.44 | Um SIGAD tem que prever procedimentos para desentranhamento de documentos integrantes de um processo, segundo norma específica na devida esfera e âmbito de competência.<br><br>Esse procedimento deve ser registrado nos metadados do processo. | O |

[30] Ver *Glossário*.

[31] Juntada por anexação é a união definitiva e irreversível de um ou mais processos ou documentos a outro processo considerado principal, desde que pertençam ao mesmo interessado e contenham o mesmo assunto.

[32] Juntada por apensação é a união provisória de um ou mais processos a um processo mais antigo, mantendo cada um a sua numeração específica, destinada ao estudo e à uniformidade de tratamento em matérias semelhantes, tendo ou não o mesmo interessado.

| Referência | Requisito | Obrig |
|---|---|---|
| 1.1.45 | Um SIGAD tem que prever procedimentos para desmembramento de documentos integrantes de um processo, segundo norma específica na devida esfera e âmbito de competência.<br><br>Esse procedimento deve ser registrado nos metadados do processo. | O |
| 1.1.46 | Um SIGAD tem que prever o encerramento[33] dos processos incluídos seus volumes e metadados. | O |
| 1.1.47 | Um SIGAD tem que prever o desarquivamento para reativação dos processos, por usuário autorizado e obedecendo a procedimentos legais e administrativos.<br><br>*Para manter a integridade do processo, somente o último volume receberá novos documentos ou peças.* | O |

## 1.5 Volumes: abertura, encerramento e metadados

Em alguns casos os dossiês/pro cessos são compartimentados em volumes ou partes, de acordo com normas e instruções estabelecidas. Essa divisão não se baseia no conteúdo intelectual dos dossiês/processos, mas em outros critérios, como dimensão, número de documentos, períodos de tempo etc. A prática tem como objetivo facilitar o gerenciamento físico dos dossiês/processos.

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

| Referência | Requisito | Obrig |
|---|---|---|
| 1.1.48 | Um SIGAD deve ser capaz de gerenciar volumes para subdividir dossiês/processos, fazendo a distinção entre dossiês/processos e volumes. | AD |
| 1.1.49 | Um SIGAD deve permitir a associação de metadados aos volumes e restringir a inclusão e alteração desses metadados a usuários autorizados. | AD |
| 1.1.50 | Um SIGAD tem que permitir que um volume herde, automaticamente, do dossiê/processo ao qual pertence, alguns metadados predefinidos, como, por exemplo, procedência, classes e temporalidade. | O |
| 1.1.51 | Um SIGAD tem que permitir a abertura de volumes para qualquer dossiê/processo que não esteja encerrado. | O |
| 1.1.52 | Um SIGAD deve permitir o registro de metadados correspondentes às datas de abertura e encerramento de volumes. | AD |

[33] Na administração pública federal, o processo é arquivado; o que se encerra é a ação.

| Referência | Requisito | Obrig |
|---|---|---|
| 1.1.53 | Um SIGAD tem que assegurar que um volume conterá somente documentos. Não é permitido que um volume contenha outro volume ou outro dossiê/processo. | O |
| 1.1.54 | Um SIGAD tem que permitir que um volume seja encerrado por meio de procedimentos regulamentares e apenas por usuários autorizados. | O |
| 1.1.55 | Um SIGAD tem que assegurar que, ao ser aberto um novo volume, o precedente seja automaticamente encerrado.<br>*Apenas o volume produzido mais recentemente pode estar aberto; os demais volumes existentes no dossiê/processo têm que estar fechados.* | O |
| 1.1.56 | Um SIGAD tem que impedir a reabertura, para acréscimo de documentos, de um volume já encerrado. | O |

## 1.6 Gerenciamento de documentos e processos/dossiês arquivísticos convencionais e híbridos

O arquivo de uma organização pode conter documentos ou dossiês/processos digitais e convencionais. Um SIGAD deve registrar os documentos ou dossiês/processos convencionais, que devem ser classificados com base no mesmo plano de classificação usado para os digitais, e ainda possibilitar a gestão de documentos ou dossiês/processos híbridos. Os documentos ou dossiês/processos híbridos são formados por uma parte digital e outra convencional.

| Referência | Requisito | Obrig |
|---|---|---|
| 1.1.57 | Um SIGAD tem que capturar documentos ou dossiês/processos convencionais e gerenciá-los da mesma forma que os digitais.<br>*Para o conceito de captura, ver item 3.* | O |
| 1.1.58 | Um SIGAD tem que ser capaz de gerenciar a parte convencional e a parte digital integrantes de dossiês/processos híbridos, associando-as com o mesmo número identificador atribuído pelo sistema e o mesmo título, além de indicar que se trata de um documento arquivístico híbrido. | O |
| 1.1.59 | Um SIGAD tem que permitir que um conjunto específico de metadados seja configurado para os documentos ou dossiês/processos convencionais e incluir informações sobre o local de arquivamento. | O |
| 1.1.60 | Um SIGAD tem que dispor de mecanismos para acompanhar a movimentação do documento arquivístico convencional, de forma que fique evidente para o usuário a localização atual do documento. | O |

| Referência | Requisito | Obrig |
|---|---|---|
| 1.1.61 | Um SIGAD tem que ser capaz de oferecer ao usuário funcionalidades para solicitar ou reservar a consulta a um documento arquivístico convencional, enviando uma mensagem para o detentor atual do documento ou para o administrador. | O |
| 1.1.62 | Um SIGAD pode incluir mecanismos de impressão e reconhecimento de códigos de barras para automatizar a introdução de dados e acompanhar a movimentação de documentos ou dossiês/processos convencionais. | F |
| 1.1.63 | Um SIGAD tem que assegurar que a recuperação de um documento ou dossiê/processo híbrido permita, igualmente, a recuperação dos metadados da parte digital e da convencional. | O |
| 1.1.64 | Sempre que os documentos ou dossiês/processos híbridos estiverem classificados quanto ao grau de sigilo, um SIGAD tem que garantir que a parte convencional e a parte digital correspondente recebam a mesma classificação de sigilo. | O |
| 1.1.65 | Um SIGAD tem que poder registrar na trilha de auditoria todas as alterações efetuadas nos metadados dos documentos ou dossiês/processos convencionais e híbridos. | O |

## 2 TRAMITAÇÃO E FLUXO DE TRABALHO

Os requisitos desta seção tratam apenas dos casos em que o SIGAD inclui recursos de automação de fluxo de trabalho (*workflow*).[34] Eles abrangem funções para controle do fluxo de trabalho e atribuição de metadados para registro da tramitação dos documentos, incluindo-se o *status* do documento (minuta, original ou cópia).

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

- tramitação do documento antes do seu registro/captura;
- tramitação após seu registro/captura;

As tecnologias de fluxo de trabalho transferem objetos digitais entre *participantes* sob o controle automatizado de um programa. São geralmente usadas para:

- gestão de processos ou tarefas, tais como registro e destinação de documentos e dossiês/processos;
- verificação e aprovação de documentos ou dossiês/processos antes do registro;
- encaminhamento de documentos ou dossiês/processos, de forma controlada, de um usuário para outro, com a identificação das ações a serem realizadas, como: “verificar documento” e “aprovar nova versão”;

[34] Ver *Glossário*.

- comunicação aos usuários sobre a disponibilidade de um documento arquivístico;
- distribuição de documentos ou dossiês/processos;
- publicação de documentos ou dossiês/processos na *web*.

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

## 2.1 Controle do fluxo de trabalho

| Referência | Requisito | Obrig |
|---|---|---|
| 2.1.1 | Um recurso de fluxo de trabalho de um SIGAD tem que fornecer os passos necessários para o cumprimento de trâmites preestabelecidos ou aleatórios. Nesse caso, cada passo significa o deslocamento de um documento ou dossiê/processo de um participante para outro, a fim de serem objeto de ações. | O |
| 2.1.2 | Um SIGAD tem que ter capacidade, sem limitações, de estabelecer o número necessário de trâmites nos fluxos de trabalho. | O |
| 2.1.3 | O fluxo de trabalho de um SIGAD tem que disponibilizar uma função para avisar um participante do fluxo de que um documento lhe foi enviado, especificando a ação necessária. | O |
| 2.1.4 | O fluxo de trabalho de um SIGAD deve permitir o uso do correio eletrônico, para que um usuário possa informar a outros usuários sobre documentos que requeiram sua atenção.<br>*Esse requisito requer a integração com um sistema de correio eletrônico existente.* | AD |
| 2.1.5 | O recurso de fluxo de trabalho de um SIGAD tem que permitir que fluxos de trabalho pré-programados sejam definidos, alterados e mantidos exclusivamente por usuário autorizado. | O |
| 2.1.6 | O administrador deve poder autorizar usuários individuais a redistribuir tarefas ou ações de um fluxo de trabalho a um usuário ou grupo diferente do previsto.<br>*Um usuário pode precisar enviar um documento a outro usuário, devido ao seu conteúdo específico ou caso o usuário responsável se encontre em licença.* | AD |

| Referência | Requisito | Obrig |
|---|---|---|
| 2.1.7 | Um recurso de fluxo de trabalho de um SIGAD tem que registrar na trilha de auditoria todas as alterações ocorridas neste fluxo. | O |
| 2.1.8 | Um recurso de fluxo de trabalho de um SIGAD tem que registrar a tramitação de um documento a fim de que os usuários possam conhecer a situação de cada um no processo. | O |
| 2.1.9 | Um recurso de fluxo de trabalho de um SIGAD deve gerir os documentos em filas de espera que possam ser examinadas e controladas pelo administrador. | AD |
| 2.1.10 | Um recurso de fluxo de trabalho de um SIGAD deve ter a capacidade de deixar que os usuários visualizem a fila de espera de trabalhos a eles destinados e selecionem os itens a serem trabalhados. | AD |
| 2.1.11 | Um recurso de fluxo de trabalho de um SIGAD deve fornecer fluxos condicionais de acordo com os dados de entrada do usuário ou a partir dos dados do sistema.<br><br>*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 a outro, conforme os dados de entrada do participante anterior; ou a definição do fluxo pode depender de um valor calculado pelo sistema.* | AD |
| 2.1.12 | Um recurso de fluxo de trabalho de um SIGAD tem que fornecer um histórico de movimentação dos documentos.<br><br>*O histórico de movimentação corresponde a um conjunto de metadados de datas de entrada e saída, nomes de responsáveis, título do documento, providências etc.* | O |
| 2.1.13 | Um recurso de fluxo de trabalho de um SIGAD pode permitir que usuários autorizados interrompam ou suspendam temporariamente um fluxo com o objetivo de executar outro trabalho.<br><br>*O fluxo só prosseguirá com a autorização do usuário.* | F |
| 2.1.14 | Um recurso de fluxo de trabalho de um SIGAD tem que incluir processamento condicional, isto é, permitir que um fluxo de trabalho seja suspenso para aguardar a chegada de um documento e prossiga *automaticamente* quando este é recebido. | O |
| 2.1.15 | Um recurso de fluxo de trabalho de um SIGAD deve poder associar limites de tempo a trâmites e/ou procedimentos individuais em cada fluxo e comunicar os itens que expiraram de acordo com esses limites. | AD |
| 2.1.16 | Um recurso de fluxo de trabalho de um SIGAD tem que reconhecer indivíduos e grupos de trabalho como participantes. | O |

| Referência | Requisito | Obrig |
|---|---|---|
| 2.1.17 | Sempre que o participante for um grupo de trabalho, um recurso de fluxo de trabalho de um SIGAD deve prever a forma de distribuição dos documentos entre os membros do grupo. Essa distribuição pode ser de duas formas:<br>• de acordo com uma sequência circular predefinida, o SIGAD envia o próximo documento independentemente da conclusão da tarefa anterior; ou<br>• à medida que cada membro conclui a tarefa, o SIGAD lhe envia o próximo documento da fila do grupo. | AD |
| 2.1.18 | Um recurso de fluxo de trabalho de um SIGAD deve permitir que a captura de documentos desencadeie, automaticamente, fluxos de trabalho. | AD |
| 2.1.19 | Um recurso de fluxo de trabalho de um SIGAD tem que fornecer meios de elaboração de relatórios completos para permitir que gestores monitorem a tramitação dos documentos e o desempenho dos participantes. | O |
| 2.1.20 | Um recurso de fluxo de trabalho de um SIGAD tem que registrar a tramitação de um documento em seus metadados. Os metadados referentes à tramitação devem registrar data e hora de envio e recebimento, e a identificação do usuário. | O |
| 2.1.21 | Um SIGAD deve manter versões dos fluxos alterados e estabelecer vínculos entre os documentos já processados ou em processamento nos fluxos alterados. | AD |
| 2.1.22 | O SIGAD deve 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. | AD |

## 2.2 Controle de versões e do status do documento

Um SIGAD tem que ser capaz de, por meio de seu recurso de fluxo de trabalho, estabelecer o *status* do documento, isto é, se é uma minuta, original ou cópia. No caso dos documentos digitais, esse *status* é estabelecido de acordo com a rota do documento no SIGAD. Assim, por exemplo:

- um documento criado no espaço individual ou do grupo, mas não transmitido, é uma minuta;
- um documento transmitido do espaço individual ou do grupo para o espaço gerencial, onde não pode mais ser alterado, e deste para fora da instituição, será sempre recebido como um original e armazenado no espaço de origem (individual, do grupo ou gerencial) como uma última minuta. Isso porque a transmissão acrescenta metadados ao documento (como data e hora da transmissão) que o tornam mais completo;

- um documento enviado do espaço individual para o do grupo, para receber comentários, é uma minuta, que deve ter seu número de versões devidamente controlado;
- quando um usuário autorizado recupera um documento do espaço gerencial e o armazena em seu próprio espaço, ele cria uma cópia. O mesmo acontece nos casos em que o usuário reencaminha um documento para outro usuário.

| Referência | Requisito | Obrig |
|---|---|---|
| 2.2.1 | Um recurso de fluxo de trabalho de um SIGAD tem que ser capaz de registrar o *status* de transmissão do documento, ou seja, se é minuta, original ou cópia. | O |
| 2.2.2 | Um SIGAD tem que ser capaz de controlar as diversas versões de um documento que está tramitando. | O |
| 2.2.3 | Um SIGAD tem que ser capaz de associar e relacionar as diversas versões de um documento. | O |
| 2.2.4 | Um SIGAD tem que manter o identificador único do documento, e o controle de versões tem que ser registrado em metadados específicos. | O |

# 3 CAPTURA

A captura consiste em declarar um documento como documento arquivístico ao incorporá-lo num SIGAD por meio das ações de registro, classificação, indexação, atribuição de metadados e arquivamento.

O arquivamento envolve procedimentos diferentes no que diz respeito aos documentos digitais e convencionais. Enquanto os primeiros são arquivados dentro do SIGAD, os convencionais seguem a forma tradicional, isto é, em pastas ou equivalentes, sendo referenciados no SIGAD. Caso um documento convencional seja acompanhado de anexos digitais armazenados em mídia móvel (disquete, discos ópticos ou óptico-magnéticos, fitas magnéticas etc.), esses anexos podem ser mantidos tanto no SIGAD como nas referidas mídias.

A captura de documentos digitais em um SIGAD pode ser feita de diversas formas:

- captura individual de documento produzido em arquivo digital fora do SIGAD, em aplicativo e formato específicos (*.doc, .pdf, .rtf*) – o registro inicial é feito pelo usuário ao capturar o documento para o SIGAD;
- captura individual de documento produzido em *workflow* ou em outro sistema de forma integrada ao SIGAD – o registro e a anexação ao sistema de gestão podem ser automáticos, complementados pelo usuário do SIGAD;
- captura em lote – inclusão, no sistema, de um grupo de documentos do mesmo tipo oriundos de outro SIGAD ou de um GED. Ex.: faturas diárias, dossiês, processos.

## 3.1 Procedimentos gerais

| Referência | Requisito | Obrig |
|---|---|---|
| 3.1.1 | A captura tem que garantir a execução das seguintes funções:<br>• registrar e gerenciar todos os documentos convencionais;<br>• registrar e gerenciar todos os documentos digitais, independentemente do contexto tecnológico;<br>• classificar todos os documentos de acordo com o plano ou código de classificação;<br>• controlar e validar a introdução de metadados. | O |
| 3.1.2 | Um SIGAD tem que ser capaz de capturar documentos digitais das formas a seguir:<br>• captura de documentos produzidos dentro do SIGAD;<br>• captura de documento individual produzido em arquivo digital fora do SIGAD;<br>• captura de documento individual produzido em *workflow* ou em outros sistemas integrados ao SIGAD;<br>• captura de documentos em lote. | O |
| 3.1.3 | Um SIGAD pode automatizar a produção de documentos por meio da exibição de formulários e modelos predefinidos pelo programa de gestão arquivística de documentos. | F |
| 3.1.4 | Um SIGAD tem que aceitar o conteúdo do documento, bem como as informações que definem sua aparência, mantendo as associações entre os vários objetos digitais que compõem o documento, isto é, anexos e *links* de hipertexto. | O |
| 3.1.5 | Um SIGAD tem que permitir a inserção de todos os metadados obrigatórios e opcionais definidos na sua configuração e garantir que se mantenham associados ao documento.<br>Os metadados obrigatórios são:<br>• nome do arquivo digital;<br>• número identificador atribuído pelo sistema;<br>• data de produção;<br>• data e hora de transmissão e recebimento;<br>• data e hora da captura;<br>• título ou descrição abreviada;[35]<br>• classificação de acordo com o plano ou código de classificação; | O |

[35] Palavra ou frase que nomeia uma unidade arquivística. Pode ser formal, quando aparece explicitamente na unidade arquivística que está sendo descrita, ou atribuída.

| Referência | Requisito | Obrig |
|---|---|---|
| | • prazos de guarda;<br>• autor (pessoa física ou jurídica);[36]<br>• redator (se diferente do autor);[37]<br>• originador;[38]<br>• destinatário (e respectivo cargo);<br>• nome do setor responsável pela execução da ação contida no documento;<br>• indicação de anotação;<br>• indicação de anexos;<br>• indicação de versão;<br>• restrição de acesso;<br>• registro das migrações e data em que ocorreram.<br>Os metadados opcionais se referem a informações mais detalhadas sobre o documento, tais como:<br>• espécie / tipo / gênero documental;<br>• associações a documentos diferentes que podem estar relacionados pelo fato de registrarem a mesma atividade ou se referirem à mesma pessoa ou situação;<br>• formato *e software* (nome e versão) em que o documento foi produzido ou capturado;<br>• máscaras de formatação (*templates*) necessárias para interpretar a estrutura do documento;<br>• assunto / descritor (diferentes do já estabelecido no código de classificação);<br>• localização física;<br>• e outros que se julgarem necessários. | |
| 3.1.6 | Um SIGAD tem que prever a inserção dos metadados obrigatórios, previstos em legislação específica na devida esfera e âmbito de competência, no momento da captura de processos. | O |
| 3.1.7 | Um SIGAD tem que ser capaz de atribuir um número identificador a cada dossiê/processo e documento capturado, que serve para identificá-lo desde o momento da captura até sua destinação final no SIGAD. | O |

[36] Nome da pessoa física ou jurídica (órgão ou entidade) com autoridade e capacidade para emitir o documento ou em nome da qual ou sob cujo comando o documento é emitido.

[37] Nome da pessoa física ou jurídica que tem autoridade e capacidade para elaborar o conteúdo do documento.

[38] Nome da pessoa física ou jurídica designada no endereço eletrônico no qual o documento é gerado ou enviado.

| Referência | Requisito | Obrig |
|---|---|---|
| 3.1.8 | O formato do número identificador atribuído pelo sistema deve ser definido no momento da configuração do SIGAD.<br><br>*O identificador pode ser numérico ou alfanumérico, ou pode incluir os identificadores encadeados das entidades superiores no ramo apropriado da hierarquia.* | O |
| 3.1.9 | Num SIGAD, o número identificador atribuído pelo sistema tem que:<br>• ser gerado automaticamente, sendo vedada sua introdução manual e alteração posterior;<br>ou<br>• ser atribuído pelo usuário e validado pelo sistema antes de ser aceito.<br><br>*Uma opção seria gerar o número identificador automaticamente, mas, nesse caso, ocultando-o do usuário e permitindo a este introduzir uma sequência não necessariamente única como um "identificador". O usuário empregaria essa sequência como um identificador, mas o SIGAD a consideraria um metadado pesquisável, definido pelo usuário.* | O |
| 3.1.10 | Um SIGAD tem que prever a adoção da numeração única de processos e/ou documentos oficiais de acordo com a legislação específica a fim de garantir a integridade do número atribuído ao processo e/ou documento na unidade protocolizadora de origem. | O |
| 3.1.11 | Um SIGAD deve utilizar tesauro ou vocabulário controlado para apoiar a atribuição do metadado assunto/descritor.<br><br>*No caso da administração pública federal, deve ser utilizada a Lista de Assuntos de Governo, conforme orientação dos Padrões de Interoperabilidade de Governo Eletrônico (e-Ping).* | AD |
| 3.1.12 | Um SIGAD tem que garantir que os metadados associados a um documento sejam inseridos somente por usuários autorizados. | O |
| 3.1.13 | Um SIGAD tem que garantir que os metadados associados a um documento sejam alterados somente por administradores e usuários autorizados e devidamente registrados em trilhas de auditoria. | O |
| 3.1.14 | Um SIGAD deve ser capaz de relacionar um documento digital (objeto digital) a mais de um dossiê ou processo, sem a sua duplicação física.<br><br>*Por exemplo, uma lista de alunos aprovados em um concurso de doutorado de determinada universidade estará associada ao dossiê "Concurso doutorado 2005" e aos dossiês de cada aluno aprovado.*<br><br>*Quando um documento digital estiver associado a mais de um dossiê, o SIGAD deve criar um registro para cada referência desse documento. Cada registro estará vinculado ao mesmo objeto digital.* | AD |

| Referência | Requisito | Obrig |
|---|---|---|
| 3.1.15 | Um SIGAD deve ser capaz de inserir, automaticamente, os metadados previstos no sistema para o maior número possível de documentos, pois isso diminui as tarefas do usuário do sistema e garante maior rigor na inserção dos metadados.<br><br>*Por exemplo, no caso de documentos com forma padronizada (formulários, modelos de requerimento, de memorando etc.), alguns metadados podem ser inseridos automaticamente, tais como número identificador, título, classificação, prazo de guarda.* | AD |
| 3.1.16 | Um SIGAD tem que garantir a visualização do registro de entrada do documento no sistema com todos os metadados inseridos automaticamente e os demais a serem atribuídos pelo usuário.<br><br>*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 |
| 3.1.17 | Um SIGAD tem que garantir a inserção de outros metadados após a captura.<br><br>*Por exemplo, data e hora de alteração e mudança de suporte.* | O |
| 3.1.18 | Sempre que um documento tiver mais de uma versão, o SIGAD tem que permitir que os usuários selecionem pelo menos uma das seguintes ações:<br><br>• registrar todas as versões do documento como um só documento arquivístico;<br><br>• registrar uma única versão do documento como um documento arquivístico;<br><br>• registrar cada uma das versões do documento, separadamente, como um documento arquivístico. | O |
| 3.1.19 | Um SIGAD deve prestar assistência aos usuários no que diz respeito à classificação dos documentos, por meio de algumas ou de todas as ações a seguir:<br><br>• tornar acessível ao usuário somente o subconjunto do plano de classificação que diz respeito à sua atividade;<br><br>• indicar as últimas classificações feitas pelo usuário;<br><br>• indicar dossiês que contenham documentos de arquivo relacionados;<br><br>• indicar classificações possíveis a partir dos metadados já inseridos, como, por exemplo, o título;<br><br>• indicar classificações possíveis a partir do conteúdo do documento. | AD |
| 3.1.20 | Um SIGAD deve permitir que um usuário transmita documentos a outro usuário para completar o processo de captura, caso os | AD |

| Referência | Requisito | Obrig |
|---|---|---|
| | procedimentos dessa captura sejam distribuídos entre vários usuários. | |
| 3.1.21 | No caso de documentos ou dossiês/processos constituídos por mais de um objeto digital, o SIGAD tem que:<br>• tratar o documento como uma unidade indivisível, assegurando a relação entre os objetos digitais;<br>• preservar a integridade do documento, mantendo a relação entre os objetos digitais;<br>• garantir a integridade do documento quando de sua recuperação, visualização e gestão posteriores;<br>• gerenciar a destinação de todos os objetos digitais que compõem o documento como uma unidade indivisível. | O |
| 3.1.22 | Um SIGAD tem que emitir um aviso caso o usuário tente registrar um documento que já tenha sido registrado no mesmo dossiê/processo. | O |

## 3.2 Captura em lote

| Referência | Requisito | Obrig |
|---|---|---|
| 3.2.1 | Um SIGAD tem que proporcionar a captura em lote de documentos gerados por outros sistemas. Esse procedimento tem que:<br>• permitir a importação de transações predefinidas de arquivos em lote;<br>• registrar, automaticamente, cada um dos documentos importados contidos no lote;<br>• permitir e controlar a edição do registro dos documentos importados;<br>• validar a integridade dos metadados.<br>*Exemplos de lotes de documento: mensagens de correio eletrônico, correspondência digitalizada por meio de escâner, documentos provenientes de um departamento, grupo ou indivíduo, transações de aplicações de um computador ou, ainda, documentos oriundos de um sistema de gestão de documentos.* | O |

## 3.3 Captura de mensagens de correio eletrônico

O correio eletrônico é um sistema usado para criar, transmitir e receber mensagens eletrônicas e outros documentos digitais por meio de redes de computadores. As

características do correio eletrônico podem dificultar o seu gerenciamento. Assim, um SIGAD tem que permitir controles de gestão para:

- capturar todas as mensagens e anexos emitidos e recebidos;
- dotar os usuários da capacidade de capturar apenas mensagens e anexos previamente selecionados.

Observação: este último procedimento requer que os usuários avaliem a pertinência e importância dos itens, bem como a possibilidade de eles não serem capturados.

| Referência | Requisito | Obrig |
|---|---|---|
| 3.3.1 | Um SIGAD tem que permitir que, na fase de configuração, seja escolhida uma das seguintes operações:<br>• capturar mensagens de correio eletrônico após selecionar quais serão objeto de registro;<br>ou<br>• capturar, automaticamente, todas as mensagens de correio eletrônico. | O |
| 3.3.2 | Um SIGAD pode permitir que os usuários tratem e capturem as mensagens de chegada a partir do seu próprio sistema de correio eletrônico. O usuário deve poder tratar cada mensagem na caixa de entrada, como se segue:<br>• visualizar cada mensagem de correio e uma indicação dos respectivos anexos, caso existam;<br>• visualizar os conteúdos dos anexos utilizando um dispositivo para visualização de documentos em diferentes formatos;<br>• registrar no SIGAD a mensagem de correio e respectivos anexos como um novo documento de arquivo;<br>• relacionar a mensagem e respectivos anexos a um documento existente no SIGAD. | F |
| 3.3.3 | Um SIGAD deve assegurar a captura do nome, e não somente do endereço, do originador do correio eletrônico. Por exemplo, “Luís Santos”, além de “lsa25@ab.br”. | AD |

## 3.4 Captura de documentos convencionais ou híbridos

O programa de gestão arquivística de documentos de um órgão ou entidade é único para documentos convencionais, digitais e híbridos. Assim, o SIGAD tem que capturar todos esses tipos de documentos.

A captura do documento convencional será realizada pelo SIGAD por meio das atividades de registro, classificação e indexação. O arquivamento será feito da forma apropriada ao suporte, formato e tipo de documento.

| Referência | Requisito | Obrig |
|---|---|---|
| 3.4.1 | O SIGAD tem que poder capturar também os documentos convencionais e/ou híbridos. | O |
| 3.4.2 | O SIGAD tem que acrescentar aos metadados dos documentos convencionais informações sobre sua localização.<br>*Essa informação só será acessada por usuários autorizados.* | O |

## 3.5 Formato de arquivo e estrutura[39] dos documentos a serem capturados

Órgãos e entidades precisam capturar uma gama diversificada de documentos com formatos de arquivo e estruturas diferentes. Os requisitos técnicos para a captura variam de acordo com a complexidade dos documentos. Em alguns ambientes não é possível identificar, antecipadamente, todas os formatos de arquivo e estruturas possíveis dos documentos, já que alguns são recebidos de fontes externas.

### Documentos automodificáveis

Alguns documentos parecem ter seu conteúdo alterado sem intervenção do usuário. Por exemplo, um modelo para elaboração de correspondência 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, é apenas sua exibição (documento conceitual) que sofre alterações conforme o *software* utilizado para visualizá-lo.

Outros documentos podem conter um código que os modifica realmente. É o caso de uma folha de cálculo com um "macro" sofisticado que a altera (por meio de *software* de aplicações utilizado para visualização) e, em seguida, guarda a folha automaticamente.

Os documentos automodificáveis devem ser evitados. Caso isso não seja possível, 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 para o SIGAD.

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

| Referência | Requisito | Obrig |
|---|---|---|
| 3.5.1 | Um SIGAD tem que possuir a capacidade de capturar documentos com diferentes formatos de arquivo e estruturas. | O |

[39] A estrutura dos documentos refere-se a um ou mais arquivos que compõem o documento, conforme exemplificado no item 3.5.3.

| Referência | Requisito | Obrig |
|---|---|---|
| 3.5.2 | Um SIGAD deve poder capturar, entre outros, os documentos a seguir:<br>• calendários eletrônicos;<br>• informações de outros aplicativos – contabilidade, folha de pagamento, desenho assistido por computador (CAD);<br>• documentos em papel digitalizados por meio de escâner;<br>• documentos sonoros;<br>• videoclipes;<br>• diagramas e mapas digitais;<br>• dados estruturados (EDI);<br>• bases de dados;<br>• documentos multimídia.<br>*A lista de documentos que um SIGAD tem que suportar varia de órgão para órgão.* | AD |
| 3.5.3 | Um SIGAD tem que capturar documentos que se apresentam com as seguintes estruturas:<br>• simples: texto, imagens, mensagens de correio eletrônico, *slides* digitais, som.<br>• composta: mensagens de correio eletrônico com anexos, páginas *web*, publicações eletrônicas, bases de dados. | O |
| 3.5.4 | Um SIGAD tem que ser capaz de incluir novos formatos de arquivos à medida que forem sendo adotados pelo órgão ou entidade. | O |

## 3.6 Estrutura dos procedimentos de gestão

A gestão arquivística de documentos digitais prevê o estabelecimento de três domínios no ambiente eletrônico: *espaço individual*, *espaço do grupo* e *espaço geral*. O *espaço individual* corresponde ao espaço definido para cada funcionário; o *espaço do grupo*, ao espaço para cada grupo, equipe, comitê; e o *espaço geral*, ao serviço de protocolo e arquivos do órgão ou entidade, e sua principal característica é que, uma vez ali, o documento não pode mais ser alterado.

As regras estabelecidas pelo sistema de gestão arquivística de documentos definem:

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

Uma vez capturados no espaço geral, os documentos e seus metadados têm que ser mantidos em versão definitiva e protegidos contra alterações deliberadas ou acidentais. O conteúdo, contexto e forma dos documentos capturados devem ser mantidos ao longo de todo o seu ciclo de vida, a fim de preservar sua autenticidade.

| Referência | Requisito | Obrig |
|---|---|---|
| 3.6.1 | Um SIGAD tem que ser capaz de reconhecer três domínios para o controle dos procedimentos de gestão: espaço individual, espaço do grupo e espaço geral. | O |
| 3.6.2 | Um SIGAD tem que ser capaz de operacionalizar as regras estabelecidas pelo sistema de gestão arquivística de documentos nos três espaços. | O |
| 3.6.3 | Um SIGAD tem que impedir que o conteúdo de um documento seja alterado por usuários e administradores, exceto se a alteração fizer parte do processo documental. (Ver seção 6.10 – *Alterar, apagar e truncar*) | O |
| 3.6.4 | Um SIGAD deve poder emitir um aviso caso se tente capturar um documento incompleto ou inconsistente a ponto de comprometer sua futura autenticidade.<br>*Por exemplo, uma correspondência sem assinatura digital válida ou uma fatura de fornecedor não identificado.* | AD |
| 3.6.5 | Um SIGAD deve poder emitir um aviso caso se tente capturar um documento cuja autenticidade não possa ser verificada no futuro. | AD |

# 4 AVALIAÇÃO E DESTINAÇÃO

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

No contexto de um SIGAD, a avaliação dos documentos refere-se à aplicação da tabela de temporalidade e destinação de documentos. Essa tabela define o prazo pelo qual os documentos têm que ser mantidos em um SIGAD e a destinação dos mesmos após esse prazo, ou seja, recolhimento ou eliminação.

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

Esta seção estabelece requisitos para a configuração e aplicação da tabela de temporalidade e destinação de documentos no SIGAD e para a exportação e eliminação de documentos de um SIGAD.

## 4.1 Configuração da tabela de temporalidade e destinação de documentos

Estes requisitos referem-se à criação e manutenção de tabelas de temporalidade em um SIGAD.

| Referência | Requisito | Obrig |
|---|---|---|
| 4.1.1 | Um SIGAD tem que prover funcionalidades para definição e manutenção de tabela de temporalidade e destinação de documentos, associada ao plano de classificação do órgão ou entidade. | O |
| 4.1.2 | Um SIGAD tem que associar, automaticamente, ao dossiê/processo o prazo e a destinação previstos na classe em que o documento foi inserido. | O |
| 4.1.3 | Um SIGAD tem que manter tabela de temporalidade e destinação de documentos com as seguintes informações:<br>• identificador do órgão ou entidade;<br>• identificador da classe;<br>• prazo de guarda na fase corrente;<br>• prazo de guarda na fase intermediária;<br>• destinação final;<br>• observações;<br>• evento que determina o início da contagem do prazo de retenção na fase corrente e na fase intermediária.<br>*A tabela de temporalidade e destinação de documentos dos integrantes do SINAR deve estar de acordo com a legislação e ser aprovada pela instituição arquivística na específica esfera de competência.*[40] | O |
| 4.1.4 | Um SIGAD tem que prever, pelo menos, as seguintes situações para destinação:<br>• apresentação dos documentos para reavaliação em data futura;<br>• eliminação;<br>• exportação para transferência;<br>• exportação para recolhimento (guarda permanente). | O |

[40] A Resolução do Conarq n. 14, de 28 de outubro de 2001, aprova a versão revisada e ampliada da Resolução do Conarq n. 4, de 28 de março de 1996, que dispõe sobre a classificação, temporalidade e destinação de documentos de arquivo relativos às atividades-meio da administração pública. Esse instrumento também orienta a elaboração de código de classificação e tabela de temporalidade e destinação de documentos para as atividades finalísticas.

| Referência | Requisito | Obrig |
|---|---|---|
| 4.1.5 | Um SIGAD tem que prever a iniciação automática da contagem dos prazos de guarda referenciados na tabela de temporalidade e destinação de documentos, pelo menos, a partir dos seguintes eventos:<br>• abertura de dossiê;<br>• arquivamento de dossiê/processo;<br>• desarquivamento de dossiê/processo;<br>• inclusão de documento em um dossiê/processo.<br>*Acontecimentos específicos, descritos na tabela de temporalidade e destinação como, por exemplo, "cinco anos a contar da data de aprovação das contas", quando não puderem ser detectados automaticamente pelo sistema, deverão ser informados ao SIGAD por usuário autorizado.* | O |
| 4.1.6 | Um SIGAD tem que prever que a definição dos prazos de guarda seja expressa por:<br>• um número inteiro de dias ou<br>• um número inteiro de meses ou<br>• um número inteiro de anos ou<br>• uma combinação de um número inteiro de anos, meses e dias. | O |
| 4.1.7 | Um SIGAD tem que limitar a definição e a manutenção (alteração, inclusão e exclusão) da tabela de temporalidade e destinação de documentos a usuários autorizados. | O |
| 4.1.8 | Um SIGAD tem que permitir que um usuário autorizado altere o prazo ou destinação prevista em um item da tabela de temporalidade e destinação de documentos e garantir que a alteração tenha efeito em todos os documentos ou dossiês/processos associados àquele item.<br>*As alterações na tabela de temporalidade e destinação só poderão ser feitas como resultado de um processo de reavaliação realizado pela comissão de avaliação do órgão ou entidade em virtude de mudança do contexto administrativo, jurídico ou cultural.*<br>*Os integrantes do SINAR deverão ainda ter suas tabelas aprovadas pela instituição arquivística na específica esfera de competência.* | O |
| 4.1.9 | Um SIGAD deve ser capaz de manter o histórico das alterações realizadas na tabela de temporalidade e destinação de documentos. | AD |
| 4.1.10 | Um SIGAD deve ser capaz de importar e exportar total ou parcialmente uma tabela de temporalidade e destinação de documento. (Ver item 12 – Interoperabilidade) | AD |

| Referência | Requisito | Obrig |
|---|---|---|
| 4.1.11 | Um SIGAD tem que prover funcionalidades para elaboração de relatórios que apóiem a gestão da tabela de temporalidade e destinação, incluindo a capacidade de:<br>• gerar relatório completo da tabela de temporalidade e destinação de documentos;<br>• gerar relatório parcial da tabela de temporalidade e destinação de documentos a partir de um ponto determinado na hierarquia do plano de classificação;<br>• gerar relatório dos documentos ou dossiês/processos aos quais foi atribuído um determinado prazo de guarda;<br>• identificar as inconsistências existentes entre a tabela de temporalidade e destinação de documentos e o plano de classificação. | O |

## 4.2 Aplicação da tabela de temporalidade e destinação de documentos

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

| Referência | Requisito | Obrig |
|---|---|---|
| 4.2.1 | Um SIGAD tem que fornecer recursos integrados à tabela de temporalidade e destinação de documentos para implementar as ações de destinação. | O |
| 4.2.2 | Para cada dossiê/processo, um SIGAD tem que acompanhar automaticamente os prazos de guarda determinados para a classe à qual pertence. | O |
| 4.2.3 | Um SIGAD tem que prover funcionalidades para informar ao usuário autorizado sobre os documentos ou dossiês/processos que já cumpriram ou estão para cumprir o prazo de guarda previsto. | O |
| 4.2.4 | Um SIGAD tem de prover funcionalidades para gerenciar o processo de destinação, que tem de ser iniciado por usuário autorizado e cumprir os seguintes passos:<br>• identificar automaticamente os documentos ou dossiês/processos que atingiram os prazos de guarda previstos;<br>• informar o usuário autorizado sobre todos os documentos ou dossiês/processos que foram identificados no passo anterior;<br>• possibilitar a alteração do prazo ou destinação previstos para aqueles documentos ou dossiês/processos, caso necessário;<br>• proceder à ação de destinação quando confirmada pelo usuário autorizado. | O |

| Referência | Requisito | Obrig |
|---|---|---|
| 4.2.5 | Um SIGAD tem sempre que pedir confirmação antes de realizar as ações de destinação. | O |
| 4.2.6 | Um SIGAD deve prever, em determinados casos, dispositivo de aviso antes do início de uma ação de destinação. Por exemplo, emitir aviso ao administrador, caso um documento arquivístico possua um determinado nível de segurança. | AD |
| 4.2.7 | Um SIGAD tem que restringir as funções de destinação a usuários autorizados. | O |
| 4.2.8 | Quando um administrador transfere documentos ou dossiês/processos de uma classe para outra, em virtude de uma reclassificação, o SIGAD tem que adotar automaticamente a temporalidade e a destinação vigentes na nova classe. | O |
| 4.2.9 | Quando um documento digital (objeto digital) estiver associado a mais de um dossiê ou processo, e tiver prazos de guarda diferentes associados a ele, o SIGAD tem que automaticamente verificar todos os prazos de guarda e as destinações previstas para esse documento e garantir que ele seja mantido em cada dossiê/processo pelo tempo definido na tabela de temporalidade e destinação de documentos, de forma que:<br>• a remoção de um documento de um dossiê/processo não prejudique a manutenção desse mesmo documento em outro dossiê/processo, até que todas as referências desse documento tenham atingido o prazo de guarda previsto;<br>• a manutenção de um documento em um dossiê/processo por prazo mais longo não obrigue a permanência desse mesmo documento em outro dossiê/processo de prazo mais curto. Nesse caso o registro do documento com prazo mais curto tem que ser removido, mas o documento é mantido no SIGAD.<br>*Quando um documento digital estiver associado a mais de um dossiê ou processo, o SIGAD deverá criar um registro para cada referência desse documento. Cada registro estará vinculado ao mesmo objeto digital.*<br>*No momento da eliminação, o objeto digital não poderá ser eliminado sem que antes se verifique a 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 |

## 4.3 Exportação de documentos

Um SIGAD deve ter capacidade de exportar documentos para apoiar as ações de transferência e recolhimento de documentos, ou ainda para realizar uma migração ou enviar uma cópia para outro local ou sistema.

Em alguns casos os documentos serão eliminados do SIGAD após a exportação; em outros, serão mantidos. Em todos os casos, é absolutamente necessário que as ações sejam executadas de maneira controlada, fazendo-se registro nos metadados e na trilha de auditoria e verificando-se os documentos relacionados.

| Referência | Requisito | Obrig |
|---|---|---|
| 4.3.1 | Um SIGAD tem que ser capaz de exportar documentos e dossiês/processos digitais e seus metadados para outro sistema dentro ou fora do órgão ou entidade. | O |
| 4.3.2 | Quando um SIGAD exportar os documentos e dossiês/processos de uma classe para executar uma ação de transferência ou recolhimento, tem que ser capaz de exportar todos os documentos e dossiês/processos da classe incluídos na ação de destinação, com seus respectivos volumes, documentos e metadados associados. | O |
| 4.3.3 | Um SIGAD tem que ser capaz de exportar um documento e dossiê/processo ou grupo de documentos e dossiês/processos numa seqüência de operações, de modo que:<br>• o conteúdo, o contexto e a estrutura dos documentos não se degradem;<br>• todos os componentes de um documento digital sejam exportados como uma unidade. Por exemplo, uma mensagem de correio eletrônico e seus respectivos anexos;<br>• todos os metadados do documento sejam relacionados a ele de forma que as ligações possam ser mantidas no novo sistema;<br>• todas as ligações entre documentos, volumes e dossiês/processos sejam mantidas. | O |
| 4.3.4 | Um SIGAD deve ser capaz de exportar dossiês/processos:<br>• em seu formato nativo (ou no formato para o qual foi migrado);<br>• de acordo com o formatos definidos em padrões de interoperabilidade;<br>• de acordo com o formato definido pela instituição arquivística que irá receber a documentação, no caso de transferência ou recolhimento. | AD |
| 4.3.5 | Um SIGAD deve ser capaz de exportar metadados nos formatos previstos pelo padrão de interoperabilidade do governo. | AD |
| 4.3.6 | Um SIGAD tem que ser capaz de exportar todos os tipos de documentos que está apto a capturar. | O |

| Referência | Requisito | Obrig |
|---|---|---|
| 4.3.7 | Um SIGAD tem que produzir um relatório detalhado sobre qualquer falha que ocorra durante uma exportação. O relatório tem que identificar os documentos e dossiês/processos que originaram erros de processamento ou cuja exportação não tenha sido bem sucedida. | O |
| 4.3.8 | Um SIGAD tem que conservar todos os documentos e dossiês/processos digitais que foram exportados, pelo menos até que tenham sido importados no sistema destinatário com êxito. | O |
| 4.3.9 | Um SIGAD tem que manter metadados relativos a documentos e dossiês/processos que foram exportados.<br><br>*O Administrador deve indicar o subconjunto de metadados que deverá ser mantido.* | O |
| 4.3.10 | Um SIGAD tem que gerar listagem em meio digital e em papel para descrever documentos e dossiês/processos digitais que estão sendo exportados.<br><br>*Este requisito se aplica principalmente nos casos em que é feita exportação para transferência ou recolhimento a uma instituição arquivística pública. Nesse caso, a listagem deverá ser produzida no formato estabelecido pela instituição arquivística recebedora.* | O |
| 4.3.11 | Um SIGAD deve possibilitar a inclusão de metadados necessários à gestão do arquivo permanente nos documentos e dossiês/processos que serão exportados para recolhimento. | AD |
| 4.3.12 | Um SIGAD pode possibilitar a ordenação dos documentos e dossiês/processos digitais a serem exportados de acordo com elementos de metadados selecionados pelo usuário. | F |
| 4.3.13 | Quando se exportar documentos e dossiês/processos híbridos, um SIGAD deve exigir do usuário autorizado a confirmação de que a parte na forma convencional dos mesmos documentos e dossiês/processos tenha passado pelo procedimento de destinação adequado antes de confirmar a exportação da parte na forma digital. | AD |
| 4.3.14 | Um SIGAD deve permitir que documentos sejam exportados mais de uma vez. | AD |

## 4.4 Eliminação

A eliminação de documentos arquivísticos deve ser realizada de acordo com o previsto na tabela de temporalidade e destinação de documentos, após a avaliação dos documentos e de acordo com a legislação vigente.[41]

[41] Lei n. 8.159, de 8 de janeiro de 1991 e Resoluções do Conarq n. 5, 7 e 20, bem como a legislação específica das esferas municipal e estadual e poderes da União.

Da mesma forma que a exportação, as ações para eliminação de documentos arquivísticos em um SIGAD têm de ser executadas de forma controlada, fazendo-se registro nos metadados e trilha de auditoria e verificando-se os documentos relacionados.

| Referência | Requisito | Obrig |
|---|---|---|
| 4.4.1 | Um SIGAD tem que restringir a função de eliminação de documentos ou dossiês/processos somente a usuários autorizados. | O |
| 4.4.2 | Um SIGAD tem que pedir confirmação da eliminação a um usuário autorizado antes que qualquer ação seja tomada com relação ao documento e dossiê/processo e cancelar o processo de eliminação se a confirmação não for dada. | O |
| 4.4.3 | Um SIGAD tem que avisar o usuário autorizado quando um documento ou dossiê/processo que estiver sendo eliminado se encontrar relacionado a outro; os sistemas também têm de suspender o processo até que seja tomada uma das medidas abaixo:<br>• confirmação pelo usuário autorizado para prosseguir ou cancelar o processo;<br>• produção de um relatório especificando os documentos ou dossiês/processos envolvidos e todas as ligações com outros documentos ou dossiês/processos. | O |
| 4.4.4 | Um SIGAD deve permitir a eliminação de documentos ou dossiês/processos de forma irreversível a fim de que não possam ser restaurados por meio da utilização normal do SIGAD nem por meio de rotinas auxiliares do sistema operacional nem por aplicações especiais de recuperação de dados. | AD |
| 4.4.5 | Quando um documento tem várias referências armazenadas no sistema, um SIGAD tem que garantir que todas essas referências sejam verificadas antes de eliminar o objeto digital.<br>*Ver requisito 4.2.9* | O |
| 4.4.6 | Um SIGAD tem que produzir um relatório detalhando qualquer falha que ocorra durante uma eliminação. O relatório tem que identificar os documentos cuja eliminação não tenha sido bem sucedida. | O |
| 4.4.7 | Quando eliminar documentos ou dossiês/processos híbridos, um SIGAD deve exigir do usuário autorizado a confirmação de que a parte na forma convencional dos mesmos seja eliminada também antes de confirmar a eliminação da parte na forma digital. | AD |
| 4.4.8 | Um SIGAD tem que gerar relatório com os documentos e dossiês/processos que serão eliminados. | O |

| Referência | Requisito | Obrig |
|---|---|---|
| | *Essa listagem deve seguir o formato da* Listagem de eliminação *conforme o estabelecido na norma vigente.* | |
| 4.4.9 | Um SIGAD tem que manter metadados relativos a documentos e dossiês/processos eliminados.<br>*O Administrador deve indicar o subconjunto de metadados que deverá ser mantido.* | O |

## 4.5 Avaliação e destinação de documentos arquivísticos convencionais e híbridos

Os documentos arquivísticos convencionais e os híbridos gerenciados pelo SIGAD devem ter os procedimentos de avaliação e destinação controlados pelo SIGAD, da mesma forma que os documentos digitais.

| Referência | Requisito | Obrig |
|---|---|---|
| 4.5.1 | Um SIGAD tem que aplicar a mesma tabela de temporalidade e destinação de documentos para os documentos convencionais, digitais ou híbridos. | O |
| 4.5.2 | Um SIGAD tem que acompanhar os prazos de guarda dos documentos convencionais e deve dar início aos procedimentos de eliminação ou transferência desses documentos, tomando em consideração suas especificidades. | O |
| 4.5.3 | Um SIGAD tem que alertar o administrador sobre a existência e a localização de uma parte convencional associada a um documento híbrido que esteja destinado a ser exportado, transferido ou eliminado. | O |
| 4.5.4 | Um SIGAD deve exportar metadados de documentos e dossiês/processos convencionais. | AD |

# 5 PESQUISA, LOCALIZAÇÃO E APRESENTAÇÃO DOS DOCUMENTOS

Um SIGAD precisa prover funcionalidades para pesquisa, localização e apresentação dos documentos arquivísticos com o objetivo de permitir o acesso a eles.

Todas essas funcionalidades têm de ser submetidas aos controles de acesso descritos na seção 6 – *Segurança*.

## 5.1 Aspectos gerais

| Referência | Requisito | Obrig |
|---|---|---|
| 5.1.1 | Um SIGAD tem que fornecer facilidades para pesquisa, localização e apresentação dos documentos. | O |
| 5.1.2 | Um SIGAD deve fornecer interface de pesquisa, localização e apresentação opcionais via ambiente *web*. | AD |
| 5.1.3 | Um SIGAD deve prever a navegação gráfica no plano de classificação, a navegação direta de uma classe para os documentos arquivísticos produzidos nesta classe e a seleção, recuperação e apresentação direta dos documentos arquivísticos e de seus conteúdos por meio desse mecanismo. | AD |

## 5.2 Pesquisa e localização

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

| Referência | Requisito | Obrig |
|---|---|---|
| 5.2.1 | Um SIGAD tem que fornecer uma série flexível 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 arquivísticos por meio de parâmetros definidos pelo usuário, com o objetivo de localizar e acessar os documentos e/ou metadados, seja individualmente ou reunidos em grupo. | O |
| 5.2.2 | Um SIGAD tem que executar pesquisa de forma integrada, isto é, apresentar todos os documentos e dossiês/processos, sejam eles digitais, híbridos ou convencionais, que satisfaçam aos parâmetros da pesquisa. | O |
| 5.2.3 | Um SIGAD tem que permitir que todos os metadados de gestão[42] de um documento ou dossiê/processo possam ser pesquisados. | O |
| 5.2.4 | Um SIGAD deve permitir que o conteúdo dos documentos em forma de texto possa ser pesquisado. | AD |
| 5.2.5 | Um SIGAD tem que permitir que um documento ou dossiê/processo possa ser recuperado por meio de um número identificador. | O |

[42] Os metadados de gestão são aqueles que apoiam a gestão arquivística do documento, tais como temporalidade e destinação prevista, código de classificação, entre outros.

| Referência | Requisito | Obrig |
|---|---|---|
| 5.2.6 | Um SIGAD tem que permitir que um documento ou dossiê/processo possa ser recuperado por meio de todas as formas de identificação implementadas, incluindo, no mínimo:<br>• identificador;<br>• título;<br>• assunto;<br>• datas;<br>• procedência/interessado;<br>• autor/redator /originador;<br>• classificação de acordo com plano ou código de classificação. | O |
| 5.2.7 | Um SIGAD deve fornecer uma interface que possibilite a pesquisa combinada de metadados e de conteúdo do documento por meio dos operadores *booleanos* “e”, “ou” e “não”. | AD |
| 5.2.8 | Um SIGAD deve permitir que os termos utilizados na pesquisa possam ser qualificados, especificando-se um metadado ou o conteúdo do documento como fonte de busca. | AD |
| 5.2.9 | Um SIGAD pode permitir o uso de períodos típicos de pedidos de pesquisa nos campos de data, como, por exemplo, “semana anterior”, “mês corrente”. | F |
| 5.2.10 | Um SIGAD deve permitir a utilização de caracteres curinga e de truncamento à direita para pesquisa de metadados.<br>*Por exemplo, o argumento de pesquisa “Bra*il“ pode recuperar “Brasil“ e “Brazil“, e o argumento de pesquisa “Arq*” pode recuperar “Arquivo”, “Arquivística”.* | AD |
| 5.2.11 | Um SIGAD deve permitir a utilização de caracteres coringa e de truncamento à direita para pesquisa no conteúdo do documento. | AD |
| 5.2.12 | Um SIGAD deve proporcionar pesquisa por proximidade, isto é, que uma palavra apareça no conteúdo do documento a uma distância máxima de outra. | AD |
| 5.2.13 | Um SIGAD deve permitir que os usuários armazenem pesquisas para reutilização posterior. | AD |
| 5.2.14 | Um SIGAD deve permitir que os usuários refinem pesquisas já realizadas. | AD |
| 5.2.15 | Quando o órgão ou entidade utilizar tesauros ou vocabulário controlado, um SIGAD deve ser capaz de realizar pesquisa dos documentos e dossiês/processos por meio da navegação nesses instrumentos. | AD |
| 5.2.16 | Um SIGAD deve permitir que usuários autorizados configurem e alterem os campos *default* de pesquisa de forma a definir metadados como campos de pesquisa. | AD |

| Referência | Requisito | Obrig |
|---|---|---|
| 5.2.17 | Um SIGAD tem que permitir a pesquisa e recuperação de uma unidade de arquivamento completa e exibir a lista de todos os documentos que a compõem, como uma unidade e num único processo de recuperação. | O |
| 5.2.18 | Um SIGAD tem que limitar o acesso a qualquer informação (metadado ou conteúdo de um documento arquivístico) se restrições de acesso e questões de segurança assim determinarem. | O |

## 5.3 Apresentação: visualização, impressão, emissão de som

Um SIGAD pode conter documentos arquivísticos com os mais diversos formatos e estruturas, e deve ter a capacidade de apresentar esses documentos ao usuário sem adulterá-los, seja exibindo-os na tela do computador, imprimindo ou emitindo som.

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

| Referência | Requisito | Obrig |
|---|---|---|
| 5.3.1 | Um SIGAD tem que apresentar o resultado da pesquisa como uma lista de documentos e dossiês/processos digitais, convencionais ou híbridos que cumpram os parâmetros da consulta e deve notificar o usuário se o resultado for nulo. | O |
| 5.3.2 | Quando o resultado de uma pesquisa for nulo, o SIGAD pode sugerir outros parâmetros aproximados que possam ser satisfeitos.<br>*Por exemplo:*<br>*Pesquisa inicial com o parâmetro "Arquivo Nacional".*<br>*O SIGAD apresenta a seguinte mensagem: Você não quis dizer "Arquivo Nacional"?* | F |
| 5.3.3 | Após apresentar o resultado da pesquisa, um SIGAD tem que oferecer ao usuário as opções:<br>• visualizar os documentos e dossiês/processos resultantes da pesquisa;<br>• redefinir os parâmetros de pesquisa e fazer nova consulta. | O |
| 5.3.4 | Um SIGAD deve permitir que os documentos e dossiês/processos apresentados em uma lista de resultados sejam selecionados e, em seguida, abertos por meio de um clique ou toque de tela ou acionamento de tecla. | AD |

| Referência | Requisito | Obrig |
|---|---|---|
| 5.3.5 | Um SIGAD deve permitir a configuração do formato da lista de resultados de pesquisa pelo usuário ou administrador, incluindo recursos e funções como:<br>• seleção da ordem em que os resultados de pesquisa são apresentados;<br>• determinação do número de resultados de pesquisa exibidos em cada tela;<br>• estabelecimento do número máximo de resultados para uma pesquisa;<br>• armazenamento dos resultados de uma pesquisa;<br>• definição dos metadados a serem exibidos nas listas de resultados de pesquisa. | AD |
| 5.3.6 | Um SIGAD deve fornecer recursos que permitam ao usuário "navegar" para o nível de agregação imediatamente superior ou inferior, como, por exemplo:<br>• de um documento para a unidade de arquivamento em que está incluído;<br>• de uma unidade de arquivamento para os documentos nela incluídos;<br>• de uma unidade de arquivamento para a respectiva classe;<br>• de uma classe para as unidades de arquivamento a ela relacionadas. | AD |
| 5.3.7 | Um SIGAD tem que ser capaz de apresentar o conteúdo de todos os tipos de documentos arquivísticos digitais capturados, de forma que:<br>• preserve as características de exibição visual e de formato apresentados pela aplicação geradora;<br>• exiba todos os componentes do documento digital em conjunto, como uma unidade. | O |
| 5.3.8 | Um SIGAD tem que ser capaz de exibir em tela todos os tipos de documentos capturados. | O |
| 5.3.9 | Um SIGAD tem que ser capaz de imprimir os documentos capturados, preservando o formato produzido pelas aplicações geradoras. | O |
| 5.3.10 | Um SIGAD tem que ser capaz de exibir/reproduzir o conteúdo de documentos que incluam imagem fixa, imagem em movimento e som. | O |
| 5.3.11 | Um SIGAD tem que proporcionar ao usuário formas flexíveis de impressão de documentos com seus metadados e possibilitar a definição dos metadados a serem impressos. | O |

| Referência | Requisito | Obrig |
|---|---|---|
| 5.3.12 | Um SIGAD tem que ser capaz de exibir em tela e imprimir todos os metadados associados aos documentos e dossiês/processos resultantes de uma pesquisa. | O |
| 5.3.13 | Um SIGAD tem que permitir a impressão de uma lista dos documentos e dossiês/processos resultantes de uma pesquisa. | O |
| 5.3.14 | Um SIGAD tem que permitir a impressão de uma lista dos documentos que compõem um dossiê/processo. | O |
| 5.3.15 | Um SIGAD deve permitir que os metadados exibidos nas listas a que se referem os requisitos 5.3.13 e 5.3.14 possam ser definidos pelo usuário. | AD |
| 5.3.16 | Um SIGAD tem que permitir que todos os documentos de um dossiê/processo sejam impressos em uma única operação, na sequência determinada pelo usuário. | O |
| 5.3.17 | Um SIGAD tem que incluir recursos destinados a transferir para suportes adequados documentos que não possam ser impressos, tais comodocumentos sonoros, vídeos e páginas *web*. | O |
| 5.3.18 | Um SIGAD deve ser capaz de apresentar os documentos arquivísticos em outros formatos além do nativo, tais como:<br>• formato *.xml* adequado para publicação;<br>• formato *.html* adequado para publicação;<br>• formato aprovado por organismos padronizadores na sua esfera de competência;<br>*No que se refere à interoperabilidade com outros sistemas, ver seção 12* – Interoperabilidade. | AD |
| 5.3.19 | Um SIGAD tem que ser capaz de realizar pesquisa e exibição de documentos e dossiês/processos, simultaneamente, para diversos usuários. | O |
| 5.3.20 | Um SIGAD deve permitir ao administrador determinar que todas as cópias em papel de documentos e dossiês/processos sejam impressas junto com metadados pré-selecionados. | AD |

# 6 SEGURANÇA

Esta seção contém um conjunto de requisitos para serviços de segurança: cópias de segurança, controle de acesso (tanto baseado em papéis de usuário como em grupos de usuários), classes de sigilo, trilhas de auditoria de sistemas, criptografia para sigilo, assinatura digital e marcas d'água digitais.

Os requisitos de identificação, autenticação de usuário e trilhas de auditoria devem integrar qualquer SIGAD. Políticas de segurança específicas poderão definir o rigor, maior ou menor, do tratamento dos demais requisitos.

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

- de controle de acesso baseado em papéis de usuário;
- de controle de acesso por grupos;
- de 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 tipo mencionado antes ou a uma combinação deles, de acordo com a legislação vigente.

Quanto ao uso da tecnologia de criptografia, tanto para sigilo como para autenticação, o rigor dos requisitos está sujeito à legislação vigente e à política de segurança específica. Muitas vezes, a criptografia é usada como mecanismo de apoio ao controle de acesso para reforçar o sigilo das informações. Os requisitos de assinatura digital e certificação digital são necessários para aquelas organizações em que documentos são assinados digitalmente ou para as verificações eletrônicas de autenticidade.

Esses requisitos não esgotam o tema segurança da informação, pois a segurança integral é sistêmica e abrange não somente a tecnologia, mas também as pessoas, processos 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, preferencialmente *off-site*.

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

| Referência | Requisito | Obrig |
|---|---|---|
| 6.1.1 | Um SIGAD tem que permitir que, sob controle do seu administrador, mecanismos de *backup* criem cópias de todas as informações nele contidas (documentos arquivísticos, metadados e parâmetros do sistema). | O |
| 6.1.2 | O administrador do SIGAD tem que manter o controle das cópias de segurança, prevendo testes de restauração. | O |
| 6.1.3 | As mídias removíveis devem ter cópias em suportes equivalentes e armazenamento *off-site*. | AD |

| Referência | Requisito | Obrig |
|---|---|---|
| 6.1.4 | Os discos rígidos devem ter *backups* armazenados em pelo menos dois locais diferentes e fisicamente distantes. | AD |
| 6.1.5 | Um SIGAD deve ser capaz de agendar, automaticamente, os *backups* com periodicidade estipulada pelo administrador. Deve permitir cópias incrementais ou completas. | AD |
| 6.1.6 | Um SIGAD deve dispor de mecanismos de assinatura digital das cópias de segurança, de modo a garantir a integridade dos dados e a identificação do responsável pelo procedimento.<br>*As assinaturas digitais possibilitam a verificação de integridade inclusive em mídias que estejam* off-site*. Essas verificações podem ser realizadas sem o auxílio do SIGAD.* | AD |
| 6.1.7 | Um SIGAD tem que incluir funções para restituir os documentos de arquivo e metadados a um estado conhecido, utilizando uma combinação de cópias restauradas e rotinas de auditoria. | O |
| 6.1.8 | Dados críticos de configuração e controle do sistema operacional e do gerenciador de bancos de dados devem ser especialmente protegidos. Mecanismos especiais de *backup* devem ser previstos para dados críticos. | AD |
| 6.1.9 | Trilhas de auditoria devem ser copiadas com frequência, prevendo-se cópias a serem armazenadas em pelo menos um local *off-site*. | AD |

## 6.2 Controle de acesso

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

### Identificação e autenticação de usuários

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

Usuários acessam dados, metadados e funções via interface do programa. A associação entre identidade do usuário e 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.

| Referência | Requisito | Obrig |
|---|---|---|
| 6.2.1 | Para implementar o controle de acesso, um SIGAD tem que manter pelo menos os seguintes atributos dos usuários, de acordo com a política de segurança:<br>• identificador do usuário; | O |

| Referência | Requisito | Obrig |
|---|---|---|
| | • autorizações de acesso;<br>• credenciais de autenticação.<br>*Senha, crachá, chave criptográfica,* token *USB,* smartcard*, biometria (de impressão digital, de retina etc.) são exemplos de credenciais de autenticação.* | |
| 6.2.2 | Um SIGAD tem que exigir que o usuário esteja devidamente identificado e autenticado antes de iniciar qualquer operação no sistema. | O |
| 6.2.3 | Um SIGAD tem que garantir que os valores dos atributos de segurança e controle de acesso, associados ao usuário, estejam dentro de conjuntos de valores válidos. | O |
| 6.2.4 | As credenciais de autenticação só devem ser alteradas pelo usuário proprietário ou pelo administrador, com a anuência do proprietário e em conformidade com a política de segurança. | AD |

### Aspectos gerais de controle de acesso

Os requisitos desta seção são aplicáveis a qualquer organização para condução de suas funções e atividades, independentemente do modelo de controle de acesso adotado, de acordo com a política de segurança.

| Referência | Requisito | Obrig |
|---|---|---|
| 6.2.5 | Um SIGAD tem que permitir acesso a funções do sistema somente a usuários autorizados e sob controle rigoroso da administração do sistema, a fim de proteger a autenticidade dos documentos arquivísticos digitais. | O |
| 6.2.6 | Se o usuário solicitar o acesso ou pesquisa de um documento arquivístico, volume ou dossiê/processo específico a que não tenha direito de acesso, um SIGAD deve fornecer uma das seguintes respostas (estabelecidas durante a configuração):<br>• mostrar o título e os metadados do documento;<br>• demonstrar a existência do dossiê/processo ou documento, mas não o respectivo título nem outro metadado;<br>• não mostrar qualquer informação do documento, nem indicar a sua existência.<br>*Essas opções são apresentadas em ordem crescente de segurança. O requisito da terceira opção (isto é, a mais rigorosa) implica que um SIGAD tem que excluir esses documentos de qualquer listagem de resultados de pesquisa. Esse procedimento é, normalmente, adequado para documentos que requeiram elevado grau de segurança e sigilo.*<br>*O SIGAD deve ser capaz de registrar e informar tentativas* | AD |

| Referência | Requisito | Obrig |
|---|---|---|
| | *indevidas de acesso.*<br><br>*Este requisito se aplica tanto a pesquisas em metadados quanto a pesquisas no próprio documento (texto livre).* | |
| 6.2.7 | Somente administradores autorizados têm que ser capazes de criar, alterar, remover ou revogar permissões associadas a papéis de usuários, grupos de usuários ou usuários individuais. | O |
| 6.2.8 | Um SIGAD deve implementar, imediatamente, alterações ou revogações dos atributos de segurança de usuários e de documentos digitais. | AD |
| 6.2.9 | Um SIGAD deve oferecer ferramentas de aumento de produtividade ao administrador, tais como a realização de operações sobre lotes ou grupos de usuários e lotes de documentos digitais, agenda de tarefas, análises de trilhas e geração de alarmes. | AD |
| 6.2.10 | Quando um SIGAD controlar o acesso por grupos de usuários, papéis de usuários e usuários individuais, deve obedecer a uma hierarquia de permissões preestabelecida na política de segurança. | AD |

### Controle de acesso por grupos de usuários

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

Estes requisitos só são aplicáveis às organizações em que há controle de acesso por grupos de usuários.

| Referência | Requisito | Obrig |
|---|---|---|
| 6.2.11 | Um SIGAD tem que implementar a política de controle de acesso a documentos por grupos de usuários considerando:<br><br>• a identidade do usuário e sua participação em grupos;<br><br>• os atributos de segurança, associados ao documento arquivístico digital, às classes e/ou aos dossiês/processos. | O |
| 6.2.12 | O acesso a documentos, a dossiês/processos ou classes, tem que ser concedido se a permissão requerida para a operação estiver associada a pelo menos um dos grupos aos quais pertença o usuário. | O |
| 6.2.13 | Um SIGAD tem que permitir que um usuário pertença a mais de um grupo. | O |
| 6.2.14 | Um SIGAD pode permitir que alguns usuários estipulem que outros usuários, papéis ou grupos de usuários podem ter acesso aos documentos sob sua responsabilidade. Essa permissão deve ser atribuída pelo administrador, de acordo com a política de segurança do órgão ou entidade. | F |

Controle de acesso por papéis de usuários

Papéis são funções ou cargos com responsabilidades e autoridades bem definidas. Operações correspondem a tarefas executadas nos documentos, dossiês/processos e classes. Atribuições de usuários são as associações entre usuários e papéis. Um usuário pode estar associado a um ou mais papéis e vice-versa. Permissões constituem garantias aprovadas para realização de operações em documentos arquivísticos.

Estes requisitos só são aplicáveis aos órgãos e entidades em que há controle de acesso por papéis de usuários.

| Referência | Requisito | Obrig |
|---|---|---|
| 6.2.15 | Um SIGAD tem que usar os seguintes atributos do usuário ao implementar a política de controle de acesso aos documentos digitais por papéis de usuários:<br>• identificação do usuário;<br>• papéis associados ao usuário. | O |
| 6.2.16 | Um SIGAD tem que usar os seguintes atributos dos documentos digitais ao implementar a política de controle de acesso por papéis:<br>• identificação do documento digital;<br>• operações permitidas aos vários papéis de usuários, sobre as classes ou unidades de arquivamento a que o documento pertence. | O |
| 6.2.17 | O acesso a documentos, dossiês/processos ou classes tem que ser concedido somente se a permissão requerida para a operação estiver presente em pelo menos um dos papéis associados ao usuário. | O |
| 6.2.18 | Um SIGAD tem que impedir que um usuário assuma papéis com direitos conflitantes. | O |
| 6.2.19 | Um SIGAD pode permitir a criação de hierarquias de papéis e o conceito de herança de permissões entre eles. | F |

## 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 documentos arquivísticos, com base na classificação do grau de sigilo, bem como à restrição de acesso à informação sensível. Informação sensível pode estar relacionada à honra e à privacidade de pessoas ou a questões estratégicas e de segredo corporativo. Os requisitos são flexíveis para atender tanto às organizações privadas como aos órgãos públicos. Os documentos produzidos pelos órgãos da administração pública estão sujeitos aos graus de sigilo definidos na legislação vigente.

Estes requisitos são aplicáveis às organizações em que o teor dos documentos produzidos e recebidos exige sigilo.

| Referência | Requisito | Obrig |
|---|---|---|
| 6.3.1 | Um SIGAD tem que implementar a classificação de grau de sigilo de documentos, dossiês/processos e classes do plano de classificação, e de todas as operações de usuários nos documentos. | O |
| 6.3.2 | Um SIGAD tem que implementar a classificação de grau de sigilo baseando-se nos seguintes atributos de segurança:<br>• grau de sigilo do documento;<br>• credencial de segurança do usuário.<br>*O grau de sigilo tem que estar associado à credencial de segurança.* | O |
| 6.3.3 | Um SIGAD tem que recusar o acesso de usuários a documentos que possuam grau de sigilo superior à sua credencial de segurança. | O |
| 6.3.4 | Um SIGAD tem que garantir que documentos sem atribuição de grau de sigilo, importados a partir de fontes externas ao SIGAD, estejam sujeitos às políticas de controle de acesso e de sigilo. | O |
| 6.3.5 | Um SIGAD tem que ser capaz de manter a marcação de sigilo original durante a importação de documentos a partir de fontes externas ao SIGAD. | O |
| 6.3.6 | Um SIGAD deve garantir que não haja ambiguidade na associação entre as marcações de grau de sigilo e outros atributos de segurança (permissões) do documento importado. | AD |
| 6.3.7 | Um SIGAD tem que permitir que um dos itens abaixo seja selecionado durante a configuração:<br>• graus de sigilo a serem atribuídos a classes e dossiês/processos;<br>• classes e dossiês/processos sem grau de sigilo. | O |
| 6.3.8 | Em caso de erro ou reavaliação, o administrador tem que ser capaz de alterar o grau de sigilo de todos os documentos arquivísticos de um dossiê/processo ou de uma classe, numa única operação. | O |
| 6.3.9 | Um SIGAD tem que 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 |

| Referência | Requisito | Obrig |
|---|---|---|
| 6.3.10 | Um SIGAD tem que permitir somente aos administradores autorizados a possibilidade de alterar a configuração dos valores predefinidos (*default*) para os atributos de segurança e marcação de graus de sigilo, quando necessário e apropriado. | O |
| 6.3.11 | Somente administradores autorizados têm que ser capazes de realizar as seguintes ações:<br>• remover ou revogar os atributos de segurança dos documentos;<br>• criar, alterar, remover ou revogar as credenciais de segurança dos usuários. | O |
| 6.3.12 | Um SIGAD tem que permitir somente ao usuário autorizado, mediante confirmação, a desclassificação ou redução do grau de sigilo de um documento | O |
| 6.3.13 | Um SIGAD deve permitir o armazenamento dos documentos sigilosos em meios físicos ou lógicos distintos. | AD |
| 6.3.14 | Um SIGAD tem que impedir que um documento sigiloso seja eliminado.<br>*Os documentos sigilosos têm que se tornar ostensivos para serem submetidos ao processo de avaliação e receberem a destinação prevista*. | O |
| 6.3.15 | Um SIGAD tem que implementar metadados nos níveis de dossiê, documento ou extrato de documento para controlar o acesso à informação sensível. | O |

## 6.4 Trilhas de auditoria

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

| Referência | Requisito | Obrig |
|---|---|---|
| 6.4.1 | Um SIGAD tem que ser capaz de registrar, na trilha de auditoria, informações acerca das ações a seguir:<br>• data e hora da captura de todos os documentos;<br>• responsável pela captura;<br>• reclassificação, desclassificação ou redução do grau de sigilo de um documento ou dossiê/processo, com a classificação inicial e final.<br>• qualquer alteração na tabela de temporalidade e destinaçãode documentos; | O |

| Referência | Requisito | Obrig |
|---|---|---|
| | • qualquer ação de reavaliação de documentos;<br>• qualquer alteração nos metadados associados a classes, dossiês/processos ou documentos;<br>• data e hora de produção, aditamento e eliminação de metadados;<br>• alterações efetuadas nas permissões de acesso que afetem um dossiê/processo, documento ou usuário;<br>• ações de exportação e importação envolvendo os documentos;<br>• tentativas de exportação (inclusive para *backup*) e importação (inclusive *restore*);<br>• usuário, data e hora de acesso ou tentativa de acesso a documentos e ao SIGAD;<br>• tentativas de acesso negado a qualquer documento;<br>• ações de eliminação de qualquer documento e seus metadados;<br>• infrações cometidas contra mecanismos de controle de acesso;<br>• mudanças no relógio gerador de carimbos de tempo;<br>• todas as ações administrativas sobre os atributos de segurança (papéis, grupos, permissões etc.);<br>• todas as ações administrativas sobre dados de usuários (cadastro, ativação, bloqueio, atualização de dados e permissões, troca de senha etc.);<br>• todos os eventos de administração e manutenção das trilhas de auditoria (alarmes, cópias, configuração de parâmetros etc.). | |
| 6.4.2 | Um SIGAD tem que registrar, em cada evento auditado, informações sobre a identidade do usuário, desde que essa identificação esteja de acordo com a política de privacidade da organização e a legislação vigente. | O |
| 6.4.3 | Um SIGAD deve permitir apenas ao administrador e ao auditor a leitura das trilhas de auditoria. | AD |
| 6.4.4 | Um SIGAD tem que assegurar que as informações da trilha de auditoria estejam disponíveis para inspeção, a fim de que uma ocorrência específica possa ser identificada e todas as informações correspondentes sejam claras e compreensíveis. | O |
| 6.4.5 | Um SIGAD deve possuir mecanismos para realização de buscas nos eventos das trilhas de auditoria.<br>*Para facilitar a visualização do relatório, os resultados podem ser apresentados de modo ordenado, mas essa ordenação não pode alterar os dados incluídos na trilha.* | AD |
| 6.4.6 | Um SIGAD tem que ser capaz de impedir qualquer modificação na trilha de auditoria. | O |

| Referência | Requisito | Obrig |
|---|---|---|
| 6.4.7 | Somente administradores autorizados têm que ser capazes de exportar as trilhas de auditoria sem afetar a trilha armazenada, ou transferir as trilhas de auditoria de um suporte de armazenamento para outro.<br><br>*A trilha de auditoria não pode ser excluída antes da data indicada na tabela de temporalidade. Porém, a transferência implica a cópia da trilha para outro espaço de armazenamento, com a subsequente liberação do espaço original. A exportação é a cópia sem liberação do espaço.* | O |
| 6.4.8 | Um SIGAD deve ser capaz de gerar um alarme para os administradores apropriados se o tamanho da trilha de auditoria exceder um limite preestabelecido.<br><br>*Esse alarme deve ser usado para indicar a proximidade do esgotamento do espaço reservado à trilha de auditoria.* | AD |
| 6.4.9 | Quando o espaço de armazenamento da trilha de auditoria atingir o limite preestabelecido, um SIGAD deve permitir somente operações auditáveis originadas por administradores.<br><br>*Todas as outras operações estarão bloqueadas até a liberação pelo administrador.* | AD |
| 6.4.10 | Um SIGAD deve ser capaz de aplicar um conjunto de regras na monitoração de eventos auditados e, com base nelas, indicar a possível violação da segurança. | AD |
| 6.4.11 | Um SIGAD deve garantir pelo menos as seguintes regras para monitoração dos eventos auditados:<br><br>• acumulação de um número predeterminado de tentativas consecutivas de *log in* com erro (autenticação malsucedida), conforme especificado pela política de segurança;<br><br>• ocorrência de vários *log in* simultâneos do mesmo usuário em locais (computadores) diferentes;<br><br>• *log in* do usuário fora do horário autorizado, após *logoff* no período normal. | AD |
| 6.4.12 | Um SIGAD tem que fornecer relatórios sobre as ações que afetam classes, unidades de arquivamento e documentos, em ordem cronológica e organizados por:<br><br>• documento arquivístico, unidade de arquivamento ou classe;<br><br>• usuário;<br><br>• tipo de ação ou operação. | O |
| 6.4.13 | Um SIGAD pode fornecer relatórios referentes a ações que afetem documentos e dossiês/processos organizados por posto de trabalho (nos casos em que for tecnicamente adequado), endereço de rede ou outra interface de acesso. | F |

| Referência | Requisito | Obrig |
|---|---|---|
| | *Alguns sistemas podem oferecer diversas interfaces de acesso aos documentos. Por exemplo, interface* web *externa, interface da intranet e interface* desktop*. Pode ser interessante o registro da interface de acesso usada.* | |
| 6.4.14 | Somente administradores autorizados têm que ser capazes de configurar o conjunto de eventos auditáveis e seus atributos. | O |
| 6.4.15 | Somente administradores autorizados, acompanhados do auditor, têm que ser capazes de configurar o conjunto de eventos auditáveis e seus atributos. | O |

## 6.5 Assinaturas digitais

Assinatura digital é uma sequência de *bits* que usa algoritmos específicos, chaves criptográficas e certificados digitais para autenticar a identidade do assinante e confirmar a integridade de um documento. Certificação digital é uma técnica, baseada em uma infraestrutura de chaves públicas, de garantia da validade de assinaturas digitais.

O uso de assinaturas digitais e de certificação digital na administração pública foi padronizado e normalizado com a criação da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

Os requisitos só são aplicáveis quando há necessidade de utilizar assinaturas digitais para assegurar autenticação, imputabilidade e irretratabilidade (ou irrefutabilidade).

| Referência | Requisito | Obrig |
|---|---|---|
| 6.5.1 | Um SIGAD deve ser capaz de garantir a origem e a integridade dos documentos com assinatura digital. | AD |
| 6.5.2 | Somente administradores autorizados têm que ser capazes de incluir, remover ou atualizar no SIGAD os certificados digitais de computadores ou de usuários. | O |
| 6.5.3 | Um SIGAD tem que ser capaz de verificar a validade da assinatura digital no momento da captura do documento. | O |
| 6.5.4 | Um SIGAD, no processo de verificação da assinatura digital, tem que ser capaz de registrar, nos metadados do documento, o seguinte:<br>• validade da assinatura verificada;<br>• registro da verificação da assinatura;<br>• data e hora em que ocorreu a verificação. | O |
| 6.5.5 | Um SIGAD deve ser capaz de armazenar, juntamente com o documento, as informações de certificação a seguir: | AD |

| Referência | Requisito | Obrig |
|---|---|---|
| | • assinatura digital;<br>• certificado digital (cadeia de certificação) usado na verificação da assinatura;<br>• lista de certificados revogados (LCR). | |
| 6.5.6 | Um SIGAD deve ser capaz de receber atualizações tecnológicas quanto à plataforma criptográfica de assinatura digital. | AD |
| 6.5.7 | Um SIGAD deve destruir ou tornar indisponíveis as chaves de criptografia que constem em listas de certificados revogados (LCR). | AD |
| 6.5.8 | Um SIGAD deve ter acesso a relógios e carimbador de tempo confiáveis para seu próprio uso.<br>*O relógio gerador do selo de tempo deve ser sincronizado com o Observatório Nacional.*[43] | AD |

## 6.6 Criptografia

Criptografia é um método de codificação de objetos digitais segundo um código secreto (chave), de modo que não possam ser apresentados de forma legível ou inteligível por uma aplicação e somente usuários autorizados sejam capazes de restabelecer sua forma original.

Esta seção trata dos serviços de segurança apoiados em criptografia. Estes requisitos só são aplicáveis a organizações em que há elevada necessidade de garantia de sigilo.

É importante salientar que, no uso de criptografia em documentos que apresentam longa temporalidade, devem ser tomadas medidas administrativas para garantir a manutenção do sigilo e do acesso. Esses documentos não devem ser armazenados criptografados. Alguns fatores que põem em risco a criptografia no longo prazo são o comprometimento ou obsolescência da chave, indisponibilidade do portador da chave e evoluções tecnológicas.

É importante lembrar mais uma vez que o Conselho Internacional de Arquivos define como longo prazo para documentos digitais um período de mais de cinco anos contados a partir da data de produção.[44]

| Referência | Requisito | Obrig |
|---|---|---|
| 6.6.1 | Um SIGAD tem que usar criptografia no armazenamento, na transmissão e na apresentação de documentos arquivísticos digitais ao implementar a política de sigilo. | O |
| 6.6.2 | Um SIGAD tem que limitar o acesso aos documentos cifrados somente àqueles usuários portadores da chave de decifração. | O |

[43] Observatório Nacional – Divisão do Serviço da Hora. Disponível em: <http://pcdsh01.on.br>.

[44] Ver CONSELHO INTERNACIONAL DE ARQUIVOS, 2005, p. 41.

| Referência | Requisito | Obrig |
|---|---|---|
| 6.6.3 | Um SIGAD tem que registrar os seguintes metadados sobre um documento cifrado:<br>• indicação sobre se está cifrado ou não;<br>• algoritmos usados na cifração;<br>• identificação do remetente;<br>• identificação do destinatário. | O |
| 6.6.4 | Um SIGAD deve poder assegurar a captura de documentos cifrados, diretamente, de uma aplicação de *software* que disponha da funcionalidade de cifração. | AD |
| 6.6.5 | Somente usuários autorizados têm que ser capazes de realizar as operações a seguir:<br>• incluir, remover ou alterar parâmetros dos algoritmos criptográficos instalados no SIGAD;<br>• incluir, remover ou substituir chaves criptográficas de programas ou usuários do SIGAD;<br>• cifrar e alterar a criptografia de documentos;<br>• remover a criptografia de um documento.<br>*A remoção da cifração pode ocorrer quando sua manutenção resultar na indisponibilidade do documento. Por exemplo, se a chave de cifração/decifração estiver embarcada em* hardware *inviolável cuja vida útil esteja prestes a se esgotar ou se o documento for desclassificado.* | O |
| 6.6.6 | Em caso de remoção da cifração do documento, os seguintes metadados adicionais têm que ser registrados na trilha de auditoria:<br>• data e hora da remoção da cifração;<br>• identificação do executor da operação;<br>• motivo da remoção da cifração. | O |
| 6.6.7 | Um SIGAD deve possuir arquitetura capaz de receber atualizações tecnológicas no que se refere à plataforma criptográfica. | AD |

## 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, que só pode ser suprimido mediante a utilização de um algoritmo ou de uma chave protegida. Tecnologias semelhantes podem ser aplicadas a sons e imagens em movimento digitalizadas.

O SIGAD pode manter, recuperar e assimilar novas tecnologias de marcas d'água.

Estes requisitos só são aplicáveis às organizações em que são usadas marcas d'água digitais.

| Referência | Requisito | Obrig |
|---|---|---|
| 6.7.1 | Um SIGAD tem que ser capaz de recuperar informação contida em marcas d'água digitais. | O |
| 6.7.2 | Um SIGAD tem que ser capaz de armazenar documentos arquivísticos digitais que contenham marcas d'água digitais, assim como informação de apoio relacionada à marca d'água. | O |
| 6.7.3 | Um SIGAD deve possuir arquitetura capaz de receber atualizações tecnológicas no que se refere à plataforma de geração e detecção de marca d'água digital. | AD |

## 6.8 Acompanhamento de transferência

Durante seu ciclo de vida, os documentos arquivísticos digitais e seus respectivos metadados podem ser transferidos de uma mídia de suporte, ou de um local, para outro, à medida que seu uso decresce e/ou se modifica. Essa transferência tanto pode ser interna, implicando, por exemplo, o deslocamento de armazenamento *on-line* para armazenamento *off-line*, como externa, envolvendo o deslocamento para outra instituição. É necessário um recurso de acompanhamento a fim de se registrar a mudança de local, para facilitar o acesso e cumprir requisitos regulamentares.

| Referência | Requisito | Obrig |
|---|---|---|
| 6.8.1 | Um SIGAD deve ser capaz de manter, para cada documento ou dossiê/processo, o histórico das movimentações e transferências de mídia sofridas por esse documento ou dossiê/processo. | AD |
| 6.8.2 | Um SIGAD tem que fornecer um recurso de acompanhamento para monitorar e registrar informações acerca do local atual e da transferência de dossiês/processos digitais e convencionais. | O |
| 6.8.3 | A função de acompanhamento de transferência tem que registrar metadados que incluam:<br>• número identificador dos documentos atribuído pelo sistema;<br>• localização atual e localizações anteriores, definidas pelo usuário;<br>• data e hora de envio/transferência;<br>• data e hora da recepção no novo local;<br>• destinatário;<br>• usuário responsável pela transferência (sempre que for adequado);<br>• 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 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 SIGAD de se autoproteger contra erros, falhas ou ataques ao próprio sistema.

Além dos requisitos de autoproteção, o SIGAD deve interagir com outros sistemas de proteção, tais como antivírus, *firewall* e *anti-spyware*.

| Referência | Requisito | Obrig |
|---|---|---|
| 6.9.1 | Um SIGAD deve fazer a verificação de vírus ou pragas antes da efetivação da captura. | AD |
| 6.9.2 | Um SIGAD deve ter dispositivos e procedimentos que reduzam a possibilidade de erros, falhas e descontinuidades no seu funcionamento, capazes de causar danos ou perdas aos documentos arquivísticos digitais. | AD |
| 6.9.3 | Após falha ou descontinuidade do sistema, quando a recuperação automática não for possível, um SIGAD tem que ser capaz de entrar em modo de manutenção, no qual é oferecida a possibilidade de restaurar o sistema para um estado seguro.<br>*Na restauração ao estado seguro, um SIGAD deve ser capaz de garantir a recuperação de perdas ocorridas, inclusive dos documentos de transações mais recentes.* | O |
| 6.9.4 | Um SIGAD deve garantir que os dados de segurança, quando replicados, sejam consistentes.<br>*Permissões de controle de acesso, chaves criptográficas e parâmetros de algoritmos criptográficos são exemplos de dados de segurança.* | AD |
| 6.9.5 | Um SIGAD tem que garantir que as funções de controle de acesso sejam invocadas antes de qualquer operação de acesso e retornem sem erros antes do prosseguimento da operação. | O |
| 6.9.6 | Um SIGAD tem que preservar um estado seguro de funcionamento, interrompendo completamente a interação com usuários comuns, quando ocorrer um dos erros a seguir:<br>• falha de comunicação entre cliente e servidor;<br>• perda de integridade das informações de controle de acesso;<br>• falta de espaço para registro nas trilhas de auditoria. | O |
| 6.9.7 | Quando não for possível escrever na trilha de auditoria, um SIGAD deve impedir toda operação de qualquer usuário e passar para o modo de manutenção. | AD |

| Referência | Requisito | Obrig |
|---|---|---|
| 6.9.8 | Um SIGAD deve detectar o reenvio de dados de autenticação e segurança de um usuário, sem conhecimento deste. O evento deve ser registrado nas trilhas, cancelando a comunicação com o sistema remoto/usuário e considerando o usuário fora do sistema. | AD |
| 6.9.9 | Um SIGAD pode atribuir a cada documento, no momento da captura, um código de manutenção de integridade baseado em criptografia robusta. | F |

## 6.10 Alterar, apagar e truncar documentos arquivísticos digitais

Os documentos arquivísticos completos não podem, em regra, ser alterados e eliminados, exceto no término do seu ciclo de vida num SIGAD. No entanto, os administradores podem precisar apagar documentos arquivísticos para corrigir erros de usuário (p. ex., declarar documentos de arquivo no dossiê/processo errado) ou para cumprir requisitos jurídicos no âmbito da legislação sobre proteção de dados. A ação de eliminar pode ter um dos significados a seguir:

- eliminação definitiva;
- retenção, acompanhada de anotação nos metadados do documento arquivístico, informando que ele não está mais sob o controle da gestão de documentos arquivísticos.

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

Às vezes, os administradores têm necessidade de publicar ou disponibilizar documentos arquivísticos que contêm informações sigilosas (seja em consequência de legislação sobre proteção de dados, seja por questões de segurança ou segredo comercial etc.). Por esse motivo, aos administradores têm que ser dada a possibilidade de retirar a informação sensível, sem afetar o documento arquivístico correspondente. Esse processo é chamado de truncamento ou corte, e o SIGAD armazena o documento original e a cópia truncada, chamada de “extrato”.

| Referência | Requisito | Obrig |
|---|---|---|
| 6.10.1 | Um SIGAD tem que permitir, a um administrador autorizado, anular a operação em caso de erro do usuário ou do sistema.<br><br>*Anular uma operação não significa apagar um documento arquivístico capturado pelo SIGAD.*<br><br>*A anulação da eliminação definitiva de documentos, por ser irreversível, não é possível.* | O |
| 6.10.2 | Um SIGAD, para evitar erros irrecuperáveis, deve inibir a eliminação (permanente ou lógica) de grupos ou lotes de documentos fora do processo regular de eliminação previsto na tabela de temporalidade e destinação de documentos. | AD |

| Referência | Requisito | Obrig |
|---|---|---|
| 6.10.3 | Em situações excepcionais, o administrador tem que ser autorizado a apagar ou corrigir dossiês/processos, volumes e documentos. Nesse caso, um SIGAD tem que:<br>• registrar integralmente a ação de apagar ou corrigir na trilha de auditoria;<br>• produzir um relatório de anomalias para o administrador;<br>• eliminar todo o conteúdo de um dossiê/processo ou volume, quando forem eliminados;<br>• garantir que nenhum documento seja eliminado se tal ação resultar na alteração de outro documento arquivístico;<br>• informar o administrador sobre a existência de ligação entre um dossiê/processo ou documento prestes a ser apagado e qualquer outro dossiê/processo ou documento, solicitando confirmação antes de concluir a operação;<br>• manter a integridade total do metadado, a qualquer momento. | O |
| 6.10.4 | Em caso de erro na inserção de metadados, o administrador terá que corrigi-lo, e o SIGAD tem que registrar essa ação na trilha de auditoria. | O |
| 6.10.5 | Um SIGAD tem que permitir a um usuário autorizado fazer um extrato (cópia truncada) de um documento, com o objetivo de não alterar o original. | O |
| 6.10.6 | Um SIGAD deve possibilitar a ocultação de informação sigilosa contida na cópia truncada do documento, permitindo:<br>• retirada de páginas de um documento;<br>• adição de retângulos opacos para ocultar nomes ou palavras sensíveis;<br>• quaisquer outros recursos necessários para formatos de vídeo ou áudio, caso existam.<br>Se o SIGAD não fornecer, diretamente, esses recursos, tem que permitir que outros pacotes de *software* os proporcionem.<br>*É essencial que, quando os recursos para truncar documentos forem empregados, nenhuma informação retirada ou ocultada seja passível de visualização na cópia truncada, na tela, nem quando impressa ou reproduzida por meios audiovisuais, independentemente da utilização de quaisquer recursos, tais como rotação, variação focal ou qualquer outra manipulação.* | AD |
| 6.10.7 | Quando uma cópia truncada é produzida, um SIGAD tem que registrar essa ação nos metadados do documento, incluindo, pelo menos, data, hora, motivo e quem a produziu. | O |
| 6.10.8 | Um SIGAD pode solicitar a quem produziu a cópia truncada que a inclua em um dossiê/processo. | F |

| Referência | Requisito | Obrig |
|---|---|---|
| 6.10.9 | Um SIGAD deve registrar uma referência cruzada a uma cópia truncada nos mesmos dossiês/processos, pastas e documentos em que se encontra o documento original. | AD |
| 6.10.10 | Um SIGAD tem que armazenar, na trilha de auditoria, qualquer alteração efetuada para satisfazer os requisitos desta seção. | O |

# 7 ARMAZENAMENTO

A estrutura de armazenamento em um SIGAD deve fazer parte de uma arquitetura tecnológica que permita a preservação e a recuperação de longo prazo dos documentos arquivísticos. Por isso, essa estrutura deve abrigar os documentos, seus metadados, os metadados do sistema (informações sobre segurança, direitos de acesso e usuários, entre outros), trilhas de auditoria e cópias de segurança. Do ponto de vista físico, tais informações residem em dispositivos de armazenamento eletrônicos, magnéticos e ópticos.

A arquitetura tecnológica para gerenciamento de arquivos digitais deve ser planejada e dimensionada de acordo com a missão e as competências da organização. Além disso, os equipamentos devem adequar-se às características *on-line* ou *off-line* das operações. Operações *on-line* são aquelas que só podem ser realizadas através do SIGAD, ao passo que operações *off-line* podem ser executadas em outros sistemas computacionais, pois estão desvinculadas do funcionamento do SIGAD.

Um SIGAD deve utilizar dispositivos e técnicas de armazenamento que garantam a integridade dos documentos arquivísticos digitais.

Os itens a seguir enumeram requisitos de armazenamento organizados segundo os critérios de durabilidade, capacidade e efetividade de armazenamento.

## 7.1 Durabilidade

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

| Referência | Requisito | Obrig |
|---|---|---|
| 7.1.1 | Um SIGAD deve utilizar, preferencialmente, dispositivos e padrões de armazenamento maduros, estáveis no mercado e amplamente disponíveis.<br><br>*Um SIGAD deve utilizar, preferencialmente, padrões abertos de armazenamento (como, por exemplo, ISO 9660:1999, definição do formato de sistema de arquivos para CD-ROM).*<br><br>*A escolha dos dispositivos de armazenamento deve contemplar padrões estáveis de mercado e fornecedores consolidados.* | AD |

| Referência | Requisito | Obrig |
|---|---|---|
| 7.1.2 | A escolha de dispositivos tem que ser revista sempre que a evolução tecnológica indicar mudanças importantes. | O |
| 7.1.3 | Atividades de migração têm que ser efetivadas, preventivamente, sempre que se torne patente ou previsível a obsolescência do padrão corrente. | O |
| 7.1.4 | Para as memórias secundárias, um SIGAD tem que manter registro de MTBF (*mean time between failure*),[45] bem como suas datas de aquisição. | O |
| 7.1.5 | Para as memórias secundárias e terciárias, um SIGAD tem que fazer o gerenciamento das mídias por meio do registro de durabilidade prevista, data de aquisição e histórico de utilização.<br><br>*As informações técnicas sobre previsibilidade de duração de mídias referidas no item/elemento 7.1.3 devem ser obtidas, preferencialmente, a partir de órgãos independentes. Quando isso não for possível, podem ser utilizadas informações de fornecedores.*<br><br>*Em ambos os casos deve ficar registrada a origem da informação.* | O |
| 7.1.6 | Para as memórias secundárias e terciárias, um SIGAD deve manter estatísticas da durabilidade efetivamente observada. | AD |
| 7.1.7 | No caso de uso de fitas magnéticas, o mecanismo de *backup* provido pelo SIGAD deve proporcionar meios para que o item/elemento 8.2.6 possa ser implementado automaticamente, integrado à ação do *backup*. | AD |
| 7.1.8 | O acesso às informações armazenadas em memória terciária deve ser efetuado, preferencialmente, mediante o uso de rede de dados.<br><br>*O objetivo é minimizar o acesso físico às mídias, visando à diminuição do desgaste. A manipulação direta das mídias deve ser restrita aos administradores do sistema, e não aos usuários comuns.* | AD |
| 7.1.9 | Quando se proceder à eliminação de documentos, as memórias de suporte têm que ser, devidamente, “sanitizadas”, isto é, ter suas informações, efetivamente, indisponibilizadas.<br><br>*Este requisito aplica-se, principalmente, às memórias secundária e terciária, por 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 |

[45] MTBF (*mean time between failure*, ou tempo médio entre falhas, é um valor relativo ao período médio entre as falhas de um sistema ou dispositivo, que permite a avaliação de sua confiabilidade ou vida útil.

## 7.2 Capacidade

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

| Referência | Requisito | Obrig |
|---|---|---|
| 7.2.1 | Um SIGAD tem que possuir capacidade de armazenamento suficiente para acomodação de todos os documentos e suas cópias de segurança.<br><br>*Para grandes volumes de dados, é conveniente o uso de dispositivos com maior capacidade unitária de armazenamento, a fim de reduzir a sobrecarga operacional.* | O |
| 7.2.2 | Em um SIGAD, tem que ser prevista a possibilidade de expansão da estrutura de armazenamento.<br><br>*A quantidade de memória primária deve ser superestimada no momento da aquisição, a fim de minimizar as indisponibilidades do SIGAD nas situações de expansão desse tipo de memória.*<br><br>*Quando da aquisição de* disk arrays*, as possibilidades de expansão dos equipamentos de controle devem ser consideradas.*<br><br>*Para* backups *em fita magnética, em sistemas com grande volume de informação, devem ser utilizados sistemas automáticos de seleção, troca e controle de fitas (*robots*).* | O |
| 7.2.3 | Um SIGAD deve permitir ao administrador configurar os limites de capacidade de armazenamento dos diversos dispositivos. | AD |
| 7.2.4 | Um SIGAD deve oferecer ao administrador facilidades para monitoração da capacidade de armazenamento.<br><br>*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.* | AD |
| 7.2.5 | Um SIGAD deve informar, automaticamente, ao administrador quando os dispositivos de armazenamento *on-line* atingirem níveis críticos de ocupação. | AD |
| 7.2.6 | Um SIGAD deve manter estatísticas de taxa de crescimento de utilização de memória secundária e terciária para informar ao administrador previsões de exaustão de recursos.<br><br>*Este tipo de estimativa possibilita ao administrador antecipar ações de expansão antes que a utilização atinja níveis críticos.* | AD |

## 7.3 Efetividade de armazenamento

| Referência | Requisito | Obrig |
|---|---|---|
| 7.3.1 | Os dispositivos de armazenamento de um SIGAD devem suportar métodos de detecção de erros para leitura e escrita de dados. | AD |
| 7.3.2 | Um SIGAD tem que utilizar técnicas de restauração de dados em caso de falhas. | O |
| 7.3.3 | Um SIGAD tem que utilizar mecanismos de proteção contra escrita, que previnam alterações indevidas e mantenham a integridade dos dados armazenados. | O |
| 7.3.4 | A infraestrutura de um SIGAD deve prever o uso de técnicas para garantir maior confiabilidade e desempenho.<br>As técnicas recomendadas incluem:<br>• espelhamento (*mirroring*) nas memórias secundárias para maior confiabilidade;<br>• partição de dados (*data stripping*) nas memórias secundárias para maior desempenho. | AD |
| 7.3.5 | A integridade dos dispositivos de armazenamento tem que ser, periodicamente, verificada. | O |

# 8 PRESERVAÇÃO

Exatamente como no caso dos documentos convencionais, a preservação de documentos arquivísticos digitais não é um fim em si mesmo. Antes possui um propósito que deve ser considerado na definição e implementação das estratégias de preservação. A razão para se preservar um determinado documento pode ser seu valor probatório e/ou informativo.

Os documentos arquivísticos digitais gerenciados por um SIGAD devem ser preservados durante todo o período previsto para sua guarda, conforme determinado na tabela de temporalidade e destinação de documentos. Ressalte-se que as características desses documentos demandam atenção específica, sobretudo em relação àqueles que serão mantidos por mais de cinco anos, o que, nesse contexto, já se considera preservação de longo prazo.

A *degradação do suporte* e a *obsolescência tecnológica* são os principais fatores de comprometimento da preservação dos documentos digitais, uma vez que ameaçam sua autenticidade, integridade e acessibilidade.

A degradação do suporte é causada por fatores como falta de controle de temperatura, umidade, luminosidade, agentes químicos e biológicos agressores, bem como pela manipulação inadequada ou baixa/má qualidade do suporte

utilizado. Além de respeitar as condições ambientais especificadas pelo fabricante, é preciso realizar a substituição dos suportes antes do fim de sua vida útil, técnica conhecida como atualização (*refreshing*).

A obsolescência tecnológica refere-se tanto a *hardware* como a *software* e formatos. É resultado das mudanças causadas pelo desenvolvimento de novas tecnologias e sua ascensão no mercado.

O *hardware* obsoleto pode ser, por exemplo, um determinado tipo de suporte (por exemplo, disco óptico, fita magnética), unidades de disco, unidades de fita magnética ou mesmo os processadores e componentes utilizados na execução de programas (*software)*. Em alguns casos, os fabricantes procuram manter a compatibilidade com o antigo *hardware*, assegurando que *software* e formatos antigos continuem sendo utilizados. No entanto, essa situação não persiste indefinidamente, pois a compatibilidade geralmente é mantida apenas em relação aos *hardware*s recém-substituídos.

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 frequentes. Os *software* podem ser, simplesmente, descontinuados, substituídos por outros equivalentes, supostamente melhores, 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 devido a mudanças ocorridas nos programas (*software)* aos quais estão associados. Novos programas (*software*) podem ser compatíveis com os formatos antigos, mas podem apresentar incorreções durante operações de leitura e escrita de dados nesses formatos.

Estas são algumas das técnicas comumente utilizadas para evitar os riscos provenientes da obsolescência tecnológica:

- preservação da tecnologia: evita a necessidade imediata de implementação de novos sistemas. Porém, a manutenção e a integração com outros sistemas podem tornar-se problemáticas ao longo do tempo. A preservação do *hardware*, em especial, é uma alternativa cara, mesmo nas situações em que é compartilhado por mais de um usuário. Além disso, essa alternativa não é exequível no longo prazo, uma vez que o *hardware* pode ser danificado de forma irreversível, ficando completamente indisponível.
- emulação: é a simulação de determinado *hardware* ou *software* por meio de *software*. Permite que um computador moderno, possivelmente mais barato e de fácil manutenção, possa executar programas (*software*) antigos, desenvolvidos, originalmente, para outra plataforma. Para evitar possíveis perdas de informação e funcionalidades, deve ser realizada com bastante rigor. A probabilidade de perda de informações e funcionalidades aumenta à medida que são utilizadas diversas camadas de emulação, como resultado da aplicação desta técnica repetidas vezes.
- conversão de dados: é empregada quando os formatos tornam-se obsoletos. Os dados em formatos antigos são convertidos para novos formatos, apoiados em *hardware* e *software* mais atuais. Esse processo não está livre de problemas,

podendo resultar em perda de informações e funcionalidades. A conversão de dados também pode ser utilizada para reduzir a quantidade de formatos utilizados e, consequentemente, de sistemas a serem mantidos e gerenciados, de modo a facilitar as ações de preservação.

- migração: a migração para novos sistemas é realizada no caso de obsolescência de *hardware*, *software* ou formatos. Envolve, inclusive, conversão de dados. Pode abranger grande quantidade de elementos – *hardware*, *software* e formatos – e, dessa forma, apresentar maior complexidade de planejamento e execução. 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 funcionalidade dos documentos arquivísticos 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 uso de métodos de preservação, sua solução pode ser muito dispendiosa. Por isso, a preocupação com a preservação deve existir desde a concepção do SIGAD e a escolha de sua base tecnológica. De modo geral, recomenda-se o uso de suportes de alta qualidade e com previsão de vida útil adequada aos propósitos de preservação, o monitoramento contínuo dos avanços tecnológicos e da degradação do suporte, a adoção de formatos abertos e a busca por soluções independentes de *hardware*, *software* e fornecedor.

As estratégias e 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.

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. Levando em conta esses aspectos, cada organização deve desenvolver e implementar sua própria estratégia de preservação de documentos arquivísticos digitais, da forma mais adequada à sua realidade e de acordo com as diretrizes fornecidas pela instituição arquivística em sua esfera de competência.

## 8.1 Aspectos físicos

| Referência | Requisito | Obrig |
|---|---|---|
| 8.1.1 | Os suportes de armazenamento de um SIGAD têm que ser acondicionados, manipulados e utilizados em condições ambientais compatíveis com sua vida útil prevista e/ou pretendida, de acordo com as especificações técnicas do fabricante e de entidades isentas, e com base em estatísticas de uso.<br><br>*A vida útil pretendida de um suporte pode ser menor que sua vida útil prevista, o que permite condições ambientais mais flexíveis.* | O |

| Referência | Requisito | Obrig |
|---|---|---|
| 8.1.2 | Um SIGAD deve permitir ao administrador especificar a vida útil prevista/pretendida dos suportes. | AD |
| 8.1.3 | Um SIGAD tem que permitir o controle da vida útil dos suportes para auxiliar no processo de atualização. | O |
| 8.1.4 | Um SIGAD deve informar, automaticamente, quais são os suportes cuja vida útil se encontra perto do fim. | AD |

## 8.2 Aspectos lógicos

| Referência | Requisito | Obrig |
|---|---|---|
| 8.2.1 | Um SIGAD tem que manter cópias de segurança.<br>*As cópias de segurança devem ser guardadas em ambientes seguros, em locais diferentes de onde se encontra a informação original.* | O |
| 8.2.2 | Um SIGAD tem que possuir funcionalidades para verificação periódica dos dados armazenados, visando à detecção de possíveis erros.<br>*Nesse caso, recomenda-se o uso de um* checksum *robusto, ou seja, que permita a constatação da integridade dos dados e seja seguro quanto a fraudes.* | O |
| 8.2.3 | Um SIGAD tem que permitir a substituição dos dados armazenados que apresentarem erros. | O |
| 8.2.4 | Um SIGAD pode permitir a correção dos erros detectados nos dados armazenados.<br>*Nesse contexto, a correção de erros refere-se à restauração de dados corrompidos.* | F |
| 8.2.5 | Um SIGAD deve informar os resultados da verificação periódica dos dados armazenados, incluindo os erros detectados, bem como as substituições e correções de dados realizadas. | AD |
| 8.2.6 | Um SIGAD deve manter um histórico dos resultados da verificação periódica dos dados armazenados. | AD |
| 8.2.7 | Ações de preservação têm que ser efetivadas sempre que se torne patente ou previsível a obsolescência da tecnologia utilizada pelo SIGAD. | O |
| 8.2.8 | Um SIGAD tem que suportar a transferência em bloco de documentos (incluindo as demais informações associadas a cada documento) para outros suportes e/ou sistemas, de acordo com as normas aplicáveis aos formatos utilizados. | O |

## 8.3 Aspectos gerais

| Referência | Requisito | Obrig |
|---|---|---|
| 8.3.1 | Um SIGAD tem que registrar, em trilhas de auditoria, as operações de preservação realizadas. | O |
| 8.3.2 | Um SIGAD deve utilizar suportes de armazenamento e recursos de *hardware* e *software* que sejam maduros, estáveis no mercado e amplamente disponíveis. | AD |
| 8.3.3 | As modificações em um SIGAD e em sua base tecnológica têm que ser verificadas num 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 |
| 8.3.4 | Um SIGAD deve utilizar normas amplamente aceitas, descritas em especificações abertas e disponíveis publicamente, no que se refere a estruturas para codificação, armazenamento e banco de dados. | AD |
| 8.3.5 | Um SIGAD deve evitar o uso de estruturas proprietárias para codificação, armazenamento ou banco de dados. Caso venha a utilizá-las, devem estar plenamente documentadas, e essa documentação, disponível para o administrador. | AD |
| 8.3.6 | Um SIGAD tem que gerir metadados relativos à preservação dos documentos e seus respectivos componentes. | O |

# 9 FUNÇÕES ADMINISTRATIVAS

| Referência | Requisito | Obrig |
|---|---|---|
| 9.1.1 | Um SIGAD tem que permitir que os administradores, de maneira controlada e sem esforço excessivo, recuperem, visualizem e reconfigurem os parâmetros do sistema e os atributos dos usuários. | O |
| 9.1.2 | Um SIGAD tem que fornecer relatórios flexíveis para que o administrador possa gerenciar os documentos e seu uso. Esses relatórios devem apresentar, no mínimo:<br>• quantidade de dossiês/processos, volumes e itens a partir de parâmetros ou atributos definidos (tempo, classe, unidade administrativa etc.);<br>• estatísticas de transações relativas a dossiês/processos, volumes e itens;<br>• atividades por usuário. | O |

| Referência | Requisito | Obrig |
|---|---|---|
| 9.1.3 | Um SIGAD tem que dispor de documentação referente a aspectos de administração do sistema. A documentação deve incluir todas as informações necessárias para o correto gerenciamento do sistema. | O |

## 10 CONFORMIDADE COM A LEGISLAÇÃO E REGULAMENTAÇÕES

Um SIGAD tem que cumprir a legislação e as regulamentações vigentes. Setores de atividades distintos apresentam requisitos legislativos e regulamentares diferenciados. Sendo assim, todos os requisitos desta seção são genéricos e têm que ser adaptados à realidade de cada órgão produtor de documentos arquivísticos.[46]

| Referência | Requisito | Obrig |
|---|---|---|
| 10.1.1 | Um SIGAD tem que estar de acordo com a legislação e as normas pertinentes, tendo em vista a admissibilidade legal e o valor probatório dos documentos arquivísticos. | O |
| 10.1.2 | Um SIGAD tem que estar de acordo com a legislação e as normas específicas para gestão e acesso de documentos arquivísticos. | O |
| 10.1.3 | Um SIGAD tem que estar em conformidade com requisitos regulamentares específicos e códigos de boa prática necessários para a execução de determinadas atividades.<br>*Este requisito pode ser personalizado para cada contexto, como, por exemplo, saúde, justiça, educação, previdência.* | O |

## 11 USABILIDADE

Um sistema de *software* com boa usabilidade[47] deve apoiar a realização de tarefas simples, diretas e objetivas, que garantam as metas de produtividade e qualidade de trabalho do usuário. Se os usuários de um SIGAD encontrarem inúmeras dificuldades de operação, sua efetiva implantação pode fracassar, ocasionando desperdício de recursos.

Para se obter maior grau de usabilidade, deve-se pensar no usuário e em suas necessidades de utilização, o que significa criar um sistema fácil de entender, de operar, e que siga padrões de boas práticas técnicas já conhecidas e bem estabelecidas. A usabilidade depende, diretamente, das tarefas específicas que os

[46] Para obter informações sobre a legislação arquivística brasileira, consulte a seção Legislação Arquivistica Brasileira, disponível em <http://www.conarq.arquivonacional.gov.br>.

[47] Uma das características de qualidade em uso do *software* é a usabilidade, conforme a norma ISO/IEC 9126:1991 Information technology – *Software* product evaluation : quality characteristics and guidelines for their use. 1991.

usuários realizam por meio do sistema, bem como do nível de conhecimento desse sistema pelos usuários envolvidos.

As recomendações para boa usabilidade estão associadas ao contexto operacional do sistema, aos diferentes tipos de usuários, tarefas, ambientes físicos e organizacionais. Ao se elaborar a descrição das características de um SIGAD, deve-se considerar a facilidade de utilização da interface, tipos de usuários, facilidade na execução de tarefas, uso de equipamentos adequados, ergonomia, ambiente e contexto de uso.

| Referência | Requisito | Obrig |
|---|---|---|
| 11.1.1 | Um SIGAD deve possuir documentação completa, clara, inteligível e organizada para instalação e uso do *software*. | AD |
| 11.1.2 | Um SIGAD deve possuir sistema de ajuda *on-line*. | AD |
| 11.1.3 | O sistema de ajuda o*n-line* fornecido pelo SIGAD deve ser vinculado à função ou tarefa executada, em todo o sistema.<br>*Exemplo: Se o usuário estiver executando uma operação de edição, uma vez acionada a ajuda, ela deve remeter ao tópico de ajuda sobre edição.* | AD |
| 11.1.4 | Um SIGAD deve permitir a personalização de conteúdo de ajuda *on-line* por adição de texto ou edição do texto existente.<br>*Exemplo: O responsável pela administração do conteúdo da ajuda pode adicionar esclarecimentos ou alterar o conteúdo das descrições, de modo a facilitar o entendimento das funções.* | AD |
| 11.1.5 | Toda mensagem de erro produzida pelo SIGAD deve ser clara e significativa, de modo a permitir que o usuário se recupere do erro ou cancele a operação. | AD |
| 11.1.6 | A interface de um SIGAD deve seguir padrões preestabelecidos e consolidados como boas práticas de projeto gráfico.<br>*Normas ou regras de interface podem ser relativas à utilização de padrão de identidade visual (ligado à "marca" da instituição ou a alguma legislação específica do estado, município ou órgão federal), bem como de guias de estilo para implementação e verificação da padronização da interface.*<br>*Exemplo: Em 2000, o Conselho Nacional de Arquivos (CONARQ) elaborou o documento "Diretrizes gerais para a construção de websites de instituições arquivísticas", que procura fornecer um referencial básico às entidades interessadas em criar ou redefinir seus sítios na Internet.* | AD |
| 11.1.7 | O SIGAD deve empregar um conjunto simples e consistente de regras de interface, privilegiando a facilidade de aprendizado das operações pelos seus usuários.<br>*O uso de um conjunto de regras em conformidade com o ambiente operacional em que o SIGAD será executado permite* | AD |

| Referência | Requisito | Obrig |
|---|---|---|
| | *que ele apresente menus, comandos e outras facilidades consistentes em toda a aplicação.*<br><br>*Essas regras de interface, quando compatíveis com outras aplicações principais já instaladas, levam à padronização da terminologia utilizada para funções, rótulos e ações no sistema.* | |
| 11.1.8 | A interface de visualização dos documentos arquivísticos deve fornecer o recurso de arrastar e soltar, se for apropriado no ambiente operacional do SIGAD. | AD |
| 11.1.9 | O SIGAD deve permitir que sua estrutura de classes e dossiês/processos possa ser visualizada em diferentes formas de apresentação. | AD |
| 11.1.10 | O usuário deve poder personalizar a interface gráfica de um SIGAD. A personalização deve incluir, pelo menos, as seguintes possibilidades:<br><br>• conteúdo de menus;<br><br>• formatos de tela;<br><br>• utilização de teclas de função;<br><br>• alteração de cor, fonte e tamanho de letra em telas e janelas;<br><br>• avisos sonoros. | AD |
| 11.1.11 | Sempre que um SIGAD utilizar janelas *pop-up* e barras de ferramentas, deve-se oferecer ao usuário a possibilidade de configurar e habilitar/desabilitar esse tipo de recurso.<br><br>*Porém, é preciso não infringir a recomendação de uso de um conjunto simples e consistente de regras de interface.* | AD |
| 11.1.12 | Sempre que um SIGAD permitir o uso de janelas, deve admitir sua movimentação, redimensionamento e gravação das modificações da aparência, possibilitando a personalização por perfil de usuário. | AD |
| 11.1.13 | Um SIGAD deve permitir a seleção de avisos sonoros e a personalização de tom e volume, bem como a gravação dessas escolhas no perfil do usuário. | AD |
| 11.1.14 | Um SIGAD deve permitir a gravação de opções *default* para entrada de dados de configuração, como:<br><br>• valores de variáveis definidas pelo usuário;<br><br>• valores iguais aos de um item anterior;<br><br>• valores que possam ser selecionados em uma lista configurável;<br><br>• valores derivados do contexto, como data, referência do dossiê/processo, identificador do usuário;<br><br>• valores predefinidos por um administrador (para campos de | AD |

| Referência | Requisito | Obrig |
|---|---|---|
| | metadados como, por exemplo, o nome da organização que está utilizando o sistema). | |
| 11.1.15 | A interface de um SIGAD com o usuário deve ser adequada a adaptações e personalizações que permitam sua utilização por usuários com necessidades especiais. Essas opções devem ser compatíveis com *software* especializado que possa vir a ser acoplado (por exemplo, leitores de tela para cegos), bem como seguir orientações específicas de acessibilidade de interface.<br><br>*Para ambientes e sítios apoiados na* web*, é importante seguir orientações específicas de acessibilidade.*[48]<br><br>*É desejável que o padrão considerado possa ser verificado por meio da aplicação de uma validação manual ou automática, de preferência visando à obtenção de certificação de acessibilidade.* | AD |
| 11.1.16 | Um SIGAD deve permitir a realização de transações ou tarefas mais frequentemente executadas com um pequeno número de interações (por exemplo, cliques de mouse) e sem mudanças excessivas de contexto. | AD |
| 11.1.17 | Um SIGAD deve estar fortemente integrado ao sistema de correio eletrônico da organização, de forma a permitir a geração de mensagens com possibilidade de manipular documentos digitais, sem necessidade de sair do SIGAD.<br><br>*Este requisito deve estar de acordo com as normas de segurança.* | AD |
| 11.1.18 | Em caso de integração do SIGAD com o sistema de correio eletrônico, deve ser possível fazer referências a documentos arquivísticos sem necessidade de envio de cópias adicionais. | AD |
| 11.1.19 | Um SIGAD deve estar integrado com o sistema padrão de edição de documentos, de modo que possa fazer uso da facilidade de gravação. | AD |
| 11.1.20 | Um SIGAD pode fornecer recursos que possibilitem o reconhecimento óptico de caracteres (como, por exemplo, OCR – *optical character recognition* e ICR – *intelligent character recognition*), quando for necessária a introdução de metadados a partir de imagens de documentos impressos ou etiquetas identificadoras de documentos. | F |
| 11.1.21 | Um SIGAD deve permitir a definição e utilização de referências cruzadas entre documentos arquivísticos digitais correlacionados, bem como a fácil navegação entre eles, inclusive com o uso de | AD |

[48] Exemplos: "e-MAG – Modelo de acessibilidade de governo eletrônico", disponível em <http://www.governoeletronico.gov.br/governoeletronico/index.wsp>; decreto n. 5.296, de 2 de dezembro de 2004, que "estabelece normas gerais e critérios básicos para a promoção da acessibilidade das pessoas portadoras de deficiência ou com mobilidade reduzida"; "Guia de acessibilidade – PRODAM", <http://prodam.sp.gov.br/acessibilidade>; "Guia de validação – SERPRO", <http://www.serpro.gov.br/acessibilidade/g_validacao.php>; "W3C – HTML validation service", <http://validator.w3c.org>.

| Referência | Requisito | Obrig |
|---|---|---|
| | *hyperlinks*. | |
| 11.1.22 | Um SIGAD deve disponibilizar pelo menos dois papéis de acesso diferenciados, um para usuário final e outro para administrador de sistema. | AD |
| 11.1.23 | Um SIGAD deve fornecer a usuários finais e administradores funções intuitivas e fáceis de usar, que requeiram poucas ações para completar uma tarefa padrão.<br>Sobretudo durante sua operação normal, um SIGAD deve ser capaz de:<br>• capturar e declarar um documento arquivístico com no máximo três cliques de mouse ou acionamentos de tecla;<br>• apresentar todos os elementos de metadados obrigatórios para a captura do documento com mínima demanda para o usuário;<br>• apresentar o conteúdo de um documento arquivístico, a partir de uma lista de pesquisa, com no máximo três cliques de mouse ou acionamentos de tecla;<br>• apresentar os metadados de um documento arquivístico com no máximo três cliques de mouse ou acionamentos de tecla. | AD |
| 11.1.24 | Um SIGAD tem que restringir o acesso às funcionalidades administrativas e impossibilitar sua visualização pelo usuário final.<br>*Exemplos: As operações não disponíveis aparecem com fonte atenuada nos menus e possuem efeito nulo quando acionadas.*<br>*O acesso às operações indisponíveis é restringido pela configuração dos menus, que não apresentam essas operações ao usuário sem permissão para executá-las.* | O |
| 11.1.25 | Um SIGAD deve levar em consideração as condições de operação, como ruído, luminosidade, necessidade de rapidez na conclusão da tarefa, demandas específicas para dispositivos móveis, ambiente *desktop/web* e necessidade de instalação automática, para configurar as formas de interação com o usuário.<br>*Exemplo: Não devem ser utilizados menus audíveis em ambientes que apresentam alto volume de ruído próximo aos terminais de usuários.* | AD |

## 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 SIGAD 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 o "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".[49] Isto se faz por meio do uso de regras e padrões de comunicação.

O governo brasileiro definiu a arquitetura e-PING – Padrões de Interoperabilidade de Governo Eletrônico, visando à interoperabilidade nas diversas esferas do poder público.[50] Nos órgãos e entidades da administração pública federal, o SIGAD tem que adotar a arquitetura e-PING a fim de aumentar a viabilidade técnica no intercâmbio de informações entre sistemas.

| Referência | Requisito | Obrig |
|---|---|---|
| 12.1.1 | Um SIGAD deve ser capaz de interoperar com outros SIGAD, permitindo, pelo menos, consulta, recuperação, importação e exportação de documentos e seus metadados.<br>*As operações de interoperabilidade devem respeitar a legislação vigente e a política de segurança.* | AD |
| 12.1.2 | Um SIGAD deve ser capaz de interoperar com outros sistemas por meio de padrões abertos de interoperabilidade.<br>*Por exemplo, padrões abertos como os estabelecidos pela e-PING, XML e Dublin Core.* | AD |
| 12.1.3 | Um SIGAD tem que aplicar os requisitos de segurança descritos neste documento para executar operações de interoperabilidade.<br>*Isso é fundamental para que as operações, feitas em ambiente com interoperabilidade, não afetem a integridade dos documentos e impossibilitem acessos não autorizados.* | O |

## 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 SIGAD de acordo com o nível de serviço a ser fornecido. Por exemplo, os períodos previstos de atendimento ("8x5" indica oito 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

[49] <http://www.governoeletronico.gov.br/governoeletronico/publicacao/noticia.wsp?tmp.noticia=241>

[50] A arquitetura e-PING do governo brasileiro está disponível em <http://www.governoeletronico.gov.br/governoeletronico/index.wsp>

como as regras de negócio da organização, a necessidade de realização de *backup*, manutenções planejadas, entre outros.

| Referência | Requisito | Obrig |
|---|---|---|
| 13.1.1 | Um SIGAD tem que se adequar ao grau de disponibilidade estabelecido pela organização. | O |

## 14 DESEMPENHO E ESCALABILIDADE

Os requisitos de desempenho enfocam a eficiência no atendimento aos usuários, de acordo com suas expectativas quanto ao tempo de resposta. Os tempos de resposta são influenciados por fatores externos ao SIGAD, como, por exemplo, infraestrutura de rede, volume de tráfego de dados e dimensionamento dos servidores e estações de trabalho.

Em um SIGAD, entende-se escalabilidade como a capacidade de um sistema responder a um aumento do número de usuários e do volume de documentos arquivísticos, mantendo o desempenho de suas respostas. Para tanto, faz-se necessário que a cada aumento de *hardware* corresponda um aumento de desempenho.

Esses acréscimos de *hardware* podem se dar pelo aumento de *hosts* (escalabilidade horizontal) ou de memória RAM, ou do poder de processamento dos *hosts* existentes (escalabilidade vertical).

| Referência | Requisito | Obrig |
|---|---|---|
| 14.1.1 | Um SIGAD deve manter estatísticas dos tempos de atendimento, discriminadas por tipo de operação. | AD |
| 14.1.2 | Um SIGAD deve ser expansível até comportar um número máximo, preestabelecido, de usuários simultâneos, provendo a continuidade efetiva dos serviços. | AD |
| 14.1.3 | Um SIGAD tem que incluir rotina de manutenção de:<br>• dados de usuários e de grupos;<br>• perfis de acesso;<br>• plano de classificação;<br>• bases de dados;<br>• tabelas de temporalidade.<br>*Essas tarefas devem atender às mudanças planejadas da organização, sem causar grande sobrecarga de administração.* | O |
| 14.1.4 | Um SIGAD deve ser escalável, a fim de permitir adaptação a organizações de diferentes tamanhos e complexidades. | AD |
| 14.1.5 | Um SIGAD deve fornecer evidências do grau de escalabilidade ao longo do tempo. | AD |

| Referência | Requisito | Obrig |
|---|---|---|
| | Avaliações quantitativas devem incluir:<br>• número máximo de sítios remotos suportados com desempenho adequado;<br>• tamanho máximo do repositório, expresso em *gigabytes* ou *terabytes*, que pode ser suportado com desempenho adequado;<br>• o número máximo de usuários simultâneos que podem ser atendidos com desempenho adequado;<br>• sobrecarga administrativa prevista para um período de cinco anos, permitindo o crescimento do número de usuários e da quantidade de registros;<br>• quantidade de reconfigurações e indisponibilidades previstas para um período de cinco anos, permitindo o crescimento do número de usuários e da quantidade de registros;<br>• quantidade de reconfigurações e indisponibilidades previstas para um período de cinco anos, permitindo mudanças substanciais na estrutura da organização, nos esquemas de classificação e na administração de usuários. | |

# Metadados

A concepção adotada neste trabalho baseou-se na definição do termo metadado conforme estabelecido no Glossário da Câmara Técnica de Documentos Eletrônicos (CTDE) do Conselho Nacional de Arquivos, isto é, “dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e/ou preservar documentos arquivísticos ao longo do tempo”.

As premissas que nortearam a elaboração deste esquema de metadados foram:

- A complementação dos requisitos do SIGAD, compreendendo a identificação de documentos (documentos simples, processos ou dossiês, que podem se apresentar em formato convencional, híbrido ou digital) e as ações de gerenciamento do seu ciclo de vida;
- O aproveitamento de elementos de metadados de esquemas similares já consagrados por organismos nacionais e internacionais, visando assegurar a interoperabilidade dos sistemas. Optamos por nos aproximar do modelo em desenvolvimento pelo Grupo de Trabalho de Padrão de Metadados do Governo Eletrônico (e-PMG), integrante dos Padrões de Interoperabilidade de Governo Eletrônico (e-PING).
- A especificação de um esquema de metadados em termos conceituais, e não o detalhamento visando à implementação.

### Metodologia

A especificação deste esquema de metadados envolveu quatro etapas:

- identificação dos metadados referidos no e-ARQ Brasil;
- complementação dos metadados a partir de normas e referências bibliográficas das áreas de arquivologia e diplomática;
- confronto do levantamento inicial com esquemas, normas e padrões de metadados semelhantes, nacionais e internacionais;
- análise, definição e aprovação do esquema.

O levantamento inicial teve como ponto de partida a identificação dos metadados referidos no próprio e-ARQ Brasil, em especial na descrição das etapas da gestão arquivística, constante da Parte I, e nos requisitos apresentados na seção de aspectos de funcionalidade do SIGAD, da Parte II. Esse levantamento limitou-se aos aspectos funcionais de organização de documentos arquivísticos (plano de classificação e manutenção dos documentos); tramitação e fluxo de trabalho; captura; avaliação e destinação de documentos; pesquisa, localização e apresentação de documentos; segurança; armazenamento; preservação; e funções administrativas.

Pesquisas feitas em normas brasileiras que regulamentam serviços de protocolo permitiram complementar a definição de elementos relacionados à identificação e ao gerenciamento de processos e dossiês. Referências bibliográficas das áreas de arquivologia e diplomática forneceram subsídios para a identificação e descrição de elementos de metadados, tais como redator, originador, interessado, juntada etc. Foram utilizados, sobretudo:

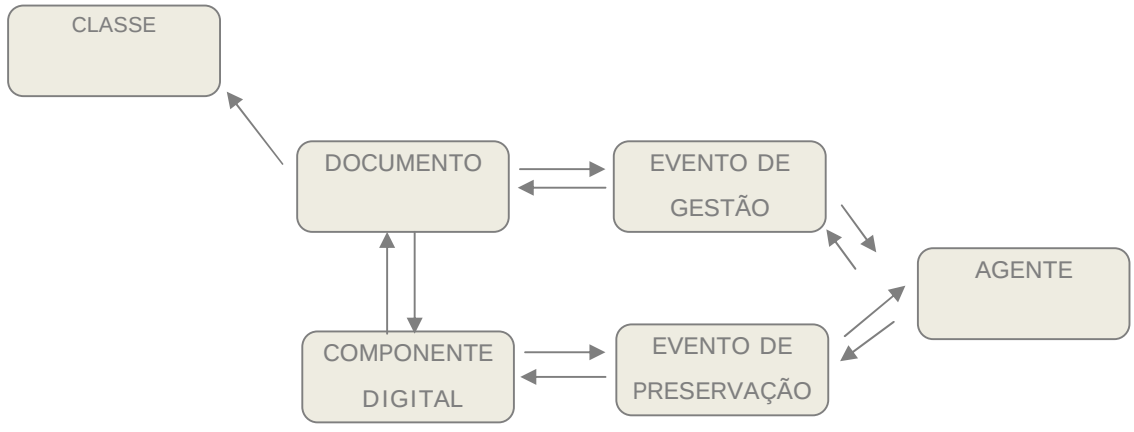
- *Dicionário brasileiro de terminologia arquivística*, Arquivo Nacional, 2005;
- *Dicionário de terminologia arquivística*, Associação dos Arquivistas Brasileiros – Núcleo Regional de São Paulo, 1996;
- *Manual de gestão de processos e de expedientes no âmbito da Universidade Estadual de Campinas*, Universidade Estadual de Campinas;
- Portaria normativa n. 5, de 19 de dezembro de 2002, do Ministério de Planejamento, Orçamento e Gestão, que dispõe sobre os procedimentos gerais para utilização dos serviços de protocolo, no âmbito da Administração Pública Federal, para os órgãos e entidades do Sistema de Serviços Gerais (SISG);
- Requisitos para apoiar a presunção de autenticidade de documentos arquivísticos eletrônicos, InterPARES, 2006;
- *Norma geral internacional de descrição arquivística – ISAD(G)*, Conselho Internacional de Arquivos, 1999.

Esquemas, normas e padrões nacionais e internacionais foram usados como referência, e aqueles voltados para a gestão arquivística de documentos, confrontados, diretamente, com o levantamento inicial de metadados, a fim de identificar as semelhanças e o oportuno aproveitamento de definições. Foram utilizados, principalmente:

- ISO 23081-1 – Records management processes – Metadata for Records, 2006;
- ISO 15836 – Dublin core metadata element set, 2003;
- e-Government metadata standard – e-GMS, United Kingdom, v. 3.0, 2004;
- Metainformação para interoperabilidade de Portugal – MIP, 2006;
- Model requirements for the management of electronic records – MoReq 2, 2007;
- Padrão de Metadados do Governo Eletrônico – e-PMG, Brasil. (minuta);
- PREMIS Data dictionary for preservation metadata – final report, 2005.

### Organização do esquema de metadados

Foram definidos metadados para as entidades: documento, evento de gestão, classe, agente, componente digital e evento de preservação. O modelo a seguir representa estas entidades e seus relacionamentos:



Este modelo deve ser entendido da seguinte maneira:

Documento refere-se aos documentos arquivísticos que são gerenciados pelo SIGAD.

- Documentos arquivísticos relacionam-se entre si, formando agregações, denominadas processos ou dossiês. Os documentos arquivísticos podem ser classificados e gerenciados de duas formas: agregados em processos ou dossiês ou individualmente (documento a documento). Os processos/dossiês, por sua vez, podem ser divididos em volumes.
- Todo documento arquivístico tem que ser relacionado a uma classe no momento da captura para o SIGAD.
- Todo documento arquivístico digital é composto por um ou mais componentes digitais.
- Ao longo do ciclo de vida, uma série de eventos ocorre no documento, e eles devem ser registrados no SIGAD. Cada documento arquivístico está relacionado a uma série de eventos de gestão.

Evento de gestão refere-se às ações de gestão que ocorrem com os documentos arquivísticos ao longo de seu ciclo de vida, como captura, tramitação, abertura e encerramento de processo/dossiê, classificação, desclassificação, eliminação, transferência, recolhimento, entre outros.

- Evento de gestão relaciona-se com o documento e com o agente responsável pela ação.

Classe refere-se aos diversos níveis de agregação do plano de classificação: classes, subclasses, grupos e subgrupos, que são organizados de forma hierárquica. Em cada classe estão associadas informações a respeito da temporalidade e da destinação prevista para os documentos nela classificados. Todas as alterações ocorridas no plano de classificação devem ficar registradas nos metadados da classe.

- As classes estão relacionadas aos documentos arquivísticos que foram nelas classificados.

Agente refere-se aos usuários que acessam o SIGAD. O agente pode se apresentar como usuário, como papel desempenhado e como grupo a que pertence. Grupos são conjuntos de usuários reunidos para realização de uma atividade em comum, por tempo determinado. Papéis são funções ou cargos com responsabilidades e autoridades bem definidas. Um usuário pode estar associado a um ou mais papéis.

- Agentes relacionam-se entre si, uma vez que os usuários podem ser agregados em papéis e grupos.
- Agente relaciona-se com o evento de gestão pelo qual foi responsável.
- Agente relaciona-se com o evento de preservação pelo qual foi responsável.

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

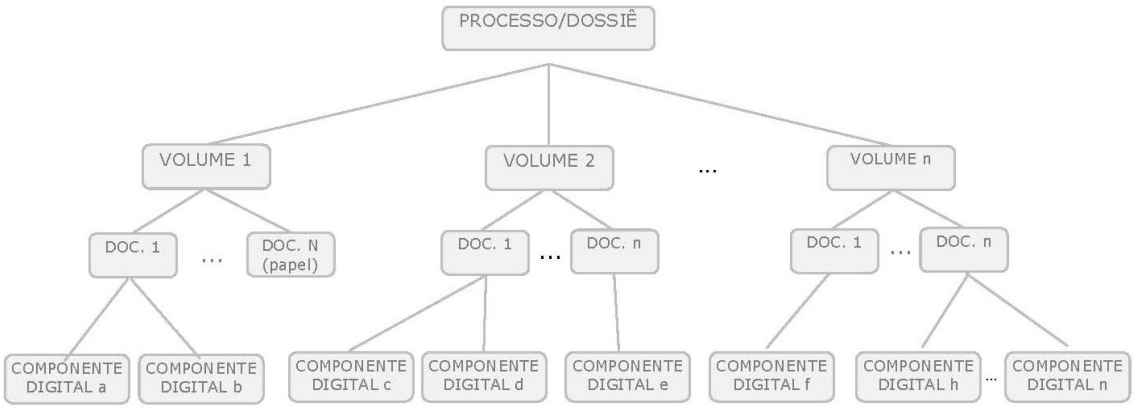
- Cada documento está relacionado a um ou mais componentes digitais. Um componente digital pode conter informações relativas a um ou mais documentos.
- Uma série de eventos de preservação ocorre nos componentes digitais para permitir o acesso continuado ao longo do tempo e deve ser registrada pelo SIGAD. Cada componente digital está relacionado a uma série de eventos de preservação.

Evento de preservação refere-se às ações de preservação realizadas nos documentos arquivísticos digitais, tais como migração (atualização, conversão), compressão, validação, decifração.

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

O documento arquivístico digital é a apresentação, em formato acessível ao ser humano, de um ou vários componentes digitais que estão relacionados entre si. Além disso, como mencionado acima, os documentos arquivísticos digitais relacionam-se formando agregações conceituais, isto é, processos e dossiês. Um processo ou dossiê pode conter um ou mais volumes. Um volume pode conter um ou mais documentos. Cada documento é composto por um ou mais componentes digitais.

O desenho abaixo ilustra os relacionamentos entre documentos arquivísticos e entre um documento arquivístico e seus componentes digitais.



Os elementos de metadados estão reunidos de acordo com a estrutura a seguir:

1 Documento

1.1 Identificador do documento
1.2 Número do documento
1.3 Número do protocolo
1.4 Identificador do processo/dossiê
1.5 Número do processo/dossiê
1.6 Identificador do volume
1.7 Número do volume
1.8 Tipo de meio
1.9 *Status*
1.10 Identificador de versão
1.11 Título
1.12 Descrição
1.13 Assunto
1.14 Autor
1.15 Destinatário
1.16 Originador
1.17 Redator
1.18 Interessado
1.19 Procedência
1.20 Identificador do componente digital
1.21 Gênero
1.22 Espécie
1.23 Tipo
1.24 Idioma
1.25 Quantidade de folhas/página
1.26 Numeração sequencial dos documentos
1.27 Indicação de anexos
1.28 Relação com outros documentos
1.29 Níveis de acesso
1.30 Data de produção
1.31 Classe
1.32 Destinação prevista
1.33 Prazo de guarda
1.34 Localização

2 Evento de gestão

2.1 Captura
2.2 Tramitação
2.3 Transferência
2.4 Recolhimento
2.5 Eliminação
2.6 Abertura_processo/dossiê
2.7 Encerramento_processo/dossiê
2.8 Reabertura_processo/dossiê
2.9 Abertura_volume
2.10 Encerramento_volume
2.11 Juntada_anexação

2.12 Juntada_apensação
2.13 Desapensação
2.14 Desentranhamento
2.15 Desmembramento
2.16 Classificação_sigilo
2.17 Desclassificação_sigilo
2.18 Reclassificação_sigilo

3 Classe

3.1 Descrição de classe
3.1.1 Classe_nome
3.1.2 Classe_código
3.1.3 Classe_subordinação
3.1.4 Registro de abertura
3.1.5 Registro de desativação
3.1.6 Reativação de classe
3.1.7 Registro de mudança de nome de classe
3.1.8 Registro de deslocamento de classe
3.1.9 Registro de extinção
3.1.10 Indicador de classe ativa/inativa
3.2 Temporalidade associada à classe
3.2.1 Classe_código
3.2.2 Prazo de guarda na fase corrente
3.2.3 Evento que determina a contagem do prazo de guarda na fase corrente
3.2.4 Prazo de guarda na fase intermediária
3.2.5 Evento que determina a contagem do prazo de guarda na fase intermediária
3.2.6 Destinação final
3.2.7 Registro de alteração
3.2.8 Observações

4 Agente

4.1 Nome
4.2 Identificador
4.3 Autorização de acesso
4.4 Credenciais de autenticação
4.5 Relação
4.6 Status do agente

5 Componente digital

5.1 Identificador do componente digital
5.2 Nome original
5.3 Características técnicas
5.4 Formato de arquivo
5.5 Armazenamento
5.6 Ambiente de *software*
5.7 Ambiente de *hardware*
5.8 Dependências
5.9 Relação com outros componentes digitais
5.10 Fixidade

6 Evento de preservação

6.1 Compressão
6.2 Decifração
6.3 Validação de assinatura digital
6.4 Verificação de fixidade
6.5 Cálculo *hash*
6.6 Migração
6.7 Replicação
6.8 Verificação de vírus
6.9 Validação

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

| | | | |
|---|---|---|---|
| Designação | | | |
| Definição | | | |
| Objetivo | | | |
| Aplica-se a | Processo \| Dossiê | Volume | Documento |
| Nota de aplicação | | | |
| Exemplos | | | |
| Requisito | | | |

Designação: Indicação do nome atribuído ao elemento;

Definição: Indica que informação deve ser registrada no elemento de metadado;

Objetivo: A referência do que se pretende alcançar com a aplicação do elemento;

Aplica-se a: Indica a obrigatoriedade da aplicação do elemento para cada nível de agregação: documento, volume, Processo/dossiê. Os valores possíveis são: obrigatório (O); obrigatório se aplicável (OA); facultativo (F); ou não se aplica (NA).

Nota de aplicação: Sugere formas de aplicação do elemento;

Exemplos: Apresenta alguns exemplos de aplicação que explicam o elemento;

Requisito: Os requisitos funcionais relacionados com o elemento de metadado.

Para os elementos de metadados relativos a evento de gestão e evento de preservação, são apresentadas, em uma tabela, as seguintes informações:

| EVENTO | DEFINIÇÃO e ELEMENTOS | OBRIG | REQ. |
|---|---|---|---|

Evento: Indicação do evento que deve ser registrado em metadado;

Definição e elementos: Indica a definição do evento e que informação deve ser registrada em metadados;

Obrig.: Indica se o elemento de metadado é de aplicação obrigatória ou não. Os valores possíveis são: obrigatório (O), obrigatório se aplicável (OA), facultativo (F) ou não se aplica (NA);

Req.: Os requisitos funcionais relacionados com o elemento de metadado.

Para os elementos de metadados relativos a classe e agente, são apresentadas, em uma tabela, as seguintes informações:

| ELEMENTO | DEFINIÇÃO | OBRIG | REQ. |
|---|---|---|---|

Elemento: Indicação do nome atribuído ao elemento;

Definição: Indica que informação deve ser registrada no elemento de metadado;

Obrig.: Indica se o elemento de metadado é de aplicação obrigatória ou não. Os valores possíveis são: obrigatório (O), obrigatório se aplicável (OA), facultativo (F) ou não se aplica (NA);

Req.: Os requisitos funcionais relacionados com o elemento de metadado.

Para os elementos de metadados referentes à identificação do componente digital foi elaborada uma ficha individual que detalha cada elemento e apresenta as informações a seguir:

| Designação |
| --- |
| Definição |
| Objetivo |
| Obrigatoriedade |
| Nota de Aplicação |
| Exemplos |
| Requisito |

Designação: Indicação do nome atribuído ao elemento;

Definição: Indica que informação deve ser registrada no elemento de metadado;

Objetivo: A referência do que se pretende alcançar com a aplicação do elemento;

Obrigatoriedade: Indica a obrigatoriedade da aplicação do elemento. Os valores possíveis são: obrigatório (O); obrigatório se aplicável (OA); facultativo (F); ou não se aplica (NA).

Nota de aplicação: Sugere formas de aplicação do elemento;

Exemplos: Apresentam-se alguns exemplos de aplicação que explicam o elemento;

Requisito: Os requisitos funcionais relacionados com o elemento de metadado.

obrigatório (O) = o elemento deve obrigatoriamente estar presente.

obrigatório se aplicável (OA) = o elemento pode ser aplicável ou não, porém se aplicável sua presença é obrigatória

facultativo (F) = o elemento não é obrigatório. Os elementos facultativos estão relacionados à implementação do sistema e cabe à instituição decidir usá-los ou não. O grau facultativo pode se tornar obrigatório para uma instituição dependendo de suas necessidades específicas.

não se aplica (NA) = não cabe o uso do elemento naquele contexto.

## 1 DOCUMENTO

Estas informações referem-se à identidade e à integridade do documento e apóiam sua identificação no sistema de gestão arquivística de documentos.

Alguns elementos de metadados de identificação devem ser aplicados nos três, em dois ou em apenas um dos níveis de agregação (processo/dossiê, volume e documento). A tabela descritiva a seguir indica o nível de agregação a ser aplicado.

## 1.1 Identificador do documento

| Designação | Identificador do documento | | |
|---|---|---|---|
| Definição | Identificador único atribuído ao documento no ato de sua captura[51] para o SIGAD. | | |
| Objetivo | Identificar de forma unívoca o documento para que o SIGAD possa gerenciá-lo. | | |
| Aplica-se a | Processo/dossiê | Volume | Documento |
| | NA<br>Ver elemento 1.4 (Identificador do processo/dossiê) | NA<br>Ver elemento 1.6 (Identificador do volume) | O |
| Nota de aplicação | Aplicável no âmbito do SIGAD.<br>Pode ser um elemento identificador simples e conter um componente para localização em ambiente eletrônico.<br>Deve, preferencialmente, ser gerado de forma automática pelo SIGAD.<br>Esse identificador tem de ser unívoco e persistente.<br>As instituições devem seguir normas específicas em seu âmbito de atuação ou esfera de competência. | | |
| Requisito | 1.6.2 / 3.1.5 / 3.1.7 / 3.1.9 / 5.2.6 / 6.8.3 | | |

## 1.2 Número do documento

| Designação | Número do documento | | |
|---|---|---|---|
| Definição | Número ou código alfanumérico atribuído ao documento no ato da sua produção. | | |
| Objetivo | Permitir a identificação precisa de um documento. | | |
| Aplica-se a | Processo/dossiê | Volume | Documento |
| | NA<br>Ver elemento 1.5 (Número do processo/dossiê) | NA<br>Ver elemento 1.7 (Número do volume) | OA |

[51] Observar a definição de captura na Parte I, item 6.1 do e-ARQ Brasil, na página 30.

| Designação | Número do documento |
|---|---|
| Nota de aplicação | Pode ser acrescido da data de produção e da sigla do órgão produtor. |
| Exemplos | *Mem.119/COAD/DIRHU;*<br>*Ofício n. 78/2008/GABIN-NA;*<br>*Aviso 123/2008-SCT-PR.* |
| Requisito | 3.1.10 |

## 1.3 Número do protocolo

| Designação | Número do protocolo | | |
|---|---|---|---|
| Definição | Número ou código alfanumérico atribuído ao documento no ato do protocolo. | | |
| Objetivo | Permitir a identificação e o controle da tramitação do documento. | | |
| Aplica-se a | Processo/dossiê | Volume | Documento |
| | Não se aplica<br>Ver elemento 1.5<br>(Número do processo / dossiê) | Não se aplica<br>Ver elemento 1.7<br>(Número do volume) | OA |
| Nota de aplicação | Pode ser acrescido da data de registro.<br>Os órgãos e entidades devem seguir normas específicas em seu âmbito de atuação ou esfera de competência.<br>Esse número deve estar disponível para o usuário. | | |
| Exemplos | *Carta: AB/11.000/2008;*<br>*Processo n. 0400.001412/2000-26.* | | |
| Requisito | 3.1.10 | | |

## 1.4 Identificador do processo/dossiê

| Designação | Identificador do Processo \| Dossiê |
|---|---|
| Definição | Identificador único atribuído ao processo ou dossiê no ato de sua captura para o SIGAD. |
| Objetivo | Identificar de forma unívoca e persistente o processo ou dossiê para que o SIGAD possa gerenciá-lo. |

| Designação | Identificador do Processo \| Dossiê | | |
|---|---|---|---|
| | Estabelecer a relação entre o processo ou dossiê e os volumes e os documentos que os integram. | | |
| Aplica-se a | Processo/dossiê | Volume | Documento |
| | O | O | O |
| Nota de aplicação | Aplicável no âmbito do SIGAD.<br>Pode ser um elemento identificador simples e conter um componente para localização em ambiente eletrônico.<br>Deve, preferencialmente, ser gerado automaticamente pelo SIGAD.<br>Esse identificador não está disponível para o usuário. É um controle interno do sistema.<br>Esse identificador tem de ser unívoco e persistente.<br>As instituições devem seguir normas específicas em seu âmbito de atuação ou esfera de competência. | | |
| Requisito | 1.6.2 / 3.1.7 / 3.1.9 / 5.2.6 | | |

## 1.5 Número do processo/dossiê

| Designação | Número do Processo/dossiê | | |
|---|---|---|---|
| Definição | Número ou código alfanumérico de registro do processo ou dossiê. | | |
| Objetivo | Identificar de forma unívoca e persistente um processo ou dossiê.<br>Permitir o controle dos registros de autuações de processos e dos registros de abertura de dossiês.<br>Permitir a pesquisa sobre processos e/ou dossiês. | | |
| Aplica-se a | Processo/dossiê | Volume | Documento |
| | O | F | NA<br>Ver elemento 1.2<br>(Número do documento) |
| Nota de aplicação | As instituições devem seguir normas específicas em seu âmbito de atuação ou esfera de competência. | | |
| Exemplos | *Processo n. 0032.000125/2008;*<br>*Processo n. 0400.001412/2000-26.* | | |
| Requisito | 3.1.10 | | |

## 1.6 Identificador do volume

| Designação | Identificador do volume | | |
|---|---|---|---|
| Definição | Identificador único atribuído ao volume do processo ou dossiê no ato de sua captura para o SIGAD. | | |
| Objetivo | Identificar de forma unívoca o volume do processo ou dossiê para que o SIGAD possa gerenciá-lo.<br>Estabelecer a relação entre o processo ou dossiê e os volumes e documentos que os integram. | | |
| Aplica-se a | Processo/dossiê<br>NA<br>Ver elemento 1.4 (Identificador do processo/dossiê) | Volume<br>O | Documento<br>O<br>Ver elemento 1.1 (Identificador do documento) |
| Nota de aplicação | Aplicável no âmbito do SIGAD.<br>Pode ser um elemento identificador simples e conter um componente para localização em ambiente eletrônico.<br>Pode ser gerado automaticamente pelo SIGAD.<br>É recomendável que possa se integrar a sistemas de identificadores persistentes.<br>As instituições devem seguir normas específicas em seu âmbito de atuação ou esfera de competência. | | |
| Requisito | 1.5 / 1.6.2 / 3.1.7 / 3.1.9 / 5.2.6 | | |

## 1.7 Número do volume

| Designação | Número do volume | | |
|---|---|---|---|
| Definição | Número de registro do volume do processo ou dossiê. | | |
| Objetivo | Identificar o volume do processo ou dossiê. | | |
| Aplica-se a | Processo/dossiê<br>NA<br>Ver elemento 1.5<br>(Número do processo/dossiê) | Volume<br>O | Documento<br>NA<br>Ver elemento 1.2<br>(Número do documento) |
| Nota de aplicação | O controle de volumes deve obedecer às normas das instituições. | | |
| Requisito | Ver seção 1.5 (Volumes: abertura, encerramento e metadados) | | |

## 1.8 Tipo de meio

| Designação | Tipo de meio | | |
|---|---|---|---|
| Definição | Identificação do meio do documento/volume/processo/dossiê: digital, não digital ou híbrido. | | |
| Objetivo | Identificar se o documento/volume/processo/dossiê é digital, não digital ou híbrido para controlar as relações entre os meios e o monitoramento de preservação. | | |
| Aplica-se a | Processo/dossiê | Volume | Documento |
| | O | O | O |
| Nota de aplicação | No documento/volume/processo/dossiê híbrido, os relacionamentos deverão ser registrados para identificar a parte não digital e a parte digital.<br>Ver elemento 1.1.28 (Relação com outros documentos). | | |
| Requisito | 1.6.1 / 1.6.2 / 3.4 / 4.3.13 | | |

## 1.9 Status

| Designação | Status | | |
|---|---|---|---|
| Definição | Indicação do grau de formalização do documento:<br>▪ minuta/rascunho (pré-original) - versão preliminar do documento;<br>▪ original – primeiro documento completo e efetivo;<br>▪ cópia – resultado da reprodução do documento. | | |
| Objetivo | Identificar o grau de formalização do documento e as relações existentes entre os originais, as minutas e as cópias.<br>Manter um controle sobre a disposição de cópias. | | |
| Aplica-se a | Processo \| Dossiê | Volume | Documento |
| | NA | NA | O |
| Nota de aplicação | Deverá haver relacionamento entre os vários graus de formalização dos documentos.<br>A organização deverá ter um plano de organização e registro do status dos documentos e da forma de relacioná-los. | | |
| Requisito | 2.2.1 | | |

## 1.10 Identificador de versão

| Designação | Identificador de versão | | |
|---|---|---|---|
| Definição | Identificação da versão do documento. | | |
| Objetivo | Identificar a versão do documento e estabelecer a relação entre as versões anteriores e posteriores. | | |
| Aplica-se a | Processo \| Dossiê | Volume | Documento |
| | NA | NA | OA |
| Nota de Aplicação | Registrar informações relativas a: identificador da versão, descrição de alterações, data/hora da produção da versão e da transmissão, e o relacionamento entre as versões.<br>É recomendável que seja gerado automaticamente pelo SIGAD.<br>Versões de documentos podem integrar processos e/ou dossiês. | | |
| Requisito | 2.2.2 / 3.1.5 / 3.1.18 | | |

## 1.11 Título

| Designação | Título | | |
|---|---|---|---|
| Definição | Elemento de descrição que nomeia o documento ou Processo \| Dossiê. Pode ser formal ou atribuído:<br>▪formal - designação registrada no documento;<br>▪atribuído - designação providenciada para identificação de um documento formalmente desprovido de titulo. | | |
| Objetivo | Identificar o documento.<br>Servir como elemento de acesso ao documento. | | |
| Aplica-se a | Processo/dossiê | Volume | Documento |
| | F | NA | O |
| Nota de aplicação | Cada instituição deverá fixar critérios para títulos atribuídos. | | |
| Exemplos | *Processo de Aquisição de Equipamentos de Informática;*<br>*Balancete da Universidade ACD 2007.* | | |
| Requisito | 1.6.2 / 3.1.5 / 5.2.6 | | |

## 1.12 Descrição

| Designação | Descrição | | |
|---|---|---|---|
| Definição | Exposição concisa do conteúdo do documento, processo ou dossiê. | | |
| Objetivo | Identificar o conteúdo do documento.<br>Facilitar a pesquisa. | | |
| Aplica-se a | Processo/dossiê<br>F | Volume<br>NA | Documento<br>F |
| Nota de aplicação | Cada instituição deverá fixar critérios e modelos com elementos básicos para a elaboração da descrição. | | |
| Exemplos | *Convênio de cooperação para desenvolvimento de aplicações do laser entre a Instituição A e a Instituição B, com recursos do Programa Nacional ABC.* | | |
| Requisito | 3.1.5 / 3.1.11 | | |

## 1.13 Assunto

| Designação | Assunto | | |
|---|---|---|---|
| Definição | Palavras-chave que representam o conteúdo do documento.<br>Pode ser de preenchimento livre ou com o uso de vocabulário controlado ou tesauro.<br>Diferente do já estabelecido no código de classificação. | | |
| Objetivo | Referir de forma sucinta o teor geral do documento. | | |
| Aplica-se a | Processo/dossiê<br>F | Volume<br>NA | Documento<br>F |
| Nota de aplicação | As instituições devem definir sua política de indexação. | | |
| Requisito | 3.1.5 / 3.1.11 / 3.2.11 / 5.2.6 | | |

## 1.14 Autor

| Designação | Autor | | |
|---|---|---|---|
| Definição | Pessoa física ou jurídica com autoridade para emitir o documento e em cujo nome ou sob cuja ordem ou responsabilidade o documento é emitido. | | |
| Objetivo | Identificar o autor do documento.<br>Fornecer informação sobre o contexto de produção do documento.<br>Demonstrar a autenticidade de um documento, indicando o responsável direto pela sua produção. | | |
| Aplica-se a | Processo/dossiê<br>O | Volume<br>NA | Documento<br>O |
| Nota de aplicação | Registrar informações tais como: nome, cargo, endereço, contato.<br>As instituições devem estabelecer normas para controlar as entradas de nomes. | | |
| Exemplos | *Santos, José ou José Santos* | | |
| Requisito | 3.1.5 / 5.2.6 | | |

## 1.15 Destinatário

| Designação | Destinatário |
|---|---|
| Definição | Pessoa física e/ou jurídica a quem foi dirigida a informação contida no documento.<br>Pode ser nominal ou geral:<br>▪ nominal– pessoas específicas;<br>▪ geral – refere-se a uma entidade maior, indeterminada. Ex.: cidadãos, povo, estudantes, a quem possa interessar, a todos os envolvidos. |
| Objetivo | Identificar o destinatário do documento.<br>Fornecer informação sobre o contexto de produção do documento.<br>Demonstrar a autenticidade de um documento, indicando a quem ele é dirigido. |

| Designação | Destinatário | | |
|---|---|---|---|
| Aplica-se a | Processo/dossiê | Volume | Documento |
| | F | NA | O |
| Nota de aplicação | Registrar informações tais como: nome, cargo, endereço, contato.<br>As instituições devem estabelecer normas para controlar as entradas de nomes. | | |
| Requisito | 3.1.5 | | |

## 1.16 Originador

| Designação | Originador | | |
|---|---|---|---|
| Definição | Pessoa física ou jurídica designada no endereço eletrônico ou *log in* em que o documento é gerado e/ou enviado. | | |
| Objetivo | Identificar o originador do documento.<br>Fornecer informação sobre o contexto de produção do documento.<br>Demonstrar a autenticidade de um documento, indicando o responsável legal pela sua emissão. | | |
| Aplica-se a | Processo/dossiê | Volume | Documento |
| | NA | NA | O |
| Nota de aplicação | Aplica-se quando o nome do originador for diferente do nome do autor ou do redator. | | |
| Requisito | 3.1.5 / 5.2.6 | | |

## 1.17 Redator

| Designação | Redator | | |
|---|---|---|---|
| Definição | Responsável pela elaboração do conteúdo do documento. | | |
| Objetivo | Identificar o redator do documento.<br>Fornecer informação sobre o contexto de produção do documento.<br>Demonstrar a autenticidade de um documento, indicando o responsável pela articulação de seu conteúdo. | | |
| Aplica-se a | Processo/dossiê | Volume | Documento |
| | NA | NA | O |

| Designação | Redator |
|---|---|
| Nota de aplicação | Aplica-se quando o nome do originador for diferente do nome do autor ou do redator. |
| Requisito | 3.1.5 / 5.2.6 |

## 1.18 Interessado

| Designação | Interessado | | |
|---|---|---|---|
| Definição | Nome e/ou identificação da pessoa física ou jurídica que tem envolvimento ou a quem interessa o assunto do documento. | | |
| Objetivo | Facilitar a pesquisa. | | |
| Aplica-se a | Processo/dossiê | Volume | Documento |
| | O | NA | NA |
| Nota de aplicação | As instituições devem controlar a forma de entrada dos nomes.<br>O interessado pode ser qualificado como, por exemplo: réu, vítima, inventariante, inventariado, apelante, apelado, requerente, solicitante.<br>Pode-se fazer o cadastro de interessados internos da organização por categorias para facilitar o registro automático, com dados de identificação. Ex.: número de matrícula, nome, documento de identificação. | | |
| Exemplos | *José da Silva;*<br>*987.745.465-73 (CPF);*<br>*59873/0001-38 (CNPJ);*<br>*8783000238 (número de matrícula).* | | |
| Requisito | 3.1.6 / 5.2.6 | | |

## 1.19 Procedência

| Designação | Procedência |
|---|---|
| Definição | Origem do registro do documento, isto é, instituição legitimamente responsável pela autuação e/ou registro do Processo \| Dossiê. |
| Objetivo | Apóia a administração das unidades de protocolo e outras unidades de registro arquivístico. |

| Designação | Procedência | | |
|---|---|---|---|
| | Apóia a presunção de autenticidade de um documento, indicando a procedência do seu registro.<br>Facilitar a pesquisa. | | |
| Aplica-se a | Processo/dossiê | Volume | Documento |
| | O | NA | OA |
| Nota de aplicação | Pode-se fazer o cadastro de procedências de organismos internos à instituição, para facilitar a automatização desse elemento, tais como: nome, sigla, número correspondente numa tabela de órgãos etc. | | |
| Exemplos | *Ministério da Educação – Gabinete do Ministro.*<br>*Fundação ABCD.* | | |
| Requisito | 1.5.3 / 3.1.6 / 5.2.6 | | |

## 1.20 Identificador do componente digital

| Designação | Identificador do componente digital | | |
|---|---|---|---|
| Definição | Identificador dos componentes digitais que integram o documento. | | |
| Objetivo | Estabelecer a relação entre o documento e os componentes digitais necessários para apresentá-lo. | | |
| Aplica-se a | Processo/dossiê | Volume | Documento |
| | NA | NA | O |
| Nota de aplicação | Um documento pode ser formado por um ou mais componentes digitais, que são os componentes físicos do documento. De forma geral, pode se dizer que os componentes digitais são os arquivos de computador que formam um documento.<br>Cada componente deve ser identificado individualmente a fim de que o documento possa ser recuperado de maneira completa. | | |
| Exemplos | *Um relatório de atividades pode ser composto por diversas seções, sendo que cada uma delas constitui um arquivo separado. Entretanto, todos esses arquivos integram-se para a representação completa do documento.*<br>*A mesma situação aplica-se a documentos estruturados em bases de dados ou, ainda, a documentos multimídia.* | | |
| Requisito | 3.1.7 / 3.1.9 / 3.1.21 | | |

## 1.21 Gênero

| Designação | Gênero | | |
|---|---|---|---|
| Definição | Indica o gênero documental, ou seja, a configuração da informação no documento de acordo com o sistema de signos utilizado na comunicação do documento. | | |
| Objetivo | Monitorar os diversos gêneros documentais de um acervo para fins de gestão arquivística.<br>Facilitar a pesquisa. | | |
| Aplica-se a | Processo/dossiê | Volume | Documento |
| | NA | NA | F |
| Nota de aplicação | É necessário que a instituição elabore uma tabela com os gêneros e suas designações, para facilitar sua indicação no registro. | | |
| Exemplos | *Audiovisual; textual; cartográfico; iconográfico; multimídia*. | | |
| Requisito | 3.1.5 | | |

## 1.22 Espécie

| Designação | Espécie | | |
|---|---|---|---|
| Definição | Indica a espécie documental, ou seja, a configuração da informação no documento de acordo com a disposição e a natureza das informações nele contidas. | | |
| Objetivo | Complementar a descrição do documento ou a identificação de titulo;<br>Facilitar a pesquisa. | | |
| Aplica-se a | Processo/dossiê | Volume | Documento |
| | NA | NA | F |
| Nota de aplicação | As instituições podem preparar, como instrumento complementar de gestão, glossários de espécies de documentos que são produzidos no cumprimento de suas funções e atividades. A existência de tabelas pode facilitar o registro desse elemento.<br>Relaciona-se com tipo documental; descrição e título. | | |
| Exemplos | *Processo; oficio; ata; relatório; projeto; prontuário.* | | |
| Requisito | 3.1.5 | | |

## 1.23 Tipo

| Designação | Tipo | | |
|---|---|---|---|
| Definição | Indica o tipo documental, ou seja, a configuração da espécie documental de acordo com a atividade que a gerou. | | |
| Objetivo | Complementar a descrição do documento ou a identificação do titulo.<br>Permite a pesquisa limitada a um determinado tipo. | | |
| Aplica-se a | Processo/dossiê | Volume | Documento |
| | NA | NA | F |
| Nota de aplicação | Há instituições que preparam, como instrumento complementar de gestão de seus documentos, glossários de tipos documentais que são produzidos no cumprimento de suas funções e atividades. A existência dessas tabelas pode facilitar o registro desse elemento.<br>Relaciona-se com espécie documental. | | |
| Exemplos | *Relatório de pesquisa; carta precatória; ofício-circular; prontuário médico; prontuário de funcionário.* | | |
| Requisito | 3.1.5 | | |

## 1.24 Idioma

| Designação | Idioma | | |
|---|---|---|---|
| Definição | Idioma(s) em que é expresso o conteúdo do documento. | | |
| Objetivo | Identificar o(s) idioma(s) do conteúdo do documento.<br>Permitir a pesquisa limitada a um determinado idioma. | | |
| Aplica-se a | Processo/dossiê | Volume | Documento |
| | NA | NA | F |
| Nota de aplicação | As instituições devem, preferencialmente, utilizar padrões para identificar idiomas, como, por exemplo, a norma ISO 639-2/RA (*Codes for the representation of names of languages – Part 2: alpha-3 code*). | | |
| Requisito | | | |

## 1.25 Quantidade de folhas/páginas

| Designação | Quantidade de folhas/páginas | | |
|---|---|---|---|
| Definição | Indicação da quantidade de folhas/páginas de um documento. | | |
| Objetivo | Permitir o controle de folhas ou páginas por processo e por volume.<br>Facilitar o registro e o acesso a um documento específico dentro do processo ou dossiê. | | |
| Aplica-se a | Processo/dossiê<br>O | Volume<br>O | Documento<br>F |
| Nota de aplicação | Usado para gerenciamento de processos convencionais, que limitam a quantidade de folhas, sugerindo a abertura de volumes.<br>As instituições devem determinar as normas para esse tipo de ação. | | |
| Requisito | 1.4.3 / Ver seção 1.5 (Volumes: abertura, encerramento e metadados) | | |

## 1.26 Numeração sequencial dos documentos

| Designação | Numeração seqüencial dos documentos | | |
|---|---|---|---|
| Definição | Numeração sequencial dos documentos inseridos em um processo. | | |
| Objetivo | Ordenar os documentos em um processo.<br>Controlar a integridade do processo.<br>Facilitar a referência a um documento específico. | | |
| Aplica-se a | Processo/dossiê<br>O | Volume<br>NA | Documento<br>NA |
| Nota de aplicação | Usado para processos e dossiês digitais.<br>Devem-se numerar os documentos na ordem em que são inseridos no processo a fim de garantir sua integridade. | | |
| Requisito | 1.4.3 | | |

## 1.27 Indicação de anexos

| Designação | Indicação de anexos | | |
|---|---|---|---|
| Definição | Indica se o documento tem anexos. | | |
| Objetivo | Registrar a existência de anexos de um determinado documento para apoiar o controle de sua integridade e facilitar o acesso. | | |
| Aplica-se a | Processo/dossiê | Volume | Documento |
| | NA | NA | O |
| Requisito | 3.15 | | |

## 1.28 Relação com outros documentos

| Designação | Relação com outros documentos | | |
|---|---|---|---|
| Definição | Registro das relações significantes de um documento com outros. Estas relações podem ser entre:<br>▪ documentos diferentes que estão relacionados por registrarem a mesma atividade, pessoa ou situação;<br>▪ diferentes níveis de agregação (dossiê, volume e documento);<br>▪ diferentes manifestações do mesmo documento. Ex.: formatos HyperText Markup Language (HTML), Open Documet Format (ODF), Portable Document Format (PDF/A) ou mesmo em papel. | | |
| Objetivo | Tornar explicito o relacionamento e facilitar o processamento automático e o gerenciamento arquivístico.<br>Demonstrar a organicidade dos documentos<br>Facilitar a pesquisa de informações de documentos relacionados. | | |
| Aplica-se a | Processo/dossiê | Volume | Documento |
| | OA | NA | OA |
| Nota de aplicação | As instituições devem estabelecer os tipos de relacionamentos que deverão ser controlados e suas restrições ou condições. Estas relações podem ser expressas das seguintes formas:<br>▪ tem parte de, é parte de (relaciona os níveis de agregação); | | |

| | |
|---|---|
| | ▪ referenciado ou ver também;<br>▪ tem extrato, é extrato de;<br>▪ é manifestação de;<br>▪ ligação para parte em papel (dossiê híbrido). |
| Requisito | 3.1.5 / 3.1.10 / 3.4 / 11.1.21 |

## 1.29 Níveis de acesso

| Designação | Níveis de acesso | | |
|---|---|---|---|
| Definição | Indicação dos níveis de acesso ao documento a partir da classificação da informação quanto ao grau de sigilo e restrição de acesso. | | |
| Objetivo | Garantir o acesso somente a pessoas autorizadas. | | |
| Aplica-se a | Processo/dossiê<br>O | Volume<br>NA | Documento<br>O |
| Nota de aplicação | As instituições devem estabelecer as normas para a classificação de sigilo de acordo com suas necessidades ou com base na legislação.<br>Relaciona-se com tabela de classificação de segurança. | | |
| Requisito | 3.1.5 / 6.3.1 | | |

## 1.30 Data de produção

| Designação | Data de produção | | |
|---|---|---|---|
| Definição | Registro cronológico (data e hora) e tópico (local) da produção do documento. | | |
| Objetivo | Indicar local e data em que foi produzido o documento. | | |
| Aplica-se a | Processo/dossiê<br>O | Volume<br>NA | Documento<br>O |
| Nota de aplicação | | | |
| Requisito | 1.3.1 / 3.1.5 / 3.3.1 / 5.2.6 | | |

## 1.31 Classe

| Designação | Classificação | | |
|---|---|---|---|
| Definição | Identificação da classe[52] do documento com base em um plano de classificação. | | |
| Objetivo | Identificar a localização intelectual do documento no âmbito da estrutura orgânica ou funcional. | | |
| Aplica-se a | Processo/dossiê | Volume | Documento |
| | O | NA | O |
| Nota de aplicação | As instituições devem estabelecer um plano de classificação para aplicar esse elemento.<br>Pode se registrar o código e/ou o nome completo da classe em que o documento está classificado. | | |
| Requisito | 1.2.1 / 1.5.3 / 3.1.5 / 3.1.10 / 5.2.6 | | |

## 1.32 Destinação prevista

| Designação | Destinação prevista | | |
|---|---|---|---|
| Definição | Indicação da próxima ação de destinação (transferência, eliminação ou recolhimento) prevista para o documento, em cumprimento à tabela de temporalidade. | | |
| Objetivo | Apoiar o controle do ciclo de vida do documento. | | |
| Aplica-se a | Processo/dossiê | Volume | Documento |
| | O | NA | O |
| Nota de aplicação | Para a finalidade deste instrumento, considera-se a transferência como uma ação de destinação.<br>As instituições devem estabelecer uma tabela de temporalidade associada ao plano de classificação para aplicar este elemento.<br>Este elemento está relacionado ao 1.1.33. | | |
| Requisito | 1.5.3 / 4.1.2 / 4.2.4 | | |

[52] O termo *classe* deverá ser entendido como designação genérica que inclui os demais níveis do plano de classificação, isto é, subclasse, grupo e subgrupo.

## 1.33 Prazo de guarda

| Designação | Prazo de guarda | | |
|---|---|---|---|
| Definição | Indicação do prazo estabelecido em tabela de temporalidade para o cumprimento da destinação. | | |
| Objetivo | Apoiar o controle do ciclo de vida do documento. | | |
| Aplica-se a | Processo/dossiê | Volume | Documento |
| | O | NA | O |
| Nota de aplicação | As instituições devem estabelecer uma tabela de temporalidade associada ao plano de classificação para aplicar esse elemento.<br>Este elemento está relacionado ao 1.1.32. | | |
| Requisito | 1.5.3 / 3.1.5 / 4.1.2 / 4.2.4 | | |

## 1.34 Localização

| Designação | Localização | | |
|---|---|---|---|
| Definição | Local de armazenamento atual do documento.<br>Pode ser um lugar (depósito, estante, repositório digital) uma notação física. | | |
| Objetivo | Permitir a localização dos documentos em qualquer mídia.<br>Monitorar o armazenamento de documentos. | | |
| Aplica-se a | Processo/dossiê | Volume | Documento |
| | OA | F | OA |
| Nota de aplicação | Deve ser utilizado, obrigatoriamente, quando o documento não se encontra no sistema de gestão arquivística de documentos, e é mantido em outra área de armazenamento, seja virtual ou física.<br>Utilizado apenas para os documentos não digitais, para a parte não digital dos documentos híbridos ou para os documentos digitais *off-line*.<br>No caso de documentos digitais *on-line*, este controle é feito com relação aos componentes digitais. Ver metadado 5.5. | | |
| Exemplos | Depósito 201, estante 8, prateleira 2;<br>Caixa 3456;<br>Centro de documentação do IFP, repositório alfa;<br>Notação XY.2540. | | |
| Requisito | 1.6.1 / 1.6.3 / 1.6.4 / 1.6.7 / 3.1.5 / 3.4.1 / 3.4.2 / 6.8.3 | | |

## 2 EVENTO DE GESTÃO

As informações a seguir referem-se a eventos de captura, movimentação e controle do ciclo de vida do documento. Para cada evento, são apresentados uma definição e os elementos de metadados que o caracterizam e que devem ser registrados.

| EVENTO | DEFINIÇÃO E ELEMENTOS | APLICA-SE A | | | REQ. |
|---|---|---|---|---|---|
| | | Processo/ dossiê | Volume | Documento | |
| 2.1 Captura | Descreve a captura do documento.<br>Registrar informações tais como: identificação do documento, data/hora da captura, responsável pela captura. | O | NA | O | 3.1.5<br>3.1.16<br>3.2.1<br>3.3.1<br>3.4.1<br>6.4.1 |
| 2.2 Tramitação | Registro da tramitação do documento.<br>Registrar informações tais como: identificação do documento, data/hora de transmissão, remetente, data/hora do recebimento, destinatário, situação do trâmite. | O | NA | O | 3.1.5<br>2.1.20 |
| 2.3 Transferência | Registro de transferência de documentos.<br>Registrar informações tais como: data/hora de envio, data/hora de recebimento, destinatário, método utilizado, responsável pela transferência, responsável pelo recebimento, localização/suporte anterior, localização/suporte atual, identificação do lote, número do termo de transferência.<br>Os sub-elementos registram as informações do evento transferência e deve ser feito um registro para cada lote transferido. | O | NA | O | 4.1.4<br>6.8.3 |

| EVENTO | DEFINIÇÃO E ELEMENTOS | APLICA-SE A | | | REQ. |
|---|---|---|---|---|---|
| | | Processo/ dossiê | Volume | Documento | |
| | No metadado do documento pode ser registrado apenas o número do lote de transferência. | | | | |
| 2.4 Recolhimento | Registrar informações tais como: data/hora de envio, data/hora de recebimento, destinatário, método utilizado, responsável pelo recolhimento, localização/suporte anterior, localização/suporte atual, identificação do lote, número do termo de recolhimento. | O | NA | O | 4.1.4 |
| 2.5 Eliminação | Indica se o documento foi eliminado.<br>Registrar informações tais como: data/hora do procedimento, responsável, número do termo de eliminação, número do edital. | O | NA | O | 4.1.4<br>4.4.9 |
| 2.6 Abertura_processo/ dossiê | Registro de abertura de um processo/dossiê num sistema de gestão arquivística.<br>Registrar informações tais como: data/hora da abertura, responsável pela abertura. | O | O | NA | 1.3.1<br>4.1.5 |
| 2.7 Encerramento_processo/ dossiê | Registro do encerramento ou arquivamento de um processo/dossiê num sistema de gestão arquivística.<br>Registrar informações tais como: data/hora do encerramento, responsável. | O | O | NA | 1.3.1<br>1.4.9 |
| 2.8 Reabertura_processo/ dossiê | Registro de reabertura de processo/dossiê.<br>Registrar informações tais como: data/hora da reabertura, responsável. | O | NA | NA | 1.4.10 |

| EVENTO | DEFINIÇÃO E ELEMENTOS | APLICA-SE A | | | REQ. |
|---|---|---|---|---|---|
| | | Processo/ dossiê | Volume | Documento | |
| 2.9 Abertura_volume | Registro de abertura de um volume num sistema de gestão arquivística.<br>Registrar informações tais como: data/hora da abertura, responsável pela abertura. | NA | O | NA | 1.5.4<br>1.5.5<br>1.5.8 |
| 2.10 Encerramento_ volume | Registro do encerramento ou arquivamento de um volume num sistema de gestão arquivística.<br>Registrar informações tais como: data/hora do encerramento, responsável. | NA | O | NA | 1.5.5<br>1.5.7<br>1.5.8<br>1.5.89 |
| 2.11 Juntada_anexação | Registro da juntada, em caráter definitivo, de documento ou processo a outro processo, na qual prevalece para referência, o número do processo mais antigo.<br>Registrar informações tais como: data/hora da anexação, responsável pela anexação, identificador do processo que foi anexado. | O | NA | NA | 1.4.5 |
| 2.12 Juntada_apensação | Registro da apensação, ou seja, juntada em caráter temporário, com o objetivo de elucidar ou subsidiar a matéria tratada, conservando cada processo sua identidade ou independência.<br>Registrar informações tais como: data/hora da apensação, responsável pela apensação, identificador do processo que foi apensado. | O | NA | NA | 1.4.5 |

| EVENTO | DEFINIÇÃO E ELEMENTOS | APLICA-SE A | | | REQ. |
|---|---|---|---|---|---|
| | | Processo/ dossiê | Volume | Documento | |
| 2.13 Desapensação | Registro da desapensação.<br>Registrar informações tais como: data/hora da desapensação, responsável pela desapensação, identificador do processo que foi desapensado. | O | NA | NA | 1.4.6 |
| 2.14 Desentranhamento | Registro de retirada autorizada de documentos de um processo.<br>Registrar informações tais como: data/hora do desentranhamento, responsável pelo desentranhamento, identificador das peças que foram desentranhadas. | O | NA | O | 1.4.7 |
| 2.15 Desmembramento | Registro de desmembramento de processos.<br>Registrar informações tais como: data/hora do desmembramento, responsável pelo desmembramento, registro dos documentos retirados, identificador do novo processo formado com os documentos retirados. | O | NA | NA | 1.4.8 |
| 2.16 Classificação_sigilo | Registro do procedimento de classificação de sigilo.<br>Registrar informações referentes à classificação de grau de sigilo, tais como: grau de sigilo, data/hora da classificação, responsável pela classificação. | O | NA | O | 1.6.8<br>Ver seção 6.3 |
| 2.17 Desclassificação_ sigilo | Registro do procedimento de desclassificação de sigilo.<br>Registrar informações referentes à desclassificação | O | NA | O | Ver seção 6.3 |

| EVENTO | DEFINIÇÃO E ELEMENTOS | APLICA-SE A | | | REQ. |
|---|---|---|---|---|---|
| | | Processo/ dossiê | Volume | Documento | |
| | do grau de sigilo, tais como: grau de sigilo, data/hora da desclassificação, responsável pela classificação. | | | | |
| 2.18 Reclassificação_ sigilo | Registro do procedimento de reclassificação de sigilo.<br>Registrar informações referentes à reclassificação do grau de sigilo, tais como: data/hora da reclassificação, responsável pela reclassificação, justificativa. | O | NA | O | Ver seção 6.3 |

# 3 CLASSE

Estas informações referem-se à configuração e administração do plano de classificação.

## 3.1 Descrição da classe

| ELEMENTO | DEFINIÇÃO | OBRIG | REQ. |
|---|---|---|---|
| 3.1.1 Classe_nome | Divisão de um plano ou código de classificação.<br>Refere-se às classes, subclasses, grupos e subgrupos. | O | 1.1.11 |
| 3.1.2 Classe_código | Divisão de um plano ou código de classificação, representada por um conjunto de símbolos, normalmente letras e/ou números convencionados<br>Refere-se às classes, subclasses, grupos e subgrupos. | O | 1.1.11 |
| 3.1.3 Classe_subordinação | Registra a subordinação da classe na hierarquia do plano. | O | 1.1.13 |
| 3.1.4 Registro de abertura | Registra a abertura de uma classe.<br>Registrar informações tais como: data/hora e responsável. | O | 1.1.4 |

| ELEMENTO | DEFINIÇÃO | OBRIG | REQ. |
|---|---|---|---|
| 3.1.5 Registro de desativação | Registra a desativação de uma classe.<br>Registrar informações tais como: data/hora e responsável. | O | 1.1.7<br>1.1.8 |
| 3.1.6 Reativação de classe | Registro de reativação da classe.<br>Registrar informações tais como: data/hora e responsável. | O | 1.1.4 |
| 3.1.7 Registro de mudança de nome de classe | Registra a mudança de nome de uma classe.<br>Registrar informações tais como: data/hora, responsável e nome anterior. | O | 1.1.5 |
| 3.1.8 Registro de deslocamento de classe | Registra o deslocamento de uma classe na hierarquia do plano de classificação, ou seja, a mudança de subordinação.<br>Registrar informações tais como: data/hora, responsável e subordinação anterior. | O | 1.1.6 |
| 3.1.9 Registro de extinção | Registra a extinção de uma classe.<br>Registrar informações tais como: data/hora e responsável. | O | 1.1.8 |
| 3.1.10 Indicador de classe ativa/inativa | Registro de classes inativas.<br>Registrar informações tais como: data/hora e responsável. | O | 1.1.4<br>1.1.7<br>1.1.8 |

## 3.2 Temporalidade associada à classe

| ELEMENTO | DEFINIÇÃO | OBRIG | REQ. |
|---|---|---|---|
| 3.2.1 Classe_código | Identificador de classe. | O | 4.1.3 |
| 3.2.2 Prazo de guarda na fase corrente | | O | 4.1.3 |
| 3.2.3 Evento que determina a contagem do prazo de guarda na fase corrente | | O | 4.1.3 |

| ELEMENTO | DEFINIÇÃO | OBRIG | REQ. |
|---|---|---|---|
| 3.2.4 Prazo de guarda na fase intermediária | | O | 4.1.3 |
| 3.2.5 Evento que determina a contagem do prazo de guarda na fase intermediária | | O | 4.1.3 |
| 3.2.6 Destinação final | Preservação ou eliminação. | O | 4.1.3 |
| 3.2.7 Registro de alteração | Registrar informações tais como: data/hora da alteração, responsável, identificador da classe que teve prazo ou destinação alterada, descrição da alteração (incluindo o prazo/destinação anterior). | O | 4.1.7<br>4.1.8<br>4.1.9 |
| 3.2.8 Observações | Informações complementares tais como: previsão de conversão de suporte, legislação relativa à justificativa de prazos. | F | 4.1.3 |

## 4 AGENTE

A tabela abaixo especifica a aplicação de cada elemento de metadado para cada um dos diferentes tipos de agentes.

| ELEMENTO | DEFINIÇÃO | APLICA-SE A<br>usuário\|papel\|grupo | | | REQ. |
|---|---|---|---|---|---|
| 4.1 Nome | Nome do agente (usuário, papel e grupo). | O | O | O | 6.2.1 |
| 4.1 Identificador | Identificador do agente (usuário, papel e grupo). | O | O | O | 6.2.1<br>6.2.3 |
| 4.3 Autorização de acesso | Nível de restrição de acesso (uso e intervenção) aos documentos e operações do sistema. | O | O | O | 6.2.1<br>6.2.3<br>6.2.8 |
| 4.4 Credenciais de autenticação | Autentica o usuário no SIGAD. Pode ser: senha, biometria, certificado digital + chave privada. | O | NA | NA | 6.2.1<br>6.2.4 |

| ELEMENTO | DEFINIÇÃO | APLICA-SE A usuário\|papel\|grupo | | | REQ. |
|---|---|---|---|---|---|
| 4.5 Relação | Relaciona o usuário a papéis e/ou ao grupo a que pertence.<br>As relações podem ser:<br>▪ tem usuário<br>▪ tem papel<br>▪ é membro de | NA<br>O<br>O | O<br>NA<br>NA | O<br>NA<br>NA | 6.2.11<br>6.2.15 |
| 4.6 Status do agente | Indica se o agente está ativo ou inativo no SIGAD. | O | O | O | 6.2.1 |

## 5 COMPONENTE DIGITAL

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

### 5.1 Identificador do componente digital

| Designação | Identificador do componente digital |
|---|---|
| Definição | Designação usada para identificar os componentes digitais que integram o documento. |
| Objetivo | Identificar de forma unívoca e persistente os componentes digitais armazenados no repositório gerenciado pelo SIGAD. Cada componente digital mantido no repositório tem que possuir um identificador único para relacioná-lo aos metadados descritivos e técnicos de forma que o SIGAD possa gerenciá-lo. |
| Obrigatoriedade | O |
| Nota de aplicação | O identificador tem que ser único no âmbito do repositório.<br>Devem ser registradas informações sobre o tipo e o valor do identificador. Caso seja utilizado somente um tipo de identificador no repositório, não é necessário explicitá-lo, bastando registrar o valor do identificador. |

| | |
|---|---|
| Exemplos | *Tipo do identificador: handle*[53]<br>*Valor do identificador: loc.music/gottieb.09601*<br>*Tipo do identificador: identificador institucional*<br>*Valor do identificador: CD269/CD269/70/10596.PCD* |
| Requisito | 3.1.21 |

## 5.2 Nome original

| Designação | Nome original |
|---|---|
| Definição | Nome original do componente digital no momento em que foi inserido no repositório, antes de ser renomeado com o identificador do repositório. |
| Objetivo | Possibilitar a identificação do componente digital por meio de seu nome original devido a razões diversas: o nome utilizado dentro do repositório pode não ser conhecido externamente; um produtor de documentos pode procurar um arquivo pelo seu nome original ou, ainda, o repositório pode necessitar reconstruir *links* originais com objetivo de disseminação. |
| Obrigatoriedade | F |
| Nota de aplicação | Quando dois sistemas/repositórios estão transferindo documentos um para outro, pode ser importante registrar o nome original do componente para verificação posterior. |
| Exemplos | *0078NR.TIF* |
| Requisito | Ver seção 8 (Preservação) |

## 5.3 Características técnicas

| Designação | Características técnicas |
|---|---|
| Definição | Propriedades técnicas de um componente digital, aplicáveis à maioria dos formatos, tais como: nível de composição, tamanho, *software* de criação e inibidores. |
| Objetivo | Fornecer informações para apoiar ações de acesso, manutenção e preservação. |
| Obrigatoriedade | OA |

[53] O Handle System é um serviço de informação que provê um identificador persistente em redes como a Internet. Disponível em: <www.handle.net>.

| | |
|---|---|
| Nota de aplicação | Nível de composição informa se o componente digital está sujeito a algum nível de compressão ou criptografia e qual é este nível. Nível de composição <0> (zero) indica que o componente digital não está sujeito a nenhum processo de compressão ou criptografia. Nível de composição <1> (um) ou maior indica que o componente digital foi submetido a um ou mais processos de compressão ou criptografia e que deve ser decodificado para que o documento possa ser acessado. Por exemplo, um arquivo A pode ser comprimido e gerar um arquivo B, que por sua vez é cifrado e gera um arquivo C. Para se ter acesso ao arquivo A é necessário decifrar o arquivo C e depois descomprimir o arquivo B.<br><br>Tamanho informa o número de bytes do componente digital. Esta informação é útil para garantir a previsão de espaço de memória suficiente para mover ou processar arquivos, bem como para previsão de capacidade de armazenamento.<br><br>Com relação ao *software* de criação, devem ser informados o nome da aplicação, a versão e a data da criação.<br><br>Inibidores são recursos que inibem o acesso, uso ou migração do componente digital. Devem ser informados o tipo de inibidor, o alvo e a chave de acesso. |
| Exemplos | *Nível de composição:* 0<br><br>*Tamanho: 345 k*<br><br>Software *de criação_nome: Microsoft Word*<br><br>Software *de criação_versão: 7*<br><br>Software *de criação_data: 2009-10-06*<br><br>*Inibidor_tipo: proteção por senha*<br><br>*Inibidor_alvo: impressão*<br><br>*Inibidor_chave: xyz* |
| Requisito | Ver seção 8 (Preservação) |

## 5.4 Formato de arquivo

| Designação | Formato |
|---|---|
| Definição | Identificação do formato de arquivo do componente digital. |
| Objetivo | O conhecimento do formato de arquivo do componente digital é essencial para o planejamento e a implementação de diversas ações de preservação como, por exemplo, a conversão devido à obsolescência do formato. |

| | |
|---|---|
| Obrigatoriedade | O |
| Nota de aplicação | Devem ser registrados, obrigatoriamente, o nome e a versão do formato.<br><br>Informações adicionais sobre o formato também podem ser registradas.<br><br>Nos casos em que não for possível identificar o formato, este deve ser registrado como “desconhecido”.<br><br>Recomenda-se o uso de formas controladas para a designação do formato, como bases de dados de registro de formato. Ex.: PRONOM[54], MIME[55]. |
| Exemplos | Nome do formato: Adobe PDF<br><br>Versão: 6.0 |
| Requisito | 3.5.5 |

## 5.5 Armazenamento

| Designação | Armazenamento |
|---|---|
| Definição | Informações sobre a localização e o suporte do componente digital, bem como os recursos necessários para armazenamento permanente. |
| Objetivo | As informações sobre localização são necessárias para encontrar o componente digital no sistema de armazenamento.<br><br>As informações sobre o suporte em que o componente digital está armazenado apóiam o monitoramento das ações de preservação necessárias, como, por exemplo, a migração. |
| Obrigatoriedade | O |
| Nota de aplicação | Caso o repositório digital utilize um identificador como o *handle*, a localização estará implícita no identificador e não será necessário registrá-la novamente.<br><br>Quanto ao suporte, devem ser registradas informações a respeito do tipo de suporte utilizado e sua vida útil. |
| Exemplos | |
| Requisito | 6.1.7 |

[54] Serviço de base de dados de formatos de arquivo gerenciada pelo The National Archives (TNA), do Reino Unido. Disponível em: <www.nationalarchives.gov.uk/pronom/>.

[55] Lista de formatos comuns na Internet disponível em: <http://www.iana.org/assignments/media-types/index.html>

## 5.6 Ambiente de *software*

| Designação | Ambiente de *software* |
|---|---|
| Definição | Informações sobre o ambiente de *software* necessário para apresentar e/ou usar os componentes digitais, incluindo a aplicação e o sistema operacional. |
| Objetivo | Dar conhecimento do ambiente de *software* necessário para uso do recurso. |
| Obrigatoriedade | O |
| Nota de aplicação | Com relação à aplicação de *software* ou sistema operacional, devem ser registradas as seguintes informações: nome, versão, tipo de *software* (por exemplo: sistema operacional, *browser*, editor de texto, planilha, *plug-in*) e documentação. |
| Exemplos | *Nome: Windows*<br>*Versão:XP*<br>*Tipo: sistema operacional*<br>*Documentação: manual do sistema*<br>*Nome: Word*<br>*Versão: 7*<br>*Tipo: editor de texto* |
| Requisito | Ver seção 8 (Preservação) |

## 5.7 Ambiente de *hardware*

| Designação | Ambiente de *hardware* |
|---|---|
| Definição | Informações sobre os componentes de *hardware* necessários para operar o *software* referenciado em 5.6, incluindo periféricos. |
| Objetivo | Dar conhecimento do ambiente de *hardware* necessário para uso do recurso. |
| Obrigatoriedade | O |
| Nota de aplicação | Devem ser registradas informações tais como: nome do componente de *hardware* necessário (que pode incluir o fabricante, o modelo e a versão), tipo de componente de *hardware* (por exemplo, processador, memória), configuração mínima recomendada para instalar e/ou operar o *hardware*, e documentação. |

| | |
|---|---|
| Exemplos | *Nome: Intel x86*<br>*Tipo: processador*<br>*Configuração mínima: 60 Mhz*<br>*Nome: RAM*<br>*Tipo: memória*<br>*Configuração mínima: 64 Mb* |
| Requisito | Ver seção 8 (Preservação) |

## 5.8 Dependências

| Designação | Dependências |
|---|---|
| Definição | Informações sobre outras dependências, que não sejam as de *software* e *hardware*, necessárias para apresentar ou usar os documentos (por exemplo, DTD, XML Schema, fontes, folha de estilo). |
| Objetivo | Dar informação sobre outros tipos de dependências, além de *software* e *hardware*, necessárias para uso do recurso. |
| Obrigatoriedade | OA |
| Nota de aplicação | Devem ser registradas informações tais como: nome do componente necessário e identificador do recurso específico (incluindo tipo e valor).<br>Em alguns casos o identificador do recurso já torna evidente o nome do componente necessário. |
| Exemplos | *Identificador_tipo: URI*<br>*Identificador_valor:*<br>*<http://www.arquivonacional.gov.br/XYZ/DTD/ojns.dtd >* |
| Requisito | Ver seção 8 (Preservação) |

## 5.9 Relação com outros componentes digitais

| Designação | Relacionamento |
|---|---|
| Definição | Registro das relações de um componente digital com outros componentes digitais ou com documentos. |
| Objetivo | Tornar explícito o relacionamento entre componentes digitais para possibilitar o processamento e acesso aos documentos e identificar os tipos de relação (estrutural ou de derivação).<br>Alguns documentos são formados por diversos componentes digitais relacionados. Estas relações são estruturais. Além |

| | |
|---|---|
| | disso, documentos podem ser armazenados de formas diferentes, como, por exemplo, documento máster e documento derivado, ou o original e cópias de *back-up*. Estas relações são de derivação. |
| Obrigatoriedade | F |
| Nota de aplicação | As relações estruturais são fundamentais para apresentar o documento ao usuário. As relações de derivação são importantes para documentar e controlar a origem do documento.<br><br>Devem ser registradas as seguintes informações para cada relacionamento: tipo de relação (estrutural ou derivação), identificação dos objetos relacionados, descrição da relação (por exemplo, é parte de).<br><br>As instituições devem estabelecer os tipos de relacionamentos mais relevantes, que deverão ser controlados nos metadados. Estas relações podem ser expressas das seguintes formas:<br><br>• tem parte de, é parte de;<br>• tem fonte de (um componente digital é uma versão de outro componente, criado por uma transformação), é fonte de (um componente derivado de outro componente por um processo de transformação);<br>• inclui, é incluído em (relação entre documento e componente digital). |
| Exemplos | *"Relatorio de atividades de 2009" inclui "relat_2009.doc"*<br><br>*"relat_2009" é fonte de "relat_2009.zip"* |
| Requisito | Ver seção 8 (Preservação) |

## 5.10 Fixidade

| Designação | Fixidade |
|---|---|
| Definição | Informações utilizadas para verificar se o componente digital sofreu mudanças não documentadas. |
| Objetivo | Verificar se o componente digital foi alterado de forma não documentada ou não autorizada, comprometendo sua autenticidade. |
| Obrigatoriedade | O |
| Nota de aplicação | Esta informação é calculada e registrada pelo sistema de maneira automática.<br><br>Atenção: este elemento de metadado não se refere à verificação da fixidade. Ele registra informações sobre |

| | |
|---|---|
| | procedimentos que garantem a autenticidade do componente digital, como cifragem, assinatura digital ou *checksum*.<br><br>Com relação à assinatura digital, devem ser registradas as seguintes informações: codificação da assinatura, gerador da assinatura, método da assinatura, valor da assinatura, regras de validação da assinatura, propriedades da assinatura, chave pública do gerador.<br><br>Com relação à cifragem e *checksum*, devem ser registradas as seguintes informações: algoritmo utilizado, resultado (da cifragem ou *checksum*), originador. |
| Requisito | 6.5.3 / 6.5.4 / 6.6.3 / 6.6.6 / Ver seção 8 (Preservação) |

## 6 EVENTO DE PRESERVAÇÃO

Estas informações referem-se a eventos de preservação ocorridos com o componente digital. Para cada evento, são apresentados uma definição e os elementos de metadados que o caracterizam e que devem ser registrados.

É importante notar que esta listagem mostra os eventos mais importantes de serem registrados. Não se esgotaram as possibilidades; os órgãos e entidades podem incluir outros eventos que julgarem necessários.

| Evento | Definição e elementos de metadado | Obrig. | Req. |
|---|---|---|---|
| 6.1 Compressão | Registro da compressão ou descompressão de documentos.<br><br>Registrar informações tais como: identificação da compressão, data da compressão, agente responsável pela compressão e resultado da compressão. | OA | 8.3.1<br>8.3.6 |
| 6.5 Decifração | Registro da decifração de documentos.<br><br>Registrar informações tais como: identificação da decifração, data da decifração, agente responsável pela decifração e resultados da decifração. | OA | 6.6.3<br>6.6.6<br>8.3.1<br>8.3.6 |
| 6.5 Validação de assinatura digital | Registro de validação da assinatura digital de um documento de acordo com o certificado digital deste.<br><br>Registrar informações tais como: identificação da validação, data da | OA | 6.5.4<br>6.5.5<br>8.3.1<br>8.3.6 |

| | | | |
|---|---|---|---|
| | validação, agente responsável pela validação e resultados da validação. | | |
| 6.4 Verificação de fixidade | Registro da verificação de fixidade de um documento, ou seja, se os recursos utilizados para garantir a fixidade (assinatura digital, marca d'água, *checksum* etc.) não foram corrompidos.<br>Registrar informações tais como: tipo de recurso de autenticação, identificação da verificação, data da verificação, agente responsável pela verificação e resultados da verificação. | OA | 6.5.5<br>6.7.2<br>8.2.6<br>8.3.1<br>8.3.6 |
| 6.5 Cálculo *hash* | Registro do cálculo *hash* de criptografia.<br>Registrar informações tais como: identificação do cálculo, data do cálculo, agente responsável pelo cálculo e detalhes do cálculo. | OA | 6.9.9<br>8.3.1<br>8.3.6 |
| 6.6 Migração | Registro de procedimento de migração de documento.<br>Registrar informações tais como: identificação da migração, data da migração, agente responsável pela migração, resultado da migração e conseqüências da migração. | OA | 3.1.5<br>8.3.1<br>8.3.6 |
| 6.7 Replicação | Registro de procedimento de replicação de documento.<br>Registrar informações tais como: identificação da replicação, data da replicação, agente responsável pela replicação e consequências da replicação. | OA | 6.10.7<br>8.3.1<br>8.3.6 |
| 6.8 Verificação de vírus | Registro de verificação de vírus no documento.<br>Registrar informações tais como: identificação da verificação, data da verificação, agente responsável pela verificação e detalhes da verificação. | OA | 6.9.1<br>8.3.1<br>8.3.6 |
| 6.9 Validação | Registro de validação de documento.<br>Registrar informações tais como: identificação da validação, data da validação, agente responsável pela validação e detalhes da validação. | OA | Ver seção 7.3 (Armazenamento) |

# Glossário

AC

*Ver* autoridade certificadora

acervo

Totalidade dos documentos de uma entidade produtora ou de uma entidade custodiadora.

acessibilidade

Facilidade no acesso ao conteúdo e ao significado de um objeto digital. (I) *Accessibility*.
*Ver também* acesso

acesso

Direito, oportunidade ou meios de encontrar, recuperar e usar a informação.
*Ver também* acessibilidade; classificação(2); credencial de segurança

anexo

Um objeto digital que segue junto com a mensagem de correio eletrônico ou com um fluxo de trabalho. (I) *Attachment*.

anotação

Informação acrescentada ao documento arquivístico após sua produção. Exemplos: “urgente”, “arquive-se”, número do protocolo, código de classificação, temporalidade, data, hora e local da transmissão, indicação de anexos e outros.

AR

*Ver* autoridade de registro

armazenamento

1 Guarda de documentos digitais em dispositivos de memória não volátil.
2 Guarda de documentos arquivísticos em local apropriado. (I) *Storage*.

arquivamento

1 Sequência de operações intelectuais e físicas que visam à guarda ordenada de documentos.
2 Ação pela qual uma autoridade determina a guarda de um documento, cessada a sua tramitação.

arquivo

1 Conjunto de documentos produzidos e acumulados por uma entidade coletiva, pública ou privada, pessoa ou família, no desempenho de suas atividades, independentemente da natureza dos suportes.
2 Instituição ou serviço que tem por finalidade a custódia, o processamento técnico, a conservação e o acesso a documentos arquivísticos.
*Ver também* arquivo digital

arquivo digital

Conjunto de *bits* que formam uma unidade lógica interpretável por um programa de computador e armazenada em suporte apropriado.
*Ver também* objeto digital

assinatura digital

Modalidade de assinatura eletrônica resultante de uma operação matemática que utiliza algoritmos de criptografia e permite aferir, com segurança, a origem e a integridade do documento. Os atributos da assinatura digital são: a) ser única para cada documento, mesmo que o signatário seja o mesmo; b) comprovar a autoria do documento digital; c) possibilitar a verificação da integridade; d) assegurar ao destinatário o "não repúdio" do documento digital, uma vez que, a princípio, o emitente é a única pessoa que tem acesso à chave privada que gerou a assinatura.
*Ver também* assinatura eletrônica; certificado digital; criptografia

assinatura eletrônica

Geração, por computador, de qualquer símbolo ou série de símbolos executados, adotados ou autorizados por um indivíduo para ser o laço legalmente equivalente à assinatura manual do indivíduo.
Ver também assinatura digital

atualização

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. (I) *Refreshing*; (F) *repiquage*; (E) *refrescamiento.*
*Ver também*: conversão; migração; reformatação

autenticação

Declaração de que um documento é *autêntico*, ou de que uma cópia reproduz fielmente o original, feita num determinado momento por pessoa jurídica com autoridade para tal (servidor público, notário, autoridade certificadora).
*Ver também* autenticidade; certificado de autenticidade, carimbo digital de tempo

autenticidade

Credibilidade de um documento enquanto documento, isto é, a qualidade de um documento ser o que diz ser e de que está livre de adulteração ou qualquer outro tipo de corrupção.
*Ver também* autenticação; certificado de autenticidade, carimbo digital de tempo

autoridade certificadora (AC)

Organização que emite certificados digitais obedecendo às práticas definidas na Infraestrutura de Chaves Públicas (ICP).
*Ver também* certificado digital; chave privada; chave pública; ICP

autoridade de registro (AR)

Organização que distribui certificados digitais aos usuários finais mediante processo de identificação estabelecido nas práticas definidas na Infraestrutura de Chaves Públicas (ICP).
*Ver também* certificado digital; chave privada; chave pública; ICP

avaliação

Processo de análise de documentos arquivísticos que estabelece seus prazos de guarda e sua destinação de acordo com os valores que lhes são atribuídos.

banco de dados

1 Ambiente computacional composto por: a) dados estruturados em bases relacionadas entre si, de acordo com um modelo de dados; b) regras que definem as operações válidas sobre os dados e garantem sua integridade.
2 Sistema gerenciador de banco de dados (SGBD): *software* que implementa o banco de dados e permite a realização de operações de manipulação de dados (inclusão, alteração, exclusão, consulta) e administrativas (gestão de usuários, cópia e restauração de dados, alterações no modelo de dados).

*Ver também* base de dados

base de dados

Conjunto de dados estruturados, com as respectivas regras de acesso, formatação e validação, e administrados por um sistema gerenciador de banco de dados (SGBD).

*Ver também* banco de dados

captura

Incorporação de um documento ao sistema de gestão arquivística, por meio de registro, classificação e arquivamento.

*Ver também* arquivamento; classificação; registro

carimbo digital de tempo

Código binário, incorporado a um documento, que registra data e hora em que ocorreu um evento, como criação, recebimento, leitura, modificação ou eliminação. É uma forma de autenticação do documento. (I) *Timestamp; digital timestamp*.

*Ver* autenticação; autenticidade

categoria de sigilo

*Ver* grau de sigilo

certificação digital

Atividade de reconhecimento em meio eletrônico que se caracteriza pelo estabelecimento de uma relação única, exclusiva e intransferível entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação. Esse reconhecimento é inserido em um certificado digital por uma autoridade certificadora.

certificado de autenticidade

Declaração escrita em que se atesta a autenticidade das reproduções dos documentos arquivísticos digitais, emitida pela instituição responsável por sua preservação.

*Ver também* autenticação; autenticidade

certificado digital

Conjunto de dados de computador, gerados por uma autoridade certificadora (AC), que se destina a registrar, de forma única, exclusiva e intransferível, a relação existente entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação.

Ver também assinatura digital; chave privada; chave pública

chave privada

Chave matemática formada por uma sequência de dígitos usada para criptografia assimétrica e criada em conjunto com a chave pública correspondente, que deve ser mantida em segredo pelo portador. Usada para assinar, digitalmente, documentos, assim como para decifrar aqueles criptografados com a chave pública correspondente.

*Ver também* assinatura digital; certificado digital; chave pública

chave pública

Chave matemática formada por uma sequência de dígitos usada para criptografia assimétrica e criada em conjunto com a chave privada correspondente, disponibilizada, publicamente, por certificado digital e utilizada

para verificar assinaturas digitais. Também pode ser usada para criptografar mensagens ou arquivos a serem decifrados com a chave privada correspondente.

*Ver também* assinatura digital; certificado digital; chave privada

ciclo vital dos documentos

Sucessivas fases por que passam os documentos arquivísticos, de sua produção à guarda permanente ou eliminação.

classificação

1 Análise e identificação do conteúdo de documentos, seleção da categoria de assunto sob a qual sejam recuperados, podendo-se-lhes atribuir códigos.
2 Atribuição a documentos ou às informações neles contidas de graus de sigilo, conforme legislação específica. Também chamada “classificação de segurança”.

*Ver também* código de classificação; grau de sigilo; plano de classificação

código de classificação

Conjunto de símbolos, normalmente letras e/ou números, derivado de um plano de classificação.

*Ver também* classificação; plano de classificação

completeza

Atributo de um documento arquivístico que se refere à presença de todos os elementos intrínsecos e extrínsecos exigidos pela organização produtora e pelo sistema jurídico-administrativo a que pertence, de modo a ser capaz de gerar consequências. (I) *Completeness*.

Ver também confiabilidade; elemento extrínseco; elemento intrínseco

componente digital

Objeto digital que é parte de um ou mais documentos digitais e os metadados necessários para ordenar, estruturar ou manifestar seu conteúdo e forma, que requer determinadas ações de preservação. (I) *Digital component*.

confiabilidade

Credibilidade de um documento arquivístico enquanto afirmação de um fato. Existe quando um documento arquivístico pode sustentar o fato ao qual se refere, e é estabelecida pelo exame da completeza, da forma do documento e do grau de controle exercido no seu processo de criação. (I) *Reliability*.
*Ver também* completeza

contexto

Ambiente em que ocorre a ação registrada no documento. Na análise do contexto de um documento arquivístico, o foco deixa de ser o documento em si e passa a

abranger toda a estrutura que o envolve. O contexto pode ser documental, jurídico-administrativo, de procedimentos, de proveniência e tecnológico.

*Ver também* contexto de procedimentos; contexto de proveniência; contexto documental; contexto jurídico-administrativo; contexto tecnológico

contexto de procedimentos

Normas internas que regulam a produção, tramitação, uso e arquivamento dos documentos da instituição.

*Ver também* contexto de proveniência; contexto documental; contexto jurídico-administrativo; contexto tecnológico

contexto de proveniência

Organogramas, regimentos e regulamentos internos que identificam a instituição produtora de documentos.

*Ver também* contexto de procedimentos; contexto documental; contexto jurídico-administrativo; contexto tecnológico

contexto documental

Código de classificação, guias, índices e outros instrumentos que situam o documento dentro do conjunto a que pertence, ou seja, no fundo de arquivo.

*Ver também* contexto; contexto de procedimentos; contexto de proveniência; contexto jurídico-administrativo; contexto tecnológico

contexto jurídico-administrativo

Leis e normas externas à instituição produtora de documentos que controlam a condução das atividades desta mesma instituição.

*Ver também* contexto de procedimentos; contexto de proveniência; contexto documental; contexto tecnológico

contexto tecnológico

Ambiente tecnológico (*hardware*, *software* e padrões) que envolve o documento.

*Ver também* contexto de procedimentos; contexto de proveniência; contexto documental; contexto jurídico-administrativo

controle de versão

Conjunto de operações que permitem gerenciar as versões de um documento arquivístico digital.

*Ver também* identificador único

conversão

Técnica de migração que pode se configurar de diversas formas, tais como: 1. conversão de dados: mudança de formato; 2. conversão de sistema computacional: mudança do modelo de computador e de seus periféricos. (I) *Conversion*.

*Ver também* migração; reformatação

correio eletrônico

Sistema usado para criar, transmitir e receber mensagens eletrônicas e outros documentos digitais por meio de redes de computadores. (I) *E-mail*.

*Ver também* mensagem eletrônica

credencial de segurança

Atributo ou conjunto de atributos associados a um usuário que definem as categorias de segurança segundo as quais o acesso é concedido.

criptografia

Método de codificação de dados com base em algoritmo específico e chave secreta, de forma que somente os usuários autorizados possam restabelecer a forma original dos dados.

*Ver também* assinatura digital; chave privada; chave pública; criptografia assimétrica; criptografia simétrica; **ICP**

criptografia assimétrica

Método de criptografia que utiliza um par de chaves diferentes que se relacionam, matematicamente, por meio de um algoritmo, de modo que o texto cifrado por uma chave só possa ser decifrado pela outra que forma com ela um par. As duas chaves envolvidas na criptografia assimétrica são denominadas chave pública e chave privada.

*Ver também* chave privada; chave pública; criptografia simétrica

criptografia de chave pública

*Ver* criptografia assimétrica

criptografia simétrica

Método de criptografia que utiliza uma chave simétrica, de maneira que o texto seja cifrado e decifrado com esta mesma chave.

*Ver também* criptografia assimétrica

custódia

Responsabilidade jurídica de guarda e proteção de arquivos, independentemente de vínculo de propriedade.

dado

Representação de todo e qualquer elemento de conteúdo cognitivo passível de ser comunicada, processada e interpretada de forma manual ou automática.

*Ver também* metadados

destinação

Decisão, com base na avaliação, sobre o encaminhamento de documentos para guarda permanente, descarte ou eliminação.

*Ver também* eliminação; recolhimento

digitalização

Processo de conversão de um documento para o formato digital, por meio de dispositivo apropriado.

documento

Unidade de registro de informações, qualquer que seja o suporte ou formato.
Ver também documento digital; documento eletrônico; suporte

documento arquivístico

Documento produzido (elaborado ou recebido) no curso de uma atividade prática, como instrumento ou resultado dessa atividade e retido para ação ou referência. (I) *Record*.

documento arquivístico digital

Documento digital reconhecido e tratado como documento arquivístico. (I) *Digital record*.

*Ver também* documento arquivístico; documento digital

documento arquivístico eletrônico

Documento eletrônico reconhecido e tratado como documento arquivístico. (I) *Electronic record*.
*Ver também* documento arquivístico; documento eletrônico

documento digital

Informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional. (I) *Digital document*.

documento eletrônico

Informação registrada, codificada em forma analógica ou em dígitos binários, acessível e interpretável por meio de equipamento eletrônico. (I) *Electronic document*.

dossiê

Conjunto de documentos relacionados entre si por ação, evento, pessoa, lugar, projeto, que constitui uma unidade.
*Ver também* dossiê híbrido; processo

dossiê híbrido

Dossiê constituído por documentos digitais e não digitais. Exemplo: projetos arquitetônicos que apresentam descrição em papel e plantas em disco óptico.

*Ver também* processo híbrido

elemento extrínseco

Atributo que caracteriza a forma externa do documento arquivístico. Exemplos: tipo, cor e tamanho da letra; apresentação (textual, gráfico, sonoro ou multimídia); selo, logomarca; assinatura digital; *links*.

*Ver também* documento arquivístico; elemento intrínseco

elemento intrínseco

Atributo que caracteriza a forma interna do documento arquivístico. Exemplos: autor, destinatário, data, local, assinatura, assunto.

*Ver também* documento arquivístico; elemento extrínseco

eliminação

Destruição de documentos que, na avaliação, foram considerados sem valor para guarda permanente.

*e-mail*

*Ver* correio eletrônico

emulação

Estratégia de preservação digital que se baseia na utilização de recursos computacionais para fazer uma tecnologia atual funcionar com as características de uma obsoleta, aceitando as mesmas entradas e produzindo as mesmas saídas.

exportação

Processo de transferência de dados de um sistema informatizado para outro, podendo haver conversão.

*Ver também* conversão

forma documental

Regras de representação que definem como o conteúdo de um documento arquivístico, seu contexto administrativo e documental, e sua autoridade são comunicados. A forma documental possui elementos extrínsecos e intrínsecos. (I) *Documentary form*.

*Ver também* elemento extrínseco; elemento intrínseco

formato de arquivo

Especificação de regras e padrões descritos, formalmente, para interpretação dos *bits* constituintes de um arquivo digital. Os formatos de arquivo podem ser: 1. *aberto*, quando as especificações são públicas (p. ex.: *.xml*, *.html*, *.odf*, *.rtf*, *.txt* e *.png*); 2. *fechado*, quando as especificações não são divulgadas pelo proprietário (p. ex.: *.doc*); 3. *proprietário*, quando as especificações são definidas por uma organização que mantém seus direitos, sendo seu uso gratuito ou não (p. ex.: *.pdf*, *.jpeg*, *.doc* e *.gif*); 4. *padronizado*, quando as especificações são produzidas por um organismo de normalização, sendo os formatos abertos e não proprietários (p. ex.: *.xml*, *.pdf/A*). (I) *Format*; (F) *format*; (E) *formato*.

gestão arquivística de documentos

Conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento de documentos arquivísticos em fase corrente e intermediária, visando sua eliminação ou recolhimento para guarda permanente. (I) *Records management.*

*Ver também* sistema de gestão arquivística de documentos; sistema informatizado de gestão arquivística de documentos

grau de sigilo

Gradação de sigilo atribuída a um documento ou parte dele em razão da natureza do seu conteúdo, com o objetivo de limitar sua divulgação a quem tenha necessidade de conhecê-lo.

*hardware*

Conjunto dos componentes físicos necessários à operação de um sistema computacional. (I)(E) *Hardware*; (F) *matériel*.

ICP

*Ver* infraestrutura de chaves públicas

identificador único

Código gerado automaticamente que identifica o dossiê, processo ou item documental de maneira a distingui-lo dos demais. (I) *File identifier*.

*Ver também* controle de versão; registro

informação

Elemento referencial, noção, ideia ou mensagem contida num documento.

infraestrutura de chaves públicas (ICP)

Conjunto de técnicas, práticas e procedimentos que estabelecem os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública. Normalmente, é constituído por uma cadeia de autoridades certificadoras composta pela autoridade certificadora raiz (AC raiz), pelas demais autoridades certificadoras (AC) e pelas autoridades de registro (AR).

*Ver também* autoridade certificadora; autoridade de registro; chave privada; chave pública; criptografia assimétrica

integridade

Estado dos documentos que se encontram completos e não sofreram nenhum tipo de corrupção ou alteração não autorizada nem documentada.[56]

item documental

Menor unidade arquivística intelectualmente indivisível.

marca d'água digital

Marca que serve para distinguir uma imagem digital com informação sobre sua proveniência e características, utilizada para proteger a propriedade intelectual. As marcas d'água sobrepõem, no mapa de *bits* de uma imagem, um desenho complexo, visível ou invisível, que só pode ser suprimido mediante a utilização de um algoritmo e de uma chave protegida. (I) *Digital watermark*.

mensagem eletrônica

Documento digital criado ou recebido por meio de um sistema de correio eletrônico. Às vezes, vem acompanhado de anexos que são transmitidos com a mensagem.

[56] Não confundir com "integridade arquivística", cujo objetivo, decorrente do princípio da proveniência, "consiste em resguardar um fundo de misturas com outros, de parcelamentos e de eliminações indiscriminadas. Também chamado integridade do fundo" (ARQUIVO NACIONAL, 2005, p. 108).

metadados

Dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e/ou preservar documentos arquivísticos ao longo do tempo.

mídia

*Ver* suporte

migração

Conjunto de procedimentos e técnicas para assegurar a capacidade dos objetos digitais de serem acessados apesar das mudanças tecnológicas. A migração consiste na transferência de um objeto digital: a) de um suporte que está se tornando obsoleto, fisicamente deteriorado ou instável para um suporte mais novo; b) de um formato obsoleto para um formato mais atual ou padronizado; c) de uma plataforma computacional em vias de descontinuidade para outra mais moderna. A migração pode ocorrer por *conversão*, *atualização* ou *reformatação*.

*Ver também* acessibilidade; conversão; objeto digital; reformatação; atualização

minuta

Versão preliminar de documento sujeita a aprovação.

objeto digital

Uma ou mais cadeias de *bits* que registram o conteúdo do objeto e de seus metadados associados. A anatomia do objeto digital é percebida em três níveis: 1. nível físico – refere-se ao objeto digital enquanto fenômeno físico que registra as codificações lógicas dos *bits* nos suportes. Por exemplo, no suporte magnético, o objeto físico é a sequência do estado de polaridades (negativa e positiva) e, nos suportes ópticos, é a sequência de estados de translucidez (transparência e opacidade); 2. nível lógico – refere-se ao objeto digital como um conjunto de sequências de *bits*, que constitui a base dos objetos conceituais; 3. nível conceitual – refere-se ao objeto digital que se apresenta de maneira compreensível para o usuário, como, por exemplo, o documento visualizado na tela do computador. (I) *Digital object*.

*Ver também* arquivo digital

organicidade

Relações que os documentos arquivísticos guardam entre si e que expressam as funções e atividades da pessoa ou organização que os produziu. A organicidade é um atributo essencial para se considerar determinado conjunto de documentos como um arquivo.
*Ver também* documento arquivístico

original

Primeiro documento completo e efetivo.

plano de classificação

Esquema de distribuição de documentos em classes de acordo com métodos de arquivamento específicos, elaborado com base no estudo das estruturas e funções de uma instituição e na análise do arquivo por ela produzido. Expressão geralmente adotada em arquivos correntes.
*Ver também* classificação; código de classificação

preservação digital

Conjunto de ações gerenciais e técnicas exigidas para superar as mudanças tecnológicas e a fragilidade dos suportes, garantindo acesso e interpretação dos documentos digitais pelo tempo que for necessário.

*Ver também* migração; atualização; emulação

processo

Conjunto de documentos reunidos, oficialmente, no decurso de ação administrativa ou judicial e que constitui uma unidade.
*Ver também* dossiê; processo híbrido

processo híbrido

Processo constituído de documentos digitais e não digitais de natureza diversa, reunidos, oficialmente, no decurso de ação administrativa ou judicial e que formam uma unidade conceitualmente indivisível.

*Ver também* dossiê híbrido

programa de computador

Sequência lógica de instruções que o computador é capaz de executar para obter um resultado específico.

recolhimento

Entrada de documentos em arquivos permanentes.

recuperação da informação

Processo de pesquisa, localização e apresentação de documentos em um sistema de informação. A pesquisa é feita por meio da formulação de estratégias de busca para identificação e localização de documentos e/ou seus metadados. A apresentação pode se dar por visualização em tela, impressão, leitura de dados de áudio e/ou vídeo.

reformatação

1 Técnica de migração que consiste na mudança da forma de apresentação de um documento para fins de acesso ou preservação dos dados, como, por exemplo, a impressão ou transformação de documentos digitais em microfilme (tecnologia COM) ou a transferência de documentos de um sistema computacional para uma mídia móvel (tecnologia COLD).
2 Supressão de todos os dados de uma unidade de armazenamento. (I) *Reformatting*.
*Ver também* conversão; migração; atualização

registro

Procedimento que formaliza a captura do documento arquivístico no sistema de gestão arquivística por meio da atribuição de um identificador único e de outros metadados (data, classificação, título) que descrevem o documento.
*Ver também* identificador único

sistema de informação

Conjunto organizado de políticas, procedimentos, pessoas, equipamentos e programas computacionais que produzem, processam, armazenam e proveem acesso à informação. (I) *Information system*.

sistema de gestão arquivística de documentos

Conjunto de procedimentos e operações técnicas cuja interação permite a eficiência e a eficácia da gestão arquivística de documentos.
*Ver também* gestão arquivística de documentos; sistema informatizado de gestão arquivística de documentos

sistema informatizado de gestão arquivística de documentos

Conjunto de procedimentos e operações técnicas característico do sistema de gestão arquivística de documentos, processado eletronicamente e aplicável em ambientes digitais ou híbridos, isto é, compostos de documentos digitais e não digitais.

*Ver também* captura; gestão arquivística de documentos

*software*

*Ver* programa de computador

suporte

Base física sobre a qual a informação é registrada. (I) *Medium, storage medium*.

tramitação

Curso do documento desde a sua produção ou recepção até o cumprimento de sua função administrativa. Também chamado movimentação ou trâmite.

transferência

Passagem de documentos do arquivo corrente para o arquivo intermediário.

trilha de auditoria

Conjunto de informações registradas que permite o rastreamento de intervenções ou tentativas de intervenção no documento arquivístico digital ou no sistema computacional. (I) *Audit trail*.

valor primário

Valor atribuído aos documentos em função do interesse que possam ter para a entidade produtora, levando-se em conta sua utilidade para fins administrativos, legais e fiscais.

valor secundário

Valor atribuído aos documentos em função do interesse que possam ter para a entidade produtora e outros usuários, tendo em vista sua utilidade para fins diferentes daqueles para os quais foram, originalmente, produzidos.

versão

Uma ou mais variantes de um mesmo documento. (I) *Version*.

*Ver também* controle de versão; minuta

# Referências


ARQUIVO NACIONAL (Brasil). *Gestão de documentos*: conceitos e procedimentos básicos. Rio de Janeiro, 1993. (Publicações Técnicas, n. 47).

_____. *Curso de gestão de documentos*. Rio de Janeiro, 2004.

_____. *Dicionário brasileiro de terminologia arquivística*. Rio de Janeiro, 2005. (Publicações Técnicas, n. 51)

BRASIL. Ministério da Defesa. Marinha. *Normas sobre documentação administrativa e arquivamento na Marinha (NODAM)*. Brasília, 2000.

CONSELHO INTERNACIONAL DE ARQUIVOS. Comité de arquivos correntes em ambiente electrónico. *Documentos de arquivo electrónicos*: manual para arquivistas. Paris, 2005. (Estudo n. 16 do ICA). Disponível em: <http://www.ica.org/en/node/30444>. Acesso em: 14 maio 2010.

_____. Committee on electronic records. *Guide for managing electronic records from an archival perspective*. Paris, 1997. (ICA Studies, n. 8). Disponível em: <http://www.ica.org/en/node/30019>. Acesso em: 14 maio 2010.

_____. *ISAD(G)*: Norma geral internacional de descrição arquivistica. 2ª edição, adotada pelo Comitê de Normas de Descrição, Estocolmo, Suécia, 19-22 de setembro de 1999, versão final aprovada pelo CIA. Rio de Janeiro: Arquivo Nacional, 2001. (Publicações Técnicas, n. 49).

CONSELHO NACIONAL DE ARQUIVOS (Brasil). *Classificação, temporalidade e destinação de documentos de arquivo relativos às atividades-meio da administração pública*. Rio de Janeiro: Arquivo Nacional, 2001.

COSTA, Eliezer Arantes. *Gestão estratégica*. São Paulo: Saraiva, 2003.

DURANTI, Luciana (Ed.) *The long-term preservation of the authentic electronic records*: findings of the InterPARES project. San Miniato: Archilab, 2005

_____. The InterPARES Project. In: *Authentic records in the electronic age*. Vancouver: University of British Columbia, 2000.

_____ et al. *Preservation of the integrity of electronic records*. Dordrecht: Kluwer Academic, 2002.

_____; MACNEIL, Heather. The protection of the integrity of electronic records: an overview of the UBC-MAS research project. *Archivaria*, Ottawa, n. 42, p. 46-67, Fall 1996.

ERLANDSSON, Alf. *Electronic records management*: a literature review. Paris: International Council on Archives / Committee on Electronic Records, 1997. (Studies, 10).

ESTADOS UNIDOS. Department of Defense. *Design criteria standard for electronic records management software applications*: DOD 5015.2-STD. Washington, 2002.

INSTITUTO DOS ARQUIVOS NACIONAIS (Portugal). Torre do Tombo. Instituto de Informática. Modelo de requisitos para a gestão de arquivos eletrônicos. In:_____. *Recomendações para a gestão de documentos de arquivo eletrônicos*. Lisboa, 2002. v. 2.

INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS. *InterPARES Project*. Disponível em: <http://www.interpares.org>. Acesso em: 14 maio 2010.

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (Estados Unidos). *Disposition of federal records*: a records management handbook. Washington, 2000 (web edition of 1997 printed publication). Disponível em: <http://www.archives.gov/records-mgmt/pdf/dfr-2000.pdf >. Acesso em: 14 maio 2010.

_____. *Electronic records management initiative*. Disponível em: <http://www.archives.gov /records-mgmt/initiatives/erm-overview.html>. Acesso em14 maio 2010.

PUBLIC RECORD OFFICE (Reino Unido). *Management, appraisal and preservation of electronic records guidelines*. Disponível em: <http://www.nationalarchives.gov.uk/recordsmanagement/management-appraisal-preservation.htm>. Acesso em: 14 maio 2010.

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

ROUSSEAU, Jean-Yves; COUTURE, Carol. *Os fundamentos da disciplina arquivística*. Lisboa: D. Quixote, 1994.

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

STANDARDS AUSTRALIA INTERNATIONAL. *Australian standard AS ISO 15489 - Records management.* Part 1: general [and] Part 2: guidelines. Sidney, 2002. Disponível em: <http://www.standards.org.au>. Acesso em: 14 maio 2010.

THE NATIONAL ARCHIVES (Reino Unido). *Requirements for electronic records management system:* 1- Functional requirements – 2002 revision: final revision. Kew, 2002.

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. Disponível em: <http://unesdoc.unesco.org/images/0013/001300/130071e.pdf>. Acesso em: 14 maio 2010.

UNIVERSIDADE ESTADUAL DE CAMPINAS. Sistema de Arquivos. *Manual de gestão de processos e de expedientes no âmbito da Universidade Estadual de Campinas*. Disponível em: <http://www.unicamp.br/siarq/arq_setoriais/manual_protocolo_expediente.pdf>. Acesso em: 14 maio 2010.