Conarq
CONSELHO NACIONAL DE ARQUIVOS

e-ARQ Brasil

Modelo de Requisitos
para Sistemas Informatizados
de Gestão Arquivística de Documentos

Câmara Técnica de Documentos Eletrônicos

e-ARQ Brasil

Modelo de Requisitos para Sistemas Informatizados
de Gestão Arquivística de Documentos

Versão 2
Adotada pelo Conselho Nacional de Arquivos
em junho de 2021

2022 | Maio

Praça da República, 173 ● Rio de Janeiro ● RJ ● 20211-350
e-mail: conarq@an.gov.br

Presidente da República
[redacted]

Ministro da Justiça e Segurança Pública
[redacted]

Presidente do Conselho Nacional de Arquivos
Ricardo Borda D'Água de Almeida Braga

Coordenador de Apoio ao Conselho Nacional de Arquivos
Antonio Laurindo dos Santos Neto

Coordenadora-geral de Acesso e Difusão Documental
Patricia Reis Longhi

Coordenadora de Pesquisa e Difusão do Acervo
Leticia dos Santos Grativol

Preparação
José Claudio Mattar

Revisão
Maria Cristina Martins

Diagramação
Alzira Reis

Capa
Tânia Maria Cuba Bittencourt

Dados Internacionais de Catalogação-na-Publicação (CIP)
(Biblioteca Maria Beatriz Nascimento – Arquivo Nacional)

Conselho Nacional de Arquivos (Brasil).
e-ARQ Brasil: Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos. [recurso eletrônico] / Câmara Técnica de Documentos Eletrônicos. 2. versão. – Dados eletrônicos (1 arquivo : 1 MB). – Rio de Janeiro : Arquivo Nacional, 2022.

Formato: PDF.
Requisitos do sistema: Adobe Acrobat Reader.
Modo de acesso: World Wide Web.
ISBN: 978-85-7009-007-2

1. Sistemas informatizados. 2. Gestão Arquivística de Documentos. I. Título

CDD 025.04

Ficha catalográfica elaborada por Dayo de Araújo Silva Côrbo (CRB 7/5633)

EQUIPE TÉCNICA DE ELABORAÇÃO DO E-ARQ BRASIL

Integrantes da Câmara Técnica de Documentos Eletrônicos que participaram da segunda versão

Brenda Couto de Brito Rocco – Universidade Federal do Estado do Rio de Janeiro
Carlos Augusto Silva Ditadi – Arquivo Nacional
Claudia Lacombe Rocha – Arquivo Nacional (presidente)
Daniel Flores – Universidade Federal Fluminense
Eloi Juniti Yamaoka – Serviço Federal de Processamento de Dados
João Alberto de Oliveira Lima – Senado Federal
Luís Fernando Sayão – Comissão Nacional de Energia Nuclear
Marco Aurélio Rodrigues Braga – Ministério da Economia
Margareth da Silva – Universidade Federal Fluminense
Neire do Rossio Martins – Arquivista
Rosely Curi Rondinelli – Arquivista
Vanderlei Batista dos Santos – Câmara dos Deputados

Consulta pública do e-ARQ Brasil

Câmara Técnica Consultiva

Brenda Couto de Brito Rocco – Universidade Federal do Estado do Rio de Janeiro
Claudia Lacombe Rocha – Arquivo Nacional (coordenadora)
Eloi Juniti Yamaoka – Serviço Federal de Processamento de Dados
Luís Fernando Sayão – Comissão Nacional de Energia Nuclear
Neire do Rossio Martins – Arquivista

Contribuições à consulta pública

Andressa Cristiani Piconi, Carlos Eduardo Carvalho Amand, Cristiane Rodrigues da Silva, Daniela Francescutti Martins Hott, Fábio Nascimento de Souza, Fabricio Vieira Valmant, Fernando Basseto, Jonas Ferrigolo Melo, Josedete Gonçalves Xavier, Luís Pereira dos Santos, Márcio Aparecido Nogueira Viana, Marilda Martins Coelho, Walter Wysk Koch.

Arquivo Público do Estado da Paraíba (APEPB), Associação dos Arquivistas da Paraíba (AAPB), Grupo de Estudos Arquivísticos (GEArq), Informind Treinamentos, Universidade Federal de Santa Catarina, Universidade Federal de Santa Maria.

Agradecemos a colaboração de Ana Maria Camargo, Luciana Duranti e Kenneth Thibodeau gentilmente prestada por meio de troca de mensagens de correio eletrônico.

SUMÁRIO

PREFÁCIO

A Câmara Técnica de Documentos Eletrônicos (CTDE),[1] do Conselho Nacional de Arquivos (CONARQ), apresenta a segunda versão do Modelo de requisitos para sistemas informatizados de gestão arquivística de documentos – e-ARQ Brasil.

A primeira versão desse documento foi publicada em 2006, com a disponibilização da Parte I e dos "Aspectos de funcionalidades", sendo complementada em 2009 com o esquema de metadados. Ao longo dos anos de 2017 a 2020, foi realizada uma atualização, que resultou na versão 2 que ora apresentamos.

O decurso da atualização foi longo, pois envolveu estudos teóricos, retroalimentação de iniciativas de adoção de Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD) e análise de documentos similares e afins, novos ou atualizados. Dentre eles destacamos novas versões do *Model requirements for the management of electronic records – MoReq* (MoReq 2 e MoReq 2010); o modelo de requisitos apresentado pelo Conselho Internacional de Arquivos em 2008 – *Principles and functional requirements for records in electronic office environments* e a versão de 2015 do dicionário de dados para metadados de preservação – PREMIS.

Além disso, o acompanhamento ou a participação na implementação de SIGADs na Unicamp, Câmara dos Deputados e DATAPREV, por parte de alguns integrantes da CTDE, municiou o trabalho de atualização do e-ARQ Brasil. Mais recentemente, integrantes da CTDE participaram da avaliação de duas soluções a partir dos requisitos do e-ARQ Brasil, que foram desenvolvidas no âmbito da Advocacia-Geral da União e do Tribunal Regional Federal da 2ª região. Essas experiências provocaram reflexões e a revisão de alguns requisitos funcionais, bem como evidenciaram a necessidade de maior detalhamento dos metadados.

Também foi levantada a legislação correlata aos documentos arquivísticos, em âmbito nacional, posterior à publicação da primeira versão do e-ARQ Brasil. Em alguns casos, os novos atos legislativos trouxeram impactos nos procedimentos relativos à gestão dos documentos arquivísticos, o que levou à necessidade de adequações dos requisitos.

No que diz respeito aos "Aspectos de funcionalidades" da versão 1, os requisitos foram separados em funcionais e não funcionais. Parte dos requisitos funcionais foi reagrupada em uma nova seção denominada "Elaboração de documentos", que concentra todos os requisitos relacionados à elaboração de documentos, avulsos ou processos. Foi também criada uma seção na parte de segurança, denominada "Assinatura cadastrada mediante identificação do usuário e senha". Além disso, diversos requisitos funcionais e não funcionais foram alterados, de maneira a corresponder aos contextos normativo e tecnológico atuais, bem como adequados para atender a questões apontadas nas experiências de desenvolvimento e implantação de SIGAD.

Uma grande mudança foi feita no esquema de metadados, principalmente no detalhamento daqueles que se referem aos eventos. Foi proposto um modelo para os metadados de eventos, similar ao apresentado no dicionário de dados do PREMIS, que registra um conjunto de informações específicas para cada evento. Nessa versão apresentamos quatro grupos de eventos (gestão do ciclo de vida, gestão do processo, gerenciamento de classe e preservação), e em cada um deles é apontada uma lista de tipos de eventos que devem ser registrados. Os "eventos de gestão" rela-

1 Por força do decreto n. 9.759, de 11 de abril de 2019, esta câmara técnica foi extinta.

cionados na primeira versão do e-ARQ Brasil foram divididos em dois grupos, um que diz respeito aos eventos de gestão ocorridos ao longo do ciclo de vida do documento e outro que concentra os procedimentos de protocolo. Os metadados relativos aos instrumentos de gestão (Código de classificação e Tabela de temporalidade e destinação de documentos) foram reorganizados em dois grupos: identificação da classe e gerenciamento da classe. Os metadados do primeiro grupo registram informações oriundas do plano de classificação e da tabela de temporalidade relativas a uma determinada classe/subclasse/grupo/subgrupo, e o segundo grupo refere-se aos eventos de gerenciamento dos instrumentos de gestão.

Alguns conceitos foram revistos, objetivando maior rigor e precisão. Nesse sentido, há que se ressaltar o uso dos termos "relação orgânica" e "organicidade" ao longo do documento. A relação orgânica diz respeito à relação de um documento com os demais que registram a mesma ação, nesse sentido é uma característica dos documentos arquivísticos. Já a organicidade está relacionada ao conjunto documental como um todo, sendo, portanto, uma característica do arquivo e não do documento. Nessa perspectiva, foram feitos alguns ajustes no uso desses dois termos ao longo do documento, bem como reformulados e inseridos outros tantos considerados relevantes.

Por fim, de forma geral, a versão 2 do e-ARQ Brasil trouxe adequação terminológica, alinhamento com padrões, especificações e legislação mais atuais e aprimorou a organização dos requisitos e a especificação dos metadados. Com isso, a CTDE espera oferecer um documento atual, rigoroso e útil para a comunidade arquivística brasileira.

Claudia Lacombe Rocha
Presidente da Câmara Técnica de Documentos Eletrônicos (2004-2019)

INTRODUÇÃO

A elaboração do e-ARQ Brasil foi baseada em documentos similares já publicados no início dos anos 2000, por diferentes instituições europeias e americanas. Na ocasião, o documento base utilizado foi o Modelo de requisitos para a gestão de arquivos eletrônicos – MoReq, publicado em 2001 pelo DLM Forum e Comissão Europeia. A decisão de se elaborar um modelo de requisitos próprio, diferenciado do MoReq, foi em razão da necessidade de se introduzirem procedimentos e conceitos que fossem compreensíveis e adequados à legislação brasileira, bem como à nossa tradição administrativa e arquivística, que se diferencia, em muitos aspectos, do contexto europeu e norte-americano. Além disso, considerou-se necessário apresentar conceitos, métodos e diretrizes, que fundamentassem o planejamento das ações de gestão de documentos, a fim de auxiliar os profissionais em programas e projetos específicos. Outras referências importantes que subsidiaram a primeira versão foram a norma DOD 5015.2-STD – *Design criteria standard for electronic records management software applications* (USA, Department of Defense, 2002), os *Requirements for electronic records management systems: functional requirements* (UK, Public Record Office, 2020), bem como os resultados e publicações do InterPARES Project[2] e a norma AS ISO 15.489/2002 (STANDARDS AUSTRALIA INTERNATIONAL, 2002).

O e-ARQ Brasil considerou a existência de um importante acervo de documentos digitais que vem sendo tratado por especialistas de diversas áreas, entre as quais arquivologia e tecnologia da informação. O documento partiu da definição dos conceitos de documento arquivístico e documento arquivístico digital, tendo como base os fundamentos da diplomática e da arquivologia, enfatizando os conceitos e a prática de gestão de documentos, para fornecer um conjunto de requisitos que seja amplo, rigoroso e de qualidade.

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 seu acesso, pelo tempo que for necessário.

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.

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 pode incluir 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. 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.

---

2 International Research on Permanent Authentic Records in Electronic Systems. Disponível em: http://www.interpares.org. Acesso em: 30 mar. 2018.

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 sistemas que compreendem documentos digitais, não digitais e híbridos. Com relação aos documentos não digitais, o sistema apenas apoia o registro dos metadados desses documentos. No caso dos documentos digitais, o sistema inclui os próprios documentos, ou a referência a documentos digitais externos ao SIGAD, além dos metadados.

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 todos os 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 visem produzir e manter documentos arquivísticos em formato digital.

O e-ARQ Brasil é especialmente dirigido a:

- profissionais da gestão arquivística de documentos: para orientar a execução desses serviços a partir de uma abordagem arquivística;
- profissionais de tecnologia da informação: para orientar o desenvolvimento de um SIGAD em conformidade com os requisitos exigidos;
- auditores: 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;
- instituições acadêmicas e organizações de formação profissional: como um documento de referência e recurso de ensino para a formação em gestão arquivística de documentos.

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.

de tratamento jurídico por parte do Conselho Nacional de Arquivos, vinculado ao Arquivo Nacional, órgão do Ministério da Justiça e Segurança Pública, 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, isto é, se de forma modular ou completa. Alguns capítulos ou seções de requisitos não são integralmente obrigatórios para apoiar a realização da gestão arquivística dos documentos, ficando sua adoção a critério da organização, de acordo com seu contexto. 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.

Por último, observa-se que a gestão arquivística de documentos imagéticos, audiovisuais e sonoros, dentre outros, demandam metadados específicos de gestão e descrição que não estão contemplados por esta norma. Apenas para ilustrar, citam-se os seguintes: a) fotografias: cromia e dimensão expressiva; b) registros sonoros: duração, entrevistador, depoente; c) filmes: cromia, direção e duração; d) mapas: escala métrica etc. Quando o SIGAD contemplar esses documentos, deverão ser implementados metadados específicos para garantir sua incorporação no programa de gestão documental da instituição.

4 Normas e outras orientações de referência

4.1. Normas

a. Sobre especificação de requisitos funcionais de segurança:

   - ISO/IEC 15408-1:2009 – Evaluation criteria for IT security.

b. Sobre gestão de documentos:

   - ABNT NBR ISO 15489-1:2018 – Gestão de documentos de arquivo. Parte 1: Conceitos e princípios.
   - ABNT NBR ISO 30300:2016 – Sistema de gestão de documentos de arquivo – Fundamentos e vocabulário.
   - ABNT NBR ISO 30301:2016 – Sistema de gestão de documentos de arquivo – Requisitos.
   - ABNT NBR ISO 30302:2017 – Sistema de gestão de documentos de arquivo – Diretrizes para implementação.

c. Sobre preservação:

- ISO 14721:2012 – Reference model for an open archival information system (OAIS).

d. Sobre metadados:

- ABNT NBR ISO 23081-1:2019 – Metadados para documentos de arquivo – Parte 1: Princípios.
- ABNT NBR ISO 23081-2:2020 – Gerenciamento de metadados para documentos de arquivo – Parte 2: Problemas conceituais e implementação.
- ISO 15836-1:2017 – Information and documentation – the Dublin Core metadata2 element.

4.2. Resoluções do Conselho Nacional de Arquivos

- Resolução do CONARQ n. 1, de 18 de outubro de 1995

  Dispõe sobre a necessidade da adoção de planos e/ou códigos de classificação de documentos nos arquivos correntes, que considerem a natureza dos assuntos resultantes de suas atividades e funções.

- Resolução do CONARQ n. 5, de 30 de setembro de 1996

  Dispõe sobre a publicação de editais para a eliminação de documentos nos Diários Oficiais da União, Distrito Federal, Estados e Municípios.

- 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.

- Resolução do CONARQ n. 24, de 3 de agosto de 2006

  Estabelece diretrizes para a transferência e recolhimento de documentos arquivísticos digitais para instituições arquivísticas públicas.

- Resolução do CONARQ n. 36, de 19 de dezembro de 2012

  Dispõe sobre a adoção das diretrizes para a gestão arquivística do correio eletrônico corporativo pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR).

- Resolução do CONARQ n. 37, de 19 de abril de 2012

  Aprova diretrizes para a presunção de autenticidade de documentos arquivísticos digitais.

- Resolução do CONARQ n. 39, de 29 de abril de 2014

  Estabelece diretrizes para a implementação de repositórios digitais confiáveis para a transferência e recolhimento de documentos arquivísticos digitais para instituições arquivísticas dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR). [Com a nova redação dada pela Resolução n. 43, de 4 de setembro de 2015]

- Resolução do CONARQ n. 40, de 9 de dezembro de 2014

  Dispõe sobre os procedimentos para a eliminação de documentos no âmbito dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR).

- Resolução do CONARQ n. 45, de 14 de fevereiro de 2020

  Trata de diretrizes para elaboração e uso dos instrumentos técnicos de gestão de documentos pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR).

4.3. Normas e 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 eletrônicos, 2002.
- MoReq 2010 – Modular Requirements for Records Systems, 2011.
- 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, versão 1.1, 2014.
- PREMIS Data Dictionary for Preservation Metadata – version 3, 2015.

4.5. Orientações para gestão e preservação de documentos digitais

- Directrices para la preservación del patrimonio digital, UNESCO, 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. The National Archives, UK.

5 Organização da especificação

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

A Parte I contém nove capítulos, alguns divididos em seções, 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 requisitos funcionais, requisitos não funcionais, metadados, glossário e referências.

Requisitos funcionais são aqueles que especificam uma função que o sistema deve ser capaz de realizar sob o ponto de vista do usuário final. No e-ARQ Brasil, os requisitos funcionais compreendem oito capítulos, divididos em seções, e tratam de organização de documentos (incluindo o plano de classificação), captura, avaliação (incluindo a destinação), recuperação da informação, elaboração de documentos, tramitação, segurança e preservação.

Requisitos não funcionais são aqueles que não estão diretamente relacionados à funcionalidade do sistema, mas que são relevantes para a sua implementação. Dessa forma, ressalta-se que, quando da implantação de um SIGAD, é necessário verificar e observar o cumprimento desses requisitos, considerando os contextos jurídico, administrativo e tecnológico de cada instituição de maneira a cumprir com os requisitos desta especificação. No e-ARQ Brasil, os requisitos não funcionais compreendem sete capítulos, e tratam de armazenamento, funções administrativas, conformidade com a legislação e regulamentações, usabilidade, interoperabilidade, disponibilidade, desempenho e escalabilidade.

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 documento, classe, componente digital, eventos de gestão do ciclo de vida, eventos de gestão do processo, eventos de gerenciamento da classe, eventos de preservação e agente.

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:

(O) obrigatórios quando indicados pela frase: "O SIGAD **tem que**..."

(AD) altamente desejáveis quando indicados pela frase: "É **altamente desejável** que o SIGAD ..."

(F) facultativos quando indicados pela frase: "O SIGAD **pode**..."

TEM = o requisito é imprescindível.

ALTAMENTE DESEJÁVEL = 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.

Alguns capítulos ou seções são integralmente opcionais, e a decisão pela adoção daquele conjunto de requisitos como um todo dependerá do contexto da organização, de necessidades identificadas e de controles e procedimentos adotados. Esses casos são apontados nos respectivos preâmbulos.

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 SIGAD 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 de 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 1980 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 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 1990, 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 não digital, 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 não digitais, 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[3] dos documentos e seu acesso contínuo. Estes e outros problemas requerem a adoção de medidas preventivas para minimizá-los.

Ao considerar 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 desses documentos tornou-se o principal foco de estudo da comunidade arquivística internacional. Nos últimos anos, projetos de-

3 Há que esclarecer que preservação de longo prazo abrange tanto os documentos de valor permanente como aqueles que, embora desprovidos de valor permanente, precisam ser mantidos no arquivo corrente e intermediário por longo tempo, conforme estabelecido em tabela de temporalidade e destinação, como, por exemplo, as pastas funcionais.

senvolvidos 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[4] 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. 8.159/1991, tem por finalidade definir a política nacional de arquivos públicos e privados, e exercer orientação normativa, visando à gestão documental e à proteção especial aos documentos de arquivo.[5] É um órgão colegiado, vinculado ao Arquivo Nacional, composto por plenário e câmaras técnicas. A sua presidência é do Arquivo Nacional, e do plenário participam representantes dos poderes Executivo, Legislativo e Judiciário federais, dos arquivos públicos estaduais e do Distrito Federal, dos arquivos municipais, das associações de arquivistas, e de instituições de ensino e pesquisa, organizações ou instituições com atuação na área de tecnologia da informação e comunicação, arquivologia, história ou ciência da informação.

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.[6]

Foi, portanto, no âmbito do CONARQ, que a Câmara Técnica de Documentos Eletrônicos (CTDE) redigiu e elaborou a primeira versão do *Modelo de requisitos para sistemas informatizados de gestão arquivística de documentos – e-ARQ Brasil*, aprovado em 2009. A segunda versão é resultante de um trabalho cuidadoso de revisão, realizado no período de 2017 a 2020, no qual foram feitas atualizações e reorganização do conteúdo, visando a maior precisão das especificações.

---

4 Entende-se por instituição arquivística aquela que tem como finalidade a custódia, o processamento técnico, a conservação e o acesso a documentos (ARQUIVO NACIONAL, 2005, p. 27).

5 Conforme art. 1º do decreto n. 4.073, de 3 de janeiro de 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2002/d4073.htm. Acesso em: 24 jan. 2020.

6 Conforme arts. 10 a 13 do decreto n. 4.073, de 3 de janeiro de 2002. http://www.planalto.gov.br/ccivil_03/decreto/2002/d4073.htm. Acesso em: 24 jan. 2020.

2 Base conceitual

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 anexo.

O que é documento?

É uma unidade de registro de informações, qualquer que seja o formato ou o suporte. (ARQUIVO NACIONAL, 2005)

O que é documento arquivístico?

É um documento produzido (elaborado ou recebido), no curso de uma atividade prática, como instrumento ou resultado de tal atividade, e retido para ação ou referência. (CONARQ/CTDE, 2020, p. 24)

O que é documento digital?

É a informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional. (CONARQ/CTDE, 2020, p. 25)

O que é documento arquivístico digital?

É um documento digital reconhecido e tratado como um documento arquivístico. (CONARQ/CTDE, 2020, p. 25)

Em outras palavras: é um documento codificado em dígitos binários, acessível e interpretável por meio de sistema computacional, que foi produzido (elaborado ou recebido), no curso de uma atividade prática, como instrumento ou resultado de tal atividade, e retido para ação ou referência.

E os documentos não digitais?

São todos os documentos que se apresentam em suporte, formato e codificação diferentes dos digitais, tais como: documentos em papel, documentos em películas e documentos eletrônicos analógicos.

Em seguida, é preciso esclarecer o conceito de SIGAD e diferenciá-lo de outros sistemas informatizados, que tratam de informações e de documentos, porém com foco diferente da gestão arquivística.

O que é SIGAD?

É um sistema informatizado que apoia a gestão arquivística de documentos.

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

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

SIGAD ou por ele geridos. Deve-se também considerar os documentos híbridos, compostos por partes digitais e não digitais, gerenciando cada uma dessas partes adequadamente.

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 conceituar o termo sistema e, então, apresentar as características de sistema de informação, sistema informatizado, gestão arquivística de documentos, sistema de gestão arquivística de documentos e sistema informatizado de gestão arquivística de documentos (SIGAD), assumidas no e-ARQ Brasil.

Sistema

Conjunto de elementos interdependentes distribuído por entradas (recursos), saídas (resultados), realimentação (controle) e meio ambiente. Este último, embora se constitua em um elemento externo ao sistema, exerce alguma influência sobre ele e é responsável pela demarcação de suas fronteiras.

Sistema de informação

Conjunto organizado, não necessariamente informatizado, de políticas, procedimentos, pessoas e equipamentos 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.

Sistema informatizado

Sistema que apoia o acesso e a gestão de dados, informação e/ou documentos em um ambiente computacional. A maioria dos sistemas não possui funcionalidades de gestão arquivística de documentos.

Gestão arquivística de documentos

Conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento dos documentos em idades corrente e intermediária, visando a 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.

Sistema informatizado de gestão arquivística de documentos (SIGAD)

É uma solução informatizada que visa o controle do ciclo de vida dos documentos, desde a produção até a destinação final, seguindo os princípios da gestão arquivística de documentos. Pode compreender um *software* particular ou um determinado número de *softwares* integrados, adquiridos ou desenvolvidos por encomenda.

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 ambientes que gerenciam documentos digitais, não digitais e híbridos.

Um SIGAD inclui operações como: captura de documentos, aplicação do plano de classificação, controle sobre os prazos de guarda e destinação, armazenamento seguro e procedimentos que garantam o acesso e a preservação em médio e longo prazos de documentos arquivísticos digitais e não digitais.

No caso dos documentos digitais, um SIGAD deve abranger todos os documentos arquivísticos digitais do órgão ou entidade, ou seja, textos, filmes, fotografias, registros sonoros, mensagens de correio eletrônico, páginas web, bases de dados, dentre outros.

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;[7]
- gestão dos documentos a partir do plano de classificação para manter a relação orgânica entre os documentos;
- registro de metadados associados aos documentos para descrever os contextos desses mesmos documentos (jurídico-administrativo, de proveniência, de procedimentos, documental e tecnológico);[8]
- estabelecimento de relacionamento entre documentos digitais, não digitais e híbridos;
- manutenção da autenticidade dos documentos;
- aplicação de tabela de temporalidade e destinação de documentos, permitindo a seleção dos documentos para eliminação ou para guarda permanente;
- exportação de documentos para apoiar a transferência e o recolhimento;
- apoio à preservação dos documentos.

É preciso esclarecer que um SIGAD se diferencia de sistemas de Gerenciamento Eletrônico de Documentos (GED) e de *Enterprise Content Management* (ECM), que também realizam gerenciamento de documentos, mas não necessariamente com abordagem arquivística. A seguir apresentam-se as características de GED e ECM.

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 mensagens 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.

7 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.

8 Ver Glossário.

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.

Enterprise Content Management (ECM)

Termo amplo para tecnologia digital, estratégias e métodos utilizados para capturar, gerir, acessar, integrar, medir e armazenar informação. Pode incluir módulos específicos para documentos que apoiam as atividades das organizações e ajudam no processo de tomada de decisão.

Com base nestas definições, podemos tecer as seguintes considerações:

- um sistema de informação pode abarcar 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 e protocolo, entre outros;
- um GED ou um ECM tratam os documentos de maneira compartimentada, enquanto o SIGAD parte de uma concepção orgânica, qual seja, a de que os documentos possuem uma interrelação que reflete as atividades da instituição que os criou. Além disso, diferentemente do SIGAD, o GED ou o ECM nem sempre incorporam o conceito arquivístico de ciclo de vida[9] 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.

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

Idealmente, a gestão arquivística dos documentos digitais deve ser realizada a partir da captura destes documentos em um SIGAD. No entanto, nem sempre é possível que o SIGAD capture todos os documentos da organização, que vêm sendo crescentemente produzidos e mantidos em sistemas de negócio.

> **O que é sistema de negócio?[10]**
>
> É um sistema informatizado cuja principal função é apoiar a realização de atividades específicas na organização e que produzem e mantêm dados, informações e documentos sobre essas atividades. Alguns exemplos são sistemas de recursos humanos, atividades financeiras, acadêmicos, prontuários e informação geográfica. Tradicionalmente, esses sistemas mantêm o registro das atividades na forma de tabelas de banco de dados, podendo, em certos casos, manter documentos em forma manifestada compreensível para os indivíduos, nos formatos mais diversos, como, por exemplo: pdf, txt, jpg, dwg, shp.

Quando da existência de sistemas de negócio que produzem documentos digitais potencialmente arquivísticos,[11] é fundamental que esses documentos sejam identificados, para que sejam sub-

9 O ciclo de vida dos documentos se refere "às sucessivas fases por que passam os documentos de um arquivo, da sua produção à guarda permanente ou eliminação" (ARQUIVO NACIONAL, 2005, p. 47).

10 Essa definição tomou como base o International Council on Archives. *Principles and functional requirements for records in electronic office environments*. Recordkeeping requirements for multiple functions supported by one business system (2013). Disponível em: https://www.ica.org/sites/default/files/11.%20Recordkeeping%20Requirements%20for%20Multiple%20Functions%20supported%20by%20one%20Business%20System.pdf. Acesso em: 24 jan. 2020.

11 Documentos arquivísticos são aqueles que registram as atividades dos órgãos ou entidades. No entanto, o simples registro de ações não é suficiente para que se tenha um documento arquivístico capaz de sustentá-las. É necessário que essa entidade cumpra com todas as características diplomáticas, quais sejam: ação, forma fixa, conteúdo estável, relação orgânica, pessoas e contexto identificável. Eventualmente, os documentos digitais produzidos e mantidos em

metidos aos procedimentos de gestão arquivística (registro, classificação e destinação) de maneira adequada. A gestão arquivística de documentos digitais produzidos em sistemas de negócio pode ser feita de três maneiras:

- implementação de funcionalidades para que os sistemas de negócio exportem os documentos arquivísticos e seus metadados para um SIGAD (nesse caso os documentos são mantidos e gerenciados no SIGAD);
- integração dos sistemas de negócio com um SIGAD (nesse caso os documentos são mantidos no sistema de negócio e a gestão arquivística é realizada pelo SIGAD por meio da interação entre os dois sistemas);
- implementação de funcionalidades de gestão arquivística de documentos no próprio sistema de negócio (nesse caso os documentos são mantidos e gerenciados no sistema de negócio até a destinação final, ou seja, eliminação ou guarda permanente).

Os requisitos para estas opções serão objeto de um documento complementar ao e-ARQ Brasil.

3 Aspectos essenciais da 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, são documentos arquivísticos, os quais, de acordo com a norma ISO 15.489, 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.

A Câmara Técnica de Documentos Eletrônicos (CTDE) define gestão arquivística de documentos[12] como o conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento de documentos arquivísticos em idades corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente.

sistemas de negócio não cumprem com todas as características diplomáticas, configurando-se como documentos potencialmente arquivísticos. Nesse caso, o sistema de negócio deverá ser alterado para que os documentos passem a ter todas essas características, tornando-se, de fato, arquivísticos.

12 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.

No bojo do conceito de gestão arquivística de documentos, estão o ciclo vital e a teoria das três idades.

Entende-se por ciclo vital as sucessivas fases por que passam os documentos de um arquivo, desde a produção até a guarda permanente ou eliminação, isto é, produção, utilização e destinação final, conforme detalhado abaixo:

- produção: consiste na elaboração, recebimento e retenção dos documentos em razão da execução das atividades de um órgão ou entidade.
- utilização: consiste na tramitação do documento para o cumprimento da função administrativa, bem como seu arquivamento após cessar o trâmite.
- destinação: consiste na aplicação da decisão, após processo de avaliação, de quais documentos serão eliminados e quais serão encaminhados para a guarda permanente.

Em relação à teoria das três idades, esta preconiza que os documentos arquivísticos passam por períodos distintos de acordo com a frequência e tipo de uso, a saber:

- corrente: documentos que estão em curso, isto é, tramitando ou que foram arquivados, mas são objeto de consultas frequentes, sendo conservados nos locais onde foram produzidos sob a responsabilidade do órgão produtor;
- intermediária: documentos que não são mais de uso corrente, mas que, por ainda conservarem algum interesse administrativo, aguardam, no arquivo intermediário, o cumprimento do prazo estabelecido em tabela de temporalidade e destinação, para serem eliminados ou recolhidos ao arquivo permanente;
- permanente: 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, fontes de prova em questões judiciais e administrativas, bem como em pesquisas acadêmicas. A propósito, lembramos que, segundo Rousseau e Couture (1994, p. 118), "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". 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.

A implementação de um programa de gestão arquivística de documentos pressupõe a existência de dois instrumentos fundamentais, quais sejam o código de classificação de documentos de arquivo e a tabela de temporalidade e destinação de documentos de arquivo.

O CONARQ estabeleceu critérios para elaboração desses instrumentos de gestão arquivística, regulamentando em suas resoluções a classificação, avaliação e os procedimentos de eliminação, transferência e recolhimento.

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.

De acordo com a norma AS ISO 15.489:2002, a gestão arquivística de documentos compreende:

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

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.

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

4 Definição da política arquivística[13]

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.

13 Este capítulo utilizou como texto base a norma AS ISO 15.489.2:2002 (STANDARDS AUSTRALIA INTERNATIONAL, 2002, p. 1).

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.

5 Designação de responsabilidades[14]

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.

6 Planejamento do programa de gestão arquivística de documentos[15]

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;

14 Este capítulo utilizou como texto base a norma AS ISO 15.489.2:2002 (STANDARDS AUSTRALIA INTERNATIONAL, 2002, p. 1-2).

15 Este capítulo utilizou como texto base a norma AS ISO 15.489.2:2002 (STANDARDS AUSTRALIA INTERNATIONAL, 2002, p. 2–7).

- definição, a partir do levantamento da produção documental, dos tipos de documentos que devem ser mantidos e produzidos, e das informações que 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 não digitais, 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.

7 Implantação do programa de gestão arquivística de documentos[16]

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 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.

16 Este capítulo utilizou como texto base a norma AS ISO 15.489.2:2002 (STANDARDS AUSTRALIA INTERNATIONAL, 2002, p. 2–7).

7.1. 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 o acesso aos 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 características do documento arquivístico: relação orgânica, unicidade, confiabilidade, autenticidade e acessibilidade.

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

a. Relação orgânica[17]

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

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.

---

17 Na primeira versão do e-ARQ Brasil, publicada em 2011, a *relação orgânica* foi expressa como *organicidade*. Entretanto, percebeu-se que a utilização do termo relação orgânica era mais adequada. Isto porque esta última se refere à relação que um documento tem com os demais documentos que participam da mesma ação. Já organicidade se refere a uma característica do conjunto documental, ou seja, o fundo. Assim, podemos dizer que os documentos de um fundo possuem relação orgânica, logo, ele é dotado de organicidade.

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[18]

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[19] 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 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.

Exigência: para assegurar a autenticidade dos documentos arquivísticos, o programa de gestão arquivística tem que garantir sua identidade[20] e integridade.[21] 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 o acesso, o programa de gestão arquivística deve garantir a transmissão de documentos para outros sistemas sem perda de informação e de funcionalidade. O SIGAD 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.

---

18 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.

19 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).

20 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.

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

7.2. Metodologia do planejamento e da implantação 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, e 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 uma 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.

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/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 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. Análise dos sistemas existentes

Consiste em identificar e analisar 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 informatizado 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*, levando em conta a maturidade de tecnologia e a disponibilidade de suporte técnico, considerando que o sistema deve ser modular, evolutivo e expansível;
- plano de segurança da informação (física e lógica) e de contingência, incluindo sistema de *backup*, controle de acesso e infraestrutura adequada e segura;
- 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 SIGAD;
- 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 do sistema de gestão arquivística de documentos

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, garantindo 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.

7.3. Suspensão ou extinção do SIGAD

Quando um SIGAD, ou um sistema de negócios que mantém documentos arquivísticos, 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 do acesso aos documentos inseridos no sistema suspenso ou extinto.

8 Procedimentos e operações técnicas do sistema de gestão arquivística de documentos digitais e não digitais[22]

8.1. Captura

A captura consiste em declarar um documento como um documento arquivístico, incorporando-o ao sistema de gestão arquivística por meio, no mínimo, das seguintes ações:

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

O objetivo principal da captura é declarar o documento como arquivístico ao demonstrar a relação orgânica dos documentos.

Quando da incorporação de um documento ao sistema de gestão arquivística, ele passa a seguir as rotinas de tramitação, quando for o caso, e arquivamento. Uma vez capturado, o documento pode ser incluído num fluxo de trabalho e, posteriormente, arquivado, ou ser imediatamente arquivado. No caso dos documentos em papel o documento é arquivado em uma pasta, no caso dos documentos digitais o SIGAD realiza o arquivamento reunindo os documentos logicamente, por exemplo, registrando em metadados o identificador do dossiê/processo e o código de classificação.

Tradicionalmente, nos sistemas de gestão arquivística de documentos em papel, a captura é feita quando o documento é registrado, classificado e/ou arquivado.

Um SIGAD deve capturar e registrar todos os documentos arquivísticos que foram produzidos em outros sistemas informatizados da organização. Eventualmente, o SIGAD poderá também incluir funcionalidades de produção de documentos, que serão capturados automaticamente no momento do registro, bem como fluxo de trabalho.

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;
- os critérios de acesso a esses documentos;
- por quanto tempo serão retidos.

22 Este capítulo utilizou como texto base a norma AS ISO 15.489.2:2002 (STANDARDS AUSTRALIA INTERNATIONAL, 2002, p. 13–20).

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.

8.1.1. 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 pelo órgão ou entidade 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.

No caso do SIGAD apoiar a produção de documentos internamente, poderá controlar a identificação/numeração de documentos, tais como, ofícios, memorandos, pareceres, relatórios, decretos, instruções normativas e outros.

O registro dos documentos no SIGAD, no momento da captura, pode equivaler ao registro de protocolo. As atividades de protocolo são constituídas pelo conjunto de operações que visam ao 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 SIGAD;
- data e hora do registro;
- título ou descrição abreviada: palavra, frase ou grupo de caracteres que nomeiam um 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 *login* 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;[23]
- 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;[24]
- 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;[25]
- destinação final;
- documentos anexos.

8.1.2. 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;

---

23 Ver 6.1.2 – Classificação na norma AS ISO 15.489.2:2002.

24 Ver 6.1.4 – Atribuição de restrição de acesso na norma AS ISO 15.489.2:2002.

25 Ver 6.2 – Avaliação, temporalidade e destinação na norma AS ISO 15.489.2:2002.

- 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.

8.1.3. 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:

- tipo documental: configuração que assume uma espécie documental, de acordo com a atividade que a gerou. São exemplos de tipos documentais: atestado de frequência de pessoal, atestado de saúde ocupacional, nota fiscal, 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.

8.1.4. 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 vigente estabelece procedimentos específicos para seu tratamento, incluindo a definição de graus de sigilo e demais restrições de acesso a serem atribuídas a cada documento.

Os documentos que dizem respeito à segurança da sociedade e do Estado, a sigilo comercial, bancário, industrial, telefônico, segredo de justiça, dentre outros, 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 de acesso deve ser feita no momento da captura no SIGAD, 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, o grau de sigilo ou outras restrições legais de acesso;
- atribuir o grau de sigilo, quando se tratar daqueles documentos produzidos pela instituição;
- identificar o grau de sigilo informado, quando se tratar daqueles recebidos pela instituição, e outras restrições legais de acesso ao documento;
- registrar o grau de sigilo e as restrições de acesso no sistema de gestão arquivística de documentos.

8.1.5. 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.

A operação de arquivamento dos documentos digitais se diferencia do arquivamento dos documentos não digitais 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, a operação de arquivar significa que o SIGAD irá automaticamente armazenar o(s) arquivo(s) em um dispositivo de armazenamento (operação física) e registrar, em metadados, elementos que estabeleçam a relação orgânica entre os documentos (operação lógica), como, por exemplo, identificador do documento, número do processo/dossiê e código de classificação.

8.2. 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[26] 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 documentos de valor eventual (de eliminação sumária) daqueles de valor probatório e/ou informativo.

26 Ver capítulo 2 da Parte I, "O que é gestão arquivística de documentos?".

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 o 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 ou classificados em quaisquer graus de sigilo 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 daquele 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.[27]

Não deverão ser encaminhados ao recolhimento documentos com classificação em grau de sigilo e/ou submetidos à criptografia, antes de sua desclassificação e/ou remoção da criptografia.

Os procedimentos de transferência e recolhimento de documentos digitais para instituição arquivística que impliquem a 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.

8.3. 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

27 Legislação que regula o recolhimento no âmbito do poder Executivo federal: lei n. 8.159, de 8 de janeiro de 1991, e resolução do CONARQ n. 2, de 1995. Disponível em: www.gov.br/conarq/pt-br. Acesso em: 24 jan. 2020.

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.

8.4. 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;
- registro de acesso em trilha de auditoria.

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,[28] existem regras, normas e legislação[29] que estabelecem diferentes razões, graus de sigilo e tipos de restrição de acesso a serem atribuídos a cada documento, além de definirem as autoridades competentes para fazê-lo (ver seção 8.1.4 – 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. O mesmo se dá em relação aos documentos referentes a sigilo comercial, bancário, industrial, telefônico, segredo de justiça etc., que possuem legislações específicas.

Adicionalmente, deverá ser aposta restrição de acesso a documentos preparatórios ou informação neles contidas, sempre que sua disponibilidade possa comprometer o andamento da transação.[30]

---

28 Sobre o sigilo ver lei n. 12.527, de 18 de novembro de 2011, e sua regulamentação. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 24 jan. 2020.

29 Decreto n. 7.845, de 14 de novembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Decreto/D7845.htm. Acesso em: 24 jan. 2020. Decreto n. 7.724, de 16 de maio de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Decreto/D7724.htm. Acesso em: 24 jan. 2020.

30 Conforme inciso XII do art. 3º, e art. 20 do decreto n. 7.724, de 16 de maio de 2012.

Um sistema de gestão arquivística deve impedir que usuários não autorizados tenham acesso aos documentos seja por classificação de sigilo, seja por outras restrições legais. 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 SIGAD 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 registra 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 quem executou cada ação 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.

A trilha de auditoria é também um documento arquivístico, que serve para apoiar a autenticidade dos documentos gerenciados pelo SIGAD. Como tal, tem que ser avaliada e ter um tempo de guarda e destinação previstos.

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 não digitais, 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 (*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 não digital. Essas medidas devem considerar os seguintes aspectos:

- as salas reservadas a computadores servidores, equipamentos de rede e ao armazenamento dos documentos digitais devem ter temperatura ambiente e umidade relativa do ar controladas, 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.

8.5. Armazenamento

Armazenar é guardar os documentos arquivísticos em local apropriado. No caso dos documentos digitais, esse armazenamento se dá em dispositivos de memória não voláteis.

As considerações e ações relativas ao armazenamento dos documentos arquivísticos não digitais 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 não digitais 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, acesso e utilização. Os procedimentos de conversão e migração devem detalhar as mudanças ocorridas nos sistemas e nos formatos dos documentos (ver seção 8.6 – 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 8.4 – Segurança: controle de acesso, trilhas de auditoria e cópias de segurança);
- características físicas do suporte e do ambiente: fatores como tipo de suporte, peso, grau de contaminação do documento e do ambiente, temperatura e umidade influenciam a adequação das condições de armazenamento. Nesse sentido, devem ser adotados procedimentos – como controle e verificação do tempo de vida útil e da estabilidade dos suportes – para prevenir danos aos documentos. É importante que os meios de acondicionamento sejam robustos e adequados ao formato e à quantidade de documentos. As áreas de depósito devem ter amplitude adequada, estabilidade de temperatura e de níveis de umidade, proteção contra sinistro, contaminação (isótopos radioativos, toxinas, mofo) e infestação de insetos ou micro-organismos. Os documentos digitais devem passar, periodicamente, pela troca de suporte, isto é, as informações contidas num suporte devem ser transferidas para outro. Essa técnica é denominada atualização (*refreshing*).
- frequência de uso: o uso mais ou menos frequente dos documentos deve ser levado em conta na seleção das opções de armazenamento. No caso dos documentos não digitais, as opções envolvem acondicionamento (pastas suspensas, caixas) e localização dos depósitos (próximos ou distantes da área de trabalho). Já em relação aos documentos digitais, as opções podem envolver armazenamento on-line (acesso imediato) ou off-line, nas chamadas "mídias removíveis" de armazenamento (disco óptico, fita magnética), em diferentes graus de disponibilidade e velocidade.

- custo relativo das opções de armazenamento dos documentos: além do custo dos dispositivos de armazenamento, devem ser considerados, para sua manipulação, os valores dos equipamentos e do *software* de controle. 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*[31] 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.

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.

8.6. 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 acesso, 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 não digitais, 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.

31 Valor calculado a partir dos dados que permite verificar se houve alteração.

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 de suporte (*refreshing*) e conversão.[32]

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.

O SIGAD pode interoperar com um Repositório Arquivístico Digital Confiável (RDC-Arq) para armazenar documentos de guarda longa e os destinados à guarda permanente.

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.

9 Instrumentos utilizados na gestão arquivística de documentos[33]

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:

32 Ver Glossário.

33 Este capítulo utilizou como texto base a norma AS ISO 15.489.2:2002 (STANDARDS AUSTRALIA INTERNATIONAL, 2002, p. 8–12).

- 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.

9.1. Plano ou 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.[34]

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 plano ou 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.

9.2. 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;

34 Cf. *Dicionário brasileiro de terminologia arquivística* (ARQUIVO NACIONAL, 2005, p. 132).

- destinação final (eliminação ou guarda permanente);
- observações necessárias a sua aplicação.

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 idade 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 idade 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.

9.3. Manual de gestão arquivística de documentos

O órgão ou entidade deve elaborar um manual com o objetivo de estabelecer procedimentos regulares no tocante a 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 digital do 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.

9.4. 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.

9.5. 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.

9.6. 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)

Dentre os requisitos apresentados a seguir, são considerados imprescindíveis para um SIGAD os que constam dos seguintes capítulos:

1. Organização dos documentos arquivísticos
2. Captura
3. Avaliação: temporalidade e destinação
7. Segurança
8. Preservação

No caso do SIGAD apoiar a produção de documentos dentro do sistema, também são considerados imprescindíveis os que constam dos seguintes capítulos:

5. Elaboração de documentos
6. Tramitação e fluxo de trabalho

REQUISITOS FUNCIONAIS

1 Organização dos documentos arquivísticos

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.[35]

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, de acordo com um plano de classificação. Daqui em diante deve-se entender classe como um termo genérico que inclui os demais níveis do plano de classificação, isto é, subclasse, grupo e subgrupo.

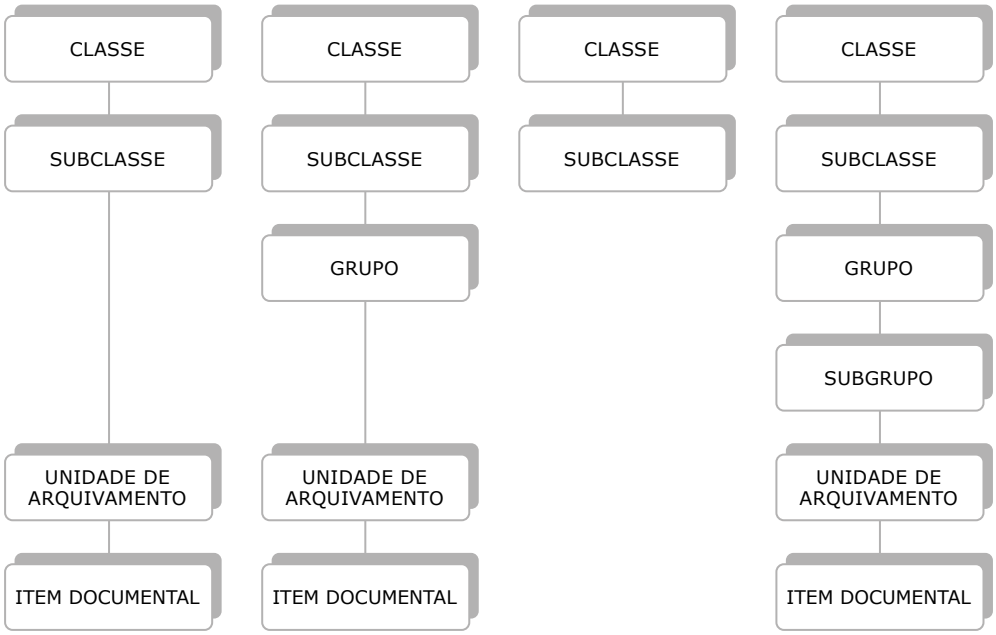
Como não há, necessariamente, o agrupamento físico dos documentos digitais, eles são reunidos em unidades lógicas de arquivamento por meio de metadados, como, por exemplo, número identificador, título e código.

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.

---

35 Unidade de arquivamento é o documento considerado para fins de classificação, arranjo, armazenamento e notação. Uma unidade de arquivamento pode ser um dossiê ou processo 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.

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 SIGAD para apoiar a configuração do plano de classificação no SIGAD, ou seja, como criar e manter um plano de classificação em um SIGAD.

Referência	Requisito	Obrig.[36]
1.1.1	Um SIGAD tem que incluir e ser compatível com o plano de classificação do órgão ou entidade, com as seguintes informações: • identificador da classe; • nome da classe; • código da classe; • subordinação da classe; • indicação de permissão de uso; • indicação de classe ativa/inativa. *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.	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

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

Referência	Requisito	Obrig.
1.1.5	Um SIGAD tem que registrar a mudança de nome, identificador e código 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, bem como o desmembramento ou fusão de classes. Nesse caso, é necessário fazer o registro do deslocamento nos metadados do plano de classificação.	O
1.1.7	Um SIGAD tem que permitir que apenas usuários autorizados tornem inativa uma classe em que não sejam mais classificados documentos.	O
1.1.8	Um SIGAD tem que permitir que um usuário autorizado apague uma classe inativa.	O
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 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 utilizarem ambos, separadamente ou em conjunto, na mesma aplicação: • atribuição de um código numérico ou alfanumérico; • atribuição de um termo que identifique cada classe.	O
1.1.12	É altamente desejável que um SIGAD preveja um atributo associado às classes para registrar a permissão de uso daquela classe para classificar um documento. *Em algumas classes, não é permitido incluir documentos. Nesse caso, os documentos devem ser classificados apenas nos níveis subordinados.* *Por exemplo, no Código de classificação e Tabela de temporalidade e destinação de documentos relativos às atividades-meio do Poder Executivo federal:* *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. *Entende-se por termo completo toda a hierarquia referente àquela classe. Por exemplo:* *MATERIAL: AQUISIÇÃO: MATERIAL PERMANENTE: COMPRA* *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
1.1.16	É altamente desejável que um SIGAD seja capaz de importar e exportar, total ou parcialmente, um plano de classificação. Ver capítulo 13 – Interoperabilidade	AD

Referência	Requisito	Obrig.
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: • gerar relatório completo do plano de classificação; • gerar relatório parcial do plano de classificação a partir de um ponto determinado na hierarquia; • gerar relatório dos documentos ou dossiês/processos classificados em uma ou mais classes do plano de classificação; • gerar relatório de documentos classificados por unidade administrativa.	O
1.1.18	É altamente desejável que um SIGAD possibilite a consulta ao plano de classificação a partir de qualquer atributo ou combinação de atributos, e emita relatório com os resultados obtidos.	AD

1.2. 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.
1.2.1	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
1.2.2	Um SIGAD tem que manter tabela de temporalidade e destinação de documentos com as seguintes informações: • identificador da classe; • prazo de guarda na idade corrente; • evento que determina o início de contagem do prazo de retenção na idade corrente; • prazo de guarda na idade intermediária; • evento que determina o início de contagem do prazo de retenção na idade intermediária; • destinação final; • sigilo associado à classe; • observações. *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.*	O
1.2.3	Um SIGAD tem que prever, pelo menos, as seguintes situações para destinação: • apresentação dos documentos para reavaliação em data futura; • eliminação; • exportação para transferência; • exportação para recolhimento (guarda permanente).	O

Referência	Requisito	Obrig.
1.2.4	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: • abertura de dossiê/processo; • arquivamento de dossiê/processo; • desarquivamento de dossiê/processo; • inclusão de documento sigiloso em um dossiê/processo, se aplicável. *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
1.2.5	Um SIGAD tem que prever que a definição dos prazos de guarda seja expressa por: • um número inteiro de meses ou • um número inteiro de anos.	O
1.2.6	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
1.2.7	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. *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.* *Os integrantes do SINAR deverão ainda ter suas tabelas aprovadas pela instituição arquivística na específica esfera de competência.*	O
1.2.8	É altamente desejável que um SIGAD seja capaz de manter o histórico das alterações realizadas na tabela de temporalidade e destinação de documentos.	AD
1.2.9	É altamente desejável que um SIGAD seja capaz de importar e exportar total ou parcialmente uma tabela de temporalidade e destinação de documento. Ver capítulo 13 – Interoperabilidade	AD
1.2.10	Um SIGAD tem que prover funcionalidades para elaboração de relatórios que apoiem a gestão da tabela de temporalidade e destinação, incluindo a capacidade de: • gerar relatório completo da tabela de temporalidade e destinação de documentos; • gerar relatório parcial da tabela de temporalidade e destinação de documentos a partir de um ponto determinado na hierarquia do plano de classificação; • gerar relatório dos documentos ou dossiês/processos aos quais foi atribuído um determinado prazo de guarda.	O

1.3. 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 à associação de metadados.

Referência	Requisito	Obrig.
1.3.1	Um SIGAD tem que permitir a classificação das unidades de arquivamento somente nas classes autorizadas. Ver requisito 1.1.12	O
1.3.2	Um SIGAD tem que permitir a classificação de um número ilimitado de unidades de arquivamento dentro de uma classe.	O
1.3.3	Um SIGAD tem que utilizar o termo completo da classe para identificar uma unidade de arquivamento, tal como especificado no requisito 1.1.13.	O
1.3.4	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. *A alteração de metadado só deve ser realizada para correção de erro.*	O
1.3.5	Um SIGAD tem que associar os metadados das unidades de arquivamento conforme estabelecido no padrão de metadados.	O
1.3.6	Um SIGAD tem que permitir que uma nova unidade de arquivamento herde, da classe em que foi classificada, alguns metadados predefinidos. *Exemplos desta herança são prazos de guarda previstos na tabela de temporalidade e destinação e restrição de acesso.*	O
1.3.7	Um SIGAD tem que 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.	O
1.3.8	Um SIGAD pode permitir a alteração conjunta de um determinado metadado em um grupo de unidades de arquivamento previamente selecionado.	F
1.3.9	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
1.3.10	Quando uma unidade de arquivamento ou documento é reclassificado, é altamente desejável que um SIGAD mantenha o registro de suas posições anteriores à reclassificação, de forma a manter um histórico.	AD
1.3.11	Quando uma unidade de arquivamento ou documento é reclassificado, é altamente desejável que um SIGAD permita que o administrador introduza as razões para a reclassificação.	AD
1.3.12	Um SIGAD pode permitir que os usuários criem referências cruzadas para unidades de arquivamento afins.	F
1.3.13	Um SIGAD tem que associar, automaticamente, ao dossiê/processo o prazo e a destinação previstos na classe em que o documento foi inserido.	O

2 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, atribuição de restrição de acesso e arquivamento.[37]

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

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

- captura individual de documento digital produzido 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 arquivística 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, de um GED ou de um sistema de negócios. Ex.: faturas diárias, dossiês, processos, folhas de pagamento, boletins de notas de alunos, pedidos de financiamento.

2.1. Procedimentos gerais

Referência	Requisito	Obrig.
2.1.1	A captura tem que garantir a execução das seguintes funções: • registrar e gerenciar todos os documentos não digitais; • registrar e gerenciar todos os documentos digitais ou híbridos, independentemente do contexto tecnológico; • classificar todos os documentos de acordo com o plano ou código de classificação; • controlar e validar a introdução de metadados.	O
2.1.2	Um SIGAD tem que ser capaz de capturar documentos digitais das formas a seguir: • captura de documentos produzidos dentro do SIGAD; • captura de documento digital produzido fora do SIGAD; • captura de documento produzido em *workflow* ou em outros sistemas integrados ao SIGAD; • captura de documentos em lote.	O
2.1.3	Um SIGAD tem que ser capaz de capturar e manter todos os componentes digitais do documento. *Os componentes digitais armazenam informações de conteúdo, da forma documental e as relações entre elas.*	O

37 A captura deve seguir os procedimentos de protocolo previstos na legislação específica no âmbito e esfera de atuação do órgão ou entidade.

Referência	Requisito	Obrig.
2.1.4	Um SIGAD tem que permitir o registro dos metadados em conformidade com o indicado na seção a eles dedicada nesse modelo de requisitos e garantir que se mantenham associados ao documento, componente digital ou classe.	O
2.1.5	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
2.1.6	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
2.1.7	O formato do número identificador atribuído pelo SIGAD deve ser definido no momento da configuração do SIGAD. *O identificador pode ser numérico ou alfanumérico, ou pode incluir os identificadores encadeados das entidades superiores no ramo apropriado da hierarquia.*	O
2.1.8	Num SIGAD, o número identificador atribuído pelo sistema tem que: • ser gerado automaticamente, sendo vedada sua introdução manual e alteração posterior; ou • ser atribuído pelo usuário e validado pelo SIGAD antes de ser aceito. *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
2.1.9	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
2.1.10	É altamente desejável que um SIGAD utilize tesauro ou vocabulário controlado para apoiar a atribuição do metadado assunto/descritor. *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
2.1.11	Um SIGAD tem que garantir que os metadados associados a um documento sejam inseridos somente por usuários autorizados.	O
2.1.12	Um SIGAD tem que garantir que os metadados associados a um documento sejam alterados somente por usuários autorizados e devidamente registrados em trilhas de auditoria.	O
2.1.13	É altamente desejável que um SIGAD seja capaz de inserir, automaticamente, os metadados previstos no SIGAD para o maior número possível de documentos, pois isso diminui as tarefas do usuário do SIGAD e garante maior rigor na inserção dos metadados. *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

Referência	Requisito	Obrig.
2.1.14	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. *Por exemplo, o SIGAD pode atribuir, automaticamente, o número identificador, a data de captura, o título, o originador, e requerer que o usuário preencha os demais metadados.*	O
2.1.15	Um SIGAD tem que garantir a inserção de outros metadados após a captura. *Por exemplo, data e hora de alteração e mudança de suporte.*	O
2.1.16	Sempre que um documento tiver mais de uma versão, o SIGAD tem que permitir que os usuários selecionem pelo menos uma das seguintes ações: • registrar todas as versões do documento como um só documento arquivístico; • registrar uma única versão do documento como um documento arquivístico; • registrar cada uma das versões do documento, separadamente, como um documento arquivístico. *Um SIGAD não deve considerar minutas como versão. Cada versão deve ser dotada de completeza.*	O
2.1.17	É altamente desejável que um SIGAD preste assistência aos usuários no que diz respeito à classificação dos documentos, por meio de algumas ou de todas as ações a seguir: • tornar acessível ao usuário somente o subconjunto do plano de classificação que diz respeito à sua atividade; • indicar as últimas classificações feitas pelo usuário; • indicar dossiês que contenham documentos de arquivo relacionados; • indicar classificações possíveis a partir dos metadados já inseridos, como, por exemplo, o título; • indicar classificações possíveis a partir do conteúdo do documento.	AD
2.1.18	É altamente desejável que um SIGAD permita que um usuário transmita documentos a outro usuário para completar o processo de captura, caso os procedimentos dessa captura sejam distribuídos entre vários usuários.	AD
2.1.19	No caso de documentos constituídos por mais de um componente digital, o SIGAD tem que: • tratar o documento como uma unidade indivisível, assegurando a relação entre os componentes digitais; • preservar a integridade do documento, mantendo a relação entre os componentes digitais; • garantir a integridade do documento quando de sua recuperação, visualização e gestão posteriores; • gerenciar a destinação de todos os componentes digitais que compõem o documento como uma unidade indivisível.	O

2.2. Captura em lote

Referência	Requisito	Obrig.
2.2.1	Um SIGAD tem que proporcionar a captura em lote de documentos gerados por outros sistemas. Esse procedimento tem que: • permitir a importação de transações predefinidas de arquivos em lote; • registrar, automaticamente, cada um dos documentos importados contidos no lote; • permitir e controlar a edição do registro dos documentos importados; • validar a integridade dos metadados. *Exemplos de 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 ou sistema de negócio.*	O

2.3. 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 dotar os usuários da capacidade de capturar 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.
2.3.1	Um SIGAD tem que capturar mensagens de correio eletrônico após selecionadas quais serão objeto de registro.	O
2.3.2	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: • visualizar cada mensagem de correio e uma indicação dos respectivos anexos, caso existam; • visualizar os conteúdos dos anexos utilizando um dispositivo para visualização de documentos em diferentes formatos; • registrar no SIGAD a mensagem de correio e respectivos anexos como um novo documento de arquivo; • relacionar a mensagem e respectivos anexos a um documento existente no SIGAD; • capturar automaticamente metadados de data e hora da transmissão da mensagem e todos os destinatários.	F
2.3.3	É altamente desejável que um SIGAD assegure a captura do nome, e não somente do endereço, do originador do correio eletrônico. Por exemplo, "Luís Santos", além de "lsa25@ab.br".	AD

2.4. Captura de documentos não digitais ou híbridos

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

A captura do documento não digital 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.
2.4.1	O SIGAD tem que ser capaz de capturar também os documentos não digitais e/ou híbridos.	O
2.4.2	O SIGAD tem que acrescentar aos metadados dos documentos não digitais informações sobre sua localização. *Essa informação só será acessada por usuários autorizados.*	O
2.4.3	O SIGAD tem que garantir que a parte digital de um documento ou processo/dossiê híbrido seja tratada de forma análoga aos documentos ou processos/dossiês inteiramente digitais.	O
2.4.4	O SIGAD tem que tratar um documento ou processo/dossiê híbrido como uma unidade indivisível, assegurando a relação entre a parte digital e a não digital.	O

2.5. Formato de arquivo e estrutura[38] 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, todos 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 SIGAD 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 uma macro sofisticada 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.

38 A estrutura dos documentos refere-se a um ou mais arquivos que compõem o documento, conforme exemplificado no requisito 2.5.2.

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.
2.5.1	Um SIGAD tem que possuir a capacidade de capturar documentos com diferentes formatos de arquivo e estruturas.	O
2.5.2	Um SIGAD tem que capturar documentos que se apresentam com as seguintes estruturas: • simples: texto, imagens, mensagens de correio eletrônico, *slides* digitais, som. • composta: mensagens de correio eletrônico com anexos, publicações eletrônicas.	O
2.5.3	É altamente desejável que um SIGAD possa capturar, entre outros, os documentos a seguir: • agendas eletrônicas; • informações de outros aplicativos – contabilidade, folha de pagamento, desenho assistido por computador (CAD); • documentos em papel digitalizados por meio de escâner; • documentos sonoros; • videoclipes; • diagramas e mapas digitais; • dados estruturados (EDI); • bases de dados; • documentos multimídia; • páginas web. *A lista de documentos que um SIGAD tem que suportar varia de órgão para órgão.* *Quando não for viável o SIGAD capturar o objeto digital, ele tem que ser capaz de realizar a captura por meio do registro do documento, para possibilitar seu gerenciamento.*	AD
2.5.4	Um SIGAD tem que ser capaz de incluir novos formatos de arquivos à medida que forem sendo adotados pelo órgão ou entidade.	O
2.5.5	Um SIGAD tem que ser capaz de registrar em metadados as informações relativas à dependência de *software*, quando capturar documentos em formatos diferentes dos previstos pelo programa de gestão de documentos do órgão ou entidade.	O

2.6. 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 domínio definido para cada funcionário; o *espaço do grupo*, ao domínio 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.
2.6.1	Em caso do SIGAD apoiar a produção de documentos, ele tem que ser capaz de reconhecer três domínios para o controle dos procedimentos de gestão: espaço individual, espaço do grupo e espaço geral.	O
2.6.2	Em caso do SIGAD apoiar a produção de documentos, ele tem que ser capaz de operacionalizar as regras estabelecidas pelo sistema de gestão arquivística de documentos nos três espaços.	O
2.6.3	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 7.12 – Alterar, apagar e truncar documentos arquivísticos digitais	O
2.6.4	É altamente desejável que um SIGAD possa emitir um aviso caso se tente capturar um documento incompleto ou inconsistente a ponto de comprometer sua futura autenticidade. *Por exemplo, uma correspondência sem assinatura digital válida ou uma fatura de fornecedor não identificado.*	AD
2.6.5	É altamente desejável que um SIGAD possa emitir um aviso caso se tente capturar um documento cuja autenticidade não possa ser verificada no futuro.	AD

3 Avaliação: temporalidade e destinação

Os requisitos deste capítulo referem-se a funcionalidades que servem para apoiar os 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 sua destinação 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.

Este capítulo estabelece requisitos para a aplicação da tabela de temporalidade e destinação de documentos no SIGAD e para a exportação e eliminação de documentos de um SIGAD.

3.1. 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, que devem ser realizados antes de se proceder às ações de destinação propriamente ditas.

Referência	Requisito	Obrig.
3.1.1	Um SIGAD tem que fornecer recursos integrados à tabela de temporalidade e destinação de documentos para implementar as ações de destinação.	O
3.1.2	Para cada dossiê/processo, um SIGAD tem que acompanhar automaticamente os prazos de guarda determinados para a classe à qual pertence.	O
3.1.3	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
3.1.4	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: • identificar automaticamente os documentos ou dossiês/processos que atingiram os prazos de guarda previstos; • informar o usuário autorizado sobre todos os documentos ou dossiês/processos que foram identificados no passo anterior; • possibilitar a alteração do prazo ou destinação previstos para aqueles documentos ou dossiês/processos, caso necessário; • proceder à ação de destinação quando confirmada pelo usuário autorizado.	O
3.1.5	Um SIGAD tem sempre que pedir confirmação antes de realizar as ações de destinação.	O
3.1.6	É altamente desejável que um SIGAD preveja, 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 restrição de acesso.*	AD
3.1.7	Um SIGAD tem que restringir as funções de destinação a usuários autorizados.	O
3.1.8	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

3.2. Exportação de documentos

É altamente desejável que um SIGAD tenha 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.
3.2.1	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
3.2.2	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
3.2.3	Um SIGAD tem que ser capaz de exportar um documento e dossiê/processo ou grupo de documentos e dossiês/processos numa sequência de operações, de modo que: • o conteúdo, o contexto e a estrutura dos documentos não se degradem; • todos os componentes de um documento digital sejam exportados como uma unidade. Por exemplo, uma mensagem de correio eletrônico e seus respectivos anexos; • todos os metadados do documento sejam relacionados a ele de forma que as ligações possam ser mantidas no novo sistema; • todas as ligações entre documentos, volumes e dossiês/processos sejam mantidas.	O
3.2.4	É altamente desejável que um SIGAD seja capaz de exportar dossiês/processos: • em seu formato nativo (ou no formato para o qual foi migrado); • de acordo com os formatos definidos em padrões de interoperabilidade; • de acordo com o formato definido pela instituição arquivística que irá receber a documentação, no caso de transferência ou recolhimento.	AD
3.2.5	É altamente desejável que um SIGAD seja capaz de exportar metadados nos formatos previstos em padrões de interoperabilidade de governo.	AD
3.2.6	Um SIGAD tem que ser capaz de exportar todos os tipos de documentos que está apto a capturar.	O
3.2.7	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
3.2.8	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
3.2.9	Um SIGAD tem que manter metadados relativos a documentos e dossiês/processos que foram exportados. *O administrador deve indicar o subconjunto de metadados que deverá ser mantido*.	O

Referência	Requisito	Obrig.
3.2.10	Um SIGAD tem que gerar listagem para descrever documentos e dossiês/processos digitais que estão sendo exportados. *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 na forma documental estabelecida pela instituição arquivística recebedora.*	O
3.2.11	É altamente desejável que um SIGAD possibilite a inclusão de metadados necessários à gestão do arquivo permanente nos documentos e dossiês/processos que serão exportados para recolhimento.	AD
3.2.12	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
3.2.13	Quando se exportarem documentos e dossiês/processos híbridos, é altamente desejável que um SIGAD exija do usuário autorizado a confirmação de que a parte na forma não digital dos mesmos documentos e dossiês/processos tenha passado pelo procedimento de destinação adequado antes de confirmar a exportação da parte na forma digital.	AD

3.3. 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.[39]

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.

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

Referência	Requisito	Obrig.
3.3.1	Um SIGAD tem que restringir a função de eliminação de documentos ou dossiês/processos somente a usuários autorizados.	O
3.3.2	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
3.3.3	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. *A eliminação será devidamente registrada em trilha de auditoria.*	O

39 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.

Referência	Requisito	Obrig.
3.3.4	Um SIGAD tem que avisar ao 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: confirmação pelo usuário autorizado para prosseguir ou cancelar o processo; produção de um relatório especificando os documentos ou dossiês/processos envolvidos e todas as ligações com outros documentos ou dossiês/processos.	O
3.3.5	É altamente desejável que um SIGAD permita 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
3.3.6	Quando um documento tem várias referências armazenadas no sistema, um SIGAD tem que garantir que todas essas referências sejam verificadas antes de eliminar o arquivo digital. *Esse requisito deve ser considerado quando um SIGAD relacionar um documento digital a mais de um dossiê ou processo, sem a duplicação física do arquivo digital.* *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.* *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 arquivo digital.*	O
3.3.7	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
3.3.8	Quando eliminar documentos ou dossiês/processos híbridos, é altamente desejável que um SIGAD exija do usuário autorizado a confirmação de que a parte na forma não digital desses documentos ou dossiês/processos seja eliminada também antes de confirmar a eliminação da parte digital.	AD
3.3.9	Um SIGAD tem que gerar relatório com os documentos e dossiês/processos que serão eliminados. *Essa listagem deve seguir o formato da* Listagem de eliminação *conforme o estabelecido na norma vigente.*	O
3.3.10	Um SIGAD tem que manter metadados relativos a documentos e dossiês/processos eliminados. *O administrador deve indicar o subconjunto de metadados que deverá ser mantido.*	O

3.4. Avaliação e destinação de documentos arquivísticos não digitais e híbridos

Os documentos arquivísticos não digitais 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.
3.4.1	Um SIGAD tem que aplicar a mesma tabela de temporalidade e destinação de documentos para os documentos não digitais, digitais ou híbridos.	O
3.4.2	Um SIGAD tem que acompanhar os prazos de guarda dos documentos não digitais e deve dar início aos procedimentos de eliminação ou transferência desses documentos, tomando em consideração suas especificidades.	O
3.4.3	Um SIGAD tem que alertar o administrador sobre a existência e a localização de uma parte não digital associada a um documento híbrido que esteja destinado a ser exportado, transferido ou eliminado.	O
3.4.4	É altamente desejável que um SIGAD exporte metadados de documentos e dossiês/processos não digitais.	AD

4 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 no capítulo 7 – Segurança.

4.1. Aspectos gerais

Referência	Requisito	Obrig.
4.1.1	Um SIGAD tem que fornecer facilidades para pesquisa, localização e apresentação dos documentos.	O
4.1.2	É altamente desejável que um SIGAD forneça outras formas de interface de pesquisa, localização e apresentação opcionais via ambiente web.	AD
4.1.3	É altamente desejável que um SIGAD preveja 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

4.2. 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.
4.2.1	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
4.2.2	Um SIGAD tem que executar pesquisa de forma integrada, isto é, apresentar todos os documentos e dossiês/processos, sejam eles digitais, híbridos ou não digitais, que satisfaçam aos parâmetros da pesquisa.	O
4.2.3	Um SIGAD tem que permitir que todos os metadados de gestão[40] de um documento ou dossiê/processo possam ser pesquisados.	O
4.2.4	É altamente desejável que um SIGAD permita que o conteúdo dos documentos em forma de texto possa ser pesquisado.	AD
4.2.5	Um SIGAD tem que permitir que um documento ou dossiê/processo possa ser recuperado por meio de um número identificador.	O
4.2.6	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: • identificador; • título; • assunto; • datas; • interessado; • autor/redator /originador; • classificação de acordo com plano ou código de classificação.	O
4.2.7	É altamente desejável que um SIGAD forneça uma interface que possibilite a pesquisa combinada de metadados e de conteúdo do documento por meio dos operadores *booleanos* "e", "ou" e "não".	AD
4.2.8	É altamente desejável que um SIGAD permita que os termos utilizados na pesquisa possam ser qualificados, especificando-se um metadado ou o conteúdo do documento como fonte de busca.	AD
4.2.9	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
4.2.10	É altamente desejável que um SIGAD permita a utilização de caracteres curinga e de truncamento à direita para pesquisa de metadados. *Por exemplo, o argumento de pesquisa "Bra*il" pode recuperar "Brasil" e "Brazil", e o argumento de pesquisa "Arq*" pode recuperar "Arquivo", "Arquivística".*	AD

40 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.
4.2.11	É altamente desejável que um SIGAD permita a utilização de caracteres curinga e de truncamento à direita para pesquisa no conteúdo do documento.	AD
4.2.12	É altamente desejável que um SIGAD proporcione pesquisa por proximidade, isto é, que uma palavra apareça no conteúdo do documento a uma distância máxima de outra.	AD
4.2.13	É altamente desejável que um SIGAD permita que os usuários armazenem pesquisas para reutilização posterior.	AD
4.2.14	É altamente desejável que um SIGAD permita que os usuários refinem pesquisas já realizadas.	AD
4.2.15	Quando o órgão ou entidade utilizar tesauros ou vocabulário controlado, é altamente desejável que um SIGAD seja capaz de realizar pesquisa dos documentos e dossiês/processos por meio da navegação nesses instrumentos.	AD
4.2.16	É altamente desejável que um SIGAD permita a pesquisa de termos já em desuso, fazendo relação com os termos atualizados, com o apoio de um tesauro ou vocabulário controlado, caso existam.	AD
4.2.17	É altamente desejável que um SIGAD permita que usuários autorizados configurem e alterem os campos *default* de pesquisa de forma a definir metadados como campos de pesquisa.	AD
4.2.18	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
4.2.19	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

4.3. 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 SIGAD deve ter a capacidade de operar/executar os programas (*software*) adicionais necessários e a configuração adequada, como, por exemplo, *plug-in* e configuração de navegador.

Referência	Requisito	Obrig.
4.3.1	Um SIGAD tem que apresentar o resultado da pesquisa como uma lista de documentos e dossiês/processos digitais, não digitais ou híbridos que cumpram os parâmetros da consulta e deve notificar o usuário se o resultado for nulo.	O
4.3.2	Quando o resultado de uma pesquisa for nulo, o SIGAD pode sugerir outros parâmetros aproximados que possam ser satisfeitos. *Por exemplo:* *Pesquisa inicial com o parâmetro "Arquivo Naiconal".* *O SIGAD apresenta a seguinte mensagem: Você não quis dizer "Arquivo Nacional"?*	F
4.3.3	Após apresentar o resultado da pesquisa, um SIGAD tem que oferecer ao usuário as opções: • visualizar os documentos e dossiês/processos resultantes da pesquisa; • redefinir os parâmetros de pesquisa e fazer nova consulta.	O
4.3.4	É altamente desejável que um SIGAD permita 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
4.3.5	É altamente desejável que um SIGAD permita a configuração do formato da lista de resultados de pesquisa pelo usuário ou administrador, incluindo recursos e funções como: • seleção da ordem em que os resultados de pesquisa são apresentados; • determinação do número de resultados de pesquisa exibidos em cada tela; • estabelecimento do número máximo de resultados para uma pesquisa; • armazenamento dos resultados de uma pesquisa; • definição dos metadados a serem exibidos nas listas de resultados de pesquisa.	AD
4.3.6	É altamente desejável que um SIGAD forneça recursos que permitam ao usuário "navegar" para o nível de agregação imediatamente superior ou inferior, como, por exemplo: • de um documento para a unidade de arquivamento em que está incluído; • de uma unidade de arquivamento para os documentos nela incluídos; • de uma unidade de arquivamento para a respectiva classe; • de uma classe para as unidades de arquivamento a ela relacionadas.	AD
4.3.7	Um SIGAD tem que ser capaz de apresentar o conteúdo de todos os documentos arquivísticos digitais definidos pelo programa de gestão de documentos, de forma que: • preserve as características de exibição visual e de formato apresentados pela aplicação geradora; • exiba todos os componentes do documento digital em conjunto, como uma unidade. *No caso de necessidade de captura de documentos em formatos de arquivo não previstos no programa de gestão de documentos, o SIGAD tem que permitir o* download *do documento para que possa ser visualizado em outro ambiente.*	O

Referência	Requisito	Obrig.
4.3.8	Em caso do SIGAD imprimir os documentos, tem que manter a forma documental apresentada pelas aplicações geradoras. *No caso de necessidade de captura de documentos em formatos de arquivo não previstos no programa de gestão de documentos, o SIGAD tem que permitir o* download *do documento para que possa ser visualizado em outro ambiente.*	O
4.3.9	É altamente desejável que o SIGAD seja capaz de exibir/reproduzir o conteúdo de documentos que incluam imagem fixa, imagem em movimento e som.	AD
4.3.10	Um SIGAD pode possibilitar a definição dos metadados a serem impressos.	F
4.3.11	Um SIGAD tem que ser capaz de exibir em tela todos os metadados associados aos documentos e dossiês/processos resultantes de uma pesquisa.	O
4.3.12	Um SIGAD tem que permitir a impressão de uma lista dos documentos e dossiês/processos resultantes de uma pesquisa.	O
4.3.13	Um SIGAD tem que permitir a impressão de uma lista dos documentos que compõem um dossiê/processo.	O
4.3.14	É altamente desejável que um SIGAD permita que os metadados exibidos nas listas a que se referem os requisitos 4.3.12 e 4.3.13 possam ser definidos pelo usuário.	AD
4.3.15	Um SIGAD tem que permitir que todos os documentos de um dossiê/processo sejam impressos em uma ou mais operações.	O
4.3.16	Um SIGAD tem que ter mecanismos destinados a exportar, para fins de reprodução, documentos que não possam ser impressos, tais como documentos sonoros, vídeos e multimídia.	O
4.3.17	É altamente desejável que um SIGAD seja capaz de apresentar os documentos arquivísticos em outros formatos além do nativo, tais como: • formato *.xml* adequado para publicação; • formato *.html* adequado para publicação; • formato aprovado por organismos padronizadores na sua esfera de competência. *No que se refere à interoperabilidade com outros sistemas, ver capítulo 13 – Interoperabilidade.*	AD
4.3.18	Um SIGAD tem que ser capaz de realizar pesquisa e exibição de documentos e dossiês/processos, simultaneamente, para diversos usuários.	O
4.3.19	É altamente desejável que um SIGAD permita ao administrador determinar que todas as cópias em papel de documentos e dossiês/processos sejam impressas junto com metadados pré-selecionados.	AD

5 Elaboração de documentos

Os requisitos deste capítulo referem-se a funcionalidades que apoiam a elaboração de documentos, ou seja, a redação e a configuração destes documentos, bem como a formação de dossiês/ processos.

É facultativo que um SIGAD apoie a elaboração de documentos. Assim, a adoção e a obrigatoriedade dos requisitos apontados neste capítulo devem ser atendidas quando, e somente quando, um SIGAD apoiar a elaboração de documentos.

5.1. Procedimentos gerais

Referência	Requisito	Obrig.
5.1.1	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
5.1.2	Um SIGAD pode vincular à automatização da produção de documentos: • numeração automática por espécie documental; • classificação arquivística; • marcação de sigilo legal; • autuação de processo; • outras.	F

5.2. Gerenciamento dos dossiês/processos

Esses requisitos 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.

Referência	Requisito	Obrig.
5.2.1	Um SIGAD tem que registrar nos metadados as datas de abertura e de encerramento do dossiê/processo. *Essa data pode servir de parâmetro para aplicação dos prazos de guarda e destinação do dossiê/processo.*	O
5.2.2	Um SIGAD tem que emitir um aviso caso o usuário anexe um documento que já tenha sido anexado no mesmo dossiê/processo.	O
5.2.3	Um SIGAD tem que permitir que um dossiê/processo seja encerrado por meio de procedimentos regulamentares e somente por usuários autorizados.	O
5.2.4	Um SIGAD tem que permitir a consulta aos dossiês/processos já encerrados por usuários autorizados.	O
5.2.5	Um SIGAD tem que impedir o acréscimo de novos documentos a dossiês/processos já encerrados. *Dossiês/processos encerrados devem ser reabertos para receber novos documentos*.	O
5.2.6	Um SIGAD tem que garantir sempre a integridade da relação hierárquica entre classe, dossiê/processo, volume e documento, independentemente de atividades de manutenção, ações do usuário ou falha de componentes do SIGAD. *Em hipótese alguma pode o SIGAD permitir que uma ação do usuário ou falha do SIGAD* dê origem a inconsistência em sua base de dados.	O

5.3. 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.
5.3.1	Um SIGAD tem que prever a formação/autuação de processos,[41] por usuário autorizado conforme estabelecido em legislação específica.	O
5.3.2	É altamente desejável que um SIGAD preveja funcionalidades para apoiar a identificação de processos relativos à mesma ação ou interessado, e emita um aviso. *Essa funcionalidade pode ser utilizada sob demanda do usuário, para identificar a existência de processos específicos, ou para apoiar controles/restrições do sistema na execução de atividade específica, como, por exemplo, juntada de processos por anexação.*	AD
5.3.3	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
5.3.4	Um SIGAD tem que impedir a renumeração dos documentos integrantes de um processo digital. *Este requisito tem por objetivo impedir a exclusão não autorizada de documentos de um processo. Casos especiais que autorizem a renumeração, como no caso dos documentos do processo acessório na juntada por anexação, devem obedecer à legislação específica na devida esfera e âmbito de competência.*	O
5.3.5	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*[42] ou *apensação*.[43] Este procedimento deve ser registrado nos metadados do processo.	O
5.3.6	Um SIGAD tem que prever procedimentos para desapensação de processos segundo a legislação específica na devida esfera e âmbito de competência. Esse procedimento deve ser registrado nos metadados do processo.	O
5.3.7	Um SIGAD tem que prever procedimentos para desentranhamento de documentos integrantes de um processo, segundo norma específica na devida esfera e âmbito de competência. Esse procedimento deve ser registrado nos metadados do processo.	O

41 Ver Glossário.

42 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.

43 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.
5.3.8	Um SIGAD tem que prever procedimentos para desmembramento de documentos integrantes de um processo, segundo norma específica na devida esfera e âmbito de competência. Esse procedimento deve ser registrado nos metadados do processo.	O
5.3.9	Um SIGAD tem que prever o encerramento[44] dos processos incluídos seus volumes e metadados.	O
5.3.10	Um SIGAD tem que prever o desarquivamento para reativação dos processos, por usuário autorizado e obedecendo a procedimentos legais e administrativos. *Para manter a integridade do processo, somente o último volume receberá novos documentos ou peças.*	O

5.4. Volumes: abertura, encerramento e metadados

Em alguns casos os dossiês/processos 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.
5.4.1	É altamente desejável que um SIGAD seja capaz de gerenciar volumes para subdividir dossiês/processos, fazendo a distinção entre dossiês/processos e volumes.	AD
5.4.2	É altamente desejável que um SIGAD permita a associação de metadados aos volumes e restrinja a inclusão e alteração desses metadados apenas a usuários autorizados.	AD
5.4.3	Um SIGAD tem que permitir que um volume herde, automaticamente, do dossiê/processo ao qual pertence, alguns metadados predefinidos, como, por exemplo, classes e temporalidade.	O
5.4.4	Um SIGAD tem que permitir a abertura de volumes para qualquer dossiê/processo que não esteja encerrado.	O
5.4.5	É altamente desejável que um SIGAD permita o registro de metadados correspondentes às datas de abertura e encerramento de volumes.	AD
5.4.6	Um SIGAD tem que assegurar que um volume conterá somente documentos. Não é permitido que um volume contenha outro volume ou outro dossiê/processo. *Em caso de juntada por anexação de processo a processo, o sistema deverá encerrar o último volume do processo principal e, na sequência, incluir cada um dos volumes do processo anexado.*	O
5.4.7	Um SIGAD tem que permitir que um volume seja encerrado por meio de procedimentos regulamentares e apenas por usuários autorizados.	O

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

Referência	Requisito	Obrig.
5.4.8	Um SIGAD tem que assegurar que, ao ser aberto um novo volume, o precedente seja automaticamente encerrado. *Apenas o volume produzido mais recentemente pode estar aberto; os demais volumes existentes no dossiê/processo têm que estar encerrados.*	O
5.4.9	Um SIGAD tem que impedir a reabertura, para acréscimo de documentos, de um volume já encerrado.	O

5.5. Gerenciamento de documentos e processos/dossiês arquivísticos não digitais e híbridos

O arquivo de uma organização pode conter documentos ou dossiês/processos digitais e não digitais. É altamente desejável que um SIGAD registre os documentos ou dossiês/processos não digitais, 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 não digital.

Referência	Requisito	Obrig.
5.5.1	Um SIGAD tem que capturar documentos ou dossiês/processos não digitais e gerenciá-los da mesma forma que os digitais. *Para o conceito de captura, ver capítulo 2.*	O
5.5.2	Um SIGAD tem que ser capaz de gerenciar a parte não digital 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
5.5.3	Um SIGAD tem que permitir que um conjunto específico de metadados seja configurado para os documentos ou dossiês/processos não digitais e incluir informações sobre o local de arquivamento.	O
5.5.4	Um SIGAD tem que dispor de mecanismos para acompanhar a movimentação do documento arquivístico não digital, de forma que fique evidente para o usuário a localização atual do documento.	O
5.5.5	Um SIGAD tem que ser capaz de oferecer ao usuário funcionalidades para solicitar ou reservar a consulta a um documento arquivístico não digital, enviando uma mensagem para o detentor atual do documento ou para o administrador.	O
5.5.6	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 não digitais.	F
5.5.7	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 não digital.	O
5.5.8	Sempre que os documentos ou dossiês/processos híbridos estiverem classificados quanto ao grau de sigilo, um SIGAD tem que garantir que a parte não digital e a parte digital correspondente recebam a mesma classificação de sigilo.	O
5.5.9	Um SIGAD tem que poder registrar na trilha de auditoria todas as alterações efetuadas nos metadados dos documentos ou dossiês/processos não digitais e híbridos.	O

6 Tramitação e fluxo de trabalho

Os requisitos deste capítulo tratam apenas dos casos em que o SIGAD inclui recursos de automação de fluxo de trabalho (*workflow*). Assim, esse conjunto de requisitos como um todo é facultativo e a adoção e a obrigatoriedade apontadas neste capítulo devem ser seguidas quando, e somente quando, um SIGAD apoiar a automação de fluxo de trabalho.

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

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

- tramitação do documento antes do seu registro/captura ou
- tramitação após seu registro/captura.

Há que ressaltar que fluxo de trabalho não é a mesma coisa que tramitação de documentos controlada pelo sistema de protocolo, o qual realiza registro e autuação para formação de processos. O fluxo de trabalho tem uma amplitude maior, podendo incluir a produção e o trâmite de documentos, mas não os procedimentos de controle de protocolo.

As tecnologias de fluxo de trabalho transferem documentos 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";
- 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 SIGAD). A tarefa tem que ser distribuída entre os usuários do grupo, e, após ser cumprida por um membro desse grupo, o documento segue o fluxo previsto. Quando o participante é um *software,* a tarefa é direcionada a uma função de programa, que a realiza automaticamente e reencaminha o documento ao fluxo previsto.

6.1. Controle do fluxo de trabalho

Referência	Requisito	Obrig.
6.1.1	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
6.1.2	Um SIGAD tem que ter capacidade, sem limitações, de estabelecer o número necessário de trâmites nos fluxos de trabalho.	O
6.1.3	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
6.1.4	É altamente desejável que o fluxo de trabalho de um SIGAD permita o uso do correio eletrônico, para que um usuário possa informar a outros usuários sobre documentos que requeiram sua atenção. *Esse requisito requer a integração com um sistema de correio eletrônico existente.*	AD
6.1.5	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
6.1.6	É altamente desejável que o administrador possa autorizar usuários individuais a redistribuir tarefas ou ações de um fluxo de trabalho a um usuário ou grupo diferente do previsto. *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
6.1.7	Um recurso de fluxo de trabalho de um SIGAD tem que registrar na trilha de auditoria todas as alterações ocorridas neste fluxo.	O
6.1.8	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 documento no fluxo.	O
6.1.9	É altamente desejável que um recurso de fluxo de trabalho de um SIGAD gerencie os documentos em filas de espera que possam ser examinadas e controladas por usuário autorizado.	AD
6.1.10	É altamente desejável que um recurso de fluxo de trabalho de um SIGAD tenha 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
6.1.11	É altamente desejável que um recurso de fluxo de trabalho de um SIGAD forneça fluxos condicionais de acordo com os dados de entrada do usuário ou a partir dos dados do SIGAD. *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
6.1.12	Um recurso de fluxo de trabalho de um SIGAD tem que fornecer um histórico de movimentação dos documentos. *O histórico de movimentação corresponde a um conjunto de metadados de datas de entrada e saída, nomes de responsáveis, título do documento, providências etc.*	O

Referência	Requisito	Obrig.
6.1.13	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. *O fluxo só prosseguirá com a autorização do usuário.*	F
6.1.14	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 for recebido.	O
6.1.15	É altamente desejável que um recurso de fluxo de trabalho de um SIGAD possa 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
6.1.16	Um recurso de fluxo de trabalho de um SIGAD tem que reconhecer indivíduos e grupos de trabalho como participantes.	O
6.1.17	Sempre que o participante for um grupo de trabalho, é altamente desejável que um recurso de fluxo de trabalho de um SIGAD preveja a forma de distribuição dos documentos entre os membros do grupo. Essa distribuição pode ser de duas formas: • de acordo com uma sequência circular predefinida, o SIGAD envia o próximo documento independentemente da conclusão da tarefa anterior; ou • à medida que cada membro conclui a tarefa, o SIGAD lhe envia o próximo documento da fila do grupo.	AD
6.1.18	É altamente desejável que um recurso de fluxo de trabalho de um SIGAD permita que a captura de documentos desencadeie, automaticamente, fluxos de trabalho.	AD
6.1.19	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
6.1.20	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
6.1.21	É altamente desejável que um SIGAD mantenha versões dos fluxos alterados e estabeleça vínculos entre os documentos já processados ou em processamento nos fluxos alterados.	AD
6.1.22	O SIGAD tem que assegurar que qualquer modificação nos atributos dos fluxos leve em conta os documentos a ele vinculados.	O

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

Referência	Requisito	Obrig.
6.2.1	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
6.2.2	Um SIGAD tem que manter o identificador único do documento, e controlar as diversas versões deste documento.	O

7 Segurança

Este capítulo 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, autenticação de documentos por assinatura digital ou outro meio, carimbo digital de tempo, 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.

7.1. 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.

Os requisitos de cópias de segurança não são necessariamente funcionalidades do SIGAD. Na maior parte das vezes os procedimentos são realizados independentemente do sistema informatizado, pela área de infraestrutura de TI. Destaca-se, ainda, que os requisitos 7.1.2, 7.1.3, 7.1.4 e 7.1.9 são considerados *não* funcionais.

Referência	Requisito	Obrig.
7.1.1	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
7.1.2	O administrador do SIGAD tem que manter o controle das cópias de segurança, prevendo testes de restauração.	O
7.1.3	É altamente desejável que as mídias removíveis tenham cópias em suportes equivalentes e armazenamento *off-site*.	AD
7.1.4	É altamente desejável que os discos rígidos tenham *backups* armazenados em pelo menos dois locais diferentes e fisicamente distantes.	AD
7.1.5	É altamente desejável que um SIGAD seja capaz de agendar, automaticamente, os *backups* com periodicidade estipulada pelo administrador. Deve permitir cópias incrementais ou completas.	AD
7.1.6	É altamente desejável que um SIGAD disponha de mecanismos que garantam a integridade das cópias de segurança, bem como a identificação do responsável pelo procedimento.	AD
7.1.7	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
7.1.8	É altamente desejável que dados críticos de configuração e controle do sistema operacional e do gerenciador de bancos de dados sejam especialmente protegidos. Mecanismos especiais de *backup* devem ser previstos para dados críticos.	AD
7.1.9	É altamente desejável que as trilhas de auditoria sejam copiadas com frequência, prevendo-se cópias a serem armazenadas em pelo menos um local *off-site*.	AD

7.2. 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.

Observe-se que o controle de acesso pode ser uma funcionalidade do SIGAD ou pode ser utilizada uma aplicação externa de controle de acesso que interopera com o SIGAD. Assim, esse conjunto de requisitos como um todo é facultativo e a adoção e a obrigatoriedade apontadas nesta seção devem ser seguidas quando, e somente quando, o controle de acesso for realizado pelo SIGAD.

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.
7.2.1	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: • identificador do usuário; • autorizações de acesso; • credenciais de autenticação. *Senha, crachá, chave criptográfica,* token *USB,* smartcard*, biometria (de impressão digital, de retina etc.) são exemplos de credenciais de autenticação.*	O
7.2.2	Um SIGAD tem que exigir que o usuário esteja devidamente identificado e autenticado antes de iniciar qualquer operação no SIGAD.	O
7.2.3	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
7.2.4	É altamente desejável que as credenciais de autenticação sejam 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.
7.2.5	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
7.2.6	Se o usuário solicitar o acesso ou pesquisa de um documento arquivístico, volume ou dossiê/processo específico a que não tenha direito de acesso, é altamente desejável que um SIGAD forneça uma das seguintes respostas (estabelecidas durante a configuração): • mostrar o título e os metadados do documento; • demonstrar a existência do dossiê/processo ou documento, mas não o respectivo título nem outro metadado; • não mostrar qualquer informação do documento, nem indicar a sua existência. *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.* *O SIGAD deve ser capaz de registrar e informar tentativas indevidas de acesso.* *Este requisito se aplica tanto a pesquisas em metadados quanto a pesquisas no próprio documento (texto livre).*	AD
7.2.7	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
7.2.8	É altamente desejável que um SIGAD aplique, imediatamente, alterações ou revogações dos atributos de segurança de usuários e de documentos digitais.	AD
7.2.9	É altamente desejável que um SIGAD ofereça 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
7.2.10	Quando um SIGAD controlar o acesso por grupos de usuários, papéis de usuários e usuários individuais, é altamente desejável que obedeça 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.
7.2.11	Um SIGAD tem que aplicar a política de controle de acesso a documentos por grupos de usuários considerando: • a identidade do usuário e sua participação em grupos; • os atributos de segurança, associados ao documento arquivístico digital, às classes e/ou aos dossiês/processos.	O
7.2.12	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
7.2.13	Um SIGAD tem que permitir que um usuário pertença a mais de um grupo.	O
7.2.14	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.
7.2.15	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: • identificação do usuário; • papéis associados ao usuário.	O
7.2.16	Um SIGAD tem que usar os seguintes atributos dos documentos digitais ao implementar a política de controle de acesso por papéis: • identificação do documento digital; • operações permitidas aos vários papéis de usuários, sobre as classes ou unidades de arquivamento a que o documento pertence.	O
7.2.17	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
7.2.18	Um SIGAD tem que impedir que um usuário assuma papéis com direitos conflitantes.	O
7.2.19	Um SIGAD pode permitir a criação de hierarquias de papéis e o conceito de herança de permissões entre eles.	F

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

Os documentos produzidos pelos órgãos da administração pública estão sujeitos aos graus de sigilo e demais caracterizações de restrição de acesso definidos na legislação vigente.

Os requisitos descritos nesta seção referem-se aos documentos arquivísticos com classificação de grau de sigilo ou outras restrições legais de acesso. Informação com restrição legal de acesso pode estar relacionada a dados pessoais sensíveis,[45] a documentos preparatórios cuja disponibilidade possa comprometer o andamento de uma atividade, ou, ainda, a sigilos comercial, bancário, industrial, telefônico, segredo de justiça etc., que possuem legislações específicas. Os requisitos são flexíveis para atender tanto às organizações privadas como aos órgãos públicos.

Referência	Requisito	Obrig.
7.3.1	Um SIGAD tem que implementar a classificação de grau de sigilo e demais caracterizações de restrição de acesso de documentos, dossiês/processos e classes do plano de classificação, e de todas as operações de usuários nos documentos.	O
7.3.2	Um SIGAD tem que implementar a identificação de restrições legais de acesso baseando-se nos seguintes atributos de segurança: • tipo de restrição legal de acesso; • credencial de segurança do usuário. *Os tipos de restrição legal podem ser documentos preparatórios, dados pessoais, sigilo comercial, bancário, industrial, telefônico, segredo de justiça etc.*	O
7.3.3	Um SIGAD tem que tratar a classificação de grau de sigilo baseando-se nos seguintes atributos de segurança: • grau de sigilo do documento; • credencial de segurança do usuário; • identificação da autoridade classificadora. *O grau de sigilo tem que estar associado à credencial de segurança.* *Incluem-se também os documentos recebidos com classificação de grau de sigilo.*	O
7.3.4	É altamente desejável que um SIGAD formalize a decisão de classificação da informação em qualquer grau de sigilo, conforme legislação vigente. *A título de exemplo, o Poder Executivo federal utiliza o Termo de Classificação de Informação – TCI, conforme estabelecido no decreto n. 7.724, de 16 de maio de 2012, que registra as seguintes informações:* • *código de indexação de documento;* • *grau de sigilo;* • *categoria na qual se enquadra a informação;* • *tipo de documento;* • *data da produção do documento;* • *indicação de dispositivo legal que fundamenta a classificação;* • *razões da classificação;* • *indicação do prazo de sigilo, contado em anos, meses ou dias, ou do evento que defina o seu termo final;* • *data da classificação;* • *identificação da autoridade que classificou a informação.*	AD

45 Lei n. 13.709, de 14 de agosto de 2018. Inciso II do art. 5º que define "dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural". Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 24 jan. 2020.

Referência	Requisito	Obrig.
7.3.5	Um SIGAD tem que recusar o acesso de usuários a documentos que possuam grau de sigilo superior à sua credencial de segurança.	O
7.3.6	Um SIGAD tem que garantir que documentos sem atribuição de grau de sigilo ou identificação de outras restrições de acesso, provenientes de fontes externas ao SIGAD, estejam sujeitos às políticas de controle de acesso e de sigilo.	O
7.3.7	Um SIGAD tem que ser capaz de manter a marcação de restrição de acesso original durante a importação de documentos a partir de fontes externas ao SIGAD.	O
7.3.8	É altamente desejável que um SIGAD garanta que não haja ambiguidade na associação entre as marcações de grau de sigilo e outros atributos de segurança (permissões) do documento importado.	AD
7.3.9	Um SIGAD tem que permitir que um dos itens abaixo seja selecionado durante a configuração: • graus de sigilo e restrições de acesso a serem atribuídos a classes e dossiês/processos; • classes e dossiês/processos sem grau de sigilo ou outras restrições de acesso.	O
7.3.10	Em caso de erro ou reavaliação, o administrador autorizado tem que ser capaz de alterar o grau de sigilo ou outra restrição de acesso de todos os documentos arquivísticos de um dossiê/processo ou de uma classe, numa única operação. *A informação quanto à desclassificação, reclassificação, redução do prazo de sigilo ou alteração de restrição de acesso deverá ser registrada conforme legislação em vigor.*	O
7.3.11	Um SIGAD tem que garantir que o grau de sigilo ou outra restrição de acesso de um documento importado esteja associado a um usuário autorizado com a credencial de segurança pertinente para receber o documento.	O
7.3.12	Um SIGAD tem que permitir que somente administradores autorizados sejam capazes de realizar as seguintes ações: • remover ou revogar os atributos de segurança dos documentos; • criar, alterar, remover ou revogar as credenciais de segurança dos usuários.	O
7.3.13	Um SIGAD tem que permitir somente ao usuário autorizado, mediante confirmação, a desclassificação, redução do grau de sigilo ou alteração de restrição de acesso de um documento. *A informação quanto à desclassificação, reclassificação, redução do prazo de sigilo ou alteração de restrição de acesso deverá ser registrada conforme legislação em vigor.*	O
7.3.14	É altamente desejável que um SIGAD permita o armazenamento dos documentos sigilosos em meios físicos ou lógicos distintos dos documentos não sigilosos.	AD
7.3.15	Um SIGAD tem que impedir que um documento com classificação de sigilo seja eliminado. *Os documentos com classificação de sigilo têm que se tornar ostensivos antes de receberem a destinação prevista*.	O
7.3.16	Um SIGAD tem que implementar metadados nos níveis de dossiê, documento ou cópia truncada de documento para controlar o acesso à informação com restrição de acesso.	O

7.4. 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.
7.4.1	Um SIGAD tem que ser capaz de registrar, na trilha de auditoria, informações acerca das ações a seguir: • data e hora da captura de todos os documentos; • responsável pela captura; • reclassificação, desclassificação ou redução do grau de sigilo de um documento ou dossiê/processo, com a classificação inicial e final; • qualquer alteração na tabela de temporalidade e destinação de documentos; • qualquer ação de reavaliação de documentos; • qualquer alteração nos metadados associados a classes, dossiês/processos ou documentos; • data e hora de produção, aditamento e eliminação de metadados; • ações de exportação e importação envolvendo os documentos; • usuário, data e hora de acesso ou tentativa de acesso a documentos e ao SIGAD; • tentativas de acesso negado a qualquer documento; • ações de eliminação de qualquer documento e seus metadados; • tentativas de exportação (inclusive para *backup*) e importação (inclusive *restore*); • alterações efetuadas nas permissões de acesso que afetem um dossiê/processo, documento ou usuário; • infrações cometidas contra mecanismos de controle de acesso; • todas as ações administrativas sobre os atributos de segurança (papéis, grupos, permissões etc.); • todas as ações administrativas sobre dados de usuários (cadastro, ativação, bloqueio, atualização de dados e permissões, troca de senha etc.); • todos os eventos de administração e manutenção das trilhas de auditoria (alarmes, cópias, configuração de parâmetros etc.).	O
7.4.2	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
7.4.3	Um SIGAD tem que permitir a leitura das trilhas de auditoria apenas a usuários autorizados.	O
7.4.4	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
7.4.5	É altamente desejável que um SIGAD possua mecanismos para realização de buscas nos eventos das trilhas de auditoria. *Para facilitar a visualização do relatório, os resultados podem ser apresentados de modo ordenado, mas essa ordenação não pode alterar os dados incluídos na trilha.*	AD
7.4.6	Um SIGAD tem que ser capaz de impedir qualquer modificação na trilha de auditoria.	O

Referência	Requisito	Obrig.
7.4.7	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. *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
7.4.8	É altamente desejável que um SIGAD seja capaz de gerar um alarme para os administradores apropriados se o tamanho da trilha de auditoria exceder um limite preestabelecido. *Esse alarme deve ser usado para indicar a proximidade do esgotamento do espaço reservado à trilha de auditoria.*	AD
7.4.9	Quando o espaço de armazenamento da trilha de auditoria atingir o limite preestabelecido, é altamente desejável que um SIGAD permita somente operações auditáveis originadas por administradores. *Todas as outras operações estarão bloqueadas até a liberação pelo administrador.*	AD
7.4.10	É altamente desejável que um SIGAD seja capaz de aplicar um conjunto de regras na monitoração de eventos auditados e, com base nelas, indicar a possível violação da segurança.	AD
7.4.11	É altamente desejável que um SIGAD garanta pelo menos as seguintes regras para monitoração dos eventos auditados: • acumulação de um número predeterminado de tentativas consecutivas de *login* com erro (autenticação malsucedida), conforme especificado pela política de segurança; • ocorrência de vários *login* simultâneos do mesmo usuário em locais (computadores) diferentes; • *login* do usuário fora do horário autorizado, após *logoff* no período normal.	AD
7.4.12	Um SIGAD tem que fornecer relatórios sobre as ações que afetam classes, unidades de arquivamento e documentos, em ordem cronológica e organizados por: • documento arquivístico, unidade de arquivamento ou classe; • usuário; • tipo de ação ou operação.	O
7.4.13	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. *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.*	F
7.4.14	Somente administradores autorizados têm que ser capazes de configurar o conjunto de eventos auditáveis e seus atributos.	O
7.4.15	Um SIGAD tem que ser capaz de arquivar periodicamente a trilha de auditoria como documento arquivístico.	O

7.5. Assinatura digital

O documento digital pode ser assinado por meio do uso de assinatura digital baseada em chave pública ou assinatura cadastrada mediante identificação do usuário e senha.

Assinatura digital é usada comumente como um elemento de autenticação. A autenticação é uma declaração de autenticidade por meio da adição de elementos ou afirmações. No caso dos documentos digitais esses elementos ou afirmações podem ser, por exemplo: assinatura digital baseada em chave pública, selo digital de tempo e marca d'água digital.

A assinatura digital baseada em chave pública 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). Assim, esse conjunto de requisitos como um todo é facultativo e a obrigatoriedade apontada nesta seção deve ser seguida quando, e somente quando, um SIGAD fizer uso de assinaturas digitais.

Referência	Requisito	Obrig.
7.5.1	É altamente desejável que um SIGAD seja capaz de prover meios para se verificar a origem e a integridade dos documentos com assinatura digital.	AD
7.5.2	Somente administradores autorizados têm que ser capazes de incluir, remover ou atualizar no SIGAD os certificados digitais de computadores ou de usuários.	O
7.5.3	Um SIGAD tem que ser capaz de verificar a validade da assinatura digital no momento da captura do documento.	O
7.5.4	Um SIGAD, no processo de verificação da assinatura digital, tem que ser capaz de registrar, como metadado, o seguinte: • validade da assinatura verificada; • registro da verificação da assinatura; • data e hora em que ocorreu a verificação.	O
7.5.5	É altamente desejável que um SIGAD seja capaz de armazenar, juntamente com o componente digital, conforme os metadados do e-ARQ Brasil, as informações de certificação a seguir: • assinatura digital; • certificado digital (cadeia de certificação) usado na verificação da assinatura.	AD
7.5.6	É altamente desejável que um SIGAD seja capaz de receber atualizações tecnológicas quanto à plataforma criptográfica de assinatura digital.	AD

7.6. Carimbo digital do tempo

Carimbo digital do tempo é um componente digital vinculado a um documento digital, emitido por uma Autoridade de Carimbo do Tempo (ACT) que serve como evidência de que uma informação digital existia numa determinada data e hora no passado. É um elemento diplomático de autenticação. No contexto arquivístico, pode registrar a data e a hora em que ocorreu um evento, como produção, recebimento, leitura, modificação ou eliminação de documento.

O carimbo digital do tempo, calculado a partir do *hash* do documento, é o registro da data e da hora em que a requisição do carimbo digital do tempo (*Time Stamp Request* – TSQ) com o *hash* do documento chegou à Autoridade de Carimbo do Tempo, e não se refere necessariamente à data e hora de produção do documento.

O uso de carimbo digital do tempo na administração pública foi padronizado e normalizado com a criação da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).[46] A utilização de carimbos de tempo no âmbito da ICP-Brasil é facultativa. Documentos assinados digitalmente são válidos com ou sem o carimbo digital do tempo. No entanto, recomenda-se sua utilização quando da produção de documentos arquivísticos.

Os requisitos são aplicáveis quando há necessidade de utilizar carimbo digital do tempo para assegurar autenticação, imputabilidade e irretratabilidade (ou irrefutabilidade) em relação a um determinado ponto no tempo. Assim, esse conjunto de requisitos como um todo é facultativo e a obrigatoriedade apontada nesta seção deve ser seguida quando, e somente quando, um SIGAD fizer uso de carimbo digital do tempo.

Referência	Requisito	Obrig.
7.6.1	Um SIGAD tem que ter acesso a relógios e carimbador de tempo confiáveis para seu próprio uso.	O
7.6.2	Um SIGAD tem que ser capaz de verificar a validade do carimbo digital do tempo no momento da captura do documento.	O
7.6.3	Um SIGAD, no processo de verificação do carimbo digital do tempo, tem que ser capaz de registrar, nos metadados do documento, o seguinte: • validade do carimbo digital do tempo; • registro da verificação do carimbo digital do tempo; • data e hora em que ocorreu a verificação.	O

46 Ver DOC_ICP-11, 12, 13 e 14. Disponível em: https://www.gov.br/iti/pt-br/assuntos/legislacao/documentos-principais.

7.7. 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. É um elemento diplomático de autenticação. 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. Assim, esse conjunto de requisitos como um todo é facultativo e a adoção e a obrigatoriedade apontadas nesta seção devem ser seguidas quando, e somente quando, um SIGAD apoiar o uso de marcas d'água digitais.

Referência	Requisito	Obrig.
7.7.1	Um SIGAD tem que ser capaz de recuperar informação contida em marcas d'água digitais.	O
7.7.2	Um SIGAD tem que ser capaz de armazenar documentos arquivísticos digitais que contenham marcas d'água digitais.	O
7.7.3	É altamente desejável que um SIGAD possua arquitetura capaz de receber atualizações tecnológicas no que se refere à plataforma de geração e detecção de marca d'água digital.	AD

7.8. Assinatura cadastrada mediante identificação do usuário e senha

A assinatura do documento pode dar-se também por meio do registro em metadados da identificação do autor. Esse registro deve ser realizado automaticamente pelo SIGAD e requer a validação da senha do usuário no momento da assinatura. A identificação do autor pode dar-se por meio do registro em metadado do seu nome, do seu id no SIGAD ou outra forma de identificação que seja reconhecida pelo SIGAD.

Estes requisitos só são aplicáveis a organizações que permitem a autenticação do documento por meio de assinatura cadastrada mediante identificação e senha do usuário. Assim, esse conjunto de requisitos como um todo é facultativo e a adoção e a obrigatoriedade apontadas nesta seção devem ser seguidas quando, e somente quando, um SIGAD fizer uso desta forma de autenticação.

Referência	Requisito	Obrig.
7.8.1	Um SIGAD tem que ser capaz de garantir a autoria de um documento que tenha sido autenticado por meio da identificação do autor após confirmação de senha, nos documentos produzidos e mantidos dentro do SIGAD.	O
7.8.2	Um SIGAD tem que registrar a identificação do autor como metadado de autenticação do documento após verificação da senha do usuário.	O
7.8.3	É altamente desejável que um SIGAD faça uso de *checksum* para apoiar a verificação da integridade do documento que foi autenticado após confirmação de senha.	AD

7.9. Criptografia

Criptografia é um método de codificação de documentos 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. Assim, esse conjunto de requisitos como um todo é facultativo e a adoção e a obrigatoriedade apontadas nesta seção devem ser seguidas quando, e somente quando, um SIGAD fizer uso de criptografia.

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.[47]

Referência	Requisito	Obrig.
7.9.1	Um SIGAD tem que usar criptografia no armazenamento, na transmissão e na apresentação de documentos arquivísticos digitais ao implementar a política de sigilo.	O
7.9.2	Um SIGAD tem que limitar o acesso aos documentos cifrados somente àqueles usuários portadores da chave de decifração.	O
7.9.3	Um SIGAD tem que registrar os seguintes metadados sobre um documento cifrado: • indicação sobre se está cifrado ou não; • algoritmos usados na cifração; • identificação do remetente; • identificação do destinatário.	O
7.9.4	É altamente desejável que um SIGAD possa assegurar a captura de documentos cifrados, diretamente, de uma aplicação de *software* que disponha da funcionalidade de cifração.	AD
7.9.5	Somente usuários autorizados têm que ser capazes de realizar as operações a seguir: • incluir, remover ou alterar parâmetros dos algoritmos criptográficos instalados no SIGAD; • incluir, remover ou substituir chaves criptográficas de programas ou usuários do SIGAD; • cifrar e alterar a criptografia de documentos; • remover a criptografia de um documento. *A remoção da cifração pode ocorrer quando sua manutenção resultar na indisponibilidade do documento. Por exemplo, se a chave de cifração/decifração estiver embarcada em* hardware *inviolável cuja vida útil esteja prestes a se esgotar ou se o documento for desclassificado.*	O

47 Ver CONSELHO INTERNACIONAL DE ARQUIVOS, 2005, p. 41.

Referência	Requisito	Obrig.
7.9.6	Em caso de remoção da cifração do documento, os seguintes metadados adicionais têm que ser registrados na trilha de auditoria: • data e hora da remoção da cifração; • identificação do executor da operação; • motivo da remoção da cifração.	O
7.9.7	É altamente desejável que um SIGAD possua arquitetura capaz de receber atualizações tecnológicas no que se refere à plataforma criptográfica.	AD

7.10. Acompanhamento de mudança de suporte ou de local

Durante seu ciclo de vida, os documentos arquivísticos digitais e seus respectivos metadados podem ser deslocados de um suporte (ou de um local) para outro, à medida que seu uso decresce e/ou se modifica. Essa mudança 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.
7.10.1	É altamente desejável que um SIGAD seja capaz de manter, para cada documento ou dossiê/processo, o histórico das mudanças de mídia sofridas por esse documento ou dossiê/processo.	AD
7.10.2	Um SIGAD tem que fornecer um recurso de acompanhamento para monitorar e registrar informações acerca do local atual e do deslocamento de dossiês/processos digitais e não digitais.	O
7.10.3	A função de acompanhamento de mudança de suporte ou de local tem que registrar metadados que incluam: • identificador do documento atribuído pelo SIGAD; • localização atual e localizações anteriores (definidas pelo usuário); • data e hora do envio/deslocamento; • data e hora da recepção no novo local; • destinatário; • usuário responsável pela mudança de suporte ou de local (sempre que for adequado); • método da mudança de suporte ou de local.	O

7.11. Autoproteção

Num ambiente digital, a autoproteção consiste na capacidade do sistema informatizado 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, *anti-spyware* e *firewall*.

Referência	Requisito	Obrig.
7.11.1	É altamente desejável que um SIGAD faça a verificação de vírus ou pragas antes da efetivação da captura.	AD
7.11.2	É altamente desejável que um SIGAD tenha 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
7.11.3	Após falha ou descontinuidade do SIGAD, 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 SIGAD para um estado seguro. *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
7.11.4	É altamente desejável que um SIGAD garanta que os dados de segurança, quando replicados, sejam consistentes. *Permissões de controle de acesso, chaves criptográficas e parâmetros de algoritmos criptográficos são exemplos de dados de segurança.*	AD
7.11.5	Um SIGAD tem que preservar um estado seguro de funcionamento, interrompendo completamente a interação com usuários comuns, quando ocorrer um dos erros a seguir: • falha de comunicação entre cliente e servidor; • perda de integridade das informações de controle de acesso; • falta de espaço para registro nas trilhas de auditoria.	O
7.11.6	Quando não for possível escrever na trilha de auditoria, é altamente desejável que um SIGAD impeça toda operação de qualquer usuário e passe para o modo de manutenção.	AD
7.11.7	Um SIGAD pode atribuir a cada componente digital do documento, no momento da captura, um código de manutenção de integridade baseado em criptografia robusta.	F

7.12. 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 corte, e o SIGAD armazena o documento original e a cópia truncada (produto do corte).

Referência	Requisito	Obrig.
7.12.1	Um SIGAD tem que permitir, a um administrador autorizado, anular a operação em caso de erro do usuário ou do sistema. *Anular uma operação não significa apagar um documento arquivístico capturado pelo SIGAD.* *A anulação da eliminação definitiva de documentos, por ser irreversível, não é possível.*	O
7.12.2	É altamente desejável que um SIGAD, para evitar erros irrecuperáveis, iniba 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
7.12.3	Em situações excepcionais, o administrador tem que ser autorizado a apagar ou corrigir dossiês/processos, volumes e documentos. Nesse caso, um SIGAD tem que: • registrar integralmente a ação de apagar ou corrigir na trilha de auditoria; • produzir um relatório de anomalias para o administrador; • eliminar todo o conteúdo de um dossiê/processo ou volume, quando forem eliminados; • garantir que nenhum documento seja eliminado se tal ação resultar na alteração de outro documento arquivístico; • 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; • manter a integridade total do metadado, a qualquer momento.	O
7.12.4	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

Referência	Requisito	Obrig.
7.12.5	Um SIGAD tem que permitir a um usuário autorizado fazer uma cópia truncada de um documento, com o objetivo de não alterar o original. *Se o SIGAD não fornecer, diretamente, esses recursos, tem que permitir que outros pacotes de* software *os proporcionem.*	O
7.12.6	Um SIGAD tem que possibilitar a ocultação de informação sigilosa contida no documento original, permitindo: • retirada de páginas de um documento; • adição de retângulos opacos para ocultar nomes ou palavras sensíveis; • quaisquer outros recursos necessários para formatos de vídeo ou áudio, caso existam. *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.*	O
7.12.7	Quando uma cópia truncada é produzida, um SIGAD tem que registrar essa ação nos metadados do documento e da cópia truncada, incluindo, pelo menos, data, hora, motivo e quem a produziu.	O
7.12.8	É altamente desejável que um SIGAD registre uma referência cruzada a uma cópia truncada nos mesmos dossiês/processos e documentos em que se encontra o documento original.	AD
7.12.9	Um SIGAD tem que armazenar, na trilha de auditoria, qualquer alteração efetuada para satisfazer os requisitos desta seção.	O

8 Preservação

Exatamente como no caso dos documentos não digitais, a preservação de documentos arquivísticos digitais não é um fim em si mesmo. 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, no contexto tecnológico, 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 acesso.

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 de suporte (*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 (como o disco óptico, fita magnética), unidades de disco rígido, 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 *softwares* 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: é a manutenção de um parque de equipamentos e programas para replicação de uma configuração mais antiga. Possibilita o acesso aos documentos originais no ambiente em que foram produzidos, porém, a manutenção e a integração com outros sistemas podem tornar-se problemáticas ao longo do tempo. A preservação do *hardware*, em especial, é uma alternativa cara, mesmo nas situações em que é compartilhado por mais de um usuário. Além disso, essa alternativa não é exequível no longo prazo, uma vez que o *hardware* pode ser danificado de forma irreversível, ficando completamente indisponível;
- emulação: é um processo que permite, por meio de *software*, a imitação de *software e hardware* em outro ambiente computacional. Permite que um computador moderno, possivelmente mais barato e de fácil manutenção, possa executar programas (*software*) antigos, desenvolvidos, originalmente, para outra plataforma. Para evitar possíveis perdas de informação e funcionalidades, deve ser realizada com bastante rigor. A probabilidade de perda de informações e funcionalidades aumenta à medida que são utilizadas diversas camadas de emulação, como resultado da aplicação desta técnica repetidas vezes;
- migração: é a transferência periódica dos documentos de um ambiente computacional para outro. Na preservação de documentos digitais a migração é correntemente realizada por meio da atualização de suporte e/ou conversão de formatos;
- atualização de suporte: consiste em copiar os documentos de um suporte para outro, sem mudar sua codificação, para evitar perdas decorrentes da deterioração do suporte. É amplamente utilizada e não provoca nenhuma perda ou alteração no documento, uma vez que a cadeia de bits copiada para o outro suporte é rigorosamente idêntica à inicial;
- conversão de formatos: é a conversão de um formato para outro, motivada principalmente para contornar a obsolescência tecnológica. Os documentos em formatos obsoletos são convertidos para novos formatos, apoiados em *hardware* e *software* mais atuais. Esse processo não está livre de problemas, podendo resultar em perda de informações e funcionalidades. A conversão também pode ser utilizada para reduzir a quantidade de formatos utilizados e, consequentemente, de sistemas a serem mantidos e gerenciados, de modo a facilitar as ações de preservação. Neste caso é chamada de normalização de formatos.

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.

O SIGAD pode interoperar com um Repositório Arquivístico Digital Confiável (RDC-Arq) para armazenar documentos de guarda longa e os destinados à guarda permanente.

Neste capítulo, 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 sua política de preservação digital, que deve estar em conformidade com as diretrizes fornecidas pela instituição arquivística em sua esfera de competência.

Destaca-se que existem requisitos de preservação funcionais e não funcionais. São considerados requisitos não funcionais: 8.1.1, 8.2.1, 8.2.7, 8.3.2, 8.3.3, 8.3.4 e 8.3.5.

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. *A vida útil pretendida de um suporte pode ser menor que sua vida útil prevista, o que permite condições ambientais mais flexíveis.*	O
8.1.2	É altamente desejável que um SIGAD permita 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 a implementação da estratégia de atualização de suportes.	O
8.1.4	É altamente desejável que um SIGAD informe, 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. *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 e documentos armazenados, visando à detecção de possíveis erros. *Nesse caso, recomenda-se o uso de um* checksum *robusto, ou seja, que permita a constatação da integridade dos dados e seja seguro quanto a fraudes.*	O
8.2.3	Um SIGAD tem que permitir a substituição dos dados e documentos armazenados que apresentarem erros.	O
8.2.4	Um SIGAD pode permitir a correção dos erros detectados nos dados e documentos armazenados. *Nesse contexto, a correção de erros refere-se à restauração de dados corrompidos.*	F
8.2.5	É altamente desejável que um SIGAD informe 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	É altamente desejável que um SIGAD mantenha um histórico dos resultados da verificação periódica dos dados e documentos 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	É altamente desejável que um SIGAD utilize 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	É altamente desejável que um SIGAD utilize 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	É altamente desejável que um SIGAD evite 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

REQUISITOS NÃO FUNCIONAIS

9 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 documentos 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.

9.1. Durabilidade

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

Referência	Requisito	Obrig.
9.1.1	É altamente desejável que um SIGAD utilize, preferencialmente, dispositivos e padrões de armazenamento maduros, estáveis no mercado e amplamente disponíveis. *Um SIGAD deve utilizar, preferencialmente, padrões abertos de armazenamento.* *A escolha dos dispositivos de armazenamento deve contemplar padrões estáveis de mercado e fornecedores consolidados.*	AD
9.1.2	A escolha de dispositivos tem que ser revista sempre que a evolução tecnológica indicar mudanças importantes.	O
9.1.3	Atividades de migração têm que ser efetivadas, preventivamente, sempre que se torne patente ou previsível a obsolescência do padrão corrente.	O
9.1.4	Para as memórias secundárias, um SIGAD tem que manter registro de MTBF (*mean time between failure*),[48] bem como suas datas de aquisição.	O
9.1.5	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. *As informações técnicas sobre previsibilidade de duração de mídias referidas no requisito 9.1.3 devem ser obtidas, preferencialmente, a partir de órgãos independentes. Quando isso não for possível, podem ser utilizadas informações de fornecedores.* *Em ambos os casos deve ficar registrada a origem da informação.*	O
9.1.6	Para as memórias secundárias e terciárias, é altamente desejável que um SIGAD mantenha estatísticas da durabilidade efetivamente observada.	AD
9.1.7	O acesso às informações armazenadas em memória terciária deve ser efetuado, preferencialmente, mediante o uso de rede de dados. *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 SIGAD, e não aos usuários comuns.*	AD
9.1.8	Quando se proceder à eliminação de documentos, as memórias de suporte têm que ser, devidamente, "sanitizadas", isto é, ter suas informações, efetivamente, indisponibilizadas. *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

48 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.

9.2. Capacidade

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

Referência	Requisito	Obrig.
9.2.1	Um SIGAD tem que possuir capacidade de armazenamento suficiente para acomodação de todos os documentos e suas cópias de segurança. *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
9.2.2	Em um SIGAD, tem que ser prevista a possibilidade de expansão da estrutura de armazenamento. *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.* *Quando da aquisição de* disk arrays*, as possibilidades de expansão dos equipamentos de controle devem ser consideradas.* *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
9.2.3	É altamente desejável que um SIGAD permita ao administrador configurar os limites de capacidade de armazenamento dos diversos dispositivos.	AD
9.2.4	É altamente desejável que um SIGAD ofereça ao administrador facilidades para monitoração da capacidade de armazenamento. *Esse controle indica, por exemplo, capacidade utilizada, capacidade disponível e taxa de ocupação. Tais informações são úteis para subsidiar ações de expansão em tempo hábil.*	AD
9.2.5	É altamente desejável que um SIGAD informe, automaticamente, ao administrador quando os dispositivos de armazenamento on-line atingirem níveis críticos de ocupação.	AD
9.2.6	É altamente desejável que um SIGAD mantenha estatísticas de taxa de crescimento de utilização de memória secundária e terciária para informar ao administrador previsões de exaustão de recursos. *Este tipo de estimativa possibilita ao administrador antecipar ações de expansão antes que a utilização atinja níveis críticos.*	AD

9.3. Efetividade de armazenamento

Referência	Requisito	Obrig.
9.3.1	É altamente desejável que os dispositivos de armazenamento de um SIGAD suportem métodos de detecção de erros para leitura e escrita de dados.	AD
9.3.2	Um SIGAD tem que utilizar técnicas de restauração de dados em caso de falhas.	O
9.3.3	Um SIGAD tem que utilizar mecanismos de proteção contra escrita, que previnam alterações indevidas e mantenham a integridade dos dados armazenados.	O
9.3.4	É altamente desejável que a infraestrutura de um SIGAD preveja o uso de técnicas para garantir maior confiabilidade e desempenho. As técnicas recomendadas incluem: • espelhamento (*mirroring*) nas memórias secundárias para maior confiabilidade; • partição de dados (*data stripping*) nas memórias secundárias para maior desempenho.	AD
9.3.5	A integridade dos dispositivos de armazenamento tem que ser, periodicamente, verificada.	O

10 Funções administrativas

Referência	Requisito	Obrig.
10.1.1	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
10.1.2	Um SIGAD tem que fornecer relatórios flexíveis para que o administrador possa gerenciar os documentos e seu uso. Esses relatórios devem apresentar, no mínimo: • quantidade de dossiês/processos, volumes e itens a partir de parâmetros ou atributos definidos (tempo, classe, unidade administrativa etc.); • estatísticas de transações relativas a dossiês/processos, volumes e itens; • atividades por usuário.	O
10.1.3	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

11 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. Assim, todos os requisitos desta seção são genéricos e têm que ser adaptados à realidade de cada órgão produtor de documentos arquivísticos.[49]

Referência	Requisito	Obrig.
11.1	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
11.2	Um SIGAD tem que estar de acordo com a legislação e as normas específicas para gestão e acesso de documentos arquivísticos.	O
11.3	Um SIGAD tem que estar em conformidade com requisitos regulamentares específicos e códigos de boa prática necessários para a execução de determinadas atividades. *Este requisito pode ser personalizado para cada contexto, como, por exemplo, saúde, justiça, educação, previdência.*	O

49 Para obter informações sobre a legislação arquivística brasileira, consulte a seção Legislação Arquivística, no sítio do CONARQ, disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica.

12 Usabilidade

Um sistema de *software* com boa usabilidade deve apoiar a realização de tarefas simples, diretas e objetivas, que garantam as metas de produtividade e qualidade de trabalho do usuário. 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 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.
12.1.1	É altamente desejável que um SIGAD possua documentação completa, clara, inteligível e organizada para instalação e uso do *software*.	AD
12.1.2	É altamente desejável que um SIGAD possua sistema de ajuda on-line.	AD
12.1.3	É altamente desejável que o sistema de ajuda on-line fornecido pelo SIGAD seja vinculado à função ou tarefa executada, em todo o sistema. *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
12.1.4	É altamente desejável que um SIGAD permita a personalização de conteúdo de ajuda on-line por adição de texto ou edição do texto existente. *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
12.1.5	É altamente desejável que toda mensagem de erro produzida pelo SIGAD seja clara e significativa, de modo a permitir que o usuário se recupere do erro ou cancele a operação.	AD
12.1.6	É altamente desejável que a interface de um SIGAD siga padrões preestabelecidos e consolidados como boas práticas de projeto gráfico. *Normas ou regras de interface podem ser relativas à utilização de padrão de identidade visual (ligado à "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.* *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

Referência	Requisito	Obrig.
12.1.7	É altamente desejável que um SIGAD empregue um conjunto simples e consistente de regras de interface, privilegiando a facilidade de aprendizado das operações pelos seus usuários. *O uso de um conjunto de regras em conformidade com o ambiente operacional em que o SIGAD será executado permite que ele apresente menus, comandos e outras facilidades consistentes em toda a aplicação.* *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.*	AD
12.1.8	É altamente desejável que a interface de visualização dos documentos arquivísticos forneça o recurso de arrastar e soltar, se for apropriado no ambiente operacional do SIGAD.	AD
12.1.9	É altamente desejável que o SIGAD permita que sua estrutura de classes e dossiês/processos possa ser visualizada em diferentes formas de apresentação.	AD
12.1.10	É altamente desejável que o usuário possa personalizar a interface gráfica de um SIGAD. A personalização deve incluir, pelo menos, as seguintes possibilidades: • conteúdo de menus; • formatos de tela; • utilização de teclas de função; • alteração de cor, fonte e tamanho de letra em telas e janelas; • avisos sonoros.	AD
12.1.11	É altamente desejável que um SIGAD, sempre que utilizar janelas *pop-up* e barras de ferramentas, ofereça ao usuário a possibilidade de configurar e habilitar/desabilitar esse tipo de recurso. *Porém, é preciso não infringir a recomendação de uso de um conjunto simples e consistente de regras de interface.*	AD
12.1.12	É altamente desejável que, sempre que um SIGAD permitir o uso de janelas, admita sua movimentação, redimensionamento a gravação das modificações da aparência, possibilitando a personalização por perfil de usuário.	AD
12.1.13	É altamente desejável que um SIGAD permita a seleção de avisos sonoros e a personalização de tom e volume, bem como a gravação dessas escolhas no perfil do usuário.	AD
12.1.14	É altamente desejável que um SIGAD permita a gravação de opções *default* para entrada de dados de configuração, como: • valores de variáveis definidas pelo usuário; • valores iguais aos de um item anterior; • valores que possam ser selecionados em uma lista configurável; • valores derivados do contexto, como data, referência do dossiê/processo, identificador do usuário; • valores predefinidos por um administrador (para campos de metadados como, por exemplo, o nome da organização que está utilizando o sistema).	AD

Referência	Requisito	Obrig.
12.1.15	É altamente desejável que a interface do SIGAD com o usuário seja adequada a adaptações e personalizações que permitam sua utilização por usuários com deficiência ou mobilidade reduzida, de acordo com as políticas de inclusão da organização. 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. *Para ambientes e sítios apoiados na web, é importante seguir orientações específicas de acessibilidade.*[50] *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
12.1.16	É altamente desejável que um SIGAD permita 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
12.1.17	É altamente desejável que um SIGAD esteja 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. *Este requisito deve estar de acordo com as normas de segurança.*	AD
12.1.18	Em caso de integração do SIGAD com o sistema de correio eletrônico, é altamente desejável que seja possível fazer referências a documentos arquivísticos sem necessidade de envio de cópias adicionais.	AD
12.1.19	É altamente desejável que um SIGAD esteja integrado com o sistema padrão de edição de documentos, de modo que possa fazer uso da facilidade de gravação.	AD
12.1.20	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
12.1.21	É altamente desejável que um SIGAD permita a definição e utilização de referências cruzadas entre documentos arquivísticos digitais correlacionados, bem como a fácil navegação entre eles, inclusive com o uso de *hyperlinks*. *O uso de* hiperlinks *deve ser limitado a documentos dentro do mesmo processo/dossiê.* Hiperlinks *com documentos externos ao ambiente, ou mesmo em outros processos/dossiês, podem ficar obsoletos ao longo do tempo, comprometendo a completitude do processo/dossiê.*	AD
12.1.22	É altamente desejável que um SIGAD disponibilize pelo menos dois papéis de acesso diferenciados, um para usuário final e outro para administrador de sistema.	AD

50 Exemplos: "eMAG – Modelo de Acessibilidade em Governo Eletrônico", disponível em: https://www.gov.br/governodigital/pt-br/acessibilidade-digital/modelo-de-acessibilidade; 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", disponível em: http://prodam.sp.gov.br/acessibilidade; "W3C – Markup Validation Service", disponível em: https://validator.w3.org/; lei n. 13.146, de 6 de julho de 2012, que "institui a lei brasileira de inclusão da pessoa com deficiência".

Referência	Requisito	Obrig.
12.1.23	É altamente desejável que um SIGAD forneça a usuários finais e administradores funções intuitivas e fáceis de usar, que requeiram poucas ações para completar uma tarefa padrão. Sobretudo durante sua operação normal, um SIGAD deve ser capaz de: • capturar e declarar um documento arquivístico com no máximo três cliques de *mouse* ou acionamentos de tecla; • apresentar todos os elementos de metadados obrigatórios para a captura do documento com mínima demanda para o usuário; • 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; • apresentar os metadados de um documento arquivístico com no máximo três cliques de *mouse* ou acionamentos de tecla.	AD
12.1.24	Um SIGAD tem que restringir o acesso às funcionalidades administrativas e impossibilitar sua visualização pelo usuário final. *Exemplos: as operações não disponíveis aparecem com fonte atenuada nos menus e possuem efeito nulo quando acionadas.* *O acesso às operações indisponíveis é restringido pela configuração dos menus, que não apresentam essas operações ao usuário sem permissão para executá-las.*	O
12.1.25	É altamente desejável que um SIGAD leve 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. *Exemplo: não devem ser utilizados menus audíveis em ambientes que apresentam alto volume de ruído próximo aos terminais de usuários.*	AD

13 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.

Este capítulo 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 SIGAD. Isto se faz por meio do uso de regras e padrões de comunicação.

O governo brasileiro definiu a arquitetura ePING – Padrões de Interoperabilidade de Governo Eletrônico, visando à interoperabilidade nas diversas esferas do poder público.[51] Nos órgãos e entidades da administração pública federal, o SIGAD tem que adotar a arquitetura ePING a fim de aumentar a viabilidade técnica no intercâmbio de informações entre sistemas.

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

51 A arquitetura e-PING do governo brasileiro está disponível em: http://eping.governoeletronico.gov.br/. Acesso em: 24 jan. 2020.

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

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

15 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.
15.1.1	É altamente desejável que um SIGAD mantenha estatísticas dos tempos de atendimento, discriminadas por tipo de operação.	AD
15.1.2	É altamente desejável que um SIGAD seja expansível até comportar um número máximo, preestabelecido, de usuários simultâneos, provendo a continuidade efetiva dos serviços.	AD
15.1.3	Um SIGAD tem que incluir rotina de manutenção de: • dados de usuários e de grupos; • perfis de acesso; • plano de classificação; • bases de dados; • tabelas de temporalidade. *Essas tarefas devem atender às mudanças planejadas da organização, sem causar grande sobrecarga de administração.*	O
15.1.4	É altamente desejável que um SIGAD seja escalável, a fim de permitir adaptação a organizações de diferentes tamanhos e complexidades.	AD

15.1.5	É altamente desejável que um SIGAD forneça evidências do grau de escalabilidade ao longo do tempo. Avaliações quantitativas devem incluir: • tamanho máximo do repositório que pode ser suportado com desempenho adequado; • o número máximo de usuários simultâneos que podem ser atendidos com desempenho adequado; • sobrecarga administrativa prevista para um período de cinco anos, permitindo o crescimento do número de usuários e da quantidade de registros; • quantidade de reconfigurações e indisponibilidades previstas para um período de cinco anos, permitindo o crescimento do número de usuários e da quantidade de registros; • 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.	AD

METADADOS

A concepção adotada neste trabalho baseou-se na definição do termo metadado como "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 não digital, 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).

Nessa segunda versão do e-ARQ Brasil a organização dos metadados foi alterada, principalmente com relação aos metadados de classe e no que diz respeito ao registro dos eventos.

Os metadados de classe foram separados em "Identificação da classe" e "Eventos de gerenciamento da classe". Os primeiros dizem respeito às informações relativas a cada classe, incluindo as relacionadas a prazo de guarda e destinação previstos. Os segundos dizem respeito às alterações realizadas em cada classe, tais como, mudança de subordinação, mudança de prazo de guarda etc.

Os metadados relativos aos eventos (gestão do ciclo de vida, gestão do processo, gerenciamento de classe e preservação) foram estruturados de maneira a registrar um conjunto de informações relativas a cada evento realizado/controlado pelo SIGAD, que identificam o evento, o agente responsável por ele e os resultados ou consequências do evento. Para cada grupo de eventos foram também listados os tipos de eventos previstos para registro em metadados. Essa modelagem baseou-se na proposta apresentada no dicionário de dados do PREMIS.

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 funcionais e não funcionais 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. Na revisão desta segunda versão, foram consultadas as seguintes referências:

- *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 interministerial MJ/MP n. 1.677, de 7 de outubro de 2015, que define os procedimentos gerais para o desenvolvimento das atividades de protocolo no âmbito dos órgãos e entidades da administração pública federal;
- 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:

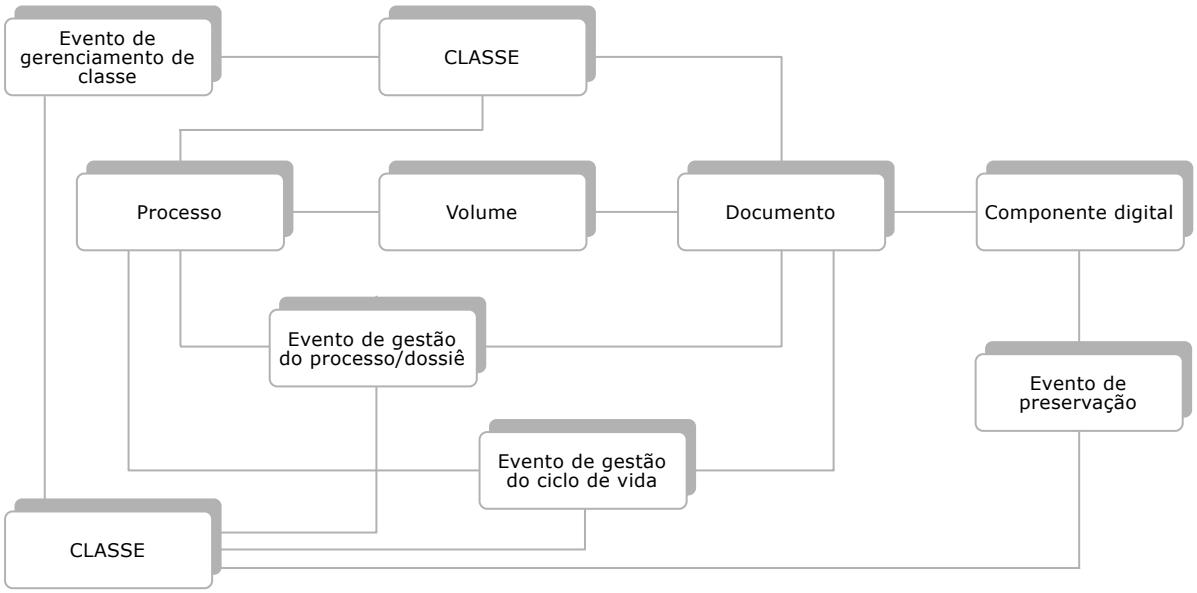
- ABNT NBR ISO 23081-1:2019 – Informação e documentação – Processos de gestão de documentos de arquivo – Metadados para documentos de arquivo;
- ISO 15836:2017 – Dublin Core metadata element, set. 2017;
- e-Government metadata standard – e-GMS, United Kingdom, v. 3.0, 2004;
- Metainformação para interoperabilidade de Portugal – MIP, 2006;
- Model requirements for the management of electronic records – MoReq 2, 2007;

- Padrão de Metadados do Governo Eletrônico – e-PMG, Brasil;
- PREMIS – Data dictionary for preservation metadata, version 3, 2015.

Organização do esquema de metadados

Foram definidos metadados para as entidades: *documento* (documento, volume e processo/dossiê), *evento de gestão do ciclo de vida*, *evento de gestão de processos/dossiês*, *classe*, *evento de gerenciamento de classe*, *componente digital*, *evento de preservação* e *agente*.

A seguir apresenta-se um modelo que representa estas entidades e seus relacionamentos de forma simplificada. Anexo encontra-se o Modelo de Entidades e Relacionamentos (MER) elaborado, a partir do esquema de metadados, com maior nível de detalhe.



Este modelo deve ser entendido da seguinte maneira:

Documento refere-se ao documento que foi capturado pelo SIGAD, isto é, declarado como arquivístico e incorporado ao sistema por meio de registro, classificação, arquivamento etc. Esta é a entidade mais importante de um 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. Esta prática tem origem nos documentos não digitais, de forma a possibilitar que os volumes tenham tamanho e peso de fácil manejo. No caso dos documentos digitais, tal prática pode se mostrar apropriada em situações em que a divisão em volumes facilite a manipulação dos processos/dossiês, como, por exemplo, nas atividades de seleção, transferência etc.

Em geral, a maior parte dos *processos/dossiês* não apresenta mais de um *volume*. Neste caso, o conceito de *volume* é transparente para os usuários.

Os *documentos arquivísticos* são:

- armazenados em um *volume* de um *processo/dossiê*; ou classificados diretamente em alguma *classe*.
- Todo documento arquivístico tem que ser relacionado a um volume ou 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 do ciclo de vida e eventos de gestão de processos.

Evento de gestão do ciclo de vida refere-se às ações de gestão que ocorrem com os documentos arquivísticos ao longo de seu ciclo de vida, como captura, classificação, desclassificação, eliminação, transferência, recolhimento, entre outros.

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

Evento de gestão dos processos/dossiês refere-se aos procedimentos de protocolo realizados com os processos, como abertura de volume/processo/dossiê, encerramento de volume/processo/dossiê, tramitação, juntada, desapensação, desentranhamento, desmembramento, entre outros.

- Evento de gestão dos processos/dossiês relaciona-se com o documento (quando aplicável), com o processo, 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. Um plano de classificação é composto por uma hierarquia de classes, subclasses, grupos, subgrupos numa estrutura de árvore, que podem ser identificados por códigos. No contexto do e-ARQ Brasil, a entidade classe refere-se, de forma genérica, aos níveis citados. Assim, quando um requisito trata da classe, estão sendo considerados todos os níveis do plano de classificação.

Em cada classe estão também associadas informações a respeito da temporalidade e da destinação prevista para os documentos nela classificados.

Uma *classe* que tenha outras *classes* a ela subordinadas não pode conter *processos/dossiês* ou *documentos arquivísticos*.

Todas as alterações ocorridas no plano de classificação e na tabela de temporalidade e destinação devem ficar registradas nos eventos de gerenciamento de classe.

As classes estão relacionadas a:

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

Evento de gerenciamento de classe refere-se às ações de manutenção do código de classificação e da tabela de temporalidade e destinação de documentos, que implicam a alteração dos atributos das classes, tais como: alteração de nome da classe, alteração de subordinação, alteração de temporalidade prevista, dentre outros.

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

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.

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 documento está relacionado a um ou mais componentes digitais.
- Cada componente digital está relacionado a uma série de eventos de preservação.

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

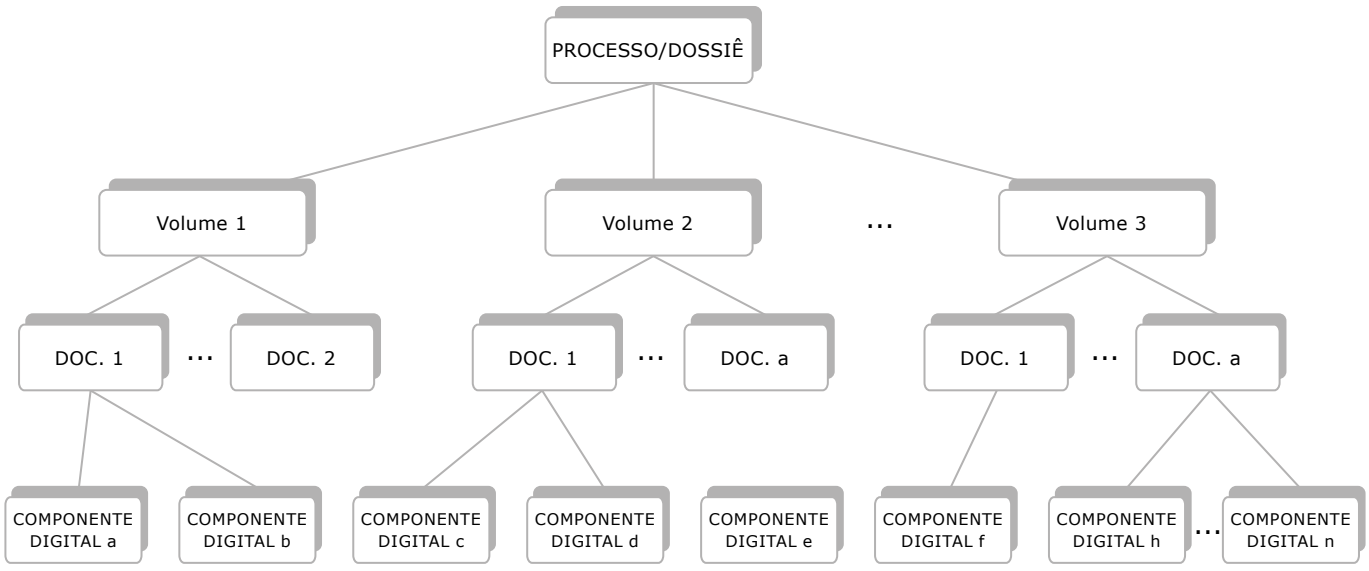
- Evento de preservação relaciona-se com o componente digital e com o agente responsável pela ação de preservação.

Agente refere-se aos usuários que acessam o SIGAD.

- Agente relaciona-se com o evento de gestão do ciclo de vida pelo qual foi responsável.
- Agente relaciona-se com o evento de gestão dos processos/dossiês pelo qual foi responsável.
- Agente relaciona-se com o evento de preservação pelo qual foi responsável.
- Agente relaciona-se com o evento de gerenciamento de classe pelo qual foi responsável.

O documento arquivístico digital é a apresentação, em formato acessível ao ser humano ou a um sistema, de um ou vários componentes digitais que estão relacionados entre si. 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 a seguir 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 de protocolo do processo
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. Identificador do componente digital
1.20. Gênero
1.21. Espécie
1.22. Tipo
1.23. Idioma
1.24. Quantidade de folhas
1.25. Numeração sequencial dos documentos
1.26. Indicação de anexos
1.27. Indicação de anotação
1.28. Unidade responsável pela execução da ação
1.29. Relação com outros documentos
1.30. Níveis de acesso
1.31. Previsão de desclassificação
1.32. Data de produção
1.33. Local de produção
1.34. Classe
1.35. Destinação prevista
1.36. Prazo de guarda
1.37. Localização

2 Evento de gestão

2.1. Eventos de gestão do ciclo de vida

2.1.1. Identificador do evento

2.1.2. Tipo de evento

2.1.3. Identificador do processo/dossiê

2.1.4. Identificador do documento

2.1.5. Identificador do lote

2.1.6. Data e hora do evento

2.1.7. Agente responsável pelo evento

2.1.8. Detalhe do evento

2.2. Eventos de gestão do processo/dossiê

2.2.1. Identificador do evento

2.1.2. Tipo do evento

2.1.3. Identificador do processo

2.1.4. Identificador do volume

2.1.5. Data e hora do evento

2.1.6. Agente responsável pelo evento

2.1.7. Identificador do documento

3 Classe

3.1. Identificador da classe

3.2. Nome da classe

3.3. Código da classe

3.4. Subordinação da classe

3.5. Indicação de permissão de uso

3.6. Indicação de classe ativa/inativa

3.7. Prazo na idade corrente

3.8. Evento de contagem na idade corrente

3.9. Prazo na idade intermediária

3.10. Evento de contagem na idade intermediária

3.11. Destinação final

3.12. Sigilo associado à classe

3.13. Observação

4 Evento de gerenciamento de classe

4.1. Identificador do evento
4.2. Tipo do evento
4.3. Identificador da classe afetada
4.4. Data e hora do evento
4.5. Agente responsável pelo evento
4.6. Valor anterior do atributo

5 Componente digital

5.1. Identificador do componente digital
5.2. Nome original
5.3. Tamanho
5.4. Software de criação
5.5. Nível de composição
5.6. Inibidor
5.7. Formato de arquivo
5.8. Localização
5.9. Suporte
5.10. Dependência de software
5.11. Dependência de hardware
5.12. Outras dependências
5.13. Relação com outros componentes digitais
5.14. Fixidade
5.15. Assinatura digital

6 Evento de preservação

6.1. Identificador do evento
6.2. Tipo de evento
6.3. Identificação de componente digital
6.4. Data e hora do evento
6.5. Agente responsável pelo evento
6.6. Resultado do evento
6.7. Detalhes do evento

7 Agente

7.1. Identificador do agente
7.2. Nome do agente
7.3. Status do agente

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

Designação: indicação do nome atribuído ao elemento.

Rótulo: nome padrão que tem que ser utilizado para identificar o elemento a fim de facilitar a interoperabilidade de sistemas.

Definição: indica que informação deve ser registrada no elemento de metadado.

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

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

Repetibilidade: indica se a informação pode ser registrada mais de uma vez para um mesmo documento, volume ou processo/dossiê.

Nota de aplicação: sugere formas de aplicação do elemento.

Exemplos: apresenta alguns exemplos de aplicação que explicam o elemento.

Regra de preenchimento: regra que especifica os valores, a codificação ou a lista de autoridades (lista de valores autorizados) convencionados para o preenchimento do elemento.

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

Equivalência: referências para elementos equivalentes de outros esquemas de metadados.

Para os elementos de metadados referentes a identificação *de classe, agente* e *componente digital* foi elaborada uma ficha individual que detalha cada elemento e apresenta as seguintes informações:

Designação
Rótulo
Definição
Objetivo
Obrigatoriedade
Repetibilidade
Nota de aplicação
Exemplos
Regra de preenchimento
Requisito
Equivalência

Designação: indicação do nome atribuído ao elemento.

Rótulo: nome padrão que tem que ser utilizado para identificar o elemento a fim de facilitar a interoperabilidade de sistemas.

Definição: indica qual informação deve ser registrada no elemento de metadado.

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

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

Repetibilidade: indica se a informação pode ser registrada mais de uma vez para um mesmo documento, volume ou processo/dossiê.

Nota de aplicação: sugere formas de aplicação do elemento.

Exemplos: apresenta alguns exemplos de aplicação que explicam o elemento.

Regra de preenchimento: regra que especifica os valores, a codificação ou a lista de autoridades (lista de valores autorizados) convencionados para o preenchimento do elemento.

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

Equivalência: referências para elementos equivalentes de outros esquemas de metadados.

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

Designação
Rótulo
Definição
Obrigatoriedade
Repetibilidade
Regra de preenchimento
Requisito
Equivalência

Designação: indicação do nome atribuído ao elemento.

Rótulo: nome padrão que tem que ser utilizado para identificar o elemento a fim de facilitar a interoperabilidade de sistemas.

Definição: indica que informação deve ser registrada no elemento de metadado.

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

Repetibilidade: indica se a informação pode ser registrada mais de uma vez para um mesmo documento, volume ou processo/dossiê.

Regra de preenchimento: regra que especifica os valores, a codificação ou a lista de autoridades (lista de valores autorizados) convencionados para o preenchimento do elemento.

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

Equivalência: referências para elementos equivalentes de outros esquemas de metadados.

Nota a respeito do preenchimento de data/hora

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

1 Documento

Estas informações referem-se à identidade e à integridade (componentes da autenticidade) do documento e apoiam 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**		
Rótulo	earq.documento.id		
Definição	Identificador único atribuído pelo SIGAD ao documento no ato de sua captura[52] para o sistema.		
Objetivo	Identificar de forma unívoca o documento para que o SIGAD possa gerenciá-lo.		
Aplica-se a	Processo/dossiê **NA** Ver elemento 1.4 (Identificador do processo/dossiê)	Volume **NA** Ver elemento 1.6 (Identificador do volume)	Documento **O**
Repetibilidade	-	-	Não repetível
Nota de aplicação	Aplicável no âmbito do SIGAD. Esse identificador tem de ser unívoco e persistente. Esse metadado deve ser registrado de forma estruturada, em dois subelementos, conforme a seguir: documento.idTipo documento.idValor Caso seja utilizado somente um tipo de identificador no SIGAD, não é necessário explicitá-lo, bastando registrar o valor do identificador. Pode ser um elemento identificador simples e conter um componente para localização em ambiente eletrônico.		
Exemplos	documento.idTipo: *handle*[53] documento.idValor: *loc.music/gottlieb.09601* documento.idTipo: *identificador institucional* documento.idValor: *CD269/CD269/70/10596.PCD*		
Regra de preenchimento	Deve, preferencialmente, ser gerado de forma automática pelo SIGAD. As instituições devem seguir normas específicas em seu âmbito de atuação ou esfera de competência para geração desse identificador.		
Requisito	2.1.4 / 2.1.6 / 2.1.8 / 4.2.6 / 5.5.2 / 7.10.3		
Equivalência	e-PMG: identificador.idDoSistema (*identifier.systemID*)		

52 Observar a definição de captura na Parte I, seção 8.1 do e-ARQ Brasil.

53 O *Handle System* é um serviço de informação que provê um identificador persistente em redes como a internet. Disponível em: www.handle.net.

1.2. Número do documento

Designação	Número do documento		
Rótulo	earq.documento.numero		
Definição	Número ou código alfanumérico atribuído ao documento no ato da sua produção.		
Objetivo	Permitir a identificação precisa de um documento.		
Aplica-se a	Processo/dossiê **NA** Ver elemento 1.5 (Número de protocolo do processo)	Volume **NA** Ver elemento 1.7 (Número do volume)	Documento **OA**
Repetibilidade	-	-	Não repetível
Nota de aplicação	Em geral é uma numeração seriada correspondente a uma espécie documental, tal como memorandos, ofícios, avisos, portarias, ordens de serviço e outros. Pode ser acrescido da data de produção e da sigla do órgão produtor.		
Exemplos	*Mem.119/COAD/DIRHU;* *Ofício n. 78/2008/GABIN-AN;* *Aviso 123/2008-SCT-PR.*		
Regra de preenchimento	Deve, preferencialmente, ser gerado de forma automática pelo SIGAD. As instituições devem seguir normas específicas em seu âmbito de atuação ou esfera de competência para geração desse número.		
Requisito	2.1.9		
Equivalência	--		

1.3. Número do protocolo

Designação	Número do protocolo		
Rótulo	earq.documento.protocolo		
Definição	Número ou código alfanumérico atribuído ao documento no ato do seu registro no protocolo.		
Objetivo	Permitir a identificação e o controle da tramitação do documento.		
Aplica-se a	Processo/dossiê **NA** Ver elemento 1.5 (Número de protocolo do processo)	Volume **NA** Ver elemento 1.7 (Número do volume)	Documento **OA**
Repetibilidade	-	-	Não repetível
Nota de aplicação	Pode ser acrescido da data de registro. Esse número deve estar visível para o usuário.		
Exemplos	*Carta: AB/11.000/2008;* *Número de protocolo: 00400.001412/2000-26.*		
Regra de preenchimento	Os órgãos e entidades devem seguir normas específicas em seu âmbito de atuação ou esfera de competência. Deve, preferencialmente, ser gerado automaticamente pelo SIGAD.		
Requisito	2.1.9		
Equivalência	--		

1.4. Identificador do processo/dossiê

Designação	**Identificador do processo | dossiê**		
Rótulo	earq.processoDossie.id		
Definição	Identificador único atribuído pelo SIGAD ao processo ou dossiê no ato de sua captura para o sistema.		
Objetivo	Identificar de forma unívoca e persistente o processo ou dossiê para que o SIGAD possa gerenciá-lo. Estabelecer a relação entre o processo ou dossiê e os volumes e documentos que os integram.		
Aplica-se a	Processo/dossiê **O**	Volume **NA**	Documento **NA**
Repetibilidade	Não repetível	-	-
Nota de aplicação	Aplicável no âmbito do SIGAD. Pode ser um elemento identificador simples e conter um componente para localização em ambiente eletrônico. Esse identificador não está disponível para o usuário. É um controle interno do sistema. Esse identificador tem de ser unívoco e persistente.		
Exemplos	--		
Regra de preenchimento	Deve, preferencialmente, ser gerado automaticamente pelo SIGAD. As instituições devem seguir normas específicas em seu âmbito de atuação ou esfera de competência.		
Requisito	2.1.6 / 2.1.8 / 4.2.6 / 5.5.2		
Equivalência	e-PMG: identificador.idDoSistema (*identifier.systemID*)		

1.5. Número de protocolo do processo

Designação	Número de protocolo do processo		
Rótulo	earq.processo.protocolo		
Definição	Número ou código alfanumérico de registro no protocolo do processo.		
Objetivo	Identificar o número de registro no protocolo do processo. Permitir o controle dos registros de autuações de processos. Permitir a pesquisa sobre processos.		
Aplica-se a	Processo **O** Ver elemento 1.3 (Número do protocolo)	Volume **NA**	Documento **NA** Ver elemento 1.2 (Número do documento)
Repetibilidade	Não repetível	-	-
Nota de aplicação	Em alguns casos o número de registro no protocolo do documento avulso é atribuído seguindo a mesma sistemática do processo. Assim, os metadados 1.5 e 1.3 podem ser tratados como o mesmo elemento de metadados e registrados no mesmo campo. Dossiê não recebe número de protocolo.		
Exemplos	*Processo n. 00302.000125/2008;* *Processo n. 04060.001412/2000-26.*		
Regra de preenchimento	As instituições devem seguir normas específicas em seu âmbito de atuação ou esfera de competência. Deve, preferencialmente, ser gerado automaticamente pelo SIGAD.		
Requisito	2.1.9		
Equivalência	--		

1.6. Identificador do volume

Designação	Identificador do volume		
Rótulo	earq.volume.id		
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. Estabelecer a relação entre o processo ou dossiê e os volumes e documentos que os integram.		
Aplica-se a	Processo/dossiê **NA** Ver elemento 1.4 (Identificador do processo/ dossiê)	Volume **O**	Documento **NA** Ver elemento 1.1 (Identificador do documento)
Repetibilidade	-	Não repetível	-
Nota de aplicação	Aplicável no âmbito do SIGAD. Deve, preferencialmente, ser gerado automaticamente pelo SIGAD. Pode ser um elemento identificador simples e conter um componente para localização em ambiente eletrônico. É recomendável que possa se integrar a sistemas de identificadores persistentes. O identificador de volume não se aplica aos documentos avulsos, ou seja, os que não foram inseridos em processos ou dossiês.		
Exemplos	--		
Regra de preenchimento	Deve, preferencialmente, ser gerado automaticamente pelo SIGAD. As instituições devem seguir normas específicas em seu âmbito de atuação ou esfera de competência.		
Requisito	2.1.6 / 2.1.8 / 4.2.6 / 5.4 / 5.5.2		
Equivalência	e-PMG: identificador.idDoSistema (*identifier.systemID*)		

1.7. Número do volume

Designação	Número do volume		
Rótulo	earq.volume.numero		
Definição	Número de registro do volume do processo ou dossiê.		
Objetivo	Identificar o volume do processo ou dossiê.		
Aplica-se a	Processo/dossiê **NA** Ver elemento 1.5 (Número de protocolo do processo)	Volume **O**	Documento **NA** Ver elemento 1.2 (Número do documento)
Repetibilidade	-	Não repetível	-
Nota de aplicação	O controle de volumes deve obedecer às normas das instituições.		
Exemplos	--		
Regra de preenchimento	Deve, preferencialmente, ser gerado automaticamente pelo SIGAD.		
Requisito	Ver seção 5.4 (Volumes: abertura, encerramento e metadados)		
Equivalência	--		

1.8. Tipo de meio

Designação	Tipo de meio		
Rótulo	earq.documento.meio earq.processo.meio		
Definição	Identificação do meio do documento/volume/processo/dossiê: *digital, não digital* ou *híbrido*.		
Objetivo	Identificar se o documento/volume/processo/dossiê é digital, não digital ou híbrido para controlar as relações entre os meios e o monitoramento de preservação.		
Aplica-se a	Processo/dossiê **F**	Volume **NA**	Documento **O**
Repetibilidade	Não repetível	-	Não repetível
Nota de aplicação	No documento/volume/processo/dossiê híbrido, os relacionamentos deverão ser registrados para identificar a parte não digital e a parte digital. Ver elemento *1.29* (Relação com outros documentos).		
Exemplos	--		
Regra de preenchimento	--		
Requisito	2.4 / 3.2.13 / 5.5.1 / 5.5.2		
Equivalência	Nobrade: 1.5 Dimensão e suporte / 4.4 Características físicas e requisitos técnicos		

1.9. Status

Designação	Status		
Rótulo	earq.documento.status		
Definição	Indicação do grau de formalização do documento: *minuta* - versão preliminar do documento; *original* – primeiro documento completo e efetivo; *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. Manter um controle sobre a disposição de cópias.		
Aplica-se a	Processo | Dossiê **NA**	Volume **NA**	Documento **O**
Repetibilidade	-	-	Não repetível
Nota de aplicação	Deverá haver relacionamento entre os vários graus de formalização dos documentos. A organização deverá ter um plano de organização e registro do status dos documentos e da forma de relacioná-los. No caso do SIGAD apoiar a elaboração de documentos, o metadado status registra o grau de formalização do documento: minuta, quando ainda está sendo elaborado; original, quando se torna completo e efetivo; cópia, quando é feita uma reprodução a partir do original. Em geral, as minutas não são capturadas, ou seja, não são registradas e arquivadas no espaço geral. No entanto, em alguns casos, minutas de documentos avulsos são inseridas em um processo/dossiê, para fins de análise e prosseguimento da ação.		
Exemplos	--		
Regra de preenchimento	Deve, preferencialmente, ser gerado automaticamente pelo SIGAD. Valores sugeridos: minuta, original, cópia.		
Requisito	6.2.1		
Equivalência	--		

1.10. Identificador de versão

Designação	Identificador de versão		
Rótulo	earq.documento.versao		
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 **NA**	Volume **NA**	Documento **OA**
Repetibilidade	-	-	Não repetível
Nota de aplicação	Registrar informações relativas a: identificador da versão, descrição de alterações, data/hora da produção da versão e da transmissão, e o relacionamento entre as versões. Versões de documentos podem integrar processos e/ou dossiês.		
Exemplos	--		
Regra de preenchimento	É recomendável que seja gerado automaticamente pelo SIGAD.		
Requisito	2.1.4 / 2.1.17 / 6.2.2		
Equivalência	e-PMG: identificador.versao		

1.11. Título

Designação	Título		
Rótulo	dc.title		
Definição	Elemento de descrição que nomeia o documento ou processo/dossiê. Pode ser formal ou atribuído: *formal* - designação registrada no documento; *atribuído* - designação providenciada para identificação de um documento formalmente desprovido de título.		
Objetivo	Identificar o documento. Servir como elemento de acesso ao documento.		
Aplica-se a	Processo/dossiê **F**	Volume **NA**	Documento **O**
Repetibilidade	Não repetível	-	Não repetível
Nota de aplicação	--		
Exemplos	*Processo de aquisição de equipamentos de informática;* *Balancete da Universidade ACD 2007.*		
Regra de preenchimento	Cada instituição deverá fixar critérios para títulos atribuídos.		
Requisito	2.1.4 / 4.2.6 / 5.5.2		
Equivalência	Nobrade: 1.2 Título e-PMG: Título (*Title*) Dublin Core: Título (*dc.title*)		

1.12. Descrição

Designação	Descrição		
Rótulo	dc.description		
Definição	Exposição concisa do conteúdo do documento, processo ou dossiê.		
Objetivo	Identificar o conteúdo do documento. Facilitar a pesquisa.		
Aplica-se a	Processo/dossiê **F**	Volume **NA**	Documento **F**
Repetibilidade	Não repetível	-	Não repetível
Nota de aplicação			
Exemplos	*Convênio de cooperação para desenvolvimento de aplicações do laser entre a instituição A e a instituição B, com recursos do Programa Nacional ABC.*		
Regra de preenchimento	Cada instituição deverá fixar critérios e modelos com elementos básicos para a elaboração da descrição.		
Requisito	2.1.4 / 2.1.10		
Equivalência	e-PMG: Descrição (*description.abstract*) Dublin Core: Descrição (*dc.description*)		

1.13. Assunto

Designação	Assunto		
Rótulo	dc.subject		
Definição	Palavras-chave que representam o conteúdo do documento. Diferente do já estabelecido no código de classificação.		
Objetivo	Referir de forma sucinta o teor geral do documento.		
Aplica-se a	Processo/dossiê **F**	Volume **NA**	Documento **F**
Repetibilidade	Repetível	-	Repetível
Nota de aplicação	As instituições devem definir sua política de indexação.		
Exemplos	--		
Regra de preenchimento	Pode ser de preenchimento livre ou com o uso de vocabulário controlado ou tesauro.		
Requisito	2.1.4 / 2.1.10 / 4.2.6		
Equivalência	e-PMG: Assunto.palavra-chave (*subject.keyword*) Dublin Core: Assunto (*dc.subject*)		

1.14. Autor

Designação	Autor		
Rótulo	earq.documento.autor earq.processo.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. Fornecer informação sobre o contexto de produção do documento. Demonstrar a autenticidade de um documento, indicando o responsável direto pela sua produção.		
Aplica-se a	Processo/dossiê **O**	Volume **NA**	Documento **O**
Repetibilidade	Repetível	-	Repetível
Nota de aplicação	Não confundir com autor de processo judicial (autor x réu).		
Exemplos	*Santos, José ou José Santos* *Ministério da Justiça*		
Regra de preenchimento	As instituições devem estabelecer normas para controlar as entradas de nomes.		
Requisito	2.1.4 / 4.2.6		
Equivalência	Nobrade: 1.2 Título[54] e-PMG: criador.autor (*creator.autor*)		

54 De acordo com a *Norma brasileira de descrição arquivística* – Nobrade (2006), o autor deve ser registrado como um subelemento do título. Disponível em: https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/nobrade.pdf. Acesso em: 4 fev. 2022.

1.15. Destinatário

Designação	Destinatário		
Rótulo	earq.documento.destinatario earq.processo.destinatario		
Definição	Pessoa física e/ou jurídica a quem foi dirigida a informação contida no documento. Pode ser nominal ou geral: *nominal* – pessoas específicas; *geral* – refere-se a uma entidade maior, indeterminada. Ex.: cidadãos, povo, estudantes, a quem possa interessar, a todos os envolvidos.		
Objetivo	Identificar o destinatário do documento. Fornecer informação sobre o contexto de produção do documento. Demonstrar a autenticidade de um documento, indicando a quem ele é dirigido.		
Aplica-se a	Processo/dossiê **F**	Volume **NA**	Documento **O**
Repetibilidade	Repetível	-	Repetível
Nota de aplicação	--		
Exemplos	*Santos, José ou José Santos* *Ministério da Economia* *Cidadãos brasileiros*		
Regra de preenchimento	As instituições devem estabelecer normas para controlar as entradas de nomes.		
Requisito	2.1.4		
Equivalência	e-PMG: Destinatário (*addressee*)		

1.16. Originador

Designação	Originador		
Rótulo	earq.documento.originador		
Definição	Pessoa física ou jurídica designada no endereço eletrônico ou login em que o documento é gerado e/ou enviado.		
Objetivo	Identificar o originador do documento. Fornecer informação sobre o contexto de produção do documento. Demonstrar a autenticidade de um documento, indicando o responsável legal pela sua emissão.		
Aplica-se a	Processo/dossiê **NA**	Volume **NA**	Documento **OA**
Repetibilidade	-	-	Não repetível
Nota de aplicação	Aplica-se quando o nome do originador for diferente do nome do autor ou do redator.		
Exemplos	*Santos, José ou José Santos*		
Regra de preenchimento	As instituições devem estabelecer normas para controlar as entradas de nomes.		
Requisito	2.1.4 / 4.2.6		
Equivalência	--		

1.17. Redator

Designação	Redator		
Rótulo	earq.documento.redator		
Definição	Responsável pela elaboração do conteúdo do documento.		
Objetivo	Identificar o redator do documento. Fornecer informação sobre o contexto de produção do documento. Demonstrar a autenticidade de um documento, indicando o responsável pela articulação de seu conteúdo.		
Aplica-se a	Processo/dossiê **NA**	Volume **NA**	Documento **O**
Repetibilidade	-	-	Repetível
Nota de aplicação	Registrar mesmo quando o nome do redator for igual ao nome do autor.		
Exemplos	*Santos, José ou José Santos*		
Regra de preenchimento	As instituições devem estabelecer normas para controlar as entradas de nomes.		
Requisito	2.1.4 / 4.2.6		
Equivalência	--		

1.18. Interessado

Designação	Interessado		
Rótulo	earq.documento.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 **O**	Volume **NA**	Documento **NA**
Repetibilidade	Repetível	-	-
Nota de aplicação	O interessado pode ser qualificado como, por exemplo: réu, vítima, inventariante, inventariado, apelante, apelado, requerente, solicitante. Esse metadado deve ser registrado de forma estruturada, em dois subelementos, conforme a seguir: interessadoNome interessadoTipo		
Exemplos	interessadoId: *José da Silva* interessadoTipo: solicitante interessadoId: *987.745.465-73 (CPF)* interessadoTipo: requerente interessadoId: *59873/0001-38 (CNPJ)* interessadoTipo: apelado interessadoId: *8783000238 (número de matrícula)* interessadoTipo: vítima		
Regra de preenchimento	As instituições devem estabelecer normas para controlar as entradas de nomes. Pode-se fazer o cadastro de interessados internos da organização por categorias para facilitar o registro automático, com dados de identificação. Ex.: número de matrícula, nome, documento de identificação.		
Requisito	2.1.5 / 4.2.6		
Equivalência	--		

1.19. Identificador do componente digital

Designação	Identificador do componente digital		
Rótulo	earq.componente.id		
Definição	Identificador dos componentes digitais que integram o documento.		
Objetivo	Estabelecer a relação entre o documento e os componentes digitais necessários para apresentá-lo.		
Aplica-se a	Processo/dossiê **NA**	Volume **NA**	Documento **O**
Repetibilidade	-	-	Repetível
Nota de aplicação	Um documento pode ser formado por um ou mais componentes digitais, que são os componentes físicos do documento. De forma geral, pode se dizer que os componentes digitais são os arquivos de computador que formam um documento. Cada componente deve ser identificado individualmente a fim de que o documento possa ser recuperado de maneira completa.		
Exemplos	*Um documento multimídia pode estar armazenado em diversos arquivos com as informações de texto, imagens, som e relação entre eles. É necessário que o sistema computacional leia cada um deles para apresentá-lo ao usuário.* *Um documento em formato .pdf com assinatura digital externa a ele, armazenado em dois componentes digitais.* *A mesma situação aplica-se a documentos estruturados em bases de dados.*		
Regra de preenchimento	Deve ser preenchido a partir do metadado Identificador do componente digital: componente.Id.		
Requisito	2.1.6 / 2.1.8 / 2.1.20		
Equivalência	--		

1.20. Gênero

Designação	Gênero		
Rótulo	earq.documento.genero		
Definição	Indica o gênero documental, ou seja, a configuração da informação no documento de acordo com o sistema de signos utilizado na comunicação do documento.		
Objetivo	Monitorar os diversos gêneros documentais de um acervo para fins de gestão arquivística. Facilitar a pesquisa.		
Aplica-se a	Processo/dossiê **NA**	Volume **NA**	Documento **F**
Repetibilidade	--	--	Não repetível
Nota de aplicação	--		
Exemplos	*Audiovisual; textual; cartográfico; iconográfico; multimídia*.		
Regra de preenchimento	É necessário que a instituição elabore uma tabela com os gêneros e suas designações, para facilitar sua indicação no registro.		
Requisito	2.1.4		
Equivalência	Nobrade: 1.5 Dimensão e suporte[55] e-PMG: Tipo[56] (*type*)		

55 A informação de dimensão deve ser registrada associada ao gênero.

56 No caso de documentos arquivísticos, deve-se informar o gênero do documento nesse elemento.

1.21. Espécie

Designação	Espécie		
Rótulo	earq.documento.especie		
Definição	Indica a espécie documental, ou seja, a configuração da informação no documento de acordo com a disposição e a natureza das informações nele contidas.		
Objetivo	Complementar a descrição do documento ou a identificação de título. Facilitar a pesquisa.		
Aplica-se a	Processo/dossiê **NA**	Volume **NA**	Documento **F**
Repetibilidade	-	-	Não repetível
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. Relaciona-se com tipo documental; descrição e título.		
Exemplos	*Processo; ofício; ata; relatório; projeto; prontuário.*		
Regra de preenchimento	--		
Requisito	2.1.4		
Equivalência	Nobrade: 1.5 Dimensão e suporte[57]		

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

1.22. 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 à descrição do documento ou à identificação do título. Permite a pesquisa limitada a um determinado tipo.		
Aplica-se a	Processo/dossiê **NA**	Volume **NA**	Documento **F**
Repetibilidade	-	-	Não repetível
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. Relaciona-se com espécie documental.		
Exemplos	*Relatório de pesquisa; carta precatória; ofício-circular; prontuário médico; prontuário de funcionário.*		
Regra de preenchimento	--		
Requisito	2.1.4		
Equivalência	Nobrade: 1.5 Dimensão e suporte[58]		

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

1.23. Idioma

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

1.24. Quantidade de folhas

Designação	Quantidade de folhas		
Rótulo	earq.documento.folhaNum earq.volume.folhaNum earq.processo.folhaNum		
Definição	Indicação da quantidade de folhas de um documento.		
Objetivo	Permitir o controle de folhas por processo e por volume. Facilitar o registro e o acesso a um documento específico dentro do processo ou dossiê.		
Aplica-se a	Processo/dossiê **OA**	Volume **OA**	Documento **F**
Repetibilidade	Não repetível	Não repetível	Não repetível
Nota de aplicação	Usado especialmente para gerenciamento de processos não digitais, que limitam a quantidade de folhas, sugerindo a abertura de volumes. As instituições devem determinar as normas para esse tipo de ação.		
Exemplos	--		
Regra de preenchimento	--		
Requisito	5.3.3 / Ver seção 5.4 (Volumes: abertura, encerramento e metadados)		
Equivalência	--		

1.25. Numeração sequencial dos documentos

Designação	Numeração sequencial dos documentos		
Rótulo	earq.documento.sequencia		
Definição	Numeração sequencial dos documentos inseridos em um processo.		
Objetivo	Ordenar os documentos em um processo. Controlar a integridade do processo. Facilitar a referência a um documento específico.		
Aplica-se a	Processo/dossiê **NA**	Volume **NA**	Documento **OA** *aplica-se somente aos documentos que integram um processo.
Repetibilidade	-	-	Não repetível
Nota de aplicação	Usado para ordenar os documentos (e não as folhas) nos processos digitais.		
Exemplos	--		
Regra de preenchimento	Devem-se numerar os documentos na ordem em que são inseridos no processo a fim de garantir sua integridade.		
Requisito	5.3.3		
Equivalência	--		

1.26. Indicação de anexos

Designação	Indicação de anexos		
Rótulo	earq.documento.anexo		
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 **NA**	Volume **NA**	Documento **O**
Repetibilidade	-	-	Não repetível
Exemplos	--		
Regra de preenchimento	--		
Requisito	2.1.4		
Equivalência	--		

1.27. Indicação de anotação

Designação	Indicação de anotação		
Rótulo	earq.documento.anotacao		
Definição	Indica se o documento tem anotações.		
Objetivo	Registrar a existência de anotações feitas em um documento após sua emissão, para apoiar sua autenticidade.		
Aplica-se a	Processo/dossiê **NA**	Volume **NA**	Documento **O**
Repetibilidade	-	-	Não repetível
Exemplos	*Algumas anotações comuns são: ciente, circular para ciência, grifos, atribuição de tarefas.*		
Regra de preenchimento	O sistema indica apenas se existe anotação. Os valores possíveis são: sim / não. A anotação em si ***é*** registrada em outro metadado ou em campo específico e deve ser exibida junto com o documento.		
Requisito	2.1.4		
Equivalência	--		

1.28. Unidade responsável pela execução da ação

Designação	Unidade responsável pela execução da ação		
Rótulo	earq.documento.unidadeExecucao		
Definição	Registra a unidade responsável pela execução da ação registrada no documento.		
Objetivo	Indicar a principal unidade responsável pela ação e que fica responsável pela guarda do documento antes da sua transferência, recolhimento ou eliminação.		
Aplica-se a	Processo/dossiê **NA**	Volume **NA**	Documento **O**
Repetibilidade	-	-	Não repetível
Exemplos	*Setor de compras e licitação (no caso de processos de aquisição), unidade de recursos humanos (no caso de dossiê funcional), unidade de administração escolar (dossiês dos alunos).*		
Regra de preenchimento	Preencher com o nome da unidade.		
Requisito	2.1.4		
Equivalência	--		

1.29. Relação com outros documentos

Designação	Relação com outros documentos		
Rótulo	dc.Relation		
Qualificadores	dc.Relation.isReferencedBy dc.Relation.References	Referências a outros documentos.	
	dc.Relation.isPartOf dc.Relation.hasPart	Relaciona extrato de documento com o documento original.	
Definição	Registro das relações significantes de um documento com outros documentos.		
Objetivo	Tornar explícito o relacionamento e facilitar o processamento automático e o gerenciamento arquivístico. Demonstrar a relação orgânica dos documentos. Facilitar a pesquisa de informações de documentos relacionados.		
Aplica-se a	Processo/dossiê **OA**	Volume **NA**	Documento **OA**
Repetibilidade	Repetível	-	Repetível
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: • referenciado ou ver também; • tem extrato, é extrato de. Os relacionamentos entre documento, volume e processo/dossiê são registrados em metadados específicos, tais como identificador do processo e identificador do dossiê.		
Exemplos	--		
Regra de preenchimento	--		
Requisito	2.1.4 / 2.1.9 / 2.4 / 12.1.21		
Equivalência	e-PMG: Relação (*Relation*) Dublin Core: Relação (*dc.Relation*)		

1.30. Níveis de acesso

Designação	Níveis de acesso		
Rótulo	earq.nivelDeAcesso		
Definição	Indicação dos níveis de acesso ao documento a partir da classificação de sigilo e da proteção de dados pessoais.		
Objetivo	Garantir o acesso somente a pessoas autorizadas.		
Aplica-se a	Processo/dossiê **O**	Volume **NA**	Documento **O**
Repetibilidade	Repetível	-	Repetível
Nota de aplicação	As instituições devem estabelecer as normas para as condições de acesso e indicação de sigilo, de acordo com seu contexto e com base na legislação. Relaciona-se com tabela de classificação de segurança.		
Exemplos	*Ostensivo* *Reservado* *Secreto* *Ultrassecreto* *Sigilo fiscal* *Informação pessoal* *Patente*		
Regra de preenchimento	Deve ser informado se o documento é ostensivo ou se possui algum grau de sigilo, indicando o nível de sigilo e demais hipóteses de sigilo.		
Requisito	2.1.4 / 7.3.1 / 7.3.2		
Equivalência	Nobrade: 4.1 condições de acesso e-PMG:Direitos.classificacaodoGrauDesigilo (*rights.descriptor*) Dublin Core: Direitos (*dc.rights*)		

1.31. Previsão de desclassificação

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

1.32. Data de produção

Designação	Data de produção		
Rótulo	dc.date.created		
Definição	Registro cronológico (data e hora) da produção do documento.		
Objetivo	Indicar local e data em que foi produzido o documento.		
Aplica-se a	Processo/dossiê **O**	Volume **NA**	Documento **O**
Repetibilidade	Não repetível	--	Não repetível
Nota de aplicação	--		
Exemplos	--		
Regra de preenchimento	É recomendável seguir o padrão da ISO 8601.		
Requisito	2.1.4 / 2.3.1 / 4.2.6 / 5.2.1		
Equivalência	Nobrade: 1.3 Data(s) e-PMG: data.criação (*date.created*) Dublin Core: Data (*dc.date.created*)		

1.33. Local de produção

Designação	Local de produção		
Rótulo	earq.documento.local		
Definição	Registro do local da produção do documento, também denominado de data tópica.		
Objetivo	Indicar local em que foi produzido o documento.		
Aplica-se a	Processo/dossiê **NA**	Volume **NA**	Documento **O**
Repetibilidade	-	-	Não repetível
Nota de aplicação	--		
Exemplos	--		
Regra de preenchimento	--		
Requisito	2.1.4 / 2.3.1 / 4.2.6 / 5.2.1		
Equivalência	Nobrade: 1.3 Data(s)		

1.34. Classe

Designação	Classe		
Rótulo	earq.classeId		
Definição	Identificação da classe[59] 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 **O**	Volume **NA**	Documento **O**
Repetibilidade	Não repetível	-	Não repetível
Nota de aplicação	As instituições devem estabelecer um plano de classificação para aplicar esse elemento.		
Exemplos	--		
Regra de preenchimento	Pode se registrar o código e/ou o nome completo da classe em que o documento está classificado.		
Requisito	1.3.1 / 2.1.4 / 2.1.9 / 4.2.6 / 5.4.3		
Equivalência	--		

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

1.35. Destinação prevista

Designação	Destinação prevista		
Rótulo	earq.documento.destinacao earq.processo.destinacao		
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 **O**	Volume **NA**	Documento **O**
Repetibilidade	Não repetível	-	Não repetível
Nota de aplicação	Para a finalidade deste instrumento, considera-se a transferência como uma ação de destinação. As instituições devem estabelecer uma tabela de temporalidade associada ao plano de classificação para aplicar este elemento. Este elemento está relacionado ao *1.33*.		
Exemplos	--		
Regra de preenchimento	Deve ser preenchido de forma automática pelo SIGAD. Valores permitidos: eliminação, transferência e recolhimento.		
Requisito	1.3.13 / 3.1.4 / 5.4.3		
Equivalência	Nobrade: 3.2 Avaliação, eliminação e temporalidade[60] e-PMG: Destinação.ação (*disposal.action*)		

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

1.36. Prazo de guarda

Designação	Prazo de guarda		
Rótulo	earq.documento.prazoGuarda earq.processo.prazoGuarda		
Definição	Indicação do prazo estabelecido em tabela de temporalidade e destinação de documentos para o cumprimento da destinação.		
Objetivo	Apoiar o controle do ciclo de vida do documento.		
Aplica-se a	Processo/dossiê **O**	Volume **NA**	Documento **O**
Repetibilidade	Não repetível	-	Não repetível
Nota de aplicação	As instituições devem estabelecer uma tabela de temporalidade e destinação de documentos associada ao plano de classificação para aplicar esse elemento. Este elemento está relacionado ao *1.32*.		
Exemplos	--		
Regra de preenchimento	Deve ser preenchido de forma automática pelo SIGAD.		
Requisito	1.3.13/ 2.1.4 / 3.1.4 / 5.4.3		
Equivalência	Nobrade: 3.2 Avaliação, eliminação e temporalidade[61] e-PMG: Destinação.prazoDeGuarda (*disposal.timePeriod*)		

61 Idem ao anterior.

1.37. Localização

Designação	Localização		
Rótulo	earq.documento.localização earq.volume.localização earq.processo.localização		
Definição	Local de armazenamento atual do documento. Pode ser um lugar (depósito, estante, repositório digital), uma notação física.		
Objetivo	Permitir a localização dos documentos em qualquer mídia. Monitorar o armazenamento de documentos.		
Aplica-se a	Processo/dossiê **OA**	Volume **F**	Documento **OA**
Repetibilidade	Não repetível	Não repetível	Não repetível
Nota de aplicação	Deve ser utilizado, obrigatoriamente, quando o documento é mantido em outra área de armazenamento, seja virtual ou física. Utilizado principalmente para os documentos não digitais, para a parte não digital dos documentos híbridos.		
Exemplos	*Depósito 201, estante 8, prateleira 2;* *Caixa 3.456;* *Centro de documentação do IFP, repositório alfa;* *Notação XY.2540.*		
Regra de preenchimento	As instituições devem estabelecer normas para o registro da localização dos documentos não digitais, de acordo com seu ambiente de guarda e armazenamento.		
Requisito	2.1.4 / 2.4.1 / 2.4.2 / 5.5.1 / 5.5.3 / 5.5.4 / 5.5.7 / 7.10.3		
Equivalência	e-PMG: Locao (*location*)		

2 Eventos de gestão

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

2.1. Eventos de gestão do ciclo de vida

Registra os eventos de captura, movimentação e controle do ciclo de vida do documento e processo/dossiê. Cada evento deve ser registrado pelo seguinte conjunto de elementos de metadados:

1. Identificador do evento
2. Tipo de evento
3. Identificador do processo/dossiê
4. Identificador do documento
5. Identificador do lote
6. Data e hora do evento
7. Agente responsável pelo evento
8. Detalhe do evento

Os eventos de gestão do ciclo de vida previstos são:

ECV1. Captura

Descreve a captura do documento.

ECV2. Transferência – Envio

Registro do envio de transferência de documentos.

Registrar no elemento *Detalhe do evento* informações complementares, tais como: método utilizado para o envio, localização, suporte, número do termo de transferência.

Deve ser feito um registro para cada lote transferido.

ECV3. Transferência – Recebimento

Registro do recebimento da transferência de documentos.

Registrar no elemento *Detalhe do evento* informações complementares, tais como: localização, suporte, identificador do ECV2 correspondente.

Deve ser feito um registro para cada lote transferido.

ECV4. Recolhimento – Envio

Registro do envio de recolhimento de documentos.

Registrar no elemento *Detalhe do evento* informações complementares, tais como: método utilizado para o envio, localização, suporte, número do termo de recolhimento.

ECV5. Eliminação

Registro do procedimento de eliminação.

Registrar no elemento *Detalhe do evento* informações complementares, tais como: tipo de procedimento (fragmentação, desmagnetização, doação etc.), número do termo de eliminação, número do edital.

Nota: a eliminação é precedida por uma avaliação, feita fora do sistema e que subsidia a decisão de eliminação.

ECV6. Restrição de acesso

Registro do procedimento de classificação de sigilo e de marcação de outras hipóteses de sigilo e restrição de acesso.

Quanto à classificação de sigilo, registrar no elemento *Detalhe do evento* informações complementares, tais como: grau de sigilo, fundamentação legal, data prevista para desclassificação.

Quanto às demais hipóteses de sigilo, registrar no elemento *Detalhe do evento* informações complementares, tais como: tipo de restrição de acesso (informação pessoal, bancária, fiscal, propriedade industrial), previsão de prazo para cessação da restrição (quando for o caso), justificativa.

ECV7. Alteração da restrição de acesso

Registro do procedimento de alteração da restrição de acesso, que pode ser a remoção da restrição ou a reclassificação (no caso da classificação de sigilo).

Quanto à desclassificação ou reclassificação de sigilo, registrar no elemento *Detalhe do evento* informações complementares, tais como: grau de sigilo, nova data prevista para desclassificação, motivação.

Quanto à retirada das demais hipóteses de sigilo, registrar no elemento *Detalhe do evento* informações complementares, tais como: tipo de restrição de acesso (informação pessoal, bancária, fiscal, propriedade industrial), justificativa.

2.1.1. Identificador do evento

Designação	Identificador do evento
Rótulo	earq.eventoCv.id
Definição	Identificador do evento de ciclo de vida que está sendo registrado no SIGAD.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Regra de preenchimento	Deve ser registrado automaticamente pelo SIGAD.
Requisito	2.1.4 / 7.5.4 / 7.5.5 / 7.9.3 / 7.9.6 / 7.7.2 / 7.11.1 / 7.11.9/ 7.12.7 / 8.2.6 / 8.3.1/ 8.3.6 / 9.3.1 / 9.3.2 / 9.3.3 / 9.3.4 / 9.3.5
Equivalência	--

2.1.2. Tipo de evento

Designação	Tipo de evento
Rótulo	earq.eventoCv.tipo
Definição	Identificação do tipo de evento de gestão do ciclo de vida.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Regra de preenchimento	Este elemento poderá assumir os seguintes valores: • Captura • Transferência – Envio • Transferência – Recebimento • Recolhimento – Envio • Eliminação • Atribuição de restrição de acesso • Desclassificação de Sigilo • Reclassificação de Sigilo
Requisito	2.1.4 / 7.5.4 / 7.5.5 / 7.9.3 / 7.9.6 / 7.7.2 / 7.11.1 / 7.11.9/ 7.12.7 / 8.2.6 / 8.3.1/ 8.3.6 / 9.3.1 / 9.3.2 / 9.3.3 / 9.3.4 / 9.3.5
Equivalência	--

2.1.3. Identificador do processo/dossiê

Designação	Identificador do processo/dossiê
Rótulo	earq.eventoCv.processoId
Definição	Identificador do processo/dossiê que está sendo afetado pelo evento.
Obrigatoriedade	**OA**
Repetibilidade	Repetível
Regra de preenchimento	O código deve ser obtido no metadado *1.4 identificador do processo/dossiê*.
Requisito	2.1.4 / 7.5.4 / 7.5.5 / 7.9.3 / 7.9.6 / 7.7.2 / 7.11.1 / 7.11.9/ 7.12.7 / 8.2.6 / 8.3.1/ 8.3.6 / 9.3.1 / 9.3.2 / 9.3.3 / 9.3.4 / 9.3.5
Equivalência	--

2.1.4. Identificador do documento

Designação	Identificador do documento
Rótulo	earq.eventoCv.documentoId
Definição	Identificador do documento.
Obrigatoriedade	**O**
Repetibilidade	Repetível
Regra de preenchimento	O código deve ser obtido no metadado *1.1 identificador do documento*. Obrigatório para eventos de transferência (ECV4 e ECV5), para identificar os documentos transferidos.
Requisito	2.1.4 / 7.5.4 / 7.5.5 / 7.9.3 / 7.9.6 / 7.7.2 / 7.11.1 / 7.11.9/ 7.12.7 / 8.2.6 / 8.3.1/ 8.3.6 / 9.3.1 / 9.3.2 / 9.3.3 / 9.3.4 / 9.3.5
Equivalência	--

2.1.5. Identificador do lote

Designação	Identificador do lote
Rótulo	earq.eventoCv.loteId
Definição	Identificador do lote que está sendo afetado pelo evento.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Regra de preenchimento	O código pode ser gerado automaticamente no evento Transferência-envio, Transferência-recebimento, Recolhimento e Eliminação.
Requisito	2.1.4 / 7.5.4 / 7.5.5 / 7.9.3 / 7.9.6 / 7.7.2 / 7.11.1 / 7.11.9/ 7.12.7 / 8.2.6 / 8.3.1/ 8.3.6 / 9.3.1 / 9.3.2 / 9.3.3 / 9.3.4 / 9.3.5
Equivalência	--

2.1.6. Data e hora do evento

Designação	Data e hora do evento
Rótulo	earq.eventoCv.dataHora
Definição	Data e hora que o evento foi realizado.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Regra de preenchimento	É recomendável seguir o padrão da ISO 8601:2019 – *Data elements and interchange formats — Information interchange — Representation of dates and times.*
Requisito	2.1.4 / 7.5.4 / 7.5.5 / 7.9.3 / 7.9.6 / 7.7.2 / 7.11.1 / 7.11.9/ 7.12.7 / 8.2.6 / 8.3.1/ 8.3.6 / 9.3.1 / 9.3.2 / 9.3.3 / 9.3.4 / 9.3.5
Equivalência	--

2.1.7. Agente responsável pelo evento

Designação	Agente responsável pelo evento
Rótulo	earq.eventoCv.agenteId
Definição	Agente responsável pela realização do evento. Captura: responsável pela captura Transferência – envio: responsável pelo envio dos documentos para guarda intermediária Transferência – recebimento: responsável pelo recebimento dos documentos para guarda intermediária Recolhimento – envio: responsável pelo envio dos documentos para guarda permanente Eliminação: responsável pela eliminação dos documentos Restrição de acesso: responsável pela restrição de acesso Alteração da restrição de acesso: responsável pela restrição de acesso
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Regra de preenchimento	O código deve ser obtido no metadado *4.2 identificador do agente*.
Requisito	2.1.4 / 7.5.4 / 7.5.5 / 7.9.3 / 7.9.6 / 7.7.2 / 7.11.1 / 7.11.9/ 7.12.7 / 8.2.6 / 8.3.1/ 8.3.6 / 9.3.1 / 9.3.2 / 9.3.3 / 9.3.4 / 9.3.5
Equivalência	--

2.1.8. Detalhes do evento

Designação	Detalhes do evento
Rótulo	earq.eventoCv.detalhe
Definição	Registro de informações adicionais a respeito do evento de gestão do ciclo de vida.
Obrigatoriedade	**OA**
Repetibilidade	Não repetível
Regra de preenchimento	Podem ser registradas informações tais como identificador do método de transferência; termo de transferência; identificador do termo de recolhimento; identificador do edital; fundamentação legal da classificação; motivação da desclassificação; justificativas; suporte; localização.
Requisito	2.1.4 / 7.5.4 / 7.5.5 / 7.9.3 / 7.9.6 / 7.7.2 / 7.11.1 / 7.11.9/ 7.12.7 / 8.2.6 / 8.3.1/ 8.3.6 / 9.3.1 / 9.3.2 / 9.3.3 / 9.3.4 / 9.3.5
Equivalência	--

2.2. Eventos de gestão do processo/dossiê

Registra os eventos relacionados aos procedimentos de protocolo realizados com os processos. Inclui também abertura, encerramento e reabertura de dossiês. Cada evento deve ser registrado pelo seguinte conjunto de elementos de metadados:

1 Identificador do evento

2 Tipo de evento

3 Identificador do processo/dossiê

4 Identificador do volume

5 Data e hora do evento

6 Agente responsável pelo evento

7 Identificador do documento

Os eventos de gestão de processo previstos são:

EPROC1 Abertura de volume/processo/dossiê

EPROC2 Encerramento de volume/processo/dossiê

EPROC3 Reabertura processo/dossiê

EPROC4 Juntada anexação

EPROC5 Juntada apensação

EPROC6 Desapensação

EPROC7 Desentranhamento

EPROC8 Desmembramento

EPROC9 Tramitação – Envio

EPROC10 Tramitação – Recebimento

2.2.1. Identificador do evento

Designação	Identificador do evento
Rótulo	earq.eventoCv.id
Definição	Identificador do evento de gestão de processo que está sendo registrado no SIGAD.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Regra de preenchimento	Deve ser registrado automaticamente pelo SIGAD.
Requisito	2.1.4 / 7.5.4 / 7.5.5 / 7.9.3 / 7.9.6 / 7.7.2 / 7.11.1 / 7.11.9/ 7.12.7 / 8.2.6 / 8.3.1/ 8.3.6 / 9.3.1 / 9.3.2 / 9.3.3 / 9.3.4 / 9.3.5
Equivalência	--

2.2.2. Tipo de evento

Designação	Tipo de evento
Rótulo	earq.eventoProc.tipo
Definição	Identificação do evento de gestão do processo.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Regra de preenchimento	Este elemento poderá assumir os seguintes valores: EPROC1. Abertura de volume/processo/dossiê EPROC2. Encerramento de volume/processo/dossiê EPROC3. Reabertura processo/dossiê EPROC4. Juntada anexação EPROC5. Juntada apensação EPROC6. Desapensação EPROC7. Desentranhamento EPROC8. Desmembramento EPROC9. Tramitação – Envio EPROC10. Tramitação – Recebimento
Requisito	2.1.4 / 7.5.4 / 7.5.5 / 7.9.3 / 7.9.6 / 7.7.2 / 7.11.1 / 7.11.9/ 7.12.7 / 8.2.6 / 8.3.1/ 8.3.6 / 9.3.1 / 9.3.2 / 9.3.3 / 9.3.4 / 9.3.5
Equivalência	--

2.2.3. Identificador do processo/dossiê

Designação	Identificador do processo/dossiê
Rótulo	earq.eventoProc.processoId
Definição	Identificador do processo.
Repetibilidade	Não repetível
Obrigatoriedade	**O**
Regra de preenchimento	O código deve ser obtido no metadado *1.4 identificador do processo/dossiê*.
Requisito	2.1.4 / 7.5.4 / 7.5.5 / 7.9.3 / 7.9.6 / 7.7.2 / 7.11.1 / 7.11.9/ 7.12.7 / 8.2.6 / 8.3.1/ 8.3.6 / 9.3.1 / 9.3.2 / 9.3.3 / 9.3.4 / 9.3.5
Equivalência	--

2.2.4. Identificador do volume

Designação	Identificador do volume
Rótulo	earq.eventoProc.volumeId
Definição	Identificador do volume.
Repetibilidade	Não repetível
Obrigatoriedade	**OA**
Regra de preenchimento	O código deve ser obtido no metadado *1.7 número do volume*. Esse metadado só deve ser registrado nos eventos de abertura e encerramento de volume.
Requisito	2.1.4 / 7.5.4 / 7.5.5 / 7.9.3 / 7.9.6 / 7.7.2 / 7.11.1 / 7.11.9/ 7.12.7 / 8.2.6 / 8.3.1/ 8.3.6 / 9.3.1 / 9.3.2 / 9.3.3 / 9.3.4 / 9.3.5
Equivalência	--

2.2.5. Data e hora do evento

Designação	Data e hora do evento
Rótulo	earq.eventoProc.dataHora
Definição	Data e hora que o evento foi realizado.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Regra de preenchimento	É recomendável seguir o padrão da ISO 8601:2019 – *Data elements and interchange formats — Information interchange — Representation of dates and times.*
Requisito	2.1.4 / 7.5.4 / 7.5.5 / 7.9.3 / 7.9.6 / 7.7.2 / 7.11.1 / 7.11.9/ 7.12.7 / 8.2.6 / 8.3.1/ 8.3.6 / 9.3.1 / 9.3.2 / 9.3.3 / 9.3.4 / 9.3.5
Equivalência	--

2.2.6. Agente responsável pelo evento

Designação	Agente responsável pelo evento
Rótulo	earq.eventoProc.agenteId
Definição	Agente responsável pela realização do evento.
Obrigatoriedade	**OA**
Repetibilidade	Não repetível
Regra de preenchimento	O código deve ser obtido no metadado *4.2 identificador do agente*.
Requisito	2.1.4 / 7.5.4 / 7.5.5 / 7.9.3 / 7.9.6 / 7.7.2 / 7.11.1 / 7.11.9/ 7.12.7 / 8.2.6 / 8.3.1/ 8.3.6 / 9.3.1 / 9.3.2 / 9.3.3 / 9.3.4 / 9.3.5
Equivalência	--

2.2.7. Identificador do documento

Designação	Identificador do documento
Rótulo	earq.eventoProc.DocId
Definição	Identificador do documento.
Obrigatoriedade	**OA**
Repetibilidade	Repetível
Regra de preenchimento	Obrigatório para o evento EPROC7 para registrar os documentos que foram desentranhados.
Requisito	2.1.4 / 7.5.4 / 7.5.5 / 7.9.3 / 7.9.6 / 7.7.2 / 7.11.1 / 7.11.9/ 7.12.7 / 8.2.6 / 8.3.1/ 8.3.6 / 9.3.1 / 9.3.2 / 9.3.3 / 9.3.4 / 9.3.5
Equivalência	--

3 Classe

Estas informações referem-se à configuração e à administração do plano ou código de classificação e da tabela de temporalidade e destinação de documentos.

Esses metadados registram as informações descritivas relativas a cada uma das classes do plano ou código de classificação, incluindo a temporalidade e a destinação previstas.

3.1. Identificador da classe

Designação	Identificador da classe
Rótulo	earq.classe.id
Definição	Identificador único atribuído pelo SIGAD à classe no ato de sua criação no sistema.
Objetivo	Identificar de forma unívoca a classe para que o SIGAD possa gerenciá-la.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Nota de aplicação	Refere-se às classes, subclasses, grupos e subgrupos.
Exemplos	--
Regra de preenchimento	Deve, preferencialmente, ser gerado de forma automática pelo SIGAD.
Requisito	--
Equivalência	--

3.2. Nome da classe

Designação	Nome da classe
Rótulo	earq.classe.nome
Definição	Nome de uma divisão de um plano ou de um código de classificação.
Objetivo	Registrar a denominação das diversas classes[62] do plano ou código de classificação adotado.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Nota de aplicação	Refere-se às classes, subclasses, grupos e subgrupos.
Exemplos	*"Pessoal", "Recrutamento e seleção", "Material permanente" e "Compra".*
Regra de preenchimento	Registrar a denominação específica da classe, sem repetir a do nível hierárquico superior.
Requisito	1.1.11
Equivalência	--

62 Recorda-se que para fins deste documento a menção à classe refere-se a todos os níveis do plano ou código de classificação: classe, subclasse, grupo e subgrupo.

3.3. Código da classe

Designação	Código da classe
Rótulo	earq.classe.codigo
Definição	Código relativo a uma divisão de um plano ou de um código de classificação.
Objetivo	Registrar o código atribuído à classe respectiva.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Nota de aplicação	Refere-se às classes, subclasses, grupos e subgrupos.
Exemplos	*020, 021, 033.1, 033.11*
Regra de preenchimento	--
Requisito	1.1.11
Equivalência	--

3.4. Subordinação da classe

Designação	Subordinação da classe
Rótulo	earq.classe.subordinacao
Definição	Subordinação da classe na hierarquia do plano de classificação ou do código de classificação.
Objetivo	Recuperar a relação hierárquica das diversas classes de um plano ou código de classificação.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Nota de aplicação	A obrigatoriedade não se aplica às classes de primeiro nível.
Exemplos	*033 (código hierárquico superior ao 033.1)*
Regra de preenchimento	Registrar o código da classe imediatamente superior.
Requisito	1.1.13
Equivalência	--

3.5. Indicação de permissão de uso

Designação	Indicação de permissão de uso
Rótulo	earq.classe.indicadorUso
Definição	Indicação se a classe pode ser utilizada para classificar documentos ou se é apenas parte da estrutura hierárquica do plano de classificação.
Objetivo	Apoiar o SIGAD para restringir o uso apenas das classes autorizadas para classificar documentos.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Nota de aplicação	Uma classe sem permissão de uso para classificar não pode ser subordinada a uma classe com permissão de uso.
Exemplos	--
Regra de preenchimento	Valores previstos: sim ou não.
Requisito	1.1.12
Equivalência	--

3.6. Indicação de classe ativa/inativa

Designação	Indicação de classe ativa/inativa
Rótulo	earq.classe.indicadorAtiva
Definição	Indicação se a classe está ativa ou inativa para uso.
Objetivo	Apoiar o SIGAD para restringir o uso apenas das classes ativas na classificação de novos documentos.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Nota de aplicação	As classes inativas são aquelas que não são mais utilizadas, mas que não podem ser eliminadas devido ao fato de existirem documentos nela classificados anteriormente.
Exemplos	--
Regra de preenchimento	Valores previstos: ativa ou inativa.
Requisito	1.1.4 / 1.1.7 / 1.1.8
Equivalência	--

3.7. Prazo na idade corrente

Designação	Prazo na idade corrente
Rótulo	earq.classe.prazoCorrente
Definição	Prazo de guarda previsto para a idade corrente.
Objetivo	Apoiar o SIGAD na contagem do tempo de guarda do documento na idade corrente.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Nota de aplicação	Esse elemento é utilizado pelo SIGAD em conjunto com o elemento *Evento de contagem na idade corrente* para identificar os documentos que já atingiram o prazo previsto.
Exemplos	*6 meses, 2 anos, 7 anos.*
Regra de preenchimento	Preencher conforme o prazo previsto na tabela de temporalidade e destinação de documentos. No caso do prazo previsto na tabela de temporalidade e destinação de documentos ser "enquanto vigora", o valor do elemento *Prazo na idade corrente* será 0 (zero), associado ao evento "fim da vigência do documento".
Requisito	1.2.2
Equivalência	--

3.8. Evento de contagem na idade corrente

Designação	Evento de contagem na idade corrente
Rótulo	earq.classe.eventoCorrente
Definição	Evento que dispara o início da contagem do prazo de guarda na idade corrente.
Objetivo	Apoiar o SIGAD na contagem do tempo de guarda do documento na idade corrente.
Obrigatoriedade	OA
Repetibilidade	Não repetível
Nota de aplicação	Esse elemento é utilizado pelo SIGAD em conjunto com o elemento *Prazo na idade corrente* para identificar os documentos que já atingiram o prazo previsto.
Exemplos	*Eventos: aprovação de contas, fim da vigência do documento, permanência do servidor público na instituição, conclusão do caso, trânsito em julgado.*
Regra de preenchimento	Preencher conforme previsto na tabela de temporalidade e destinação de documentos. Quando o evento não for especificado, considera-se o arquivamento como evento de início da contagem do prazo de guarda.
Requisito	1.2.2
Equivalência	--

3.9. Prazo na idade intermediária

Designação	Prazo na idade intermediária
Rótulo	earq.classe.prazoIntermediaria
Definição	Prazo de guarda previsto para a idade intermediária.
Objetivo	Apoiar o SIGAD na contagem do tempo de guarda do documento na idade intermediária.
Obrigatoriedade	**OA**
Repetibilidade	Não repetível
Nota de aplicação	Esse elemento é utilizado pelo SIGAD em conjunto com o elemento *Evento de contagem na idade intermediária* para identificar os documentos que já atingiram o prazo previsto.
Exemplos	*6 meses, 2 anos, 7 anos.*
Regra de preenchimento	Preencher conforme o prazo previsto na tabela de temporalidade e destinação de documentos.
Requisito	1.2.2
Equivalência	--

3.10. Evento de contagem na idade intermediária

Designação	Evento de contagem na idade intermediária
Rótulo	earq.classe.eventoIntermediaria
Definição	Evento que dispara o início da contagem do prazo de guarda na idade intermediária.
Objetivo	Apoiar o SIGAD na contagem do tempo de guarda do documento na idade intermediária.
Obrigatoriedade	**OA**
Repetibilidade	Não repetível
Nota de aplicação	Esse elemento é utilizado pelo SIGAD em conjunto com o elemento *Prazo na idade intermediária* para identificar os documentos que já atingiram o prazo previsto.
Exemplos	*Eventos: aprovação de contas, vigência do contrato, permanência do servidor público na instituição, conclusão do caso, trânsito em julgado.*
Regra de preenchimento	Preencher conforme previsto na tabela de temporalidade e destinação de documentos. Quando o evento não for especificado, considera-se a transferência como evento de início da contagem do prazo de guarda.
Requisito	1.2.2
Equivalência	--

3.11. Destinação final

Designação	Destinação final
Rótulo	earq.classe.destinacao
Definição	Destinação final prevista para o documento: preservação ou eliminação.
Objetivo	Apoiar o SIGAD na produção das listagens de eliminação e de recolhimento.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Nota de aplicação	--
Exemplos	--
Regra de preenchimento	Preencher conforme previsto na tabela de temporalidade e destinação de documentos. Valores previstos: eliminação ou preservação.
Requisito	1.2.2
Equivalência	--

3.12. Sigilo associado à classe

Designação	Sigilo associado à classe
Rótulo	earq.classe.sigilo
Definição	Restrição de acesso aos documentos, aplicada de forma geral aos documentos de uma classe.
Objetivo	Automatizar a atribuição de restrição de acesso a documentos que possuam informação pessoal, sensível e outras previstas em legislação vigente.
Obrigatoriedade	**OA**
Repetibilidade	Não repetível
Nota de aplicação	Aplica-se a restrição de acesso aos documentos que possuam informação pessoal, sensível e outras previstas em legislação vigente. O valor previsto nesse elemento da classe deve ser herdado automaticamente pelo documento (elemento de identificação do documento – *Níveis de acesso*) no momento da classificação. Não confundir com a atribuição de grau de sigilo (confidencial, reservado, secreto e ultrassecreto) a documentos.
Exemplos	*Informação pessoal (no caso da classe Apuração de responsabilidade e ação disciplinar).*
Regra de preenchimento	Utilizar os valores previstos para o elemento de identificação do documento – *Níveis de acesso,* excetuando-se os relativos à atribuição de grau de sigilo (confidencial, reservado, secreto e ultrassecreto).
Requisito	1.1.12
Equivalência	--

3.13. Observação

Designação	Observação
Rótulo	earq.classe.observacao
Definição	Registra informações adicionais sobre a classe.
Objetivo	Registrar informações não previstas que podem ser relevantes para a gestão de documentos.
Obrigatoriedade	**F**
Repetibilidade	Não repetível
Nota de aplicação	--
Exemplos	*Informações complementares tais como: previsão de conversão de suporte, legislação sobre os prazos de guarda.*
Regra de preenchimento	--
Requisito	1.2.2
Equivalência	--

4 Eventos de gerenciamento da classe

Registra os eventos de gerenciamento do plano ou do código de classificação.

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

1 Identificador do evento

2 Tipo de evento

3 Identificador da classe afetada

4 Data e hora do evento

5 Agente responsável pelo evento

6 Valor anterior do atributo

Os eventos de gerenciamento da classe previstos são:

EPROC1 Abertura de classe

EPROC2 Desativação de classe

EPROC3 Reativação de classe

EPROC4 Mudança de nome de classe

EPROC5 Deslocamento de classe

EPROC6 Extinção de classe

EPROC7 Alteração de prazo corrente

EPROC8 Alteração de evento corrente

EPROC9 Alteração de prazo intermediária

EPROC10 Alteração de evento intermediária

EPROC11 Alteração de destinação

EPROC12 Alteração de sigilo associado à classe

4.1. Identificador do evento

Designação	Identificador do evento
Rótulo	earq.eventoClasse.id
Definição	Identificador do evento de gerenciamento de classe que está sendo registrado no SIGAD.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Regra de preenchimento	Deve ser registrado automaticamente pelo SIGAD.
Requisito	1.1.4 / 1.1.5 / 1.1.6 / 1.1.7 / 1.1.8 / 1.2.6 / 1.2.7 / 1.2.8
Equivalência	--

4.2. Tipo de evento

Designação	Tipo de evento
Rótulo	earq.eventoClasse.tipo
Definição	Identificação do tipo de evento de gerenciamento de classe.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Regra de preenchimento	Este elemento poderá assumir os seguintes valores: • Abertura de classe • Desativação de classe • Reativação de classe • Mudança de nome de classe • Deslocamento de classe • Extinção de classe • Alteração de prazo corrente • Alteração de evento corrente • Alteração de prazo intermediária • Alteração de evento intermediária • Alteração de destinação • Alteração de sigilo associado à classe
Requisito	1.1.4 / 1.1.5 / 1.1.6 / 1.1.7 / 1.1.8 / 1.2.6 / 1.2.7 / 1.2.8
Equivalência	--

4.3. Identificador da classe afetada

Designação	Identificador da classe afetada
Rótulo	earq.eventoClasse.classeId
Definição	Identificador da classe afetada pelo evento de gerenciamento de classe que está sendo registrado.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Regra de preenchimento	O identificador deve ser obtido no elemento *3.1.1 earq.classe.id*.
Requisito	1.1.4 / 1.1.5 / 1.1.6 / 1.1.7 / 1.1.8 / 1.2.6 / 1.2.7 / 1.2.8
Equivalência	--

4.4. Data e hora do evento

Designação	Data e hora do evento
Rótulo	earq.eventoClasse.dataHora
Definição	Data e hora que o evento foi realizado.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Regra de preenchimento	É recomendável seguir o padrão da ISO 8601:2019 – *Data elements and interchange formats — Information interchange — Representation of dates and times.*
Requisito	1.1.4 / 1.1.5 / 1.1.6 / 1.1.7 / 1.1.8 / 1.2.6 / 1.2.7 / 1.2.8
Equivalência	--

4.5. Agente responsável pelo evento

Designação	Agente responsável pelo evento
Rótulo	earq.eventoClasse.agenteId
Definição	Identificar o agente responsável pelo evento.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Regra de preenchimento	O identificador deve ser obtido no elemento *4.1 identificador do agente*.
Requisito	1.1.4 / 1.1.5 / 1.1.6 / 1.1.7 / 1.1.8 / 1.2.6 / 1.2.7 / 1.2.8
Equivalência	--

4.6. Valor anterior do atributo

Designação	Valor anterior do atributo
Rótulo	earq.eventoClasse.valorAnterior
Definição	O valor do elemento antes da realização do evento.
Objetivo	Possibilitar a recuperação histórica dos conteúdos alterados.
Obrigatoriedade	**OA**
Repetibilidade	Não repetível
Regra de preenchimento	Antes de realizar a alteração, copiar o valor do elemento específico de *Identificação da classe* que está sendo alterado (earq.classe.nome, earq.classe.codigo, earq.classe.subordinacao, earq.classe.indicadorUso, earq.classe.indicadorAtiva, earq.classe.prazoCorrente, earq.classe.eventoCorrente, earq.classe.prazoIntermediaria, earq.classe.eventoIntermediaria, earq.Classe.destinacao, earq.classe.sigilo, earq.classe.observacao). Obrigatórios para os eventos EGC7, EGC8, EGC9, EGC10, EGC11 e EGC12.
Requisito	1.1.4 / 1.1.5 / 1.1.6 / 1.1.7 / 1.1.8 / 1.2.6 / 1.2.7 / 1.2.8
Equivalência	--

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
Rótulo	earq.componente.id
Definição	Designação usada para identificar no SIGAD os componentes digitais que integram o documento.
Objetivo	Identificar de forma unívoca e persistente os componentes digitais dos documentos armazenados 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**
Repetibilidade	Não repetível
Nota de aplicação	O identificador do componente digital tem que ser único no âmbito do SIGAD.
Exemplos	*IU24548* *10.1016/S1057-2317(03)00016-X* *http://purl.oclc.org /OCLC/PURL/FAQ*
Regra de preenchimento	Pode ser utilizado um identificador persistente, tal como DOI,[63] Handle System, mas isso não é obrigatório. Esta é uma decisão de implementação, e o tipo de identificador e a regra de formação deste devem estar claramente documentados.
Requisito	2.1.20
Equivalência	Premis:ObjectIdentifierValue

63 DOI – Digital Object Identifier. Disponível em: https://www.doi.org/. Acesso em: 24 jan. 2020.

5.2. Nome original

Designação	Nome original
Rótulo	earq.componente.nomeOriginal
Definição	Nome original do arquivo referente ao componente digital no momento em que foi capturado no SIGAD, antes de ser renomeado com o identificador do SIGAD.
Objetivo	Possibilitar a identificação do componente digital por meio de seu nome original devido a razões diversas: o nome utilizado dentro do SIGAD pode não ser conhecido externamente; um produtor de arquivos pode procurar um documento pelo nome original do arquivo ou, ainda, o SIGAD pode necessitar reconstruir *links* originais com objetivo de acesso.
Obrigatoriedade	**F**
Repetibilidade	Não repetível
Nota de aplicação	Quando um SIGAD está importando documento de outro SIGAD, deve-se registrar o nome original do componente para verificação posterior.
Exemplos	*0078NR.TIF*
Regra de preenchimento	O conteúdo deve ser obtido automaticamente no momento da captura do documento para o SIGAD.
Requisito	Ver capítulo 4 (Pesquisa, localização e apresentação dos documentos) e 8 (Preservação).
Equivalência	Premis:originalName

5.3. Tamanho

Designação	Tamanho
Rótulo	earq.componente.tamanho
Definição	Informa o tamanho do componente digital em bytes.
Objetivo	Esta informação é útil para garantir a previsão de espaço de memória suficiente para mover ou processar arquivos, bem como para previsão de capacidade de armazenamento.
Obrigatoriedade	**F**
Repetibilidade	Não repetível
Nota de aplicação	O tamanho deve ser sempre indicado na mesma unidade (bytes), pois dessa forma fica dispensado o registro da unidade de medida. No caso de transferência desse metadado para outro sistema, é necessário que a outra parte esteja ciente da unidade de medida.
Exemplos	*Tamanho: 345687*
Regra de preenchimento	Deve ser obtido automaticamente pelo SIGAD.
Requisito	Ver capítulo 8 (Preservação)
Equivalência	Premis:size

5.4. *Software* de criação

Designação	*Software* de criação
Rótulo	earq.componente.softwareCriacao
Definição	Informação a respeito do *software* utilizado para criar o componente digital.
Objetivo	Fornecer informações a respeito do *software* que criou o componente, para identificação de um *software* compatível para apresentação do documento ou para fins de conversão visando à preservação.
Obrigatoriedade	**F**
Repetibilidade	Não repetível
Nota de aplicação	Devem ser informados o nome do *software*, a versão e a data da criação do componente digital. Esse metadado deve ser registrado de forma estruturada, em três subelementos, conforme a seguir: earq.componente.SoftwareCriacao**Nome** earq.componente.SoftwareCriacao**Versao** earq.componente.SoftwareCriacao**Data**
Exemplos	*earq.componente.SoftwareCriacaoNome: MS Word* *earq.componente.SoftwareCriacaoVersao: 7* *earq.componente.SoftwareCriacaoVersao: 2009-10-06*
Regra de preenchimento	Pode ser extraído automaticamente do arquivo no momento da captura, uma vez que esse metadado é comumente registrado internamente no arquivo.
Requisito	Ver capítulo 8 (Preservação)
Equivalência	Premis:creatingApplicationName Premis:creatingApplicationVersion Premis:dateCreatedByApplication

5.5. Nível de composição

Designação	Nível de composição
Rótulo	earq.componente.nivelComposicao
Definição	Informação sobre se o componente digital está sujeito a um ou mais processos de compressão, criptografia ou empacotamento, bem como qual é esse nível.
Objetivo	Fornecer informações para orientar as intervenções necessárias para o acesso ao documento.
Obrigatoriedade	**OA**
Repetibilidade	Não repetível
Nota de aplicação	Nível de composição <**0**> (zero) indica que o componente digital não está sujeito a nenhum desses processos. Nível de composição <**1**> (um) ou maior indica que o componente digital foi submetido a um ou mais processos de compressão, criptografia ou empacotamento e que deve ser processado para que o documento possa ser acessado. Por exemplo, um arquivo **A** pode ser comprimido e gerar um arquivo **B**, que por sua vez é cifrado e gera um arquivo **C**. Para se ter acesso ao arquivo **A** é necessário decifrar o arquivo **C** e depois descomprimir o arquivo **B**.
Exemplos	*0, 1, 2, ..., desconhecido*
Regra de preenchimento	Zero, números inteiros positivos ou "desconhecido".
Requisito	Ver capítulo 8 (Preservação)
Equivalência	Premis:CompositionLevel

5.6. Inibidor

Designação	Inibidor
Rótulo	earq.componente.inibidor
Definição	Recursos que inibem o acesso, uso ou migração do componente digital.
Objetivo	Informar se um arquivo está criptografado, se tem proteção por senha, bem como as informações necessárias para sua decifração e acesso.
Obrigatoriedade	**F**
Repetibilidade	Não repetível
Nota de aplicação	Devem ser informados o tipo de inibidor, o alvo e a chave de acesso. Esse metadado deve ser registrado de forma estruturada, em três subelementos, conforme a seguir: Componente.InibidorTipo – refere-se ao método utilizado; Componente.InibidorAlvo – refere-se ao conteúdo ou à função protegida pelo inibidor; Componente.InibidorChave – refere-se à chave ou senha para decifração. A chave deve ser indicada, quando conhecida. No entanto, não é recomendável ser armazenada na forma de texto em um banco de dados não seguro.
Exemplos	*Componente.InibidorTipo: DES* *Componente.InibidorAlvo: All content* *Componente.Inibidorchave: 65kgedr5*
Regra de preenchimento	Quando um documento produzido externamente ao SIGAD tem um inibidor, é preciso que estas informações sejam fornecidas como metadados e enviadas juntamente com o documento capturado. Recomenda-se o uso de formas controladas para o subelemento "InibidorTipo", preferencialmente a tabela sugerida no PREMIS Data dictionary:[64] DES, PGP, Blowfish e Password Protection. Quando o subelemento "InibidorAlvo" não é informado, assume-se que é todo o conteúdo do componente digital. Recomenda-se o uso de formas controladas para o subelemento "InibidorAlvo", preferencialmente a tabela sugerida no PREMIS Data dictionary:[65] All content, Function:play, Function:print.
Requisito	Ver capítulo 8 (Preservação)
Equivalência	Premis:inhibitorType Premis:inhibitorTarget Premis:inhibitorKey

64 Lista controlada pela Library of Congress, sugerida no PREMIS Data Dictionary. Disponível em: http://id.loc.gov/vocabulary/preservation/inhibitorType.html. Acesso em: 24 jan. 2020.

65 Lista controlada pela Library of Congress, sugerida no PREMIS Data Dictionary. Disponível em: http://id.loc.gov/vocabulary/preservation/inhibitorTarget.html. Acesso em: 24 jan. 2020.

5.7. Formato de arquivo

Designação	Formato
Rótulo	earq.componente.formato
Definição	Identificação do formato de arquivo do componente digital.
Objetivo	O conhecimento do formato de arquivo do componente digital é essencial para o planejamento e a implementação de diversas ações de preservação como, por exemplo, a conversão devido à obsolescência do formato.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Nota de aplicação	Esse metadado deve ser registrado de forma estruturada, em dois subelementos, conforme a seguir: earq.componente.formatoNome earq.componente.formatoVersao Informações adicionais sobre o formato também podem ser registradas. Nos casos em que não for possível identificar o formato, este deve ser registrado como "desconhecido", e posteriormente identificado.
Exemplos	*earq.componente.formatoNome: Adobe PDF* *earq.componente.formatoVersao: 6.0*
Regra de preenchimento	Recomenda-se o uso de formas controladas para a designação do formato, como bases de dados de registro de formato. Ex.: PRONOM,[66] MIME.[67] Deve ser identificado automaticamente pelo SIGAD no momento da captura.
Requisito	2.1.4
Equivalência	Premis:formatName Premis:formatVersion

66 Serviço de base de dados de formatos de arquivo gerenciada pelo The National Archives (TNA), do Reino Unido. Disponível em: https://www.nationalarchives.gov.uk/PRONOM/Default.aspx/. Acesso em: 24 jan. 2020.

67 Lista de formatos digitais mais comuns na internet. Disponível em: https://www.iana.org/assignments/media-types/media-types.xhtml. Acesso em: 24 jan. 2020.

5.8. Localização

Designação	Localização
Rótulo	earq.componente.localizacao
Definição	Informações sobre a localização do componente digital.
Objetivo	As informações sobre localização são necessárias para encontrar o componente digital no sistema de armazenamento.
Obrigatoriedade	**OA**
Repetibilidade	Repetível
Nota de aplicação	Caso o SIGAD utilize um identificador como o *handle*, a localização estará implícita no identificador e não será necessário registrá-la novamente. Esse metadado deve ser registrado de forma estruturada, em dois subelementos, conforme a seguir: earq.componente.localizacaoTipo earq.componente.localizacaoValor
Exemplos	*earq.componente.localizacaoTipo: URI* *earq.componente.localizacaoValor: https://www.gov.br/conarq/pt-br* *earq.componente.localizacaoTipo: NTFS* *earq.componente.localizacaoValor: C:\MyDocuments\Textos\Preservacao_digital*
Regra de preenchimento	De forma geral, a localização deve ser preenchida automaticamente pelo SIGAD.
Requisito	7.1.7
Equivalência	Premis:contentLocationType Premis:contentLocationValue

5.9. Suporte

Designação	Suporte
Rótulo	earq.componente.suporte
Definição	Suporte físico no qual o componente digital está armazenado.
Objetivo	As informações sobre o suporte em que o componente digital está armazenado apoiam o monitoramento das ações de preservação necessárias, como, por exemplo, a atualização de suporte.
Obrigatoriedade	**F**
Repetibilidade	Não repetível
Nota de aplicação	Quanto ao suporte, devem ser registradas informações a respeito do tipo de suporte utilizado e sua vida útil. Os responsáveis pela preservação digital devem gerenciar a obsolescência das mídias de armazenamento. Em geral, esse monitoramento é realizado no nível do sistema de armazenamento, e não especificamente para cada item documental ou componente digital.
Exemplos	*Fita magnética, HD, CD-ROM, DVD.*
Regra de preenchimento	--
Requisito	7.1.7
Equivalência	Premis:storageMedium

5.10. Dependência de *software*

Designação	Dependência de *software*
Rótulo	earq.componente.sw
Definição	Informações sobre o ambiente de *software* necessário para apresentar e/ou usar os componentes digitais, incluindo a aplicação e o sistema operacional.
Objetivo	Dar conhecimento do ambiente de *software* necessário para uso do recurso.
Obrigatoriedade	**OA**
Repetibilidade	Repetível
Nota de aplicação	Esse metadado deve ser registrado de forma estruturada, em quatro subelementos, conforme a seguir: earq.componente.swNome earq.componente. swVersao earq.componente.swTipo earq.componente.swDocumentacao
Exemplos	*earq.componente.swNome: Windows* *earq.componente.swVersao: XP* *earq.componente.swTipo: sistema operacional* *earq.componente.swDocumentacao: manual do sistema* *earq.componente.swNome: Word* *earq.componente.swVersao: 7* *earq.componente.swTipo: aplicativo/visualizador*
Regra de preenchimento	No caso de não haver uma versão formal do *software*, pode se indicar o ano em que foi lançado. Valores sugeridos para tipo de *software*: sistema operacional, aplicativo/visualizador, *driver*, biblioteca. Com relação à documentação, pode se indicar um identificador persistente que aponte para documentação do *software*, dentro ou fora do SIGAD.
Requisito	Ver capítulo 8 (Preservação)
Equivalência	Premis:swName Premis:swVersion Premis:swType Premis:swOtherInformation

5.11. Dependência de *hardware*

Designação	Dependência de *hardware*
Rótulo	earq.componente.hw
Definição	Informações sobre os componentes de *hardware* necessários para operar o *software* referenciado em *earq.componente.sw*, incluindo periféricos.
Objetivo	Dar conhecimento do ambiente de *hardware* necessário para uso do recurso.
Obrigatoriedade	**OA**
Repetibilidade	Repetível
Nota de aplicação	Esse metadado deve ser registrado de forma estruturada, em três subelementos, conforme a seguir: earq.componente.hwNome earq.componente.hwTipo earq.componente.hwOutrasInformacoes
Exemplos	*earq.componente.hwNome: Intel x86* *earq.componente.hwTipo: processador* *earq.componente.hwOutrasInformacoes: configuração mínima 60 Mhz* *earq.componente.hwNome: RAM* *earq.componente.hwTipo: memória* *earq.componente.hwOutrasInformacoes: configuração mínima 64 Mb*
Regra de preenchimento	Na informação sobre o nome do *hardware*, deve se registrar o fabricante, o modelo e a versão, quando pertinente. Valores sugeridos para tipo de *hardware*: processador, memória, dispositivos de entrada/saída, dispositivo de armazenamento. Outras informações podem incluir a configuração mínima recomendada ou documentação pertinente. Com relação à documentação, pode se indicar um identificador persistente que aponte para documentação do *hardware*, dentro ou fora do SIGAD.
Requisito	Ver capítulo 8 (Preservação)
Equivalência	Premis:hwName Premis:hwType Premis:hwOtherInformation

5.12. Outras dependências

Designação	Outras dependências
Rótulo	earq.componente.outrasDependencias
Definição	Informações sobre outras dependências, que não sejam as de *software* e *hardware*, necessárias para apresentar ou usar os documentos (por exemplo, DTD, XML Schema, fontes, folha de estilo).
Objetivo	Dar informação sobre outros tipos de dependências, além de *software* e *hardware*, necessárias para uso do recurso.
Obrigatoriedade	**OA**
Repetibilidade	Repetível
Nota de aplicação	Esse metadado deve ser registrado de forma estruturada, em dois subelementos, conforme a seguir: earq.componente.outrasDependenciasTipo earq.componente.outrasDependenciasId Em alguns casos o identificador do recurso já torna evidente o tipo do componente necessário.
Exemplos	*earq.componente.outrasDependenciasTipo: URI* *earq.componente.outrasDependenciasId: http://www.arquivonacional.gov.br/XYZ/DTD/ojns.dtd*
Regra de preenchimento	--
Requisito	Ver capítulo 8 (Preservação)
Equivalência	Premis:dependencyName Premis:dependencyIdentifierType Premis:dependencyIdentifierValue

5.13. Relação com outros componentes digitais

Designação	Relação
Rótulo	earq.componente.relacao
Definição	Registro das relações de um componente digital com outros componentes digitais.
Objetivo	Tornar explícito o relacionamento entre componentes digitais para possibilitar o processamento e acesso aos documentos. Alguns documentos são formados por diversos componentes digitais relacionados. Estas relações são estruturais.
Obrigatoriedade	**OA**
Repetibilidade	Repetível
Nota de aplicação	As relações estruturais são fundamentais para apresentar o documento ao usuário. Devem ser registradas as seguintes informações para cada relacionamento: identificação dos objetos relacionados, tipo da relação (por exemplo, é parte de). As instituições devem estabelecer os tipos de relacionamentos mais relevantes, que deverão ser controlados nos metadados. Estas relações podem ser expressas das seguintes formas: • *tem parte de, é parte de* (expressa as relações estruturais); • *tem fonte de* (um componente digital é uma versão de outro componente, criado por uma transformação), *é fonte de* (um componente derivado de outro componente por um processo de transformação).
Exemplos	*"relat_2009.pdf" é fonte de "relat_2009.zip"*
Regra de preenchimento	--
Requisito	Ver capítulo 8 (Preservação)
Equivalência	Premis:relationshiptype Premis:relationshipSubType Premis:relatedObjectIdentifier

5.14. Fixidade

Designação	Fixidade
Rótulo	earq.componente.fixidade
Definição	Informações utilizadas para verificar se o componente digital sofreu mudanças não documentadas.
Objetivo	Verificar se o componente digital foi alterado de forma não documentada ou não autorizada, comprometendo sua autenticidade.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Nota de aplicação	Esse elemento registra informações do código *hash*[68] do componente digital, e de como este foi gerado, de forma a permitir a verificação da fixidade no futuro. Esse elemento não se refere à verificação da fixidade, que deve ser registrada no evento correspondente. Para se realizar a verificação da fixidade, um código *hash* deve ser previamente gerado e armazenado, para ser comparado a outro gerado posteriormente. Se os códigos coincidirem, significa que o objeto não foi alterado nesse intervalo de tempo. Esse metadado deve ser registrado de forma estruturada, em três subelementos, conforme a seguir: earq.componente.fixidadeAlgoritimo earq.componente.fixidadeCodigoHash earq.componente.fixidadeOriginador Originador refere-se ao agente que fez o cálculo do código *hash* armazenado, que pode ser calculado pelo próprio SIGAD ou ter sido enviado junto com o documento.
Exemplos	*earq.componente.fixidadeAlgoritimo: MD5* *earq.componente.fixidadeCodigoHash:* *da4f2ebd436f1cf88e5a39b3a257edf4a22be3c955ac49da2e2* *earq.componente.fixidadeOriginador: MDS*
Regra de preenchimento	Calculado e armazenado automaticamente pelo SIGAD. Recomenda-se o uso de formas controladas para a designação do algoritmo usado para gerar o código *hash*, preferencialmente a tabela sugerida no PREMIS Data Dictionary.[69] O originador deve ser representado por um identificador do agente que realizou o cálculo *hash*. Caso o originador seja um agente conhecido do SIGAD, pode se usar o Id do agente.
Requisito	Ver capítulo 8 (Preservação)
Equivalência	Premis: messageDigestAlgorithm Premis: messageDigest Premis: messageDigestOriginator

68 Note que os termos "código hash" e "checksum" são comumente usados de forma intercambiável. No entanto, o termo "checksum" é mais corretamente utilizado para o produto de uma verificação de redundância cíclica (*cyclical redundancy check* - CRC), enquanto o termo "código hash" se refere ao resultado de uma função de *hash* criptográfica, que é ao que aqui se refere.

69 Lista controlada pela Library of Congress, sugerida no PREMIS Data Dictionary. Disponível em: http://id.loc.gov/vocabulary/preservation/cryptographicHashFunctions.html. Acesso em: 24 jan. 2020.

5.15. Assinatura digital

Designação	Assinatura digital
Rótulo	earq.componente.assinatura
Definição	Informações sobre a assinatura digital aplicada aos componentes digitais.
Objetivo	Usada para autenticar quem assinou o componente digital e/ou a informação contida nele. Também é usado para armazenar as informações relacionadas a essa assinatura de forma a apoiar validações posteriores.
Obrigatoriedade	**OA**
Repetibilidade	Repetível
Nota de aplicação	Esse metadado deve ser registrado de forma estruturada, em seis subelementos, conforme a seguir: earq.componente.assinaturaCodificacao earq.signatario earq.componente.assinaturaMetodo earq.componente.assinaturaValor earq.componente.assinaturaRegrasValidacao earq.componente.assinaturaChave A informação da codificação utilizada é essencial para se interpretar corretamente o valor da assinatura e a chave. O signatário é o indivíduo, instituição ou autoridade responsável por gerar a assinatura. Método refere-se aos algoritmos utilizados para criptografar e calcular o *hash* na geração da assinatura digital. Regras de validação são as operações que devem ser realizadas para validar a assinatura digital. Chave refere-se à chave pública do signatário necessária para validar a assinatura.
Exemplos	*earq.componente.assinaturaCodificacao: Base64* *earq.signatario: Ministério da Saúde* *earq.componente.assinaturaMetodo: DSA-SHAI* *earq.componente.assinaturaValor:* *da4f2ebd436f1cf88e5a39b3a257edf4a22be3c955ac49*
Regra de preenchimento	Calculado e armazenado automaticamente pelo SIGAD. Recomenda-se o uso de formas controladas para a designação da codificação, preferencialmente a tabela sugerida no PREMIS Data Dictionary.[70] Caso o signatário seja um agente conhecido do SIGAD, pode se usar o Id do agente. Recomenda-se o uso de formas controladas para a designação do método, preferencialmente a tabela sugerida no PREMIS Data Dictionary.[71] As regras de validação podem incluir informações tais como: o método de canonização usado antes de calcular o resumo da mensagem ou se o objeto foi normalizado antes de assinar. Esse metadado pode apontar para um arquivo com a documentação dessas regras.

70 Lista controlada pela Library of Congress, sugerida no PREMIS Data Dictionary. Disponível em: http://id.loc.gov/vocabulary/preservation/cryptographicHashFunctions.html. Acesso em: 24 jan. 2020.

71 Lista controlada pela Library of Congress, sugerida no PREMIS Data Dictionary. Disponível em: http://id.loc.gov/vocabulary/preservation/signatureMethod.html. Acesso em: 24 jan. 2020.

Designação	Assinatura digital
Requisito	7.5.4 / 7.5.5
Equivalência	Premis: signatureEncoding Premis: signer Premis: signatureMethod Premis: signatureValue Premis: signatureValidationRules Premis: keyInformation

6 Eventos de preservação

Estas informações referem-se a eventos de preservação ocorridos com o componente digital. 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.

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

1 Identificador do evento

2 Tipo de evento

3 Identificação do componente digital

4 Data e hora do evento

5 Agente responsável pelo evento

6 Resultado do evento

7 Detalhes do evento

Os eventos de preservação previstos são:

EPRES1 Compressão

Registro da compressão ou descompressão de componentes digitais.

EPRES2 Decifração

Registro da decifração de componentes digitais criptografados.

EPRES3 Validação de assinatura digital

Registro da validação da assinatura digital de um documento, no momento da captura, por meio da conferência com o certificado digital.

EPRES4 Cálculo *hash*

Registro do cálculo *hash* do arquivo, a ser armazenado no elemento de metadado do componente digital *earq.componente.fixidade*, que serve para apoiar a verificação de fixidade ao longo do tempo.

EPRES5 Verificação de fixidade[72]

Registro da verificação da fixidade do componente digital.

EPRES6 Migração

Registro de procedimento de migração do componente digital.

EPRES7 Replicação

Registro de procedimento de replicação do componente digital.

EPRES8 Verificação de vírus

Registro de verificação de vírus no componente digital.

EPRES9 Validação

Registro da validação do documento.

6.1. Identificador do evento

Designação	Identificador do evento
Rótulo	earq.ePres.id
Definição	Identificador do evento de preservação que está sendo registrado no SIGAD.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Regra de preenchimento	Deve ser registrado automaticamente pelo SIGAD.
Requisito	2.1.4 / 7.5.4 / 7.5.5 / 7.9.3 / 7.9.6 / 7.7.2 / 7.11.1 / 7.11.9/ 7.12.7 / 8.2.6 / 8.3.1/ 8.3.6 / 9.3.1 / 9.3.2 / 9.3.3 / 9.3.4 / 9.3.5
Equivalência	--

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

6.2. Tipo de evento

Designação	Tipo de evento
Rótulo	earq.ePres.tipo
Definição	Categoriza o tipo de evento de preservação.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Regra de preenchimento	Este elemento poderá assumir, no mínimo, os seguintes valores: • Compressão • Decifração • Validação de assinatura digital • Cálculo *hash* • Verificação de fixidade • Migração • Replicação • Verificação de vírus • Validação
Requisito	2.1.4 / 7.5.4 / 7.5.5 / 7.9.3 / 7.9.6 / 7.7.2 / 7.11.1 / 7.11.9/ 7.12.7 / 8.2.6 / 8.3.1/ 8.3.6 / 9.3.1 / 9.3.2 / 9.3.3 / 9.3.4 / 9.3.5
Equivalência	Premis: eventType

6.3. Componente digital

Designação	Componente digital
Rótulo	earq.ePres.componenteId
Definição	Identificador do componente digital afetado pelo evento de preservação que está sendo registrado.
Obrigatoriedade	**O**
Repetibilidade	Repetível
Regra de preenchimento	O código deve ser obtido no metadado *earq.componente.id*.
Requisito	2.1.4 / 7.5.4 / 7.5.5 / 7.9.3 / 7.9.6 / 7.7.2 / 7.11.1 / 7.11.9/ 7.12.7 / 8.2.6 / 8.3.1/ 8.3.6 / 9.3.1 / 9.3.2 / 9.3.3 / 9.3.4 / 9.3.5
Equivalência	Premis: linkingObjectIdentifierValue

6.4. Data e hora do evento

Designação	Data e hora do evento
Rótulo	earq.ePres.dataHora
Definição	Data e hora que o evento foi realizado, ou de seu início.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Regra de preenchimento	É recomendável seguir o padrão da ISO 8601:2019 – *Data elements and interchange formats — Information interchange — Representation of dates and times.*
Requisito	2.1.4 / 7.5.4 / 7.5.5 / 7.9.3 / 7.9.6 / 7.7.2 / 7.11.1 / 7.11.9/ 7.12.7 / 8.2.6 / 8.3.1/ 8.3.6 / 9.3.1 / 9.3.2 / 9.3.3 / 9.3.4 / 9.3.5
Equivalência	Premis: eventDateTime

6.5. Agente responsável pelo evento

Designação	Agente responsável pelo evento
Rótulo	earq.ePres.agenteId
Definição	Agente responsável pelo evento.
Obrigatoriedade	**O**
Repetibilidade	Repetível
Regra de preenchimento	O identificador deve ser obtido no metadado *earq.agente.id*.
Requisito	2.1.4 / 7.5.4 / 7.5.5 / 7.9.3 / 7.9.6 / 7.7.2 / 7.11.1 / 7.11.9/ 7.12.7 / 8.2.6 / 8.3.1/ 8.3.6 / 9.3.1 / 9.3.2 / 9.3.3 / 9.3.4 / 9.3.5
Equivalência	Premis: linkingAgentIdentifierValue

6.6. Resultado do evento

Designação	Resultado do evento
Rótulo	earq.ePres.Resultado
Definição	Resultado do evento de preservação.
Obrigatoriedade	**OA**
Repetibilidade	Repetível
Exemplo	*00 [código para registrar que a ação foi completada com sucesso].* *CV-01 [código para registrar que o* checksum *foi validado].*
Regra de preenchimento	Recomenda-se o uso de tabela com os resultados possíveis para padronização do preenchimento do elemento de metadado.
Requisito	2.1.4 / 7.5.4 / 7.5.5 / 7.9.3 / 7.9.6 / 7.7.2 / 7.11.1 / 7.11.9/ 7.12.7 / 8.2.6 / 8.3.1/ 8.3.6 / 9.3.1 / 9.3.2 / 9.3.3 / 9.3.4 / 9.3.5
Equivalência	Premis: eventOutcome

6.7. Detalhes do evento

Designação	Detalhes do evento
Rótulo	earq.ePres.detalhe
Definição	Registro de informações adicionais a respeito do evento de preservação.
Nota de aplicação	Pode se registrar a metodologia e/ou tecnologia (*software* e *hardware*) utilizada no evento, bem como eventuais consequências no documento.
Obrigatoriedade	**F**
Repetibilidade	Repetível
Regra de preenchimento	--
Requisito	2.1.4 / 7.5.4 / 7.5.5 / 7.9.3 / 7.9.6 / 7.7.2 / 7.11.1 / 7.11.9/ 7.12.7 / 8.2.6 / 8.3.1/ 8.3.6 / 9.3.1 / 9.3.2 / 9.3.3 / 9.3.4 / 9.3.5
Equivalência	Premis:eventDetailInformation

7 Agente

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

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

7.1. Identificador do agente

Designação	Identificador do agente
Rótulo	earq.agente.id
Definição	Código que identifica univocamente o agente no SIGAD.
Objetivo	Identificar univocamente o agente no SIGAD.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Nota de aplicação	Recomenda-se utilizar o código identificador já utilizado na instituição, tais como o número de matrícula, CPF etc.
Exemplos	*999.999.999-99* *65418932*
Regra de preenchimento	--
Requisito	7.2.1 / 7.2.3
Equivalência	--

7.2. Nome do agente

Designação	Nome do agente
Rótulo	earq.agente.nome
Definição	Nome do agente que interage com o SIGAD.
Objetivo	Identificar o nome do agente.
Obrigatoriedade	**O**
Repetibilidade	Não repetível
Nota de aplicação	Um agente pode ser uma pessoa física, jurídica ou um sistema informatizado.
Exemplos	*João da Silva* *Ministério da Educação* *SIAFI*
Regra de preenchimento	--
Requisito	7.2.1
Equivalência	--

7.3. Status do agente

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

GLOSSÁRIO

AC

Ver Autoridade Certificadora

Acessibilidade

Facilidade no acesso ao conteúdo e ao significado de um documento digital. (I) Acessibility.
Ver também: Acesso.

Acesso

Direito, oportunidade ou meios de encontrar, recuperar e usar a informação.
Ver também: Acessibilidade, Classificação de segurança, Credencial de segurança, Restrição de acesso.

ACT

Ver Autoridade de Carimbo do Tempo.

Anexo

Um documento digital que segue junto com uma mensagem de correio eletrônico ou um fluxo de trabalho. (I) Attachment.
Ver também: Correio eletrônico, Mensagem de correio eletrônico.

Anotação

Informação acrescentada ao documento arquivístico após sua produção. *Exemplo:* "urgente", "arquive-se", número do protocolo, código de classificação, temporalidade, data, hora e local da transmissão, indicação de anexos e outros.
Ver também: Documento arquivístico.

AR

Ver Autoridade de Registro.

Armazenamento

Guarda de documentos arquivísticos em local apropriado. (I) Storage.
Ver também: Armazenamento (documento digital).

Armazenamento (documento digital)

Guarda de documentos digitais em dispositivos de memória não volátil. (I) Storage.
Ver também: Armazenamento, Sistema de storage.

Arquivamento (atividade)

Sequência de operações intelectuais e físicas que visam à guarda ordenada de documentos. (ARQUIVO NACIONAL, 2005, p. 26)

Arquivamento (decisão)

Ação pela qual uma autoridade determina a guarda de um documento, cessada a sua tramitação. (ARQUIVO NACIONAL, 2005, p. 26)

Arquivo (fundo)

Conjunto de documentos produzidos e acumulados por uma entidade coletiva, pública ou privada, pessoa ou família, no desempenho de suas atividades, independentemente da natureza do suporte. (E) Fondo, (F) Fonds, (I) Archive Group.
Ver também: Organicidade, Produtor.

Arquivo (instituição ou serviço)

Instituição ou serviço que tem por finalidade a custódia, o processamento técnico, a conservação e o acesso a documento arquivístico.

Arquivo digital

Sequência de bytes ordenada e nomeada que é reconhecida por um sistema operacional. (I) File.

Ver também: Objeto digital.

Assinatura digital

Modalidade de assinatura eletrônica, resultado 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, Autenticação, Carimbo digital do tempo, Certificação digital, Certificado digital, Chave privada, Chave pública, 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, Certificação digital.

Atualização de suporte

Técnica de migração que consiste em copiar os dados de um suporte para outro, sem mudar sua codificação, para evitar perdas de dados provocadas por deterioração do suporte. (I) Refreshing, (E) Refrescamiento, (F) Repiquage.

Ver também: Migração, Conversão de formato, Preservação digital, Reformatação (migração).

Autenticação

Declaração de que um documento original é autêntico – ou que uma cópia reproduz fielmente o original – feita por uma pessoa jurídica com autoridade para tal (servidor público, notário, autoridade certificadora) num determinado momento, por meio da adição de elementos ou afirmações.

Ver também: Assinatura digital, Autenticidade, Carimbo digital do tempo, Certificado de autenticidade.

Autenticidade

Credibilidade de um documento enquanto documento, isto é, a qualidade de um documento ser o que diz ser e que está livre de adulteração ou qualquer outro tipo de corrupção. A autenticidade é composta de identidade e integridade.

Nota: identidade e integridade são constatadas à luz do contexto (jurídico-administrativo, de proveniência, de procedimentos, documental e tecnológico) no qual o documento arquivístico foi produzido e usado ao longo do tempo.

Ver também: Autenticação, Carimbo digital do tempo, Certificado de autenticidade, Documento arquivístico autêntico, Identidade, Integridade, Presunção de autenticidade.

Autoridade Certificadora (AC)

Organização que emite, renova ou revoga certificados digitais de outras autoridades certificadoras ou de titulares finais.

Ver também: Certificação digital, Chave privada, Chave pública, Infraestrutura de Chaves Públicas.

Autoridade de Carimbo do Tempo (ACT)

Organização que tem a responsabilidade de emissão de carimbo digital do tempo.

Ver também: Carimbo digital do tempo, Certificação digital, Infraestrutura de Chaves Públicas.

Autoridade Certificadora do Tempo (ACT)

Ver Autoridade de Carimbo do Tempo.

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: Certificação digital, Chave privada, Chave pública, Infraestrutura de Chaves Públicas.

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. (E) Valoración, (I) Appraisal.

Ver também: Destinação, Valor primário, Valor secundário.

Backup

Ver Cópia de segurança.

Banco de dados (ambiente computacional)

Ambiente computacional composto por: a) dados estruturados em bases de dados relacionadas entre si, segundo um modelo de dados; b) regras que definem as operações válidas sobre os dados e garantem sua integridade.

Ver também: Base de dados, Sistema Gerenciador de Banco de Dados.

Banco de dados (*software*)

Ver Sistema Gerenciador de Banco de Dados.

Base de dados

Conjunto de dados estruturados, com as respectivas regras de acesso, formatação e validação, e gerenciados por um Sistema Gerenciador de Banco de Dados - SGBD.

Ver também: Banco de dados (ambiente computacional), Sistema Gerenciador de Banco de Dados.

Captura

Declaração de um documento como documento arquivístico, incorporando-o ao sistema de gestão arquivística, por meio de, no mínimo, as seguintes ações: registro; classificação; indexação; arquivamento; e, quando couber, atribuição de restrição de acesso.

Ver também: Classificação arquivística, Registro.

Carimbo digital do tempo

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

Ver também: Assinatura digital, Autenticação, Autoridade de Carimbo do Tempo, Infraestrutura de Chaves Públicas.

Categoria de sigilo

Ver Grau de sigilo.

Certificação digital

Atividade pela qual se estabelece uma relação única, exclusiva e intransferível entre um elemento criptográfico e uma pessoa física ou jurídica.

Ver também: Assinatura digital, Assinatura eletrônica, Autoridade certificadora, Autoridade de Carimbo do Tempo, Autoridade de registro, Criptografia.

Certificado de autenticidade

Declaração de autenticidade das reproduções dos documentos arquivísticos digitais emitida pela instituição responsável por sua preservação.

Ver também: Autenticação, Autenticidade.

Certificado digital

Registro eletrônico assinado, gerado por meio de um procedimento de certificação digital, que se destina a comprovar a relação existente entre um elemento criptográfico e uma pessoa física ou jurídica. (INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, 2017)

Ver também: Assinatura digital, Chave privada, Chave pública, Criptografia assimétrica, Infraestrutura de Chaves Públicas.

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, bem como para decifrar aqueles criptografados com a chave pública correspondente.

Ver também: Assinatura digital, Autoridade certificadora, Autoridade de registro, Certificado digital, Chave pública, Criptografia, Criptografia assimétrica, Infraestrutura de Chaves Públicas.

Chave pública

Chave matemática formada por uma sequência de dígitos, usada para criptografia assimétrica, 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, Autoridade certificadora, Autoridade de registro, Certificado digital, Chave privada, Criptografia, Criptografia assimétrica, Infraestrutura de Chaves Públicas.

Ciclo vital dos documentos

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

Ver também: Gestão arquivística de documentos.

Classe

Primeiro nível hierárquico de um plano de classificação, normalmente seguido dos níveis subclasse, grupo e subgrupo.

Ver também: Plano de classificação.

Classificação arquivística

Organização dos documentos de um arquivo ou coleção, de acordo com o Plano de classificação, Código de classificação ou Quadro de arranjo. (ARQUIVO NACIONAL, 2005, p. 49)

Ver também: Captura, Código de classificação, Plano de classificação.

Classificação de segurança

Atribuição a documentos, ou às informações neles contidas, de graus de sigilo, conforme legislação específica. (ARQUIVO NACIONAL, 2005, p. 49)

Ver também: Acesso, Grau de sigilo, Restrição de acesso.

Classificação documental

Ver Classificação arquivística.

Classificação quanto ao grau de sigilo

Ver Classificação de segurança.

Código de classificação

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

Ver também: Classificação arquivística, 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 maneira 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, incluindo os metadados necessários para ordenar, estruturar ou manifestar seu conteúdo e forma, que requer determinadas ações de preservação. Um documento arquivístico digital pode ser composto por um ou mais componentes digitais. *Exemplo:* uma fotografia digital tem apenas um componente digital, que é o arquivo com a imagem, já um documento multimídia tem diversos componentes digitais, que são os arquivos com o código executável, os textos, as imagens e os registros sonoros. (I) Digital Component.

Ver também: Objeto lógico, Documento digital, Preservação digital.

Confiabilidade

Credibilidade de um documento arquivístico enquanto uma afirmação do 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 processo de sua produção. (I) Reliability.

Ver também: Completeza.

Confidencialidade

Propriedade de certos dados ou informações que não podem ser disponibilizadas ou divulgadas sem autorização.

Conteúdo estável

Característica de um documento arquivístico em que os dados e a mensagem nele contidos mantêm-se inalterados e inalteráveis, isto é, não podem ser sobrescritos, alterados, apagados ou acrescentados (INTERPARES 3 PROJECT, Team Canada, 2008). (I) Stable content.

Ver também: Fixidez, Forma fixa.

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, ou seja, seu contexto 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

Conjunto de normas internas que regulam a produção, tramitação, uso e arquivamento dos documentos da instituição.

Ver também: Contexto, 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, 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, do fundo.

Ver também: Contexto, Contexto de procedimentos, Contexto de proveniência, Contexto jurídico-administrativo, Contexto tecnológico.

Contexto jurídico-administrativo

Conjunto de leis e normas externas à instituição produtora de documentos as quais controlam a condução das atividades dessa mesma instituição.

Ver também: Contexto, 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, Contexto de procedimentos, Contexto de proveniência, Contexto documental, Contexto jurídico-administrativo, Hardware, Programa de computador.

Controle de versão

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

Ver também: Documento, Identificador único, Versão.

Conversão (dados)

Ver Conversão de formato.

Conversão de formato

Modificação de um formato para outro motivada, principalmente, pela normalização de formatos e para contornar a obsolescência tecnológica. (I) Data conversion.

Ver também: Migração, Atualização de suporte, Exportação, Formato de arquivo, Normalização de formato, Reformatação (migração).

Cópia

Resultado da reprodução de um documento, geralmente qualificada por sua função ou processo de duplicação. (ARQUIVO NACIONAL, 2005, p. 56)

Ver também: Cópia de segurança.

Cópia de segurança

Cópia feita com vistas a restaurar as informações no caso de perda ou destruição do original.

Ver também: Cópia.

Correio eletrônico

Sistema usado para criar, transmitir e receber mensagem eletrônica e outros documentos digitais por meio de rede de computadores. (I) Email System.

Ver também: Anexo, Endereço de correio eletrônico, Mensagem de correio eletrônico.

Credencial de segurança

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

Ver também: Acesso.

Criptografia

Método de codificação de dados segundo algoritmo específico e chave secreta, de forma que somente os usuários autorizados possam restabelecer sua forma original.

Ver também: Assinatura digital, Certificação digital, Chave privada, Chave pública, Criptografia assimétrica, Criptografia simétrica.

Criptografia assimétrica

Tipo de criptografia que usa um par de chaves criptográficas distintas (privada e pública) e matematicamente relacionadas. A chave pública está disponível para todos que queiram cifrar informações para o dono da chave privada ou para verificação de uma assinatura digital criada com a chave privada correspondente; a chave privada é mantida em segredo pelo seu dono e pode decifrar informações ou gerar assinaturas digitais.

Ver também: Certificado digital, Chave privada, Chave pública, Criptografia, Criptografia simétrica, Infraestrutura de Chaves Públicas.

Criptografia de chave pública

Ver Criptografia assimétrica.

Criptografia simétrica

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

Ver também: Criptografia, Criptografia assimétrica.

Custódia

Responsabilidade jurídica de guarda e proteção de arquivos, independentemente de vínculo de propriedade. (ARQUIVO NACIONAL, 2005, p. 62)

Ver também: Recolhimento.

Dado

Representação de todo e qualquer elemento de conteúdo cognitivo, passível de ser comunicada, processada e interpretada de forma manual ou automática. (ARQUIVO NACIONAL, 2005, p. 62)

Ver também: Metadados.

Descrição

Conjunto de procedimentos que leva em conta os elementos formais e de conteúdo dos documentos arquivísticos para elaboração de instrumentos de pesquisa.

Destinação

Decisão, com base na avaliação, quanto ao encaminhamento dos documentos para a guarda permanente ou eliminação.

Ver também: Avaliação, Eliminação, Recolhimento.

Digital Object Identifier

Ver DOI.

Digitalização

Processo de conversão de um documento para o formato digital, por meio de dispositivo apropriado. (ARQUIVO NACIONAL, 2005, p. 69)

Ver também: OCR, Reformatação (migração), Representante digital.

Documento

Unidade de registro de informações, qualquer que seja o formato ou o suporte. (ARQUIVO NACIONAL, 2005, p. 73)

Ver também: Controle de versão, Documento arquivístico, Documento eletrônico, Dossiê, Original, Suporte.

Documento arquivístico

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

Ver também: Anotação, Documento, Documento arquivístico armazenado, Documento arquivístico autêntico, Documento arquivístico eletrônico, Elemento extrínseco, Elemento intrínseco, Fixidez, Forma documental, Relação orgânica.

Documento arquivístico autêntico

Documento que é o que diz ser e está livre de alteração ou corrupção, ou seja, que teve sua identidade e integridade mantidas ao longo do tempo.

Ver também: Autenticidade, Documento arquivístico, Identidade, Integridade.

Documento arquivístico digital

Documento digital reconhecido e tratado como um documento arquivístico. (I) Digital Record.
Ver também: Documento arquivístico eletrônico, Fixidez.

Documento arquivístico eletrônico

Documento eletrônico reconhecido e tratado como um documento arquivístico. (I) Electronic Record.
Ver também: Documento arquivístico, Documento arquivístico digital.

Documento digital

Informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional. (I) Digital Document.
Ver também: Componente digital, Documento arquivístico digital, Documento eletrônico, Documento não digital, Documento híbrido, Dossiê híbrido, Processo híbrido.

Documento eletrônico

Informação registrada, codificada em forma analógica ou em dígitos binários, acessível e interpretável por meio de um equipamento eletrônico. (I) Electronic Document.
Nota: na literatura arquivística internacional, algumas vezes encontra-se o termo "documento eletrônico" como sinônimo de "documento digital".
Ver também: Documento, Documento arquivístico eletrônico, Documento digital, Documento não digital.

Documento híbrido

Documento constituído de partes digitais e não digitais.
Ver também: Documento digital, Documento eletrônico, Documento não digital, Representante digital.

Documento não digital

Documento que se apresenta em suporte, formato e codificação diferente dos digitais, tais como: documentos em papel, documentos em películas e documentos eletrônicos analógicos.
Ver também: Documento digital, Documento eletrônico, Documento híbrido, Representante digital.

DOI (Digital Object Identifier)

Sistema para identificação persistente de objetos digitais em redes, bem como para o intercâmbio de informações sobre propriedade intelectual desses objetos.
Nota: marca registrada da DOI Foundation. Disponível em: http://www.doi.org. Acesso em: 26 jun. 2020.

Dossiê

Conjunto de documentos, relacionados entre si por ação, evento, pessoa, lugar e/ou projeto, que constitui uma unidade.
Ver também: Documento, Dossiê híbrido, Item documental, Processo.

Dossiê híbrido

Dossiê constituído por documentos digitais e não digitais. *Exemplo:* projetos arquitetônicos que apresentam a descrição em papel e as plantas, em disco óptico.
Ver também: Documento digital, Dossiê, Processo híbrido.

E-mail

Ver Correio eletrônico.

ECM

Ver Entreprise Content Management.

Elemento extrínseco

Parte integrante do documento arquivístico que constitui sua forma externa. *Exemplo:* tipo, cor e tamanho da letra; apresentação (textual, gráfica, sonora ou multimídia); selo, logomarca; assinatura digital; links; e outros.

Ver também: Completeza, Documento arquivístico, Elemento intrínseco, Forma documental, Marca d'água digital.

Elemento intrínseco

Parte integrante do documento arquivístico que constitui sua forma interna e que transmite a ação da qual o documento participa, bem como seu contexto imediato. *Exemplo:* autor, destinatário, data, local, assinatura autógrafa, assunto e outros.

Ver também: Completeza, Documento arquivístico, Elemento extrínseco, Forma documental.

Eliminação

Destruição de documentos que, na avaliação, foram considerados sem valor para a guarda permanente (ARQUIVO NACIONAL, 2005, p. 81), impedindo qualquer possiblidade de reconstrução.

Ver também: Destinação.

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.

Ver também: Preservação digital.

Endereço de correio eletrônico

Nome único de uma caixa postal eletrônica, de uma pessoa, grupo ou organização, associado a um serviço de correio eletrônico. É formado por um identificador (nome, apelido, sigla ou código), um sinal "@" e o domínio do provedor do serviço. (I) E-mail Address.

Ver também: Correio eletrônico, Mensagem de correio eletrônico.

Entreprise Content Management (ECM)

Termo amplo para tecnologia digital, estratégias e métodos utilizados para capturar, gerir, acessar, integrar, medir e armazenar informação. Pode incluir módulos específicos para documentos que apoiam as atividades das organizações e ajudam no processo de tomada de decisão.

Ver também: Gerenciamento eletrônico de documentos.

Esquema de codificação de metadados

Definição dos valores ou da sintaxe de um elemento de metadados. *Exemplo:* pode ser uma lista controlada dos valores aceitos para um elemento de metadados em linguagem natural, um vocabulário controlado ou uma tabela de classificação. Pode também ser um esquema de codificação que define a estrutura ou sintaxe dos valores, como por exemplo, o formato DDMMAAAA para data e o formato hh:mm:ss±hh para hora. (I) Encoding Scheme.

Ver também: Esquema de metadados, Metadados.

Esquema de metadados

Plano lógico que mostra as relações entre os elementos de metadados, através do estabelecimento de regras para a utilização e gestão de metadados, especificamente no que diz respeito à semântica, à sintaxe e à obrigatoriedade do uso. (I) Metadata Schema.

Ver também: Esquema de codificação de metadados, Metadados.

Exportação

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

Ver também: Conversão de formato.

Fidedignidade

Ver Confiabilidade.

Fixidade

Integridade da cadeia de bits que constituem um componente digital. (I) Fixity.

Ver também: Fixidez, Forma fixa.

Fixidez

Qualidade de um documento que assegura a forma fixa e o conteúdo estável. (I) Fixity.

Ver também: Conteúdo estável, Documento arquivístico, Documento arquivístico digital, Fixidade, Forma fixa, Forma documental.

Forma documental

Regras de representação de acordo com as quais o conteúdo de um documento arquivístico, seu contexto administrativo e documental, e sua autoridade são comunicados. A forma documental possui elementos intrínsecos e extrínsecos. (INTERPARES 3 PROJECT, 2011), (I) Documentary Form.

Ver também: Documento arquivístico, Elemento extrínseco, Elemento intrínseco, Fixidez.

Forma fixa

Característica de um documento arquivístico que assegura que sua aparência ou apresentação documental permanece a mesma cada vez que o documento é manifestado (UNIVERSIDADE FEDERAL DA FRONTEIRA DO SUL, 2020).

Ver também: Conteúdo estável, Fixidade, Fixidez.

Formato aberto de arquivo

Quando as especificações do formato de arquivo são públicas. *Exemplo:* XML, HTML, ODF, RTF, TXT e PNG.

Ver também: Formato fechado de arquivo, Formato de arquivo, Formato não proprietário de arquivo, Formato padronizado de arquivo, Formato proprietário de arquivo.

Formato de arquivo

Especificação de regras e padrões descritos formalmente para a interpretação dos bits constituintes de um arquivo digital. Pode ser: aberto, fechado, proprietário, não proprietário e/ou padronizado. (I) Format, (F) Format, (E) Formato.

Ver também: Conversão de formato, Formato aberto de arquivo, Formato fechado de arquivo, Formato não proprietário de arquivo, Formato padronizado de arquivo, Formato proprietário de arquivo, Normalização de formato.

Formato fechado de arquivo

Quando as especificações não são divulgadas pelo proprietário. *Exemplo:* DOC.

Ver também: Formato aberto de arquivo, Formato de arquivo, Formato não proprietário de arquivo, Formato padronizado de arquivo, Formato proprietário de arquivo.

Formato não proprietário de arquivo

Quando o uso das especificações não tem restrição de licença.

Ver também: Formato aberto de arquivo, Formato de arquivo, Formato fechado de arquivo, Formato padronizado de arquivo, Formato proprietário de arquivo.

Formato padronizado de arquivo

Quando as especificações são produzidas por um organismo de normalização, sendo os formatos abertos. *Exemplo:* XML, PDF/A.

Ver também: Formato aberto de arquivo, Formato de arquivo, Formato fechado de arquivo, Formato não proprietário de arquivo, Formato proprietário de arquivo.

Formato proprietário de arquivo

Quando as especificações são definidas por uma empresa que mantém seus direitos, sendo seu uso vinculado a uma licença. *Exemplo:* PDF, JPEG, DOC e GIF.

Ver também: Formato aberto de arquivo, Formato de arquivo, Formato fechado de arquivo, Formato não proprietário de arquivo, Formato padronizado de arquivo.

GED

Ver Gerenciamento eletrônico de documentos.

Gerenciamento Eletrônico de Documentos

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.

Ver também: Entreprise Content Management, Gestão arquivística de documentos.

Gestão arquivística de documentos

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

Nota: neste documento, a expressão "gestão arquivística de documentos" é usada como sinônimo de "gestão de documentos", ressaltando a característica arquivística dessa gestão para diferenciá-la de outros tipos de gerenciamento de documentos.

Ver também: Ciclo vital dos documentos, Gerenciamento eletrônico de documentos, 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 de seu conteúdo e com o objetivo de limitar sua divulgação a quem tem necessidade de conhecê-lo.

Ver também: Classificação de segurança.

Handle System

Sistema distribuído de computadores concebido para assinalar, armazenar, administrar e resolver identificadores ou nomes persistentes de objetos digitais conhecidos como *handles*.
Ver também: Identificador persistente.

Hardware

Conjunto dos componentes físicos necessários à operação de um sistema computacional. (I) Hardware, (E) Hardware, (F) Matériel.
Ver também: Contexto tecnológico.

Hipermídia

Ampliação do conceito de hipertexto segundo a qual vários meios e armazenamento e transmissão de informação são integrados através de enlaces (hyperlinks), permitindo a utilização simultânea de sons, imagens estáticas e em movimento, e textos. (I) Hypermedia.
Ver também: Hipertexto.

Hipertexto

Forma de estruturação de documentos que permite a leitura por meio de enlaces (hyperlinks) que possibilitam a conexão direta entre os diversos itens de um documento e/ou deste para outros. (I) Hypertext.
Ver também: Hipermídia.

ICP

Ver Infraestrutura de Chaves Públicas.

Identidade

Conjunto dos atributos de um documento arquivístico que o caracterizam como único e o diferenciam de outros documentos arquivísticos. *Exemplo*: data, autor, destinatário, assunto, número identificador e número de protocolo.
Ver também: Autenticidade, Documento arquivístico autêntico, Integridade.

Identificador persistente

Identificador de longa duração de um recurso na internet que se mantém válido mesmo que a tecnologia de acesso ou a localização física do recurso identificado se modifique no tempo. (I) Persistent Identifier.
Ver também: Handle System, URN.

Identificador único

Código gerado automaticamente que identifica o dossiê, o processo ou o item documental de maneira a distingui-los dos demais. (I) Unique Identifier.
Ver também: Controle de versão, Registro.

Indexação

Processo pelo qual documentos ou informações são representados por termos, palavras-chave ou descritores, propiciando a recuperação da informação. (ARQUIVO NACIONAL, 2005, p. 107)

Informação

Elemento referencial, noção, ideia ou mensagem contidos num documento. (ARQUIVO NACIONAL, 2005, p. 107)

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 composto por uma cadeia de autoridades certificadoras formada pela autoridade certificadora raiz – AC Raiz, pelas demais autoridades certificadoras – AC e pelas autoridades de registro – AR.

Ver também: Autoridade certificadora, Autoridade de Carimbo do Tempo, Autoridade de registro, Carimbo digital do tempo, Certificado digital, Chave privada, Chave pública, Criptografia assimétrica.

Integridade

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

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

Ver também: Autenticidade, Documento arquivístico autêntico, Identidade.

Item documental

Menor unidade arquivística intelectualmente indivisível.

Ver também: Dossiê.

Marca d'água digital

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

Ver também: Elemento extrínseco.

Mensagem de correio eletrônico

Documento digital produzido ou recebido via um sistema de correio eletrônico, incluindo anexos que possam ser transmitidos com a mensagem. (I) Email Message.

Ver também: Anexo, Correio eletrônico, Endereço de correio eletrônico.

Metadados

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

Ver também: Dado, Esquema de codificação de metadados, Esquema de metadados.

Mídia

Ver Suporte.

Migração

Conjunto de procedimentos e técnicas para assegurar a capacidade de os objetos digitais serem acessados frente às 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 uma outra mais moderna.

Ver também: Atualização de suporte, Conversão de formato, Objeto digital, Preservação digital, Reformatação (migração).

Minuta

Redação preliminar de documento sujeita à aprovação. (ARQUIVO NACIONAL, 2005, p. 123)

Ver também: Original.

Normalização de formato

Conversão de formatos de arquivo para um elenco gerenciável de formatos apropriados para preservação e acesso.

Ver também: Conversão de formato, Formato de arquivo.

Objeto digital

Unidade de informação em formato digital composta de uma ou mais cadeias de bits e de metadados que a identificam e descrevem suas propriedades. (I) Digital Object.

Ver também: Arquivo digital, Componente digital, Migração.

OCR (Optical Character Recognition)

Técnica de conversão de um objeto digital do formato de imagem para o formato textual, de forma a permitir, por exemplo, edição e pesquisa no conteúdo do texto.

Ver também: Digitalização.

Optical Character Recognition

Ver OCR.

Organicidade

Atributo do conjunto de documentos arquivísticos que mantêm relação orgânica entre si. Essencial para que um determinado conjunto de documentos seja considerado um arquivo. (F) Organicité, (E) Organicidad.

Ver também: Arquivo (Fundo), Relação orgânica.

Original

Primeiro documento completo e efetivo.

Ver também: Documento, Minuta.

Plano de classificação

Esquema de distribuição de documentos em classes, de acordo com métodos de arquivamento específicos, elaborado a partir do estudo das estruturas e funções de uma instituição e da análise do arquivo por ela produzido. Expressão geralmente adotada em arquivos correntes. (ARQUIVO NACIONAL, 2005, p. 132)

Ver também: Classe, Classificação arquivística, Código de classificação.

Preservação digital

Conjunto de ações gerenciais e técnicas exigidas para superar as mudanças tecnológicas e a fragilidade dos suportes, garantindo o acesso e a interpretação de documentos digitais pelo tempo que for necessário.

Ver também: Atualização de suporte, Componente digital, Emulação, Migração.

Presunção de autenticidade

Inferência da autenticidade de um documento arquivístico feita a partir de fatos conhecidos sobre a maneira como aquele documento foi produzido e mantido.

Ver também: Autenticidade.

Processo

Conjunto de documentos oficialmente reunidos no decurso de uma ação administrativa ou judicial, que constitui uma unidade.

Ver também: Dossiê, Processo híbrido.

Processo híbrido

Processo constituído de documentos digitais e não digitais de natureza diversa, oficialmente reunidos no decurso de uma ação administrativa ou judicial, formando um conjunto conceitualmente indivisível.

Ver também: Documento digital, Dossiê híbrido.

Produtor

Pessoa física ou jurídica que produz, recebe ou acumula documentos arquivísticos em função de seu mandato/missão, funções ou atividades.

Ver também: Arquivo (Fundo), Relação orgânica.

Programa de computador

Sequência lógica de instruções que o computador é capaz de executar para obter um resultado específico.

Ver também: Contexto tecnológico, Hardware, Sistema Gerenciador de Banco de Dados.

Recolhimento

Uma das formas de entrada de documentos em arquivos permanentes, refere-se à etapa final do processo de gestão documental.

Nota: a entrada de documentos em arquivos permanentes também pode ocorrer por aquisição (doação, compra etc.).

Ver também: Custódia, Destinação, Transferência.

Recuperação da informação

Processo de pesquisa, localização e apresentação do documento em sistemas de informação. A pesquisa é feita por intermédio da formulação de estratégias de busca para identificação e localização de documentos e/ou seus metadados. A apresentação pode ser feita por meio de visualização em tela, impressão, leitura de dados de áudio e/ou vídeo.

Ver também: Sistema de informação.

Reformatação (migração)

Técnica de migração que consiste na mudança da forma de apresentação de um documento para fins de acesso ou manutenção dos dados. *Exemplo:* impressão ou transformação de documentos digitais em microfilme (tecnologia COM), ou ainda, a captura de um documento para o meio digital por intermédio da digitalização. (I) Reformatting.

Ver também: Atualização de suporte, Conversão de formato, Digitalização, Migração.

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 etc.) que descrevem o documento.

Ver também: Captura, Identificador único.

Relação orgânica

Conjunto dos vínculos que os documentos arquivísticos mantêm entre si, na medida em que representam e refletem as atividades e funções da entidade produtora. Os documentos arquivísticos não são coletados artificialmente, mas estão ligados uns aos outros por um elo que se materializa por meio do registro ou do plano de classificação ou do arquivamento, que os contextualiza no conjunto ao qual pertencem. Os documentos arquivísticos apresentam um conjunto de relações que devem ser mantidas. (I) Archival Bond.

Ver também: Documento arquivístico, Organicidade.

Repositório arquivístico digital

Repositório digital que armazena e gerencia documentos arquivísticos, seja nas fases corrente e intermediária, seja na fase permanente. (CONARQ, 2014, p. 9)

Ver também: Repositório digital.

Repositório digital

Plataforma tecnológica que apoia o gerenciamento dos materiais digitais, pelo tempo que for necessário, e é formado por elementos de *hardware*, *software* e metadados, bem como por uma infraestrutura organizacional e procedimentos normativos e técnicos. (CONARQ, 2014)

Ver também: Repositório arquivístico digital.

Representante digital

Representação em formato digital de um documento originalmente não digital. É uma forma de diferenciá-lo do documento de arquivo nato digital. (I) Digital Surrogate.

Ver também: Digitalização, Documento não digital.

Requisito funcional

Requisito que especifica uma função que o sistema deve ser capaz de realizar sob o ponto de vista do usuário final. *Exemplo:* no e-ARQ Brasil, os requisitos funcionais tratam de organização de documentos (incluindo o plano de classificação), captura, avaliação (incluindo a destinação), recuperação da informação, elaboração de documentos, tramitação, segurança e preservação.

Ver também: Requisito não funcional.

Requisito não funcional

Requisito que não está diretamente relacionado à funcionalidade do sistema, mas que são relevantes para a sua implementação. *Exemplo:* no e-ARQ Brasil, os requisitos não funcionais tratam de armazenamento, funções administrativas, conformidade com a legislação e regulamentações, usabilidade, interoperabilidade, disponibilidade, desempenho e escalabilidade.

Ver também: Requisito funcional.

Restrição de acesso

Denominação genérica para as diversas possibilidades de categorização de restrição de acesso às quais pode estar vinculado um documento.

Nota: podem ser graus (reservado, secreto e ultrassecreto) e em fase preparatória, cujo uso é restrito aos órgãos públicos, mas podem ser ainda, dentre outras previstas em legislação, sigilo quanto a informações pessoais, sigilo bancário, sigilo fiscal, segredo de justiça, sigilo telefônico, sigilo industrial etc.

Ver também: Acesso, Classificação de segurança.

SIGAD

Ver Sistema Informatizado de Gestão Arquivística de Documentos.

Sistema de armazenamento

Solução tecnológica de *hardware* e *software* utilizada para armazenar dados.

Ver também: Armazenamento (Documento digital).

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 de informação, Sistema Informatizado de Gestão Arquivística de Documentos.

Sistema de informação

Conjunto organizado, não necessariamente informatizado, de políticas, procedimentos, pessoas, equipamentos e programas computacionais que produzem, processam, armazenam e provêm acesso à informação. (I) Information System.

Ver também: Recuperação da informação, Sistema de negócio, Sistema de gestão arquivística de documentos.

Sistema de negócio

É um sistema informatizado projetado e construído para atender a processo específico da organização. *Exemplo:* sistemas de recursos humanos, atividades financeiras, acadêmicos, prontuários e informação geográfica.

Ver também: Sistema de informação, Sistema informatizado.

Sistema de storage

Ver: Sistema de armazenamento.

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: Banco de dados (ambiente computacional), Base de dados, Programa de computador.

Sistema informatizado

Sistema que apoia o acesso e a gestão de dados, informação e/ou documentos em um sistema computacional.

Ver também: Sistema de negócio, Sistema Informatizado de Gestão Arquivística de Documentos.

Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD)

Conjunto de procedimentos e operações técnicas característico do sistema de gestão arquivística de documentos, processado eletronicamente e aplicável em ambientes digitais ou em ambientes híbridos, isto é, em que existem documentos digitais e não digitais ao mesmo tempo.

Ver também: Gestão arquivística de documentos, Sistema de gestão arquivística de documentos, Trilha de auditoria.

Software

Ver Programa de computador.

Suporte

Base física sobre a qual a informação é registrada. (I) Medium, (I) Storage Medium.

Ver também: Documento.

Timestamp

Ver Carimbo digital do tempo.

Tramitação

Curso do documento desde a sua produção ou recepção até o cumprimento de sua função administrativa. Também denominado de trâmite ou movimentação. (ARQUIVO NACIONAL, 2005, p. 164)

Transferência

Passagem de documentos do arquivo corrente para o arquivo intermediário. (ARQUIVO NACIONAL, 2005, p. 165)

Nota: a transferência contempla mais que a movimentação da documentação, física ou de um sistema para outro. Abrange a assunção de que o documento concluiu seus objetivos e a formalização da passagem da responsabilidade pela manutenção dos documentos a uma unidade institucional com essa competência.

Ver também: Recolhimento.

Trilha de auditoria

Conjunto de informações registradas que permite o rastreamento de intervenções ou tentativas de intervenções feitas no documento arquivístico digital ou no sistema computacional. (I) Audit Trail.

Ver também: Sistema Informatizado de Gestão Arquivística de Documentos.

URN (Uniform Resource Name)

Nome atribuído a um recurso informacional na internet que tem por objetivo sua identificação única, de forma persistente e independente da sua localização, de modo que seja possível encontrá-lo.

Valor primário

Valor atribuído a documento em função do interesse que possa ter para a entidade produtora, levando-se em conta a sua utilidade para fins administrativos, legais e fiscais. (ARQUIVO NACIONAL, 2005, p. 171)

Ver também: Avaliação, Valor secundário.

Valor secundário

Valor atribuído a um documento em função do interesse que possa ter para a entidade produtora e outros usuários, tendo em vista a sua utilidade para fins diferentes daqueles para os quais foi originalmente produzido. (ARQUIVO NACIONAL, 2005, p. 172)

Ver também: Avaliação, Valor primário.

Versão

Uma ou mais variantes de um mesmo documento. Uma versão geralmente é uma instância de um documento feita durante seu processo de elaboração. No entanto, uma versão também pode indicar uma forma diferente do documento, tal como uma versão resumida, uma tradução ou uma adaptação. (I) Version.

Nota: subsequentes revisões de um documento são diferentes versões.

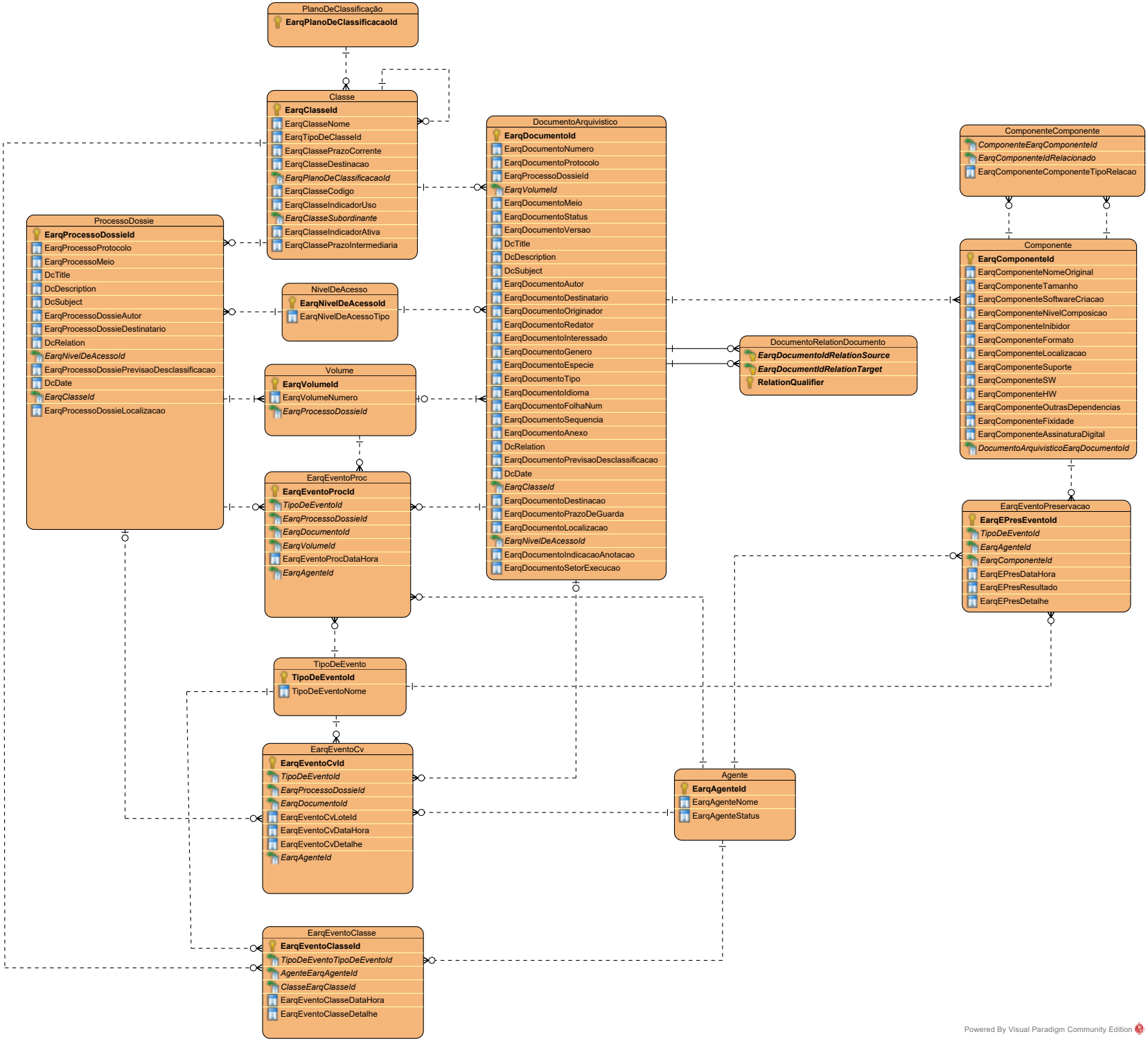
Ver também: Controle de versão.

ANEXO

Modelo de Entidades e Relacionamentos do e-ARQ Brasil

O Modelo de Entidades e Relacionamentos (MER) tem por objetivo orientar a estruturação do banco de dados na implementação de um Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD). O MER é um modelo conceitual e, como tal, é uma abstração da realidade de acordo com o e-ARQ Brasil. Como todo modelo conceitual, não trata de todos os aspectos da implementação, como o armazenamento dos componentes digitais, mas pode ser utilizado para apoiar a comunicação, o aprendizado e a análise de determinados aspectos relevantes da gestão arquivística de documentos.

O diagrama a seguir apresenta as entidades e relacionamentos mais significativos para a implementação de um SIGAD, sem esgotar todas as possibilidades.


PlanoDeClassificação
EarqPlanoDeClassificacaoId
Classe
EarqClasseId
EarqClasseNome
EarqTipoDeClasseId
EarqClassePrazoCorrente
EarqClasseDestinacao
EarqPlanoDeClassificacaoId
EarqClasseCodigo
EarqClasseIndicadorUso
EarqClasseSubordinante
EarqClasseIndicadorAtiva
EarqClassePrazoIntermediaria
DocumentoArquivistico
EarqDocumentoId
EarqDocumentoNumero
EarqDocumentoProtocolo
EarqProcessoDossieId
EarqVolumeId
EarqDocumentoMeio
EarqDocumentoStatus
EarqDocumentoVersao
DcTitle
DcDescription
DcSubject
EarqDocumentoAutor
EarqDocumentoDestinatario
EarqDocumentoOriginador
EarqDocumentoRedator
EarqDocumentoInteressado
EarqDocumentoGenero
EarqDocumentoEspecie
EarqDocumentoTipo
EarqDocumentoIdioma
EarqDocumentoFolhaNum
EarqDocumentoSequencia
EarqDocumentoAnexo
DcRelation
EarqDocumentoPrevisaoDesclassificacao
DcDate
EarqClasseId
EarqDocumentoDestinacao
EarqDocumentoPrazoDeGuarda
EarqDocumentoLocalizacao
EarqNivelDeAcessoId
EarqDocumentoIndicacaoAnotacao
EarqDocumentoSetorExecucao
ComponenteComponente
ComponenteEarqComponenteId
EarqComponenteIdRelacionado
EarqComponenteComponenteTipoRelacao
Componente
EarqComponenteId
EarqComponenteNomeOriginal
EarqComponenteTamanho
EarqComponenteSoftwareCriacao
EarqComponenteNivelComposicao
EarqComponenteInibidor
EarqComponenteFormato
EarqComponenteLocalizacao
EarqComponenteSuporte
EarqComponenteSW
EarqComponenteHW
EarqComponenteOutrasDependencias
EarqComponenteFixidade
EarqComponenteAssinaturaDigital
DocumentoArquivisticoEarqDocumentoId
ProcessoDossie
EarqProcessoDossieId
EarqProcessoProtocolo
EarqProcessoMeio
DcTitle
DcDescription
DcSubject
EarqProcessoDossieAutor
EarqProcessoDossieDestinatario
DcRelation
EarqNivelDeAcessoId
EarqProcessoDossiePrevisaoDesclassificacao
DcDate
EarqClasseId
EarqProcessoDossieLocalizacao
NivelDeAcesso
EarqNivelDeAcessoId
EarqNivelDeAcessoTipo
DocumentoRelationDocumento
EarqDocumentoIdRelationSource
EarqDocumentoIdRelationTarget
RelationQualifier
Volume
EarqVolumeId
EarqVolumeNumero
EarqProcessoDossieId
EarqEventoProc
EarqEventoProcId
TipoDeEventoId
EarqProcessoDossieId
EarqDocumentoId
EarqVolumeId
EarqEventoProcDataHora
EarqAgenteId
EarqEventoPreservacao
EarqEPresEventoId
TipoDeEventoId
EarqAgenteId
EarqComponenteId
EarqEPresDataHora
EarqEPresResultado
EarqEPresDetalhe
TipoDeEvento
TipoDeEventoId
TipoDeEventoNome
EarqEventoCv
EarqEventoCvId
TipoDeEventoId
EarqProcessoDossieId
EarqDocumentoId
EarqEventoCvLoteId
EarqEventoCvDataHora
EarqEventoCvDetalhe
EarqAgenteId
Agente
EarqAgenteId
EarqAgenteNome
EarqAgenteStatus
EarqEventoClasse
EarqEventoClasseId
TipoDeEventoTipoDeEventoId
AgenteEarqAgenteId
ClasseEarqClasseId
EarqEventoClasseDataHora
EarqEventoClasseDetalhe
Powered By Visual Paradigm Community Edition

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). Disponível em: https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/dicionrio_de_terminologia_arquivistica.pdf. Acesso em: 31 dez. 2021.

BRASIL. Padrão de metadados do governo eletrônico – e-PMG, v. 1.1, jul. 2014. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/PMGVersao1_1.pdf. Acesso em: 10 mai. 2021.

_____. Ministério da Defesa. Marinha. *Normas sobre documentação administrativa e arquivamento na Marinha (NODAM)*. Brasília, 2000.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). Resolução n. 39, de 29 de abril de 2014. Estabelece diretrizes para a implementação de repositórios arquivísticos digitais confiáveis para o arquivamento e manutenção de documentos arquivísticos digitais em suas fases corrente, intermediária e permanente, dos órgãos e entidades integrantes do Sistema Nacional de Arquivos – SINAR. Disponível em: https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/conarq_diretrizes_rdc_arq_resolucao_43.pdf. Acesso em: 31 dez. 2021.

_____. Câmara Técnica de Documentos Eletrônicos. *Glossário*: documentos arquivísticos digitais. v. 8, 2020. Disponível em: https://www.gov.br/conarq/pt-br/assuntos/camaras-tecnicas-setoriais-inativas/camara-tecnica-de-documentos-eletronicos-ctde/glosctde_2020_08_07.pd. Acesso em: 31 dez. 2021.

CONSELHO INTERNACIONAL DE ARQUIVOS (CIA). Committee on electronic records. *Guide for managing electronic records from an archival perspective*. Paris, 1997. (ICA Studies, n. 8). Disponível em: https://www.ica.org/en/ica-study-n%C2%B08-guide-managing-electronic-records-archival-perspective. Acesso em: 14 maio 2010.

_____. *ISAD(G)*: Norma geral internacional de descrição arquivística. 2. ed., 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).

_____. *ISAAR(CPF)*: Norma internacional de registro de autoridade arquivística para entidades coletivas, pessoas e famílias, adotada pelo Comitê de Normas e Descrição, Canberra, Austrália, 27-30 de outubro de 2003. 2. ed. Rio de Janeiro: Arquivo Nacional, 2004. (Publicações Técnicas, n. 50).

_____. Comité de arquivos correntes em ambiente electrónico. *Documentos de arquivo electrónicos*: manual para arquivistas. Paris, 2005. (Estudo n. 16 do ICA). Disponível em: https://www.ica.org/en/ica-study-n%C2%B016-electronic-records-workbook-archivists. Acesso em: 14 maio 2010.

COSTA, Eliezer Arantes. *Gestão estratégica*. São Paulo: Saraiva, 2003.

DLM Forum Foundation. *MoReq*: Model requirements for the management of electronic records. Luxembourg: European Communities, 2002. Disponível em: https://moreq.info/. Acesso em: 24 jan. 2020.

_____. *MoReq 2*: Model requirements for the management of electronic records update and extension. 2007. Disponível em: https://moreq.info/. Acesso em: 24 jan. 2020.

_____. *MoReq 2010*: Modular requirements for records systems. 2011. Disponível em: https://www.moreq.info/. Acesso em: 24 jan. 2020.

DURANTI, Luciana. The InterPARES Project. In: *Authentic records in the electronic age*. Vancou-

ver: University of British Columbia, 2000. Disponível em: http://www.interpares.org/documents/interpares_symposium_2000.pdf. Acesso em: 17 jan. 2022.

_____ et al. *Preservation of the integrity of electronic records*. Dordrecht: Kluwer Academic, 2002.

_____ (ed.). *The long-term preservation of the authentic electronic records*: findings of the InterPARES Project. San Miniato: Archilab, 2005.

_____; 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).

INSTITUTO DOS ARQUIVOS NACIONAIS (Portugal). Torre do Tombo. Instituto de Informática. Modelo de requisitos para a gestão de arquivos eletrônicos. v. 2. In:_____. *Recomendações para a gestão de documentos de arquivo eletrônicos*. Lisboa, 2002.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (Brasil). *Glossário*. 2017. Disponível em: https://www.gov.br/iti/pt-br/centrais-de-conteudo/glossario. Acesso em: 31 dez. 2021.

INTERNATIONAL COUNCIL ON ARCHIVES (ICA). Documentos de arquivo electrónico: manual para arquivistas. Estudo n. 16, 2005. Disponível em: https://www.ica.org/sites/default/files/ICA_Study-16-Electronic-records_PT.pdf. Acesso em: 24 jan. 2020.

_____. *Principles and functional requirements for records in electronic office environments*. Paris: International Council on Archives, 2013. Disponível em: https://www.ica.org/sites/default/files/11.%20Recordkeeping%20Requirements%20for%20Multiple%20Functions%20supported%20by%20one%20Business%20System.pdf. Acesso em: 7 jan. 2022.

INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS. *InterPARES Project*. Disponível em: http://www.interpares.org. Acesso em: 24 jan. 2020.

INTERPARES 3 PROJECT. Team Canada. *Intellectual Framework*. v. 2.0, 2008. Disponível em: http://www.interpares.org/display_file.cfm?doc=ip3_intellectual_framework.pdf. Acesso em: 31 dez. 2021.

_____. Team Brasil. *Terminology database*. 2011. Disponível em: http://www.interpares.org/ip3/ip3_terminology_db.cfm?letter=f&term=79. Acesso em: 31 dez. 2021.

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (United States). *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: 24 jan. 2020.

_____. *Electronic records management initiative*. Disponível em: http://www.archives.gov/records-mgmt/initiatives/erm-overview.html. Acesso em: 14 maio 2010.[73]

PORTUGAL. *Metainformação para interoperabilidade de Portugal – MIP.* Lisboa, 2006. Disponível em: https://arquivos.dglab.gov.pt/wp-content/uploads/sites/16/2013/10/MIP_v1-0c.pdf. Acesso em: 24 jan. 2020.

PREMIS Data Dictionary for Preservation Metadata – version 3. 2015. Disponível em: http://www.loc.gov/standards/premis/v3/premis-3-0-final.pdf. Acesso em: 24 jan. 2020.

_____. *Requirements for electronic records management systems*: functional requirements. 2002. Disponível em: https://www.nationalarchives.gov.uk/documents/requirementsfinal.pdf. Acesso em: 14 maio 2010.

RONDINELLI, Rosely Curi. *Gerenciamento arquivístico de documentos eletrônicos*: uma aborda-

73 Não se encontra mais disponível no endereço citado. A instituição informa que produziu um novo documento sobre o tema: NARA. *Transfer guidance*. Disponível em: https://www.archives.gov/records-mgmt/policy/transfer-guidance.html. Acesso em: 24 jan. 2020.

gem 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 15489:2017 – Records management.* Part 1: general [and] Part 2: guidelines. Sidney, 2002. Disponível em: https://www.standards.org.au/standards-catalogue/sa-snz/publicsafety/it-021/as--iso--15489-dot-1-colon-2017. Acesso em: 24 jun. 2020.

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: 24 jan. 2020.

UNITED KINGDOM. Public Record Office. *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.[74]

_____. e-Government Metadata Standard – e-GMS, v. 3.0, 2004. Disponível em: https://www.nationalarchives.gov.uk/documents/information-management/egms-metadata-standard.pdf. Acesso em: 24 jan. 2020.

UNIVERSIDADE ESTADUAL DE CAMPINAS. Sistema de Arquivos. *Manual de gestão de processos e de expedientes no âmbito da Universidade Estadual de Campinas*. Disponível em: https://www.siarq.unicamp.br/siarq/images/siarq/protocolos_e_arquivos/manual_protocolo_expediente.pdf. Acesso em: 24 jun. 2020.

UNIVERSIDADE FEDERAL DA FRONTEIRA DO SUL. *Glossário sobre documentos arquivísticos digitais*. 2020. Disponível em: https://portalsei.uffs.edu.br/gestao-documental/glossario-de-gestao-de-documentos. Acesso em: 31 dez. 2021.

USA. Department of Defense. *Design criteria standard for electronic records management software applications*: DOD 5015.2-STD. Washington, 2002. Disponível em: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/501502std.pdf. Acesso em: 24 jan.

74 Não se encontra mais disponível no endereço citado. UNITED KIGDOM. Public Record Office. *Appraisal policy.* Disponível em: https://www.nationalarchives.gov.uk/documents/information-management/appraisal_policy.pdf. Acesso em: 24 jan. 2020.