Conarq
CONSELHO NACIONAL DE ARQUIVOS

Câmara Técnica de Documentos Eletrônicos

MODELO DE REQUISITOS PARA SISTEMAS INFORMATIZADOS DE GESTÃO ARQUIVÍSTICA DE DOCUMENTOS

e-ARQ Brasil

2006

dezembro

Versão 1

EQUIPE TÉCNICA DE ELABORAÇÃO DO E-ARQ BRASIL

Equipe de redação da Câmara Técnica de Documentos Eletrônicos

Claudia Lacombe Rocha - Arquivo Nacional
Margareth da Silva - Arquivo Nacional
Rosely Cury Rondinelli – Museu do Índio

Integrantes da Câmara Técnica de Documentos Eletrônicos que participaram deste trabalho

Ana Pavani – PUC-RJ – até setembro de 2004
Carlos Augusto Silva Ditadi – Arquivo Nacional
Carmen Tereza Coelho Moreno – Biblioteca Nacional – até julho de 2005
Ednylton Franzosi – Ministério do Planejamento, Orçamento e Gestão
Gladys Machado Pereira Santos Lima – Marinha do Brasil
Humberto Innarelli – Universidade Estadual de Campinas
Luiz Fernando Sayão – Comissão Nacional de Energia Nuclear
Marcos de Oliveira Matos - Marinha do Brasil – até julho de 2004
Maria Izabel de Oliveira – Arquivo Nacional
Maria Rosangela da Cunha – Marinha do Brasil
Neire do Rossio Martins – Universidade Estadual de Campinas
Paulo Roberto Ferreira Passos – Presidência da Republica
Sergio Dagnino Falcão – Câmara dos Deputados
Vanderlei Batista dos Santos - Câmara dos Deputados

Colaboradores

Ana Celeste Indolfo - Arquivo Nacional
Brenda Couto de Brito Rocco - Arquivo Nacional
Elisabeth Maçulo - Arquivo Nacional
Eugênio Pacelli - Casa Civil da Presidência da República
Nilmar Saísse – Analista de Sistemas
Rodolfo de Sousa Nascimento - Arquivo Nacional
Vera Lúcia Hess de Mello Lopes - Arquivo Nacional

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

Revisão

Alba Gisele Gouget – Arquivo Nacional
Mariana Simões – Arquivo Nacional

Sumário

Introdução

Neste documento é apresentado um Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos – e-ARQ Brasil - que foi elaborado no âmbito da Câmara Técnica de Documentos Eletrônicos do Conselho Nacional de Arquivos no período de 2004 a 2006.

Esse trabalho foi desenvolvido considerando a existência de um importante legado de documentos em formato digital, cujas características vem sendo tratadas por especialistas de diversas áreas entre as quais arquivologia e tecnologia da informação. Esses especialistas conceituam o documento arquivístico e o documento arquivístico digital para poderem analisar e proporem soluções que enfrentem o desafio trazido por este formato.

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

O que é documento arquivístico?

É um documento produzido e/ou recebido por uma pessoa física ou jurídica, no decorrer das suas atividades, qualquer que seja o suporte, e dotado de organicidade.

O que é documento arquivístico digital?

É um documento arquivístico codificado em dígitos binários, produzido, tramitado e armazenado por sistema computacional. São exemplos de documentos arquivísticos digitais: textos, imagens fixas, imagens em movimento, gravações sonoras, mensagens de correio eletrônico, páginas web, bases de dados, dentre outras possibilidades de um vasto repertório de diversidade crescente.

O que é documento arquivístico convencional?

É um documento arquivístico produzido, tramitado e armazenado em formato não digital.

Além disso, foram levados em consideração os fundamentos da diplomática[1], da arquivologia, especialmente da gestão de documentos, e da tecnologia da informação para fornecer um conjunto de requisitos que seja amplo, rigoroso e de qualidade.

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

O que é e-ARQ Brasil?

É uma especificação de requisitos que estabelece um conjunto de condições a serem cumpridas pela organização produtora/recebedora de documentos, pelo sistema de gestão arquivística e pelos próprios documentos a fim de garantir a sua confiabilidade e autenticidade, assim como seu acesso.

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- independente da plataforma tecnológica em que for desenvolvido e/ou implantado.

O objeto do e-ARQ Brasil é o documento arquivístico digital. Este documento não trata de processos de digitalização, isto é, de procedimentos técnicos de conversão de um documento em qualquer suporte ou formato para o formato digital, por meio de dispositivo apropriado, como o escâner.

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

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

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

O que é SIGAD?

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

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

A produção de documentos digitais levou à criação de *sistemas informatizados de gerenciamento de documentos*. Entretanto, para se assegurar que documentos arquivísticos digitais sejam confiáveis e autênticos e que possam ser preservados com

essas características, é fundamental que os sistemas acima referidos incorporem os conceitos arquivísticos e suas implicações no gerenciamento dos documentos digitais.

Nesse sentido, é importante estabelecer a diferença entre *Sistema de Informação*, *Gestão Arquivística de Documentos*, *Sistema de Gestão Arquivística de Documentos*, *Gerenciamento Eletrônico de Documentos* (GED) e *Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD)*.

Sistema de Informação

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

Gestão Arquivística de Documentos

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

Sistema de Gestão Arquivística de Documentos

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

Gerenciamento Eletrônico de Documentos (GED)

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

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

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

Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD)

É um conjunto de procedimentos e operações técnicas, característico do sistema de gestão arquivística de documentos, processado por computador.

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

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

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

A partir dessas definições podemos tecer as seguintes considerações:

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

Requisitos arquivísticos que caracterizam um SIGAD:

• captura, armazenamento, indexação e recuperação de todos os tipos de documentos arquivísticos;

• captura, armazenamento, indexação e recuperação de todos os componentes digitais do documento arquivístico como uma unidade complexa[3];

• gestão dos documentos a partir do plano de classificação para manter a relação orgânica entre os documentos;

• implementação de metadados associados aos documentos para descrever os contextos desses mesmos documentos (jurídico-administrativo, de proveniência, de procedimentos, documental e tecnológico)[4];

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

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

[4] Ver Glossário.

• integração entre documentos digitais e convencionais;

• foco na manutenção da autenticidade dos documentos;

• avaliação e seleção dos documentos para recolhimento e preservação daqueles considerados de valor permanente;

• aplicação de tabela de temporalidade e destinação de documentos;

• transferência e o recolhimento dos documentos por meio de uma função de exportação.

• gestão de preservação dos documentos.

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

1 OBJETIVOS

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

2 ÂMBITO E UTILIZAÇÃO:

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

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

Desde que a organização estabeleça um programa de gestão arquivística de documentos, o e-ARQ Brasil é aplicável às organizações dos setores público e privado e em qualquer esfera e âmbito de atuação, servindo para diferentes tipos de documentos arquivísticos. Destina-se igualmente aos documentos relativos às atividades-meio e às atividades-fim de um órgão ou entidade e não se restringe a qualquer ramo de atividade específica. Pode ser adotado como padrão ou norma pela administração pública federal, estadual, municipal, dos poderes executivo, legislativo e judiciário a fim de uniformizar o desenvolvimento e aquisição de sistemas que visam produzir e manter documentos arquivísticos em formato digital.

O e-ARQ Brasil é especialmente dirigido a:

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

Todo o conteúdo deste documento inicial 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.

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 esse 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.

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

4 NORMAS E OUTRAS ORIENTAÇÕES DE REFERÊNCIA;

4.1 Normas:

a) Sobre especificação de requisitos de segurança funcional:

- ISO 15408 - *Common Criteria* 2.x.

b) Sobre gestão de documentos

- AS ISO 15489.1 - Australian Standard Records Management. Part 1: general, 2002.
- AS ISO 15489-2 - Australian Standard Records Management. Part 2: guidelines, 2002.

c) Sobre preservação

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

4.2 Resoluções do Conselho Nacional de Arquivos

- Resolução do CONARQ nº 14, de 24 de outubro de 2001.
  Aprova a versão revisada e ampliada da Resolução do CONARQ nº 4, de 28 de março de 1996, que dispõe sobre o Código de Classificação de Documentos de Arquivo para a Administração Pública: Atividades-Meio, a ser adotado como modelo para os arquivos correntes dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR), e os prazos de guarda e a destinação de documentos estabelecidos na Tabela Básica de Temporalidade e Destinação de Documentos de Arquivo Relativos às Atividades-Meio da Administração Pública.
- Resolução do CONARQ nº 20, de 16 de julho de 2004.
  Dispõe sobre a inserção dos documentos digitais em programas de gestão arquivística de documentos dos órgãos e entidades integrantes do Sistema Nacional de Arquivos.

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

- THE NATIONAL ARCHIVES OF ENGLAND, WALES AND THE UNITED KINGDOM. **Requirements for electronic records management systems**: 1: Functional requirements - 2002 revision: final revision. Kew:The Archives, 2002.
- UNITED STATES. Department of Defense. **Design criteria standard for electronic records management *software* applications:** DOD 5015.2-STD. Washington: The Department, 2002.

- INSTITUTO DOS ARQUIVOS NACIONAIS/TORRE DO TOMBO, E INSTITUTO DE INFORMÁTICA (Portugal). Modelo de Requisitos para a Gestão de Arquivos Electrónicos. In: **Recomendações para a gestão de documentos de arquivo electrónicos**. Lisboa:O Instituto, 2002. v. 2

4.4 Orientações para gestão e preservação de documentos digitais

- CONSELHO INTERNACIONAL DE ARQUIVOS. Comitê de arquivos correntes em ambiente electrônico. **Documentos de arquivo electrônicos**: manual para arquivistas. ICA, Estudo nº 16. Disponível em: <http://www.ica.org/biblio.php?pdocid=285> Acesso em: 08 ago 2006.
- INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS. **INTERPARES project**. Disponível em: <http://www.interpares.org>. Acesso em: 04 ago 2006.
- NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (United States). **Electronic Records Management Initiative.** Disponível em: <http://www.archives.gov/records-mgmt/initiatives/erm-overview.html>. Acesso em: 08 ago 2006.
- PUBLIC RECORD OFFICE (United Kingdom). **Management, appraisal and preservation of electronic records guidelines**. Disponível em: <http://www.nationalarchives.gov.uk/electronicrecords/advice/guidelines.htm>. Acesso em: 08 ago 2006.
- UNESCO. División de la Sociedad de la Información. **Directrices para la preservación del patrimonio digital**. Preparado por la Biblioteca Nacional de Australia. Canberra: Biblioteca Nacional de Austrália, 2002. 176p. Disponível em: http://unesdoc.unesco.org/ulis/cgi-bin/ulis.pl?database=ged&req=2&by=3&sc1=1&look=new&sc2=1&text_p=inc&text=Directrices+para+la+preservaci%F3n+del+patrimonio+digital&submit=GO>. Acesso em: 08 ago 2006.

5 ORGANIZAÇÃO DA ESPECIFICAÇÃO:

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

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

A Parte II está organizada em Aspectos de Funcionalidade, Metadados, Aspectos de Tecnologia, Glossário e Referências. Aspectos de funcionalidade contêm onze capítulos, divididos em seções e trata de: organização dos documentos (incluindo o plano de classificação), produção, tramitação, captura, destinação, recuperação da informação, segurança, armazenamento, preservação, funções administrativas e técnicas e requisitos adicionais. Cada seção compreende um preâmbulo e a relação dos requisitos relativos àquela seção. Os requisitos são apresentados em quadros numerados com o enunciado correspondente e a classificação dos níveis de obrigatoriedade.

Níveis dos requisitos:

Neste documento 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 da seguinte forma:

- são obrigatórios quando indicados pela frase: "O SIGAD tem que...";
- altamente desejáveis quando indicados pela frase: "O SIGAD deve...";
- facultativos quando indicados pela frase: "O SIGAD pode...".

Cada requisito numerado é classificado como:

(O) = Obrigatório = "O SIGAD tem que ...";

(AD) = Altamente Desejável = "O SIGAD deve ...";

(F) = Facultativo = "O SIGAD pode ...".

TEM = significa que o requisito é imprescindível.

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

PODE = significa que o requisito é opcional.

Tanto para os requisitos considerados altamente desejáveis como para os requisitos facultativos, deve ser observado que uma implementação que não inclui um 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 inclui um item altamente desejável ou facultativo deve estar preparada para interoperar com uma outra implementação que não inclui o item.

Parte I

Gestão arquivística de documentos

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 resto da instituição.

Os anos de 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 custos baixos da tecnologia levaram à disseminação do uso dos microcomputadores. Tal disseminação foi potencializada com o advento da tecnologia de rede, a qual evoluiu rapidamente das redes locais (*Local Area Network* – LAN) para as metropolitanas, nacionais e globais, sendo a *Internet* a maior delas.

O avanço da Tecnologia de Informação e Comunicação (TIC), ocorrido a partir dos anos de 1990, muda radicalmente os mecanismos de registro e de comunicação da informação nas instituições públicas e privadas. Os documentos gerados no decorrer das atividades dessas instituições, até então em meio convencional, assumem novas características, isto é, passam a ser gerados em ambientes eletrônicos, armazenados em suportes magnéticos e ópticos, em formato digital, e deixam de ser apenas entidades físicas para se tornarem entidades lógicas. Além disso, o gerenciamento dos documentos, tanto digitais como os convencionais, começa a ser feito por meio de sistema informatizado conhecido como Gerenciamento Eletrônico de Documentos – GED.

Os documentos digitais trouxeram uma série de vantagens na produção, transmissão, armazenamento e acesso que, por sua vez, acarretaram alguns problemas. A facilidade de criar e transmitir documentos traz como conseqüência a informalidade na linguagem, nos procedimentos administrativos, bem como o esvaziamento das posições hierárquicas. A facilidade de acesso pode acarretar intervenções não autorizadas que podem resultar na adulteração ou perda dos documentos. A rápida obsolescência tecnológica (*software*, *hardware* e formatos) e a degradação das mídias digitais dificultam a preservação de longo prazo dos documentos e sua acessibilidade contínua. Os problemas em questão tornam necessária a adoção de medidas preventivas para minimizá-los.

Considerando-se que os documentos arquivísticos se constituem, primeiramente, em instrumentos fundamentais para a tomada de decisões e para a prestação de contas de um órgão ou entidade 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 seu acesso contínuo. Isso só é possível por meio da implantação de um programa de gestão arquivística de documentos.

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

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

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

No Brasil, a gestão arquivística de documentos ganhou amparo legal a partir da Lei nº 8.159, de 8 de janeiro de 1991 – Lei de Arquivos - e do Decreto nº 4.073, de 3 de janeiro de 2002, que regulamenta a gestão de documentos para a Administração Pública Federal.

O Conselho Nacional de Arquivos, criado pela Lei nº 8.159, de 1991, tem por finalidade definir a política nacional de arquivos públicos e privados e exercer orientação normativa, visando a gestão documental e a proteção especial aos documentos de arquivo[6]. É um órgão colegiado, vinculado ao Arquivo Nacional, composto por um Plenário, Câmaras Técnicas, Câmaras Setoriais e Comissões Especiais. Do Plenário participam o diretor-geral do Arquivo Nacional, representantes dos poderes Executivo, Legislativo e Judiciário federais, do Arquivo Nacional, dos arquivos públicos estaduais e do Distrito Federal, dos arquivos municipais, das instituições mantenedoras de curso superior de arquivologia, representantes das associações de arquivistas e das instituições profissionais que atuam nas áreas de ensino, pesquisa, preservação ou acesso a fontes documentais.

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

É, pois no âmbito do CONARQ, que a Câmara Técnica de Documentos Eletrônicos - CTDE redigiu e elaborou o "Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos – e-ARQ Brasil".

2 O QUE É GESTÃO ARQUIVÍSTICA DE DOCUMENTOS

Os documentos produzidos e recebidos no decorrer das atividades de um órgão ou entidade, independente do suporte em que se apresentam, registram suas políticas, funções, procedimentos e decisões. Nesse sentido, constituem-se em documentos arquivísticos, os quais 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;

---

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

[6] Conforme art. 1º do decreto nº 4.073, de 2002.

[7] Conforme arts. nº 10 a nº 13 do decreto nº 4.073, de 2002.

- Possibilitar a continuidade das atividades em caso de sinistros;
- Fornecer evidência em caso de litígios;
- 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 conferir essa capacidade, os documentos arquivísticos precisam ser confiáveis, autênticos, acessíveis, compreensíveis e possam ser preservados, 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[8] como o conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento de documentos arquivísticos em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente.

No bojo do conceito de gestão arquivística de documentos está a teoria das três idades. Segundo essa teoria, os documentos passam por três idades, a saber:

- **Corrente**: refere-se aos documentos que estão em curso, isto é, tramitando ou que foram arquivados, mas que são objeto de consultas freqüentes; eles são conservados nos locais onde foram produzidos sob a responsabilidade do órgão produtor;
- **Intermediária**: refere-se aos documentos que não são mais de uso corrente mas que, por conservarem ainda algum interesse administrativo, aguardam, no arquivo intermediário, o cumprimento do prazo estabelecido em tabela de temporalidade e destinação para serem eliminados ou recolhidos ao arquivo permanente.
- **Permanente**: refere-se aos documentos que devem ser definitivamente preservados devido a seu valor histórico, probatório ou informativo.

A passagem dos documentos de uma idade para outra é definida por meio do processo de avaliação, que leva em conta a freqüência de uso dos documentos por seus produtores e a identificação de seus valores primário e secundário. O valor primário é atribuído aos documentos considerando a sua utilidade administrativa imediata, isto é, as razões pelas quais esses documentos foram criados. Já o valor secundário refere-se ao valor atribuído aos documentos em função da sua utilidade para fins diferentes daqueles para os quais foram originalmente produzidos, como, por exemplo, provas judiciais e administrativas e pesquisas acadêmicas. A propósito, lembramos que segundo Rousseau e Couture: "Enquanto todos os documentos têm um valor primário que dura mais ou menos tempo conforme os casos, nem todos têm ou adquirem necessariamente um valor secundário"[9]. No caso dos documentos que cumpriram valor primário mas não apresentam valor secundário, estes serão eliminados. Já aqueles que não são mais necessários às

[8] A CTDE entende gestão arquivística de documentos como sinônimo de gestão de documentos, ressaltando a característica arquivística dessa gestão para diferenciá-la de outros tipos de gerenciamento de documentos.

[9] Rousseau, Jean-Yves e Couture, Carol, 1994, p.118.

atividades rotineiras do órgão ou entidade que os criou mas apresentam valor secundário, serão destinados à guarda permanente.

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

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

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

A gestão arquivística de documentos compreende:

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

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

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

3 DEFINIÇÃO DA POLÍTICA ARQUIVÍSTICA

Os órgãos e entidades devem definir uma política de gestão arquivística de documentos que tenha por objetivo produzir, manter e preservar documentos confiáveis, autênticos, acessíveis, compreensíveis e possam ser preservados de maneira que possam 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

[10] Resolução do CONARQ nº 14, de 24 de outubro de 2001.
[11] Resolução do CONARQ nº 1, de 18 de outubro de 1995; Resolução do CONARQ nº 2, de 18 de outubro de 1995; Resolução do CONARQ nº 5, de 30 de setembro de 1996; Resolução do CONARQ nº 7, de 20 de maio de 1997; Resolução do CONARQ nº 20, de 16 de julho de 2004; Resolução do CONARQ nº 21, de 4 de agosto de 2004; Resolução do CONARQ nº 24, de 3 de agosto de 2006.

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 a 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 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, 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, esta deve estar articulada às demais políticas informacionais existentes no órgão ou entidade, tais como políticas de sistemas de informação 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 da gestão arquivística de documentos, e sobre o papel que cabe a cada um na produção e manutenção de documentos confiáveis e autênticos.

A política de gestão arquivística de documentos deve explicitar as responsabilidades e designar as autoridades envolvidas, de forma que, por exemplo, onde for identificada a necessidade de produzir e capturar documentos, esteja claro quem é o responsável por essas ações.

4 DESIGNAÇÃO DE RESPONSABILIDADES

A designação de responsabilidades é um dos fatores que garantem o êxito da gestão arquivística de documentos. Nesse sentido, as autoridades responsáveis terão o dever de assegurar o cumprimento das normas e dos procedimentos previstos no programa de gestão.

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

- Direção superior – é a autoridade máxima responsável pela real viabilidade da política de gestão arquivística de documentos. Caberá a ela apoiar integralmente a implantação dessa política, alocando recursos humanos, materiais e financeiros e promovendo o envolvimento de todos no programa de gestão arquivística de documentos.
- Profissionais de arquivo – são os responsáveis pelo planejamento e a implantação do programa de gestão arquivística, bem como pela avaliação e pelo controle dos trabalhos executados no âmbito do programa. Além disso, os profissionais de arquivo são responsáveis também pela disseminação das técnicas e cultura arquivísticas.
- Gerentes de unidades ou grupos de trabalho – são os responsáveis por garantir que os membros das 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, pelo desenvolvimento e pela manutenção de sistemas de informação nos quais os documentos arquivísticos digitais são gerados e usados e responsáveis pela operacionalização dos sistemas de computação e de comunicação.

5 PLANEJAMENTO E IMPLANTAÇÃO DO PROGRAMA DE GESTÃO ARQUIVÍSTICA DE DOCUMENTOS

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

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

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

- levantamento da estrutura organizacional e das atividades desempenhadas;
- levantamento da produção documental, diferenciando os documentos arquivísticos dos não arquivísticos;
- levantamento, caso existam, dos sistemas utilizados internamente para tratamento de documentos e informações;
- definição, a partir do levantamento da produção documental, dos tipos de documentos que devem ser mantidos e produzidos, e que informações devem conter;
- definição e/ou aperfeiçoamento da forma desses documentos;
- análise e revisão do fluxo dos documentos;
- elaboração e/ou revisão do plano de classificação e da tabela de temporalidade e destinação;
- definição dos metadados a serem criados no momento da produção do documento e ao longo do seu ciclo de vida;
- definição e/ou aperfeiçoamento dos procedimentos de protocolo e de arquivamento dos documentos;
- definição e/ou aperfeiçoamento dos procedimentos para acesso, uso e transmissão dos documentos;
- definição do ambiente tecnológico que compreende os sistemas (*hardware* e *software*), os formatos, os padrões e os protocolos que darão sustentação aos procedimentos de gestão e preservação de documentos, integrando, quando possível, os sistemas legados;
- definição da infra-estrutura para armazenamento dos documentos convencionais, a qual compreende área física, 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, suas metas e estratégias de implantação, divulgação e acompanhamento visando melhoria contínua.

A **implantação** do programa de gestão arquivística de documentos envolve a execução e o acompanhamento de ações e projetos, efetuados simultaneamente. Deve atender aos objetivos definidos no planejamento do programa no que se refere a capacitação de pessoal, implantação de sistemas de gestão arquivística, integração com os sistemas de informação existentes e 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 coloca em prática os planos de ação e os projetos aprovados.

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

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

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

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

O documento arquivístico deve:

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

O programa de gestão arquivística de documentos deve:

- contemplar o ciclo de vida dos documentos;
- garantir a acessibilidade dos documentos;
- manter os documentos em ambiente seguro;
- reter os documentos somente pelo período estabelecido na tabela de temporalidade e destinação;

- implementar estratégias de preservação dos documentos desde sua produção pelo tempo que for necessário.
- garantir as seguintes qualidades de um documento arquivístico: organicidade, unicidade, confiabilidade, autenticidade e acessibilidade.

A cada uma das qualidades do documento arquivístico mencionadas acima, corresponde novo conjunto de exigências a serem cumpridas pelo programa de gestão, conforme especificado abaixo.

a) Organicidade:

O documento arquivístico se caracteriza pela organicidade, ou seja, pelas relações que mantém com os demais documentos do órgão ou entidade e que refletem suas funções e atividades. Os documentos arquivísticos não são coletados artificialmente, mas estão ligados uns aos outros por um elo que se materializa no plano de classificação, o qual os contextualiza no conjunto a que 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 seqüência das atividades realizadas por meio da aplicação de um plano de classificação.

b) Unicidade:

O documento arquivístico é único no conjunto documental ao qual pertence; podem existir cópias em um ou mais grupos de documentos, mas cada cópia é única em seu lugar, porque o conjunto de suas relações com os demais documentos do grupo é sempre único.

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

c) Confiabilidade[12]:

Um documento arquivístico confiável é aquele que tem a capacidade de sustentar os fatos que atesta. A confiabilidade está relacionada ao momento em que o documento é produzido e à veracidade do seu conteúdo. Para tanto há que ser dotado de completeza[13] e ter seus procedimentos de criação bem controlados. Dificilmente pode-se assegurar a veracidade do conteúdo de um documento, ela é inferida a partir da completeza e dos procedimentos de criação. 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 da seguinte forma: no momento em que ocorre a ação, ou imediatamente após, por pessoas diretamente envolvidas na condução das atividades e devidamente autorizadas; com o

---

[12] Confiabilidade é sinônimo de fidedignidade, tradução do termo em inglês *reliability."Reliability is conferred to records by the controls exercised on the creation and by the completeness of their form."* DURANTI, 2000, p. 12, nota 2.

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

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

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

e) Acessibilidade:

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

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

5.2 Metodologia do programa de gestão

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

Os oito passos acima referidos são:

a) Levantamento preliminar

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

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

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

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 possa identificar as exigências para produzir e manter documentos.

O levantamento preliminar também implica numa apreciação geral dos pontos fortes e fracos das práticas de gestão de documentos existentes no órgão ou entidade. Essa apreciação representa 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 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 a missão e as 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 serão capturados e mantidos caso o sistema não seja projetado para tal.

Os produtos resultantes deste passo podem incluir:

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

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

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

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

Consiste em identificar que documentos devem ser produzidos, determinar a forma documental que melhor satisfaça cada função ou atividade desempenhada, e definir quem está autorizado a produzir cada documento. Essas exigências devem tomar por base a legislação vigente, as normas internas e os riscos decorrentes da falta de registro de uma atividade em documento arquivístico.

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

Os produtos resultantes deste passo podem incluir:

- lista das exigências a serem cumpridas para a produção e manutenção de documentos;

- relatório de avaliação dos riscos decorrentes da falta de registro de uma atividade em documento arquivístico;
- documento formal, regulamentando as exigências a serem cumpridas para a produção e manutenção de documentos, ou seja, quais documentos devem ser produzidos, que forma documental devem apresentar e os níveis de permissão de acesso.

d) Avaliação dos sistemas existentes

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

O objetivo deste passo é identificar as lacunas entre as exigências para a produção e manutenção de documentos e o desempenho do sistema de gestão arquivística de documentos e dos sistemas de informação e comunicação existentes. Isso fornecerá a base para o desenvolvimento de novos sistemas ou 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 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 para 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, que atenda às exigências identificadas e documentadas no passo "c" e que corrija quaisquer deficiências identificadas no passo "d", redesenhando os procedimentos e os sistemas de informação e comunicação existentes e integrando-os ao sistema de gestão arquivística de documentos.

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

- projetar 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, o quanto possível, um plano estratégico de evolução que vise minimizar os efeitos da obsolescência tecnológica.

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

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

g) Implementação do sistema de gestão arquivística de documentos

Consiste na execução do projeto por meio de:

- treinamento de pessoal;
- introdução do sistema de gestão arquivística de documentos ou adaptação do já existente;
- integração do sistema de gestão arquivística de documentos com os procedimentos e os sistemas de informação e comunicação existentes.

A implementação de um sistema de gestão arquivística de documentos é um empreendimento complexo, que deve ser realizado com um mínimo de interrupção das atividades do órgão ou entidade, e que envolve elevada prestação de contas e risco. Tais

riscos podem ser minimizados por um planejamento cuidadoso e pela documentação dos processos de implementação.

Os produtos resultantes deste passo podem incluir:

- regulamentação das políticas, diretrizes e procedimentos, por meio de normas e manuais;
- material de treinamento;
- documentação dos processos de conversão e migração dos sistemas;
- relatórios sobre avaliação de desempenho do sistema de gestão arquivística de documentos.

h) Monitoramento e ajustes

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

O desempenho é medido 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 armazenamento dos mesmos de maneira segura.

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

Os produtos resultantes deste passo podem incluir:

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

5.3 Suspensão ou extinção do SIGAD

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

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

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

6.1 Captura

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

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

Os objetivos da captura são:

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

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

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

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

Além do código de classificação, descritores, número de protocolo e número de registro, a captura pode prever a introdução de outros metadados tais como: data e hora da criação, da transmissão e do recebimento do documento; nome do autor, do originador, do

digitador e do destinatário, entre outros. Esses metadados podem ser registrados em vários níveis de detalhe, dependendo das necessidades geradas pelos procedimentos do órgão ou entidade e do seu contexto jurídico-administrativo.

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

A captura tem como pré-requisito a definição de:

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

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

Documentos que exigem captura são 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.

1.1.1 Registro

O registro consiste em formalizar a captura do documento arquivístico 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 é a atribuição de metadados.

O registro tem por objetivo demonstrar que o documento foi produzido ou recebido e capturado pelo sistema de gestão arquivística de documentos, bem 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, um documento pode receber também um número único de processo/dossiê ao qual pertence.

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

Na Administração Pública, em determinados casos, documentos formarão processos, os quais deverão ser autuados por uma unidade protocolizadora. Um processo é o documento ou o 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 a sua unicidade e integridade.

Neste sentido, deve-se seguir 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, a autuação e outros procedimentos relativos aos processos e outros documentos oficiais.

O registro inclui os seguintes metadados obrigatórios:

- número identificador atribuído pelo sistema;
- data e hora do registro;
- título ou descrição abreviada: palavra, frase ou grupo de caracteres que nomeia um documento arquivístico.;
- produtor: nome da pessoa física ou jurídica responsável pela criação do documento arquivístico;
- autor: nome da pessoa física autoridade e capacidade para emitir o documento ou em cujo nome 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* no qual o documento é gerado ou enviado.

O registro pode incluir informações descritivas mais detalhadas sobre o documento e sobre outros documentos a ele relacionados, tais como:

- data de produção;
- data e hora da 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 documentais por seu formato. São exemplos de espécies documentais ata, carta, decreto, memorando, ofício, planta, relatório;
- classificação de acordo com o código de classificação[16];
- associações a documentos diferentes que podem estar relacionados pelo fato de registrarem a mesma atividade ou se referirem à mesma pessoa ou situação;
- formato, *software* e versão e sob a qual o documento foi produzido ou no qual foi capturado;
- máscaras de formatação (*template*) necessárias para apresentar o documento;
- restrição de acesso[17];
- descritor: palavra ou grupo de palavras que, em indexação e tesauro, designa um conceito ou um assunto preciso, excluindo outros sentidos e significados;

[16] Ver 6.1.2 - Classificação

[17] Ver 6.1.4 – Atribuição de restrição de acesso

- prazos de guarda[18];
- documentos anexos.

1.1.2 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 que poderá incluir, ou não, a atribuição de um 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 tanto, deve tomar por base o conteúdo do documento, que reflete a atividade que o gerou e determina o uso da informação nele contida. A classificação também define a organização física dos documentos, constituindo-se em referencial básico para sua recuperação.

Os objetivos da classificação são:

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

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

- identificar a ação que o documento registra;
- localizar a ação ou atividade no plano de classificação;
- comparar a atividade com a estrutura organizacional para verificar se é apropriada à unidade que gerou o documento;
- aplicar a classificação ao documento.

1.1.3 Indexação

A 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 normalmente é feita com base em:

- tipologia documental: divisão de espécie documental que reúne documentos por suas características comuns no que diz respeito à fórmula diplomática, natureza de conteúdo ou técnica do registro. São exemplos de tipos documentais: atestado de freqüência de pessoal, atestado de saúde ocupacional, alvará de licença para construção, alvará de habite-se;
- título ou cabeçalho do documento;

[18] Ver 6.2 – Avaliação, temporalidade e destinação

- 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.

O objetivo da indexação é ampliar as possibilidades de busca e facilitar a recuperação dos documentos, podendo ser feita de forma manual ou automática.

1.1.4 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 documentos sigilosos, a legislação estabelece diferentes graus a serem atribuídos a cada documento.

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

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

- identificar a ação ou atividade que o documento registra;
- identificar a unidade administrativa à qual o documento pertence;
- verificar a precaução de segurança e o grau de sigilo;
- atribuir o grau de sigilo e as restrições de acesso ao documento;
- registrar o grau de sigilo e as restrições de acesso no sistema de gestão arquivística de documentos.

1.1.5 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 tal 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, juntamente com outros a ele relacionados, dentro de uma pasta ou arquivo que contém um título, ordenados conforme critérios previamente estipulados. Esse agrupamento conecta o documento aos demais documentos sobre o mesmo assunto, função ou atividade.

Um sistema de gestão arquivística de documentos em papel deverá controlar os títulos das pastas. Colocar um documento em uma pasta é um processo consciente de determinar a classificação daquele documento e arquivá-lo em uma seqüência pré-definida. Os documentos arquivados na pasta podem ser datados e numerados seqüencialmente como medida de segurança. As condições de acesso e a destinação podem ser controladas por mecanismos pré-definidos.

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

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

6.2 Avaliação, Temporalidade e Destinação

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

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

Os prazos de guarda referem-se ao tempo necessário para o arquivamento dos documentos nas fases corrente e intermediária, visando atender exclusivamente às necessidades da administração que os gerou, baseado em estimativas de uso. Nesse sentido, nenhum documento deverá 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.

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 de conhecimentos exigidos pelo processo de avaliação, que implica no estabelecimento de critérios de valor, requerem a participação de pessoas ligadas a 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 prevista para o documento no momento da captura e do registro, de acordo com os prazos e as ações previstas na tabela de temporalidade e destinação do órgão ou entidade. Essa informação deve ser registrada em um metadado associado ao documento.

---

[19] Ver item 3 na Introdução.

O sistema de gestão arquivística de documentos deve também ter capacidade de identificar os documentos que já cumpriram sua temporalidade para implementar a destinação prevista. No caso de um SIGAD, esse sistema deverá 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 rotineiro das atividades do órgão ou entidade. Essas mesmas determinações não poderão 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 a guarda permanente.

A eliminação deve ser precedida da elaboração de listagem, do edital de ciência de eliminação e do termo de eliminação, segundo a legislação vigente e deve obedecer aos seguintes princípios:

- a eliminação deverá sempre ser autorizada pela autoridade arquivística na sua esfera de competência;
- os documentos arquivísticos que estiverem pendentes, sob litígio ou investigação, não poderão ser destruídos;
- a eliminação deverá ser realizada de forma a impossibilitar a recuperação posterior de qualquer informação confidencial contida nos documentos eliminados, como por exemplo dados de identificação pessoal ou assinatura.
- todas as cópias dos documentos eliminados, incluindo cópias de segurança e cópias de preservação, independente do suporte, deverão 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 deverão ser acompanhados de listagem de transferência.

A transferência pode ser realizada de diferentes formas, como se segue abaixo:

- 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 a custódia de um órgão ou entidade diferente da 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 pela sua custódia.

Recolhimento

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

Os procedimentos de **transferência** e **recolhimento** de arquivos digitais para instituição arquivística que implicam na transposição desses documentos de um SIGAD para outro sistema informatizado, deverão adotar algumas 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.

6.3 Pesquisa, localização e apresentação dos documentos

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

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

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

[20] Lei nº 8.159, de 8 de janeiro de 1991 e Resolução do CONARQ nº 2 do CONARQ, de 1995.

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

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

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

Controle de acesso

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

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

- restrição de acesso aos documentos;
- exibição dos documentos, criptografados ou não, e dos metadados somente aos usuários autorizados;
- uso e intervenção nos documentos somente pelos usuários autorizados.

Os documentos também devem ser analisados com relação às precauções de segurança, ou seja, se são considerados ostensivos ou sigilosos. No caso dos documentos sigilosos[21], regras, normas e legislação[22] estabelecem diferentes razões para o sigilo e também diferentes graus a serem atribuídos a cada documento e as autoridades competentes para fazê-lo. (Ver seção 6.1.4 – atribuição de restrição de acesso)

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

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

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

Uso e rastreamento

O uso dos documentos pelos usuários deve ser registrado pelo sistema nos seus respectivos metadados. A gestão desse uso inclui:

- identificação da permissão de acesso dos usuários, isto é, o que ele pode acessar;
- identificação da precaução de segurança e da categoria de sigilo dos documentos;

---

[21] Lei 8.159/1991.

[22] Decreto nº 4.553 de 27 de dezembro de 2002, Decreto n° 5.301, de 9 de dezembro de 2004, e Lei nº 11.111, de 5 de maio de 2005.

- garantia de que somente os indivíduos autorizados tenham acesso a documentos classificados e aos originalmente sigilosos;
- registro de todos os acessos, tentativas de acesso e usos dos documentos (visualização, impressão, transmissão e cópia para a área de transferência) com identificação de usuário, data, hora e, se possível, a estação de trabalho;
- revisão periódica das classificações de acesso a fim de garantir sua atualização.

O rastreamento dos documentos em trilhas de auditoria é uma medida de segurança que tem por objetivo verificar a ocorrência de acesso 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 intervenções feitas no documento arquivístico digital ou no SIGAD.

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

- identificar os autores de cada operação sofrida pelos 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 tenham prazos a serem cumpridos pelo órgão ou entidade, deve-se implementar ações de rastreamento de forma a:

- determinar os passos a serem dados em resposta às atividades ou ações registradas em um documento;
- atribuir responsabilidade por uma ação a uma pessoa;
- registrar a data em que uma ação deve ser executada e a data em que ocorreu.

Cópias de segurança

O SIGAD deve prever controles para proporcionar a salvaguarda regular dos documentos arquivísticos e dos seus metadados. Deve também poder recuperá-los rapidamente em caso de perda devido a sinistros, 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.

No caso dos sistemas de gestão arquivística de documentos convencionais pode-se prever a reprodução de documentos para outros suportes como medida de segurança, como, por exemplo, por processo de microfilmagem ou digitalização.

No caso dos 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 das mesmas, em caso de perda devido a falhas de *software*, *hardware* ou mesmo

acidente. O processo reverso ao *backup* é o de restauração (*restore*), que consiste em recuperar as informações para o ambiente de produção do 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 infra-estrutura

A natureza das medidas de segurança da infra-estrutura de instalações do acervo digital diz respeito a requisitos operacionais e não é muito diferente daquela do acervo convencional. Essas medidas devem levar em conta 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 têm que ser providos em toda área de instalação e estarem de acordo com as normas de segurança estabelecidas;
- a substituição dos equipamentos contra incêndio tem que seguir uma rotina de verificação e ocorrer antes do final da vida útil prevista para os mesmos;
- o órgão ou entidade tem que prever instalações adequadas de pára-raios, com procedimentos de manutenção periódica, seguindo a legislação e normas técnicas já estabelecidas;
- a área reservada à instalação do SIGAD deverá 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 que estar de acordo com as atribuições individuais e com as regras de segurança do órgão ou entidade.

6.5 Armazenamento

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

Documentos de valor permanente, independente do formato, requerem um armazenamento criterioso desde o momento da sua criação para garantir sua preservação de longo prazo.

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

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

No caso dos documentos arquivísticos digitais, os órgãos e entidades devem dispor de políticas e diretrizes para conversão ou migração desses documentos de maneira a garantir sua autenticidade, acessibilidade e utilização. Os procedimentos de conversão e migração devem detalhar as mudanças ocorridas nos sistemas e nos formatos dos documentos (ver seção 6.6, especificamente voltada à Preservação).

Os fatores importantes na seleção das opções de armazenamento são:

- volume e estimativa de crescimento dos documentos: esse fator deve ser levado em conta para se avaliar a capacidade de armazenamento, isto é, áreas de depósito, tipos e quantidade de estante e, no caso de documentos digitais, capacidade dos dispositivos de armazenamento;
- segurança dos documentos: as instalações de armazenamento (depósitos, arquivos, computadores) deverão prever limitação de acesso aos documentos, como, por exemplo, controle das áreas de armazenamento e sistemas de detecção de entradas não autorizadas. O depósito deve estar localizado em área que não seja de risco. No caso de documentos digitais, devem ser previstos procedimentos que previnam a perda de documentos por falha do SIGAD (ver seção 6.4, Segurança – cópias de segurança e segurança da infra-estrutura);
- características físicas do suporte e do ambiente: fatores como tipo de suporte, peso, grau de contaminação do documento e do ambiente, temperatura e umidade influenciarão na adequação das condições de armazenamento. Nesse sentido, deverão ser adotados procedimentos - como o controle e verificação do tempo de vida útil e da estabilidade dos suportes - para prevenir quaisquer danos aos documentos. É importante que os meios de acondicionamento sejam robustos e adequados ao formato e à quantidade de documentos. As áreas de depósito devem ter amplitude adequada, estabilidade de temperatura e de níveis de umidade, proteção contra sinistro, contaminação (tal como isótopos radioativos, toxinas e mofo) e infestação de insetos ou microorganismos. Os documentos digitais devem passar periodicamente pela troca de suporte, isto é, transferir as informações contidas num suporte para outro. Essa técnica é conhecida por rejuvenescimento (*refreshing*).
- freqüência de uso: o uso mais ou menos freqüente dos documentos deve ser levado em conta na seleção das opções de armazenamento. No caso dos documentos convencionais, as opções envolverão acondicionamento (pastas suspensas, caixas entre outros) e localização dos depósitos (próximos ou distantes da área de trabalho). Já em relação aos documentos digitais, as opções podem envolver armazenamento *on-line* (acesso imediato) ou *off-line* nas chamadas "mídias removíveis" de armazenamento (disco óptico, fita magnética e outros) em diferentes graus de disponibilidade e velocidade.
- custo relativo das opções de armazenamento dos documentos: além do custo dos dispositivos de armazenamento, deve ser considerado os dos equipamentos para sua manipulação e *de software* de controle. Pelo previsível alto volume de custo, pode ser considerada a opção 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 acessos não autorizados. Do mesmo modo, a

utilização de *checksum*[23] permite rastrear eventuais comprometimentos de conteúdo.

Os documentos digitais são armazenados em dispositivos de armazenamento 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 de funcionamento essencial, necessária a qualquer sistema computacional. É nela que o *software* e os dados são armazenados durante a execução. Representantes típicas dessa classe são as memórias RAM (*Random Access Memory*). São memórias extremamente rápidas. Seu conteúdo é de natureza dinâmica, volátil, permanecendo 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 isolados ou combinados em *disk arrays.* Diversas tecnologias permitem, através do uso de *disk arrays,* obter-se maior desempenho e confiabilidade do que seria conseguido 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 da perda de dados é superior ao preço das mídias que fisicamente os contêm.

As memórias secundária e terciária são adequadas para armazenamento.

6.6 Preservação

Os documentos arquivísticos têm que se manter acessíveis e utilizáveis por todo o tempo que se fizer necessário, garantindo-se sua longevidade, funcionalidade e acesso contínuo. Deverão ser asseguradas as características dos documentos – tais como autenticidade e acessibilidade - pela adoção de estratégias institucionais e técnicas pró-ativas de criação e de preservação, que garantam a sua perenidade. Essas estratégias são estabelecidas por uma política de preservação.

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

[23] Valor calculado a partir dos dados para verificar que não houve alteração.

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

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 rejuvenescimento (refreshing) e conversão[24].

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

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

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

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

7 INSTRUMENTOS UTILIZADOS NA GESTÃO ARQUIVÍSTICA DE DOCUMENTOS

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

Instrumentos principais:

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

Instrumentos adicionais:

- glossário
- vocabulário controlado
- tesauro

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

- relatório de análise do contexto jurídico-administrativo do órgão ou entidade;
- relatório de riscos que envolvem as atividades desenvolvidas pelo órgão ou entidade;

[24] Ver Glossário.

- plano de contingência e plano de prevenção contra desastres;
- estrutura organizacional e delegação de competências do órgão ou entidade;
- registro dos funcionários e das permissões de acesso aos sistemas do órgão ou entidade.

7.1 Plano de Classificação e Código de Classificação

Um plano de classificação é um esquema de distribuição de documentos em classes, de acordo com métodos de arquivamento específicos, elaborado a partir do estudo das estruturas e funções de uma instituição e da análise do arquivo por ela produzido[25].

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

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

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

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

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

7.2 Tabela de temporalidade e destinação

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

A elaboração da tabela de temporalidade e destinação deverá 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 quaisquer outros que se façam necessários.

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

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

---

[25] Cf. Dicionário brasileiro de terminologia arquivística, 2005, p. 132.

- identificador de classe;
- prazos de guarda nas fases corrente e intermediária;
- destinação final (eliminação ou guarda permanente);
- observações necessárias à 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 funções como auditores, entidades investigativas, autoridades arquivísticas ou pesquisadores;
    - identificação e avaliação dos ganhos legais, financeiros, políticos, sociais e outros que o órgão ou entidade possa ter na preservação dos documentos arquivísticos para servir aos interesses da pesquisa e da sociedade como um todo;
    - cumprimento dos regulamentos da autoridade arquivística, na sua esfera de competência.

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

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

7.3 Manual de Gestão Arquivística de Documentos

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

O manual pode compreender os seguintes pontos:

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

7.4 Esquema de classificação de acesso e segurança

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

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

7.5 Glossário

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

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

7.6 Vocabulário controlado e Tesauro

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

Vocabulário controlado é um conjunto normalizado de termos que serve à indexação e a 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 relações entre eles, como, por exemplo, relação entre sinônimos.

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

Parte II

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

Aspectos de funcionalidade

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

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

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

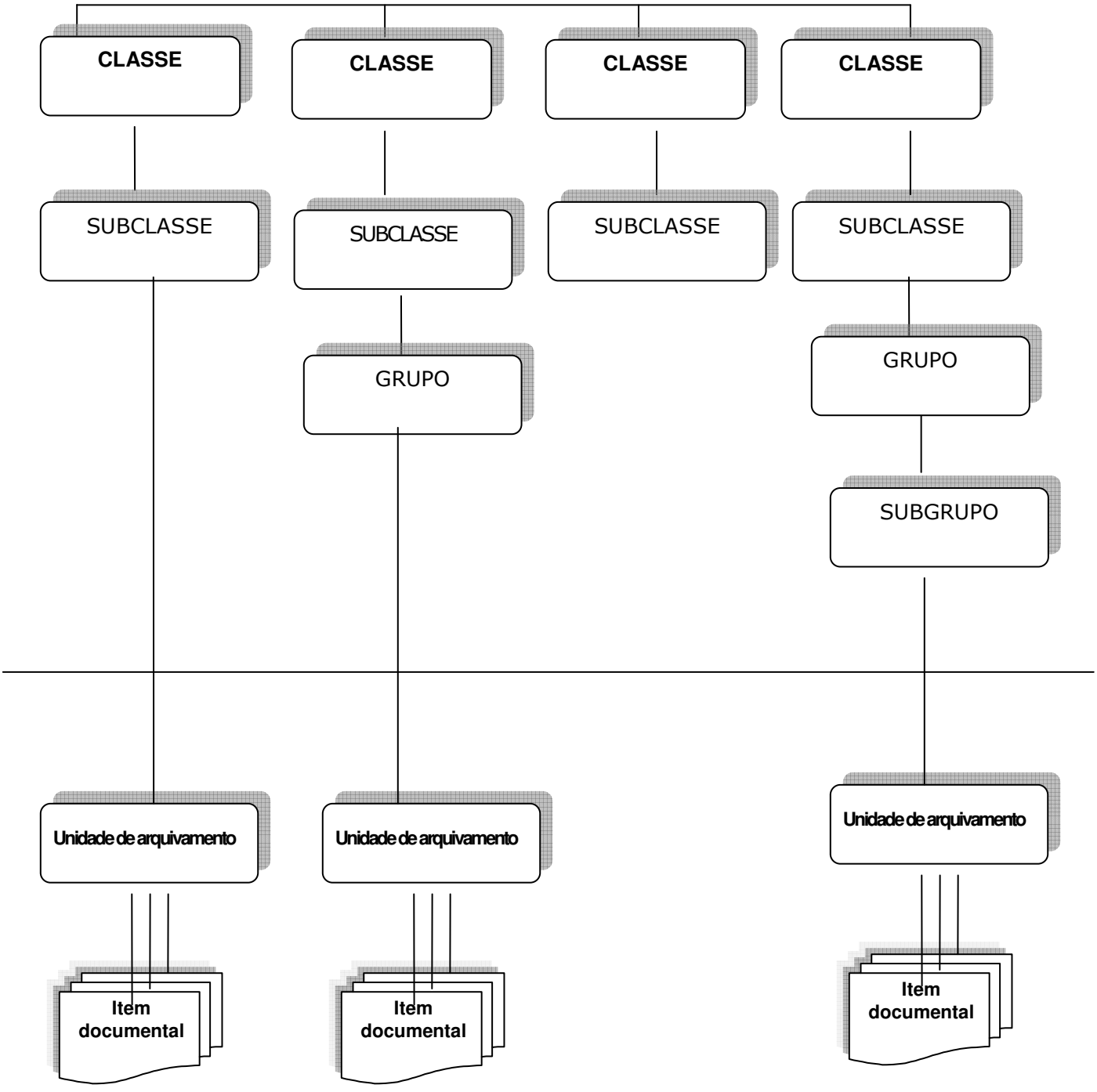
As atividades de gestão de documentos, como o controle da temporalidade e destinação dos documentos, são feitas com base nas unidades de arquivamento. Desta forma, no momento do arquivamento os documentos devem ser inseridos em uma unidade de arquivamento, que está subordinada hierarquicamente ao plano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

[26] Unidade de arquivamento é o documento tomado por base para fins de classificação, arranjo, armazenamento e notação. Uma unidade de arquivamento pode ser um dossiê, um processo ou ainda uma pasta onde estão reunidos documentos sob o mesmo código de classificação, como por exemplo, as folhas de ponto de um determinado ano, relatórios de atividades relativos a um determinado período ou atas de reunião.

[27] Daqui por diante, nesta seção, o termo classe deverá ser entendido como termo genérico que inclui os demais níveis do plano de classificação, isto é, subclasse, grupo e subgrupo.

[28] A Resolução do CONARQ nº 14, de 28 de outubro de 2001, aprova a versão revisada e ampliada da Resolução do CONARQ nº 4, de 28 de março de 1996, que dispõe sobre a classificação, temporalidade e destinação de documentos de arquivo relativos às atividades-meio da administração pública. Esse instrumento também orienta a elaboração de código de classificação e tabela de temporalidade e destinação de documentos para as atividades finalísticas.

Diagrama de organização dos documentos



1.1 Configuração e Administração do Plano de Classificação no SIGAD

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

Referência	Requisito	Obrig[29]
1.1.1	Um SIGAD tem que incluir e ser compatível com o plano de classificação do órgão ou entidade. *O plano de classificação dos integrantes do SINAR deve estar de acordo com a legislação e ser aprovado pela instituição arquivística na específica esfera de competência.*	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. *Por exemplo, quando se adotar o método decimal para codificação, cada classe poderá ter até no máximo dez subordinações e assim sucessivamente.*	O
1.1.3	Um SIGAD tem que permitir a usuários autorizados acrescentar novas classes sempre que se fizer necessário.	O
1.1.4	Um SIGAD tem que registrar a data de abertura de uma nova classe no respectivo metadado.	O
1.1.5	Um SIGAD tem que registrar a mudança de nome de uma classe já existente no respectivo metadado.	O
1.1.6	Um SIGAD tem que permitir o deslocamento de uma classe inteira, incluindo as subclasses, grupo, subgrupos e os documentos ali classificados, para um outro ponto do plano de classificação. Nesse caso, é necessário fazer o registro do deslocamento nos metadados do plano de classificação.	O
1.1.7	Um SIGAD deve permitir que usuários autorizados tornem inativa uma classe onde não serão mais classificados documentos.	AD
1.1.8	Um SIGAD tem que permitir que um usuário autorizado apague uma classe inativa. *Só pode ser apagada uma classe que não tenha documentos ali classificados*.	O
1.1.9	Um SIGAD tem que impedir a eliminação de uma classe que tenha documentos ali classificados. Essa eliminação poderá ocorrer a partir do momento em que todos os documentos ali classificados tenham sido recolhidos ou eliminados, e seus metadados apagados, ou que esses documentos tenham sido reclassificados.	O

[29] O campo obrigatoriedade na tabela apresenta a seguinte classificação:
O – obrigatório
AD – altamente desejável
F - facultativo

Referência	Requisito	Obrig[29]
1.1.10	Um SIGAD tem que permitir a associação de metadados às classes, conforme estabelecido no padrão de metadados, e deve restringir a inclusão e alteração desses mesmos metadados somente a usuários autorizados.	O
1.1.11	Um SIGAD tem que disponibilizar pelo menos dois mecanismos de atribuição de identificadores a classes do plano de classificação, prevendo a possibilidade de se utilizar ambos, separadamente ou em conjunto, na mesma aplicação: ▪ atribuição de um código numérico ou alfanumérico; ▪ atribuição de um termo que identifique cada classe.	O
1.1.12	Um SIGAD deve prever um atributo associado às classes para registrar a permissão de uso daquela classe para classificar um documento. *Em algumas classes não é permitido incluir documentos, nesses casos os documentos devem ser classificados apenas nos níveis subordinados.* *Por exemplo, no código de classificação previsto na Resolução do CONARQ nº 14:* *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 a pesquisa e navegação na estrutura do plano de classificação por meio de uma interface gráfica.	F
1.1.16	Um SIGAD deve ser capaz de importar e exportar total ou parcialmente um plano de classificação. *Ver item 12 - Interoperabilidade*	AD

Referência	Requisito	Obrig[29]
1.1.17	Um SIGAD tem que prover funcionalidades para elaboração de relatórios para apoiar a 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	Um SIGAD deve possibilitar consulta ao plano de classificação a partir de qualquer atributo ou combinação de atributos e gerar relatório com os resultados obtidos	AD

1.2 Classificação e metadados das unidades de arquivamento

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

Referência	Requisito	Obrig
1.2.1	Um SIGAD tem que permitir a classificação das unidades de arquivamento somente nas classes autorizadas. *Ver requisito 1.1.12*	O
1.2.2	Um SIGAD tem que permitir a classificação de um número ilimitado de unidades de arquivamento dentro de uma classe.	O
1.2.3	Um SIGAD tem que utilizar o termo completo da classe para identificar uma unidade de arquivamento, tal como especificado no item 1.1.13.	O
1.2.4	Um SIGAD tem que permitir a associação de metadados às unidades de arquivamento e deve restringir a inclusão e alteração desses mesmos metadados somente a usuários autorizados.	O
1.2.5	Um SIGAD tem que associar os metadados das unidades de arquivamento conforme estabelecido no padrão de metadados.	O
1.2.6	Um SIGAD tem que permitir que uma nova unidade de arquivamento herde da classe em que foi classificada, determinados metadados pré-definidos. *Exemplos desta herança são: temporalidade prevista e restrição de acesso.*	O
1.2.7	Um SIGAD deve relacionar os metadados herdados de forma que uma alteração no metadado de uma classe seja automaticamente incorporada à unidade de arquivamento que herdou esse metadado.	AD
1.2.8	Um SIGAD pode permitir a alteração conjunta de um determinado metadado em um grupo de unidades de arquivamento previamente selecionado.	F

Referência	Requisito	Obrig
1.2.9	Um SIGAD tem que permitir que uma unidade de arquivamento e seus respectivos volumes e/ou documentos sejam reclassificados por um usuário autorizado, e tem que permitir que todos os documentos já inseridos permaneçam na(s) unidade(s) de arquivamento e volume(s) que estão sendo transferidos, mantendo a relação entre os documentos, volumes e unidades de arquivamento.	O
1.2.10	Quando uma unidade de arquivamento ou documento é reclassificado, um SIGAD deve manter registro de suas posições anteriores à reclassificação, de forma a manter um histórico.	AD
1.2.11	Quando uma unidade de arquivamento ou documento é reclassificado, um SIGAD deve permitir que o administrador introduza as razões para a reclassificação.	AD
1.2.12	Um SIGAD pode permitir que os usuários criem referências cruzadas para unidades de arquivamento afins.	F

1.3 Gerenciamento dos dossiês/processos

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

Referência	Requisito	Obrig
1.3.1	Um SIGAD tem que registrar nos metadados a data de abertura e de encerramento do dossiê/processo. *Essa data pode se constituir em parâmetro para aplicação dos prazos de guarda e destinação do dossiê/processo.*	O
1.3.2	Um SIGAD tem que permitir que um dossiê/processo seja encerrado através de procedimentos regulamentares e somente por usuários autorizados.	O
1.3.3	Um SIGAD tem que permitir a consulta aos dossiês/processos já encerrados por usuários autorizados.	O
1.3.4	Um SIGAD tem que impedir o acréscimo de novos documentos a dossiês/processos já encerrados. Dossiês*/processos encerrados deverão ser reabertos para receber novos documentos*.	O
1.3.5	Um SIGAD deve ser capaz de registrar múltiplas entradas para um documento digital (objeto digital) em mais de um dossiê/processo ou pasta, sem duplicação física desse documento. *Quando um documento digital estiver associado a mais de um dossiê ou processo, o SIGAD deverá criar um registro para cada referência desse documento. Cada registro estará vinculado ao mesmo objeto digital*	AD

Referência	Requisito	Obrig
1.3.6	Um SIGAD tem que impedir a eliminação de uma unidade de arquivamento digital ou de qualquer parte de seu conteúdo em todas as ocasiões, 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
1.3.7	Um SIGAD tem que garantir a integridade da relação hierárquica entre classe, dossiê/processo, volume e documento e entre classe, pasta e documento em todos os momentos, independentemente de atividades de manutenção, ações do usuário ou falha de componentes do sistema. *Em hipótese alguma poderá ocorrer uma situação em que qualquer ação do usuário ou falha do sistema dê origem a uma inconsistência na base de dados do SIGAD.*	O

1.4 Requisitos adicionais para o gerenciamento de processos

A formação e manutenção de processos no setor público apresentam regras específicas, que os diferenciam dos dossiês, e que apóiam a manutenção 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 a sua esfera e âmbito.

Esta seção inclui requisitos específicos para a gestão dos processos, que são aplicáveis se o SIGAD capturar esse tipo de documento.

Referência	Requisito	Obrig
1.4.1	Um SIGAD tem que prever a formação/autuação de processos[30], por usuário autorizado conforme estabelecido em legislação específica.	O
1.4.2	Um SIGAD deve prever funcionalidades para apoiar a pesquisa de existência de processo relativo à mesma ação/interessado.	AD
1.4.3	Um SIGAD tem que prever que os documentos integrantes do processo digital recebam numeração seqüencial sem falhas, não se admitindo que documentos diferentes recebam a mesma numeração.	O
1.4.4	Um SIGAD tem que controlar 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 devem obedecer à legislação específica na devida esfera e âmbito de competência.*	O

[30] Ver Glossário.

Referência	Requisito	Obrig
1.4.5	Um SIGAD tem que prever procedimentos para juntada de processos segundo a legislação específica na devida esfera e no âmbito de competência. A juntada pode ser por anexação[31] ou por apensação[32]. Este procedimento deverá ser registrado nos metadados do processo.	O
1.4.6	Um SIGAD tem que prever procedimentos para desapensação de processos segundo a legislação específica na devida esfera e no âmbito de competência. Esse procedimento deverá ser registrado nos metadados do processo.	O
1.4.7	Um SIGAD tem que prever procedimentos para desentranhamento de documentos integrantes de um processo, segundo norma específica na devida esfera e no âmbito de competência. Esse procedimento deverá ser registrado nos metadados do processo.	O
1.4.8	Um SIGAD tem que prever procedimentos para desmembramento de documentos integrantes de um processo segundo norma específica na devida esfera e no âmbito de competência. Esse procedimento deverá ser registrado nos metadados do processo.	O
1.4.9	Um SIGAD tem que prever o encerramento[33] dos processos incluindo seus volumes e seus metadados.	O
1.4.10	Um SIGAD tem que prever o desarquivamento para reativação dos processos por usuário autorizado obedecendo procedimentos legais e administrativos. *Para manter a integridade do processo somente o último volume receberá novos documentos ou peças.*	O

1.5 Volumes: abertura, encerramento e metadados

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

---

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

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

[33] Na Administração Pública Federal o processo é arquivado; o que se encerra é a ação.

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

Referência	Requisito	Obrig
1.5.1	Um SIGAD deve ser capaz de gerenciar volumes para subdividir dossiês/processos, fazendo distinção entre dossiês/processos e volumes.	AD
1.5.2	Um SIGAD deve permitir a associação de metadados aos volumes e deve restringir a inclusão e a alteração desses mesmos metadados somente a usuários autorizados.	AD
1.5.3	Um SIGAD tem que permitir que um volume herde automaticamente do dossiê/processo ao qual pertence, determinados metadados pré-definidos, como por exemplo, procedência, classes e temporalidade.	O
1.5.4	Um SIGAD tem que permitir a abertura de volumes a qualquer dossiê/processo que não esteja encerrado.	O
1.5.5	Um SIGAD deve permitir o registro de metadados correspondentes as datas de abertura e de encerramento de volumes.	AD
1.5.6	Um SIGAD tem que assegurar que um volume somente conterá documentos. Não é permitido que um volume contenha outro volume ou um outro dossiê/processo.	O
1.5.7	Um SIGAD tem que permitir que um volume seja encerrado através de procedimentos regulamentares e somente por usuários autorizados.	O
1.5.8	Um SIGAD tem que assegurar que, ao abrir um novo volume, o volume precedente seja automaticamente encerrado. *Apenas o volume produzido mais recentemente pode estar aberto, todos os outros volumes existentes nesse dossiê/processo têm que estar fechados.*	O
1.5.9	Um SIGAD tem que impedir a reabertura de um volume já encerrado para acréscimo de documentos.	O

1.6 Gerenciamento de documento e processos/dossiês arquivísticos convencionais, híbridos

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

Referência	Requisito	Obrig
1.6.1	Um SIGAD tem que capturar documentos ou dossiês/processos convencionais e gerenciá-los da mesma forma que os digitais. *Para conceito de captura veja item 3.*	O

Referência	Requisito	Obrig
1.6.2	Um SIGAD tem que ser capaz de gerenciar a parte convencional e a parte digital integrantes de dossiês/processos híbridos, associando-as com o mesmo número identificador atribuído pelo sistema e título, além de indicar que se trata de um documento arquivístico híbrido.	O
1.6.3	Um SIGAD tem que permitir que um conjunto específico de metadados seja configurado para os documentos ou dossiês/processos convencionais e tem que incluir informações sobre o local de arquivamento.	O
1.6.4	Um SIGAD tem que ter mecanismos para acompanhar a movimentação do documento arquivístico convencional de forma que se evidencie ao usuário a localização atual do documento.	O
1.6.5	Um SIGAD deve ser capaz de oferecer ao usuário funcionalidades para solicitar ou reservar a consulta a um documento arquivístico convencional, enviando uma mensagem para o detentor atual desse documento ou para o administrador.	O
1.6.6	Um SIGAD pode incluir mecanismos de impressão e reconhecimento de códigos de barra para automatizar a introdução de dados e acompanhar as movimentações de documentos ou dossiês/processos convencionais.	F
1.6.7	Um SIGAD tem que assegurar que a recuperação de um documento ou dossiê/processo híbrido permita igualmente a recuperação dos metadados tanto da parte digital como da parte convencional.	O
1.6.8	Sempre que os documentos ou dossiês/processos híbridos estiverem classificados quanto ao grau de sigilo, um SIGAD deve garantir que a parte convencional e a parte digital correspondente recebam a mesma classificação de sigilo.	O
1.6.9	Um SIGAD tem que poder registrar na trilha de auditoria todas as alterações efetuadas nos metadados dos documentos ou dossiês/processos convencionais e híbridos.	O

2 TRAMITAÇÃO E FLUXO DE TRABALHO

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

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

- tramitação de um documento antes do seu registro/captura;
- tramitação posterior ao seu registro/captura;

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

- gestão de processos ou de 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 tais como: "verificar documento", "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. No caso do participante ser um indivíduo, a tarefa é direcionada para um usuário com uma identificação específica. No caso do participante ser um grupo de trabalho, a tarefa é direcionada para o grupo (formado por vários usuários, cada um com sua identificação no sistema). A tarefa tem que ser distribuída entre os usuários do grupo e após, ser cumprida por um membro do grupo, o documento segue o fluxo previsto. Quando o participante é um *software,* a tarefa é direcionada uma função de programa, que a realiza automaticamente e reencaminha o documento ao fluxo previsto.

2.1 Controle do fluxo de trabalho

Referência	Requisito	Obrig
2.1.1	Um recurso de fluxo de trabalho de um SIGAD tem que fornecer os passos necessários para o cumprimento de trâmites preestabelecidos ou *ad hoc*. 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

[34] Ver Glossário.

Referência	Requisito	Obrig
2.1.2	Um SIGAD tem que ter capacidade, sem limitações, de estabelecer o número necessário de trâmites nos fluxos de trabalho.	O
2.1.3	O fluxo de trabalho de um SIGAD tem que disponibilizar uma função para **avisar** a um participante do fluxo que um documento lhe foi enviado, especificando a ação necessária.	O
2.1.4	O fluxo de trabalho de um SIGAD deve permitir o **uso do correio eletrônico** para que um usuário possa informar a outros usuários sobre documentos que requeiram sua atenção. *Esse requisito requer a integração com um sistema de correio eletrônico existente.*	AD
2.1.5	O recurso de fluxo de trabalho de um SIGAD tem que permitir que fluxos de trabalho pré-programados sejam definidos, alterados e mantidos exclusivamente por usuário autorizado.	O
2.1.6	O Administrador deve poder autorizar usuários individuais a redistribuir tarefas ou ações presentes em um fluxo de trabalho a um usuário ou grupo diferentes daquele previsto. *Um usuário pode precisar enviar um documento a outro usuário, devido ao seu conteúdo ou no caso do usuário responsável se encontrar em licença.*	AD
2.1.7	Um recurso de fluxo de trabalho de um SIGAD tem que registrar na trilha de auditoria todas as alterações ocorridas nesse fluxo.	O
2.1.8	Um recurso de fluxo de trabalho de um SIGAD tem que registrar a tramitação de um documento a fim de que os usuários possam conhecer a situação de cada um no processo.	O
2.1.9	Um recurso de fluxo de trabalho de um SIGAD deve gerir os documentos em filas de espera que possam ser examinadas e controladas pelo Administrador.	AD
2.1.10	Um recurso de fluxo de trabalho de um SIGAD deve ter a capacidade de deixar que os usuários visualizem a fila de espera de trabalho a eles destinado e que selecionem os itens a trabalhar.	AD
2.1.11	Um recurso de fluxo de trabalho de um SIGAD deve fornecer fluxos condicionais de acordo com os dados de entrada do usuário ou os dados do sistema. *Os fluxos que remetem o documento a um dos participantes dependem de uma condição determinada por um deles. Por exemplo, um fluxo pode levar um documento a um participante ou a um outro, conforme os dados de entrada do participante anterior; ou a definição do fluxo pode depender de um valor calculado pelo sistema.*	AD
2.1.12	Um recurso de fluxo de trabalho de um SIGAD tem que fornecer um histórico de movimentação dos documentos. *O histórico de movimentação corresponde a um conjunto de metadados de datas de entrada e saída; nomes de responsáveis; titulo do documento, providências etc.*	O

Referência	Requisito	Obrig
2.1.13	Um recurso de fluxo de trabalho de um SIGAD pode permitir que usuários autorizados interrompam ou suspendam temporariamente um fluxo com o objetivo de executar outro trabalho. *O fluxo só prosseguirá com a autorização do usuário.*	F
2.1.14	Um recurso de fluxo de trabalho de um SIGAD tem que incluir processamento condicional, isto é, permitir que um fluxo de trabalho seja suspenso para aguardar a chegada de um documento e prossiga automaticamente quando este é recebido.	O
2.1.15	Um recurso de fluxo de trabalho de um SIGAD deve poder associar limites de tempo a trâmites e/ou procedimentos individuais em cada fluxo e comunicar os itens que expiraram de acordo com tais limites.	AD
2.1.16	Um recurso de fluxo de trabalho de um SIGAD tem que reconhecer indivíduos e grupos de trabalho como participantes.	O
2.1.17	Sempre que o participante for um grupo de trabalho, um recurso de fluxo de trabalho de um SIGAD deve prever a forma de distribuição dos documentos entre os membros do grupo. Essa distribuição pode ser: ▪ de acordo com uma seqüência 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
2.1.18	Um recurso de fluxo de trabalho de um SIGAD deve permitir que a captura de documentos desencadeie automaticamente fluxos de trabalho.	AD
2.1.19	Um recurso de fluxo de trabalho de um SIGAD tem que fornecer meios de elaboração de relatórios completos para permitir que gestores monitorem a tramitação dos documentos e o desempenho dos participantes.	O
2.1.20	Um recurso de fluxo de trabalho de um SIGAD tem que registrar a tramitação de um documento em seus metadados. Os metadados referentes à tramitação devem registrar data e hora de envio e de recebimento e identificação do usuário.	O
2.1.21	Um SIGAD deve manter versões dos fluxos alterados e estabelecer vínculos entre os documentos já processados ou em processamento nos fluxos alterados	AD
2.1.22	O SIGAD deve assegurar que qualquer modificação nos atributos dos fluxos, como extinção ou ampliação do número de pessoas ou extinção de autorização, leve em conta os documentos vinculados.	AD

2.2 Controle de versões e do status do documento

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

- um documento criado no espaço individual ou do grupo mas não transmitido, é uma minuta;
- um documento transmitido do espaço individual ou do grupo para o espaço gerencial, onde não poderá mais ser alterado, e daí 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 que é enviado do espaço individual para o do grupo para fins de comentários é uma minuta, que deverá ter seu número de versões devidamente controlado;
- quando um usuário autorizado recupera um documento do espaço gerencial e o armazena em seu espaço, ele cria uma cópia. O mesmo acontece quando o usuário reencaminha um documento para um outro usuário.

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

3 CAPTURA

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

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

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

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

3.1 Captura: procedimentos gerais

Referência	Requisito	Obrig
3.1.1	A captura tem que garantir a execução das seguintes funções: ▪ registrar e gerenciar todos os documentos convencionais; ▪ registrar e gerenciar todos os documentos digitais, independente do contexto tecnológico; ▪ classificar todos os documentos de acordo com o plano ou código de classificação; ▪ controlar e validar a introdução de metadados.	O
3.1.2	Um SIGAD tem que ser capaz de capturar documentos digitais das seguintes formas: ▪ captura de documentos produzidos dentro do SIGAD; ▪ captura de documento individual produzido em arquivo digital fora do SIGAD; ▪ captura de documento individual produzido em *workflow* ou outros sistemas integrado ao SIGAD; ▪ captura de documentos em lote.	O
3.1.3	Um SIGAD pode automatizar a produção de documentos por meio da exibição de formulários e modelos pré-definidos pelo programa de gestão arquivística de documentos.	F
3.1.4	Um SIGAD tem que aceitar o conteúdo do documento, bem como as informações que definem sua aparência, mantendo as associações entre os vários objetos digitais que compõem o documento, isto é, anexos e *links* de hipertexto.	O

Referência	Requisito	Obrig
3.1.5	Um SIGAD tem que permitir a inserção de todos os metadados, obrigatórios e optativos, definidos na sua configuração e garantir que se mantenham associados ao documento. Os metadados obrigatórios são: ▪ nome do arquivo digital; ▪ número identificador atribuído pelo sistema; ▪ data de produção; ▪ data e hora de transmissão e recebimento; ▪ data e hora da captura; ▪ título ou descrição abreviada[35]; ▪ classificação de acordo com o plano ou código de classificação; ▪ prazos de guarda; ▪ autor (pessoa física ou jurídica)[36]; ▪ escritor (se diferente do autor)[37]; ▪ originador[38]; ▪ destinatário (com seu cargo); ▪ nome do setor responsável pela execução da ação contida no documento; ▪ indicação de anotação; ▪ indicação de anexos; ▪ restrição de acesso; ▪ registro das migrações e data em que ocorreram. Os metadados opcionais se referem a informações mais detalhadas sobre o documento, tais como: ▪ espécie / tipo / gênero documental; ▪ indicação de versão; ▪ associações a documentos diferentes que podem estar relacionados pelo fato de registrarem a mesma atividade ou se referirem à mesma pessoa ou situação; ▪ formato *e software* (nome e versão) sob o qual o documento foi produzido ou no qual foi capturado; ▪ máscaras de formatação (template) necessárias para interpretar a estrutura do documento; ▪ assunto / descritor (diferentes do já estabelecido no código de classificação); ▪ localização física. ▪ e outros que se julgarem necessários.	O

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

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

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

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

Referência	Requisito	Obrig
3.1.6	Um SIGAD tem que prever a inserção dos metadados obrigatórios, previstos em legislação específica na devida esfera e âmbito de competência, no momento da captura de processos.	O
3.1.7	Um SIGAD tem que ser capaz de atribuir um número identificador a cada dossiê/processo e documento capturado, que serve para identificá-lo desde o momento da captura até sua destinação final dentro do SIGAD.	O
3.1.8	O formato do número identificador atribuído pelo sistema 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
3.1.9	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 sistema antes de ser aceito. *Uma opção seria gerar o número identificador automaticamente, mas nesse caso, ocultá-lo do usuário, permitindo a este introduzir uma seqüência não necessariamente única como um "identificador". O usuário empregaria essa seqüência como um identificador, mas o SIGAD a consideraria como metadado pesquisável, definido pelo usuário.*	O
3.1.10	Um SIGAD tem que prever a adoção da numeração única de processo e/ou documentos oficiais de acordo com a legislação específica a fim de garantir a integridade do número atribuído ao processo e/ou documento na unidade protocolizadora de origem.	O
3.1.11	Um SIGAD deve utilizar tesauro ou vocabulário controlado para apoiar a atribuição do metadado assunto/descritor. *No caso da Administração Pública Federal, deve ser utilizada a Lista de Assuntos de Governo, conforme orientação dos Padrões de interoperabilidade do governo eletrônico (e-Ping).*	AD
3.1.12	Um SIGAD tem que garantir que os metadados associados a um documento sejam inseridos somente por usuários autorizados.	O
3.1.13	Um SIGAD tem que garantir que os metadados associados a um documento sejam alterados somente por administradores e usuários autorizados e devidamente registrados em trilhas de auditoria.	O
3.1.14	Um SIGAD deve ser capaz de relacionar o mesmo documento digital (objeto digital) a mais de um dossiê ou processo, sem duplicação física do mesmo. *Por exemplo, uma lista de alunos aprovados em concurso de doutorado de uma determinada universidade estará associada ao dossiê "Concurso doutorado 2005" e aos diferentes dossiês de cada aluno aprovado.*	AD

Referência	Requisito	Obrig
	Quando um documento digital estiver associado a mais de um dossiê, o SIGAD deverá criar um registro para cada referência desse documento. Cada registro estará vinculado ao mesmo objeto digital.	
3.1.15	Um SIGAD deve ser capaz de inserir automaticamente os metadados previstos no sistema para o maior número possível de documentos, pois isso diminui as tarefas do usuário do sistema e garante maior rigor na inserção dos metadados. *Por exemplo, no caso de documentos com forma padronizada (formulários, modelos de requerimentos, de memorandos etc) alguns metadados podem ser inseridos automaticamente, tais como: número identificador, título, classificação, prazo de guarda.*	AD
3.1.16	Um SIGAD tem que garantir a visualização do registro de entrada do documento dentro do sistema com todos os metadados inseridos automaticamente e os demais a serem atribuídos pelo usuário. *Por exemplo, o sistema pode atribuir automaticamente o número identificador, a data de captura, o título, o originador e requerer que o usuário preencha os demais metadados.*	O
3.1.17	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
3.1.18	Sempre que um documento tiver mais de uma versão, o SIGAD tem que permitir que os usuários selecionem pelo menos uma das seguintes ações: ▪ 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.	O
3.1.19	Um SIGAD deve prestar assistência aos usuários no que diz respeito à classificação dos documentos, por meio de algumas ou de todas as ações que se seguem: ▪ tornar acessível ao usuário somente o subconjunto do plano de classificação que diz respeito à sua atividade; ▪ indicar as últimas classificações feitas pelo usuário; ▪ indicar dossiês que contenham documentos 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
3.1.20	Um SIGAD deve permitir que um usuário transmita documentos a outro usuário para completar o processo de captura, no caso dos procedimentos dessa captura serem distribuídos entre vários usuários.	AD

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

3.2 Captura em lote

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

3.3 Captura de mensagens de correio eletrônico

O correio eletrônico é um sistema usado para criar, transmitir e receber mensagens eletrônicas e outros documentos digitais por meio de redes de computadores. As características do correio eletrônico podem dificultar o seu gerenciamento. Assim, um SIGAD tem que permitir controles de gestão para:

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

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

Referência	Requisito	Obrig
3.3.1	Um SIGAD tem que permitir que, na fase de configuração, se opte por uma das seguintes operações: ▪ capturar mensagens de correio eletrônico após selecionar quais serão objeto de registro; ou ▪ capturar automaticamente todas as mensagens de correio eletrônico.	O
3.3.2	Um SIGAD pode permitir que os usuários tratem e capturem as mensagens de chegada a partir do seu próprio sistema de correio eletrônico. O usuário deve poder tratar cada mensagem na caixa de entrada, a partir do seu sistema de correio eletrônico, como se segue: ▪ visualizar cada mensagem de correio e uma indicação dos respectivos anexos, caso esses 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.	F
3.3.3	Um SIGAD deve assegurar a captura do nome e não somente do endereço do originador do correio eletrônico. Por exemplo, "Luís Santos" além de lsa25@ab.br.	AD

3.4 Captura de documentos convencionais ou híbridos

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

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

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

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

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

Documentos automodificáveis

Alguns documentos aparentam ter seus conteúdos alterados sem intervenção do usuário. Um exemplo é um modelo para elaboração de correspondência cuja data é colocada automaticamente pelo sistema e armazenada como um "campo" ou "código". Nesse caso, cada vez que o documento é exibido, a data apresentada é atualizada. Entretanto o documento lógico não se modifica, é apenas a sua exibição (documento conceitual) que sofre alterações conforme o *software* utilizado para visualizá-lo.

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

Os documentos automodificáveis devem ser evitados. Caso isso não seja possível, os documentos devem ser armazenados em formatos que desativem o código automodificador ou visualizados por meio de *software* que não desencadeie a alteração. Por exemplo: uma planilha de cálculo que contenha "macros" deve ser convertida para um formato estável, como o PDF, antes de ser capturada para o SIGAD.

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

Referência	Requisito	Obrig
3.5.1	Um SIGAD tem que possuir a capacidade de capturar documentos de diferentes formatos de arquivo e estruturas.	O
3.5.2	Um SIGAD deve poder capturar, entre outros, os seguintes documentos: ▪ calendários eletrônicos; ▪ 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. *A lista de documentos, que um SIGAD tem que suportar, irá variar de órgão para órgão.*	AD

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

Referência	Requisito	Obrig
3.5.3	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, páginas web, publicações eletrônicas, bases de dados.	O
3.5.4	Um SIGAD deve permitir que um documento composto seja capturado de qualquer uma das duas formas seguintes: ▪ como um único documento de arquivo composto; ▪ como uma série de documentos de arquivo simples relacionados, um para cada componente do documento composto.	AD
3.5.5	O SIGAD tem que ser capaz de incluir novos formatos e arquivos à medida que forem sendo adotados pelo órgão ou entidade.	O

3.6 Estrutura dos procedimentos de gestão

A gestão arquivística de documentos digitais prevê o estabelecimento de três domínios dentro do ambiente eletrônico, a saber: *espaço individual*, *espaço do grupo* e *espaço geral*. O *espaço individual* corresponde ao espaço designado a cada funcionário. O *espaço do grupo* corresponde ao espaço designado a cada grupo de trabalho, equipe, comitê etc. O *espaço geral* corresponde ao serviço de protocolo e arquivos do órgão ou entidade. Sua principal característica é que uma vez ali, o documento não poderá mais ser alterado.

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

- produzidos, recebidos, alterados, capturados (registrados, classificados, indexados e arquivados ou encaminhados), armazenados e eliminados;
- o espaço no qual os metadados serão incluídos;
- os direitos de acesso em cada espaço e a maneira pela qual 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, o contexto e a forma dos documentos capturados devem ser mantidos ao longo de todo seu ciclo de vida, a fim de preservar a sua autenticidade.

Referência	Requisito	Obrig
3.6.1	Um SIGAD tem que ser capaz de reconhecer três domínios para o controle dos procedimentos de gestão: espaço individual, espaço de grupo e espaço geral.	O
3.6.2	Um SIGAD tem que ser capaz de operacionalizar as regras estabelecidas pelo sistema de gestão arquivística de documentos nos três espaços.	O

3.6.3	Um SIGAD tem que impedir que o conteúdo de um documento seja alterado por usuários e Administradores, exceto nos casos em que a alteração fizer parte do processo documental, conforme tratado na seção 6.10 – Alterar, apagar e truncar.	O
3.6.4	Um SIGAD deve poder emitir um aviso, no caso de se tentar capturar um documento incompleto ou inconsistente de uma forma que venha a comprometer sua futura autenticidade. *Exemplo: uma correspondência sem assinatura digital válida ou uma fatura de fornecedor não identificado.*	AD
3.6.5	Um SIGAD deve poder emitir um aviso, no caso de se tentar capturar um documento em que a futura verificação de sua autenticidade não for viável.	AD

4 AVALIAÇÃO E DESTINAÇÃO

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

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

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

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

4.1 Configuração da tabela de temporalidade e destinação de documentos

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

Referência	Requisito	Obrig
4.1.1	Um SIGAD tem que prover funcionalidades para definição e manutenção de tabela de temporalidade e destinação de documentos, associada ao plano de classificação do órgão ou entidade.	O
4.1.2	Um SIGAD tem que associar, automaticamente, ao dossiê/processo o prazo e a destinação previstos na classe em que o documento foi inserido.	O
4.1.3	Um SIGAD tem que manter tabela de temporalidade e destinação de documentos com as seguintes informações: ▪ identificador do órgão ou entidade; ▪ identificador da classe; ▪ prazo de guarda na fase corrente; ▪ prazo de guarda na fase intermediária; ▪ destinação final; ▪ observações; ▪ evento que determina o início da contagem do prazo de retenção na fase corrente e na fase intermediária. *A tabela de temporalidade e destinação de documentos dos integrantes do SINAR deve estar de acordo com a legislação e*	O

[40] A Resolução do CONARQ nº 14, de 28 de outubro de 2001, aprova a versão revisada e ampliada da Resolução do CONARQ nº 4, de 28 de março de 1996, que dispõe sobre a classificação, temporalidade e destinação de documentos de arquivo relativos às atividades-meio da administração pública. Esse instrumento também orienta a elaboração de código de classificação e tabela de temporalidade e destinação de documentos para as atividades finalísticas.

Referência	Requisito	Obrig
	ser aprovada pela instituição arquivística na específica esfera de competência.[40]	
4.1.4	Um SIGAD tem que prever ao menos as seguintes situações para destinação: ▪ apresentação dos documentos para reavaliação em data futura; ▪ eliminação; ▪ exportação para transferência; ▪ exportação para recolhimento (guarda permanente).	O
4.1.5	Um SIGAD tem que prever a iniciação automática da contagem dos prazos de guarda referenciados na tabela de temporalidade e destinação de documentos a partir de pelo menos os seguintes eventos: ▪ abertura do dossiê; ▪ arquivamento do dossiê/processo; ▪ desarquivamento de dossiê/processo; ▪ inclusão de documento em um dossiê/processo. *Acontecimentos específicos, descritos na tabela de temporalidade e destinação como, por exemplo, "5 anos a contar da data de aprovação das contas", quando não puderem ser detectados automaticamente pelo sistema, deverão ser informados ao SIGAD por usuário autorizado.*	O
4.1.6	Um SIGAD tem que prever que a definição dos prazos de guarda sejam expressos por: ▪ um número inteiro de dias ou ▪ um número inteiro de meses ou ▪ um número inteiro de anos ou ▪ uma combinação de um número inteiro de anos, meses e dias.	O
4.1.7	Um SIGAD tem que limitar a definição e a manutenção (alteração, inclusão e exclusão) da tabela de temporalidade e destinação de documentos a usuários autorizados.	O
4.1.8	Um SIGAD tem que permitir que um usuário autorizado altere o prazo ou destinação prevista em um item da tabela de temporalidade e destinação de documentos e garantir que a alteração tenha efeito em todos os documentos ou dossiês/processos associados àquele item. *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
4.1.9	Um SIGAD deve ser capaz de manter o histórico das alterações realizadas na tabela de temporalidade e destinação de documentos.	AD

Referência	Requisito	Obrig
4.1.10	Um SIGAD deve ser capaz de importar e exportar total ou parcialmente uma tabela de temporalidade e destinação de documento *Ver item 12- Interoperabilidade*	AD
4.1.11	Um SIGAD tem que prover funcionalidades para elaboração de relatórios que apóiem a gestão da tabela de temporalidade e destinação, incluindo a capacidade de: ▪ 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 está atribuído um determinado prazo de guarda; ▪ identificar as inconsistências existentes entre a tabela de temporalidade e destinação de documentos e o plano de classificação.	O

4.2 Aplicação da tabela de temporalidade e destinação de documentos

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

Referência	Requisito	Obrig
4.2.1	Um SIGAD tem que fornecer recursos integrados à tabela de temporalidade e destinação de documentos para implementar as ações de destinação.	O
4.2.2	Para cada dossiê/processo, um SIGAD tem que acompanhar automaticamente os prazos de guarda determinados para a classe à qual pertence.	O
4.2.3	Um SIGAD tem que prover funcionalidades para informar ao usuário autorizado sobre os documentos ou dossiês/processos que já cumpriram ou estão para cumprir o prazo de guarda previsto.	O
4.2.4	Um SIGAD deve prover funcionalidades para gerenciar o processo de destinação, que deve 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 confirmado pelo usuário autorizado.	O
4.2.5	Um SIGAD tem sempre que pedir confirmação antes de realizar as ações de destinação.	O

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

4.3 Exportação de documentos

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

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

Referência	Requisito	Obrig
4.3.1	Um SIGAD tem que ser capaz de exportar documentos e dossiês/processos digitais e seus metadados para outro sistema dentro ou fora do órgão ou entidade.	O
4.3.2	Quando um SIGAD exportar os documentos e dossiês/processos de uma classe para executar uma ação de transferência ou recolhimento, tem que ser capaz de exportar todos os documentos e dossiês/processos da classe incluídos na ação de destinação, com seus respectivos volumes, documentos e metadados associados.	O
4.3.3	Um SIGAD tem que ser capaz de exportar um documento e dossiê/processo ou grupo de documentos e dossiês/processos numa seqüência de operações, de modo que: ▪ o conteúdo, o contexto e a estrutura dos seus documentos não se degradem; ▪ todos os componentes de um documento digital sejam exportados como uma unidade. 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
4.3.4	Um SIGAD deve ser capaz de exportar dossiês/processos: ▪ em seu formato nativo (ou no formato para o qual foi migrado); ▪ de acordo com o 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
4.3.5	Um SIGAD deve ser capaz de exportar metadados nos formatos previstos pelo padrão de interoperabilidade do governo.	AD
4.3.6	Um SIGAD tem que ser capaz de exportar todos os tipos de documentos que está apto a capturar.	O
4.3.7	Um SIGAD tem que produzir um relatório detalhando sobre qualquer falha que ocorra durante uma exportação. O relatório tem que identificar os documentos e dossiês/processos que tenham originado erros de processamento ou cuja exportação não tenha sido bem sucedida.	O
4.3.8	Um SIGAD tem que conservar todos os documentos e dossiês/processos digitais que tiverem sido exportados, pelo menos até que tenham sido importados no sistema destinatário com êxito.	O
4.3.9	Um SIGAD tem que manter metadados relativos a documentos e dossiês/processos que foram exportados. *O Administrador deve indicar o subconjunto de metadados que deverá ser mantido.*	O

Referência	Requisito	Obrig
4.3.10	Um SIGAD tem que gerar listagem em meio digital e em papel para descrever documentos e dossiês/processos digitais que estão sendo exportados. *Este requisito se aplica principalmente nos casos em que é feita exportação para transferência ou recolhimento para instituição arquivística pública. Nesse caso, a listagem deverá ser produzida no formato estabelecido pela instituição arquivística recebedora.*	O
4.3.11	Um SIGAD deve possibilitar a inclusão de metadados necessários à gestão do arquivo permanente nos documentos e dossiês/processos que serão exportados para recolhimento.	AD
4.3.12	Um SIGAD pode possibilitar a ordenação dos documentos e dossiês/processos digitais a serem exportados de acordo com elementos de metadados selecionados pelo usuário.	F
4.3.13	Quando se exportar documentos e dossiês/processos híbridos, um SIGAD deve exigir do usuário autorizado a confirmação de que a parte sob forma convencional dos mesmos documentos e dossiês/processos tenha passado pelo procedimento de destinação adequado antes de confirmar a exportação da parte sob forma digital.	AD
4.3.14	Um SIGAD deve permitir que documentos sejam exportados mais de uma vez.	AD

4.4 Eliminação

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

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

Referência	Requisito	Obrig
4.4.1	Um SIGAD tem que restringir a função de eliminação de documentos ou dossiês/processos somente a usuários autorizados.	O
4.4.2	Um SIGAD tem que pedir confirmação da eliminação a um usuário autorizado antes que qualquer ação seja tomada com relação ao documento e dossiê/processo e cancelar o processo de eliminação se a confirmação não for dada.	O
4.4.3	Um SIGAD tem que avisar o usuário autorizado quando um documento ou dossiê/processo que estiver sendo eliminado se encontrar relacionado a outro; os sistemas também têm de suspender o processo até que seja tomada uma das medidas	O

[41] Lei nº 8.159, de 8 de janeiro de 1991 e Resoluções do CONARQ nº 5, 7 e 20, bem como a legislação específica das esferas municipal e estadual e poderes da União.

Referência	Requisito	Obrig
	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.	
4.4.4	Um SIGAD deve permitir a eliminação de documentos ou dossiês/processos de forma irreversível a fim de que não possam ser restaurados por meio da utilização normal do SIGAD nem por meio de rotinas auxiliares do sistema operacional nem por aplicações especiais de recuperação de dados.	AD
4.4.5	Quando um documento tem várias referências armazenadas no sistema, um SIGAD tem que garantir que todas essas referências sejam verificadas antes de eliminar o objeto digital. *Ver requisito 4.2.9*	O
4.4.6	Um SIGAD tem que produzir um relatório detalhando qualquer falha que ocorra durante uma eliminação. O relatório tem que identificar os documentos cuja eliminação não tenha sido bem sucedida.	O
4.4.7	Quando eliminar documentos ou dossiês/processos híbridos, um SIGAD deve exigir do usuário autorizado a confirmação de que a parte sob forma convencional dos mesmos seja eliminada também antes de confirmar a eliminação da parte sob forma digital.	AD
4.4.8	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
4.4.9	Um SIGAD tem que manter metadados relativos a documentos e dossiês/processos que foram eliminados. *O Administrador deve indicar o subconjunto de metadados que deverá ser mantido.*	O

4.5 Avaliação e destinação de documentos arquivísticos convencionais e híbridos

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

Referência	Requisito	Obrig
4.5.1	Um SIGAD tem que aplicar a mesma tabela de temporalidade e destinação de documentos para os documentos convencionais, digitais ou híbridos.	O
4.5.2	Um SIGAD tem que acompanhar os prazos de guarda dos documentos convencionais e deve dar início aos procedimentos de eliminação ou transferência desses documentos, tomando em consideração suas especificidades.	O

Referência	Requisito	Obrig
4.5.3	Um SIGAD tem que alertar o administrador sobre existência e localização de uma parte convencional associada a um documento híbrido que esteja destinado a ser exportado, transferido ou eliminado.	O
4.5.4	Um SIGAD deve exportar metadados de documentos e dossiês/processos convencionais.	AD

5 PESQUISA, LOCALIZAÇÃO E APRESENTAÇÃO DOS DOCUMENTOS

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

Todas essas funcionalidades têm de ser submetidas aos controles de acesso descritos na seção 6 - SEGURANÇA.

Referência	Requisito	Obrig
5.1.1	Um SIGAD tem que fornecer facilidades para pesquisa, localização e apresentação dos documentos.	O
5.1.2	Um SIGAD deve fornecer interface de pesquisa, localização e apresentação opcionais via um ambiente *web*.	AD
5.1.3	Um SIGAD deve prever a navegação gráfica do plano de classificação, a navegação direta de uma classe para os documentos arquivísticos criados nessa classe e a seleção, recuperação e apresentação direta dos documentos arquivísticos e de seus conteúdos por meio desse mecanismo.	AD

5.2 Pesquisa e localização

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

Referência	Requisito	Obrig
5.2.1	Um SIGAD tem que fornecer uma série flexível de funções que atuem sobre os metadados relacionados com os diversos níveis de agregação (documento, unidade de arquivamento e classe) e sobre os conteúdos dos documentos arquivísticos por meio de parâmetros definidos pelo usuário, com o objetivo de localizar e acessar os documentos e/ou metadados, quer individualmente quer reunidos em grupo.	O
5.2.2	Um SIGAD tem que executar pesquisa de forma integrada, isto é, apresentar todos os documentos e dossiês/processos, sejam eles digitais, híbridos ou convencionais, que satisfaçam aos parâmetros da pesquisa.	O
5.2.3	Um SIGAD tem que permitir que todos os metadados de gestão[42] de um documento ou dossiê/processo possam ser pesquisados.	O
5.2.4	Um SIGAD deve permitir que os conteúdos sob a forma de texto dos documentos possam ser pesquisados.	AD

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

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

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

5.3 Apresentação: visualização, impressão, emissão de som

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

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

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

Referência	Requisito	Obrig
5.3.5	Um SIGAD deve permitir a configuração do formato da lista de resultados de pesquisa pelo usuário ou administrador, incluindo recursos e funções tais como: ▪ Seleção a ordem em que os resultados de pesquisa são apresentados; ▪ Determinação do número de resultados de pesquisa exibidos na tela de cada vez; ▪ Estabelecimento do número máximo de resultados para uma pesquisa; ▪ Armazenamento dos resultados de uma pesquisa; ▪ Definição dos metadados que devem ser exibidos nas listas de resultados de pesquisa.	AD
5.3.6	Um SIGAD deve fornecer recursos que permitam a um 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 nele incluídos; ▪ de uma unidade de arquivamento para a classe respectiva; ▪ de uma classe para as unidades de arquivamento a ela relacionadas.	AD
5.3.7	Um SIGAD tem que ser capaz de apresentar o conteúdo de todos os tipos de documentos arquivísticos digitais capturados de forma que: ▪ preserve as características de apresentação visual e formato apresentados pela aplicação geradora; ▪ exiba todos os componentes do documento digital em conjunto, como uma unidade.	O
5.3.8	Um SIGAD tem que ser capaz de exibir em tela todos os tipos de documentos capturados.	O
5.3.9	Um SIGAD tem que ser capaz de imprimir os documentos capturados, preservando o formato produzido pelas aplicações geradoras.	O
5.3.10	Um SIGAD tem que ser capaz de exibir / reproduzir o conteúdo de documentos que incluam imagem fixa, imagem em movimento e som.	O
5.3.11	Um SIGAD tem que proporcionar ao usuário formas flexíveis de impressão de documentos com seus metadados, incluindo a possibilidade de definição dos metadados a serem impressos.	O
5.3.12	Um SIGAD tem que ser capaz de exibir em tela e de imprimir todos os metadados associados aos documentos e dossiês/processos resultantes de uma pesquisa.	O
5.3.13	Um SIGAD tem que permitir a impressão de uma lista dos documentos e dossiês/processos resultantes de uma pesquisa.	O
5.3.14	Um SIGAD tem que permitir a impressão de uma lista dos documentos que compõem um dossiê/processo.	O
5.3.15	Um SIGAD deve permitir que os metadados exibidos nas listas a que se referem os requisitos 5.3.13 e 5.3.14 possam ser definidos pelo usuário.	AD

Referência	Requisito	Obrig
5.3.16	Um SIGAD tem que permitir que todos os documentos de um dossiê/processo sejam impressos em uma única operação, na seqüência determinada pelo usuário.	O
5.3.17	Um SIGAD tem que incluir recursos destinados a transferir para suportes adequados documentos que não possam ser impressos, tais como som, vídeo e páginas Web.	O
5.3.18	Um SIGAD deve ser capaz de apresentar os documentos arquivísticos em outros formatos além do nativo, tais como: ▪ formato XML adequado para publicação; ▪ formato HTML adequado para publicação; ▪ formato aprovado por organismos padronizadores na sua esfera de competência; *No que se refere a interoperabilidade com outros sistemas, ver seção 12 Interoperabilidade.*	AD
5.3.19	Um SIGAD tem que ser capaz de realizar pesquisa e exibição de documentos e dossiês/processos simultaneamente para diversos usuários.	O
5.3.20	Um SIGAD deve permitir que o administrador determine que todas as cópias em papel de documentos e dossiês/processos sejam impressas junto com metadados pré-selecionados.	AD

6 SEGURANÇA

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

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

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

- de controle de acesso baseado em papéis de usuário.
- de controle de acesso por grupos.
- de classificação quanto ao grau de sigilo.

Os três tipos de controle de acesso podem ser combinados e os requisitos de administração de controle de acesso devem ser adaptados a cada um dos tipos acima ou a combinação deles, de acordo com a legislação vigente.

Quanto ao uso da tecnologia de criptografia, tanto para sigilo quanto 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 de informações. Os requisitos de assinatura digital e certificação digital são necessários para aquelas organizações em que documentos são assinados digitalmente ou verificações eletrônicas de autenticidade são necessárias.

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

6.1 Cópias de segurança

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

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

Referência	Requisito	Obrig
6.1.1	Um SIGAD tem que permitir que, sob controle do seu administrador, mecanismos de *backup* criem cópias de todas as informações nele contidas (documentos arquivísticos, metadados e parâmetros do sistema).	O

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

6.2 Controle de acesso

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

Identificação e Autenticação de Usuários

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

Usuários acessam dados, metadados e funções via a interface do programa. A associação entre Identidade do Usuário e as autorizações de acesso é feita durante a fase de identificação e autenticação do usuário via a interface do programa, com base nas credenciais de autenticação.

Referência	Requisito	Obrig
6.2.1	Para implementar o controle de acesso, um SIGAD tem que manter pelo menos os seguintes atributos dos usuários, de acordo com a política de segurança: ▪ Identificador do usuário; ▪ Autorizações de acesso; ▪ Credenciais de autenticação.	O

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

Aspectos Gerais de Controle de Acesso

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

Referência	Requisito	Obrig
6.2.5	Um SIGAD tem que permitir acesso a funções do sistema somente a usuários autorizados e sob controle rigoroso da administração do sistema a fim de proteger a autenticidade dos documentos arquivísticos digitais.	O
6.2.6	Se o usuário solicitar o acesso ou pesquisa de um documento arquivístico, volume ou dossiê/processo específicos aos quais não tenha o direito de acesso, um SIGAD deve fornecer 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 existência do mesmo. *Essas opções são apresentadas em ordem crescente de segurança. O requisito da terceira opção (isto é, a mais rigorosa) implica que um SIGAD terá de excluir esses documentos de qualquer listagem dos resultados de uma pesquisa. Esse procedimento é normalmente adequado para documentos que requeiram elevados graus 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
6.2.7	Somente administradores autorizados têm que ser capazes de criar, alterar, remover ou revogar as permissões associadas a papéis de usuários, grupos de usuários ou usuários individuais.	O

Referência	Requisito	Obrig
6.2.8	Um SIGAD deve implementar imediatamente alterações ou revogações dos atributos de segurança de usuários e de documentos digitais.	AD
6.2.9	Um SIGAD deve oferecer ferramentas de aumento de produtividade ao administrador, tais como, realização de operações sobre lotes ou grupos de usuários e lotes de documentos digitais, agenda de tarefas, análises de trilhas e geração de alarmes.	AD
6.2.10	Quando um SIGAD controlar o acesso por grupos de usuários, papéis de usuários e usuários individuais, deve obedecer a uma hierarquia de permissões preestabelecida na política de segurança.	AD

Controle de Acesso por Grupos de Usuários

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

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

Referência	Requisito	Obrig
6.2.11	Um SIGAD tem que implementar a política de controle de acesso por grupos de usuários sobre documentos baseado no seguinte: ▪ 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
6.2.12	O acesso a documentos, a dossiês/processos ou classes, tem que ser concedido se a permissão requerida para a operação estiver associada a pelo menos um dos grupos aos quais o usuário pertença.	O
6.2.13	Um SIGAD tem que permitir que um usuário pertença a mais de um grupo.	O
6.2.14	Um SIGAD pode permitir que alguns usuários estipulem que outros usuários, papéis ou grupos de usuários podem ter acesso aos documentos sob sua responsabilidade. Essa permissão deve ser atribuída pelo Administrador, de acordo com a política de segurança do órgão ou entidade.	F

Controle de Acesso por Papéis de Usuários

Papéis são funções ou cargos com responsabilidades e autoridades bem definidas. Operações são tarefas executadas sobre os documentos, os dossiês/processos e as 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 são garantias aprovadas para realização de operações sobre documentos arquivísticos.

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

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

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

Os requisitos descritos nesta seção referem-se ao acesso aos documentos arquivísticos com base na classificação do grau de sigilo bem como restrição de acesso à informação sensível. Informação sensível pode estar relacionada à honra e à privacidade de pessoas ou a questões estratégicas e de segredo corporativo. Os requisitos são flexíveis para atender tanto às organizações privadas, quanto aos órgãos públicos. Órgãos da administração pública são subordinados aos graus de sigilo definidos na legislação vigente.

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

Referência	Requisito	Obrig
6.3.1	Um SIGAD tem que implementar a classificação de grau de sigilo sobre os documentos, os dossiês/processos e as classes do plano de classificação e sobre todas as operações de usuários nos documentos.	O
6.3.2	Um SIGAD tem que implementar a classificação de grau de sigilo baseando-se nos seguintes atributos de segurança para documentos e para usuários: ▪ grau de sigilo do documento; ▪ credencial de segurança do usuário. *O grau de sigilo tem que estar associado à credencial de segurança.*	O

Referência	Requisito	Obrig
6.3.3	Um SIGAD tem que recusar o acesso de usuários a documentos que possuam um grau de sigilo superior à sua credencial de segurança.	O
6.3.4	Um SIGAD tem que garantir que os documentos sem atribuição de grau de sigilo, importados a partir de fontes externas ao SIGAD, estejam sujeitos às políticas de controle de acesso e de sigilo.	O
6.3.5	Um SIGAD tem que ser capaz de manter a marcação de sigilo original durante a importação de documentos marcados com graus de sigilo, a partir de fontes externas ao SIGAD.	O
6.3.6	Um SIGAD deve garantir que não haja ambigüidade na associação entre as marcações de grau de sigilo e os outros atributos de segurança (permissões) do documento importado.	AD
6.3.7	Um SIGAD tem que permitir que um dos itens abaixo seja selecionado durante a configuração: ▪ graus de sigilo a serem atribuídos a classes e dossiês/processos; ▪ *classes e dossiês/processos sem grau de sigilo.*	O
6.3.8	Em caso de erro ou reavaliação, o administrador tem que ser capaz de alterar o grau de sigilo de todos os documentos arquivísticos de um dossiê/processo ou de uma classe, numa única operação.	O
6.3.9	Um SIGAD tem que garantir que o grau de sigilo de um documento importado esteja associado a um usuário autorizado com a credencial de segurança pertinente para receber o documento.	O
6.3.10	Um SIGAD tem que permitir somente aos administradores autorizados a possibilidade de alterar a configuração dos valores predefinidos (*default*) para os atributos de segurança e marcações de graus de sigilo, quando necessário e apropriado.	O
6.3.11	Somente administradores autorizados têm que ser 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
6.3.12	Um SIGAD tem que permitir somente ao usuário autorizado, mediante confirmação, a desclassificação ou redução do grau de sigilo de um documento	O
6.3.13	Um SIGAD deve permitir o armazenamento dos documentos sigilosos em meios físicos ou lógicos distintos.	AD
6.3.14	Um SIGAD tem que impedir que um documento sigiloso seja eliminado. *Os documentos sigilosos têm que se tornar ostensivos para serem submetidos ao processo de avaliação e serem destinados*.	O
6.3.15	Um SIGAD tem que implementar metadados nos níveis de dossiê, documento ou extrato de documento para controlar o acesso a informação sensível.	O

6.4 Trilhas de Auditoria

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

Referência	Requisito	Obrig
6.4.1	Um SIGAD tem que ser capaz de registrar na trilha de auditoria informações acerca das seguintes ações: ▪ data e hora da captura de todos os documentos; ▪ responsável pela captura; ▪ reclassificação, desclassificação ou redução do grau de sigilo de um documento ou de um dossiê/processo, com a classificação inicial e a classificação final. ▪ qualquer alteração na tabela de temporalidade e destinaçãode 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. ▪ alterações efetuadas nas permissões de acesso que afetem um dossiê/processo, um documento ou um usuário; ▪ ações de exportação e importação envolvendo os documentos; ▪ tentativas de exportação (inclusive para *backup*s) e de importação (inclusive *restore*); ▪ 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; ▪ infrações cometidas contra mecanismos de controle de acesso; ▪ mudanças no relógio gerador de carimbos de tempo; ▪ todas as ações administrativas sobre os atributos de segurança (papéis, grupos, permissões, etc); ▪ todas as ações administrativas sobre dados de usuários (cadastro, ativação, bloqueio, atualização de dados e permissões, troca de senha, etc.) ▪ todos os eventos de administração de manutenção das trilhas de auditoria (alarmes, cópias, configuração de parâmetros, etc.).	O
6.4.2	Um SIGAD tem que registrar, em cada evento auditado, informações sobre a identidade do usuário, desde que tal identificação esteja de acordo com a política de privacidade da organização e a legislação vigente.	O
6.4.3	Um SIGAD deve permitir apenas ao administrador e ao auditor a leitura das trilhas de auditoria.	AD
6.4.4	Um SIGAD tem que assegurar que as informações da trilha de auditoria estejam disponíveis para inspeção a fim de que uma ocorrência específica possa ser identificada e que todas as respectivas informações sejam claras e compreensíveis.	O

Referência	Requisito	Obrig
6.4.5	Um SIGAD deve possuir mecanismos para a realização de buscas nos eventos das trilhas de auditoria. *Para facilidade de relatório, os resultados podem ser apresentados ordenados, mas essa ordenação não pode alterar os dados contidos na trilha.*	AD
6.4.6	Um SIGAD tem que ser capaz de impedir qualquer modificação da trilha de auditoria.	O
6.4.7	Somente administradores autorizados têm que ser capazes de exportar as trilhas de auditoria sem afetar a trilha armazenada, ou transferir as trilhas de auditoria de um suporte de armazenamento para outro. *A trilha de auditoria não pode ser excluída antes da data indicada na tabela de temporalidade. Porém, a transferência implica cópia da trilha para outro espaço de armazenamento com a subseqüente liberação do espaço original. A exportação é a cópia sem a liberação do espaço.*	O
6.4.8	Um SIGAD deve ser capaz de gerar um alarme, para os administradores apropriados, se o tamanho da trilha de auditoria exceder um limite preestabelecido. *Esse alarme deve ser usado para indicar a proximidade do esgotamento de espaço reservado à trilha de auditoria.*	AD
6.4.9	Quando o espaço de armazenamento da trilha de auditoria atingir o limite preestabelecido, um SIGAD deve permitir somente operações auditáveis originadas por administradores. *Todas as outras operações estariam bloqueadas até a liberação pelo administrador.*	AD
6.4.10	Um SIGAD deve ser capaz de aplicar um conjunto de regras na monitoração de eventos auditados e, com base nessas regras indicar a possível violação da segurança.	AD
6.4.11	Um SIGAD deve garantir pelo menos as seguintes regras para a monitoração dos eventos auditados: ▪ Acumulação de um número predeterminado de tentativas consecutivas de *log in* com erro (autenticação mal sucedida), conforme especificado pela política de segurança; ▪ Ocorrência de vários *log in* simultâneos do mesmo usuário em locais (computadores) diferentes. ▪ *Login* do usuário fora do horário autorizado, após *log off* no período normal.	AD
6.4.12	Um SIGAD tem que fornecer relatórios sobre as ações que afetam classes, unidades de arquivamento e documentos, em ordem cronológica e organizados por: ▪ documento arquivístico, unidade de arquivamento ou classe; ▪ usuário; ▪ tipo de ação ou operação.	O

Referência	Requisito	Obrig
6.4.13	Um SIGAD pode fornecer relatórios referentes a ações que afetem documentos e dossiês/processos organizados por posto de trabalho (nos casos em que for tecnicamente adequado), por 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 de qual interface de acesso foi usada.*	F
6.4.14	Somente administradores autorizados têm que ser capazes de configurar o conjunto de eventos auditáveis e seus atributos.	O
6.4.15	Somente administradores autorizados, acompanhados do auditor, têm que ser capazes de configurar o conjunto de eventos auditáveis e seus atributos.	O

6.5 Assinaturas Digitais

Assinatura digital é uma seqüência 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 infra-estrutura 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 Infra-estrutura de Chaves Públicas Brasileira - ICP-Brasil.

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

Referência	Requisito	Obrig
6.5.1	Um SIGAD deve ser capaz de garantir a origem e a integridade dos documentos com assinatura digital.	AD
6.5.2	Somente administradores autorizados têm que ser capazes de incluir, remover, ou atualizar no SIGAD os certificados digitais de computadores ou de usuários.	O
6.5.3	Um SIGAD tem que ser capaz de verificar a validade da assinatura digital no momento da captura do documento.	O
6.5.4	Um SIGAD, no processo de verificação da assinatura digital, tem de ser capaz de registrar nos metadados do documento o seguinte: ▪ validade da assinatura verificada; ▪ a autoridade certificadora do certificado digital; ▪ data e hora em que a verificação ocorreu.	O
6.5.5	Um SIGAD deve ser capaz de armazenar juntamente com o documento as seguintes informações de certificação: ▪ assinatura digital; ▪ certificado digital (cadeia de certificação) usado na verificação da assinatura; ▪ Lista de Certificados Revogados - LCR;	AD

Referência	Requisito	Obrig
6.5.6	Um SIGAD deve ser capaz de receber atualizações tecnológicas quanto à plataforma criptográfica de assinatura digital.	AD
6.5.7	Um SIGAD deve destruir, ou tornar indisponíveis, as chaves de criptografia quando estas estiverem contidas em listas de certificados revogados (LCR).	AD
6.5.8	Um SIGAD deve ter acesso a relógios e carimbador de tempo confiáveis para o seu próprio uso. *O relógio gerador do selo de tempo deve ser sincronizado com o Observatório Nacional[43].*	AD

6.6 Criptografia

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

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

É importante salientar que, no uso de criptografia em documentos que apresentam longa temporalidade, devem ser tomadas medidas administrativas para garantir a manutenção do sigilo e do acesso a esses documentos. Esses documentos não devem ser armazenados criptografados. Alguns fatores que comprometem a criptografia no longo prazo são: 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 longo prazo para documentos digitais como um período a partir de 5 anos contado a partir da data de produção[44].

Referência	Requisito	Obrig
6.6.1	Um SIGAD tem que usar a criptografia no armazenamento, na transmissão e na apresentação de documentos arquivísticos digitais ao implementar a política de sigilo.	O
6.6.2	Um SIGAD tem que limitar o acesso aos documentos cifrados somente àqueles usuários portadores da chave de decifração.	O
6.6.3	Um SIGAD tem que registrar os seguintes metadados sobre um documento cifrado: ▪ indicação se está cifrado ou não; ▪ algoritmos usados na cifração; ▪ identificação do remetente; ▪ identificação do destinatário; ▪ Indicação da robustez ou grau de segurança da criptografia.	O

[43] Observatório Nacional - Divisão do Serviço da Hora, disponível em: http://pcdsh01.on.br/

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

Referência	Requisito	Obrig
6.6.4	Um SIGAD deve poder assegurar a captura de documentos cifrados, diretamente de uma aplicação de *software* que disponha da funcionalidade de cifração.	AD
6.6.5	Somente os usuários autorizados têm que ser capazes de realizar as seguintes operações: ▪ Incluir, remover ou alterar parâmetros dos algoritmos criptográficos instalados no SIGAD; ▪ Incluir, remover ou substituir chaves criptográficas de programas ou de usuários do SIGAD; ▪ Cifrar e alterar criptografia de documentos; ▪ Remover a criptografia de um documento. *A remoção da cifração pode ocorrer quando a sua manutenção resultar em indisponibilidade do documento. Por exemplo, quando a chave de cifração/decifração estiver embarcada em hardware inviolável cuja vida útil está prestes a se esgotar ou quando o documento for desclassificado.*	O
6.6.6	No caso de remoção da cifração do documento, os seguintes metadados adicionais tem 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
6.6.7	Um SIGAD deve possuir uma arquitetura capaz de receber atualizações tecnológicas quanto à plataforma criptográfica.	AD

6.7 Marcas d'água Digitais

Marcas d'água servem para marcar uma imagem digital com informação sobre a sua proveniência e características e são utilizadas para proteger propriedade intelectual. As marcas d'água sobrepõem, no mapa de *bits* de uma imagem, um desenho complexo, visível ou invisível, o qual só pode ser suprimido mediante a utilização de um algoritmo ou de uma chave protegida. Tecnologias semelhantes podem ser aplicadas a sons e a imagens em movimento digitalizadas.

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

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

Referência	Requisito	Obrig
6.7.1	Um SIGAD tem que ser capaz de recuperar informação contida em marcas d'água digitais.	O
6.7.2	Um SIGAD tem que ser capaz de armazenar documentos arquivísticos digitais que contenham marcas d'água digitais, assim como informação de apoio relacionada à marca d'água.	O
6.7.3	Um SIGAD deve possuir uma arquitetura capaz de receber atualizações tecnológicas quanto à plataforma de geração e de detecção de marca d'água digital.	AD

6.8 Acompanhamento de Transferência

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

Referência	Requisito	Obrig
6.8.1	Um SIGAD deve ser capaz de manter, para cada documento ou cada dossiê/processo, o histórico das movimentações e transferências de mídia sofridas por aquele documento ou dossiê/processo.	AD
6.8.2	Um SIGAD tem que fornecer um recurso de acompanhamento para monitorar e registrar informações acerca do local atual e da transferência de dossiês/processos digitais e convencionais.	O
6.8.3	A função de acompanhamento de transferência tem que registrar metadados que incluam: ▪ número identificador dos documentos atribuído pelo sistema; ▪ localização atual e também as localizações anteriores, definidas pelo usuário; ▪ data e hora de envio/transferência; ▪ data e hora da recepção no novo local; ▪ destinatário; ▪ Usuário responsável pela transferência (sempre que adequado); ▪ Método de transferência.	O

6.9 Autoproteção

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

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

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

Referência	Requisito	Obrig
6.9.1	Um SIGAD deve fazer a verificação de vírus ou pragas antes da efetivação da captura.	AD

Referência	Requisito	Obrig
6.9.2	Um SIGAD deve ter dispositivos e procedimentos que reduzam as possibilidades de erros, falhas e descontinuidades no seu funcionamento que causem danos ou perdas aos documentos arquivísticos digitais.	AD
6.9.3	Após falha ou descontinuidade do sistema, quando a recuperação automática não for possível, um SIGAD tem que ser capaz de entrar em modo de manutenção, no qual a possibilidade de restaurar o sistema para um estado seguro é oferecida. *Na restauração ao estado seguro, um SIGAD deve ser capaz de garantir a recuperação de perdas ocorridas, incluindo os documentos de transações mais recentes.*	O
6.9.4	Um SIGAD deve garantir que os dados de segurança, quando replicados, sejam consistentes. *Permissões de controle de acesso, chaves criptográficas e parâmetros de algoritmos criptográficos são exemplos de dados de segurança.*	AD
6.9.5	Um SIGAD tem que garantir que as funções de controle de acesso são invocadas antes de qualquer operação de acesso e retornadas sem erros antes do prosseguimento normal da operação.	O
6.9.6	Um SIGAD tem que preservar um estado seguro de funcionamento, interrompendo completamente a interação com usuários comuns, quando quaisquer dos seguintes erros ocorrerem: ▪ 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
6.9.7	Quando não for possível escrever na trilha de auditoria, um SIGAD deve impedir toda operação de qualquer usuário e passar para o modo de manutenção.	AD
6.9.8	Um SIGAD deve detectar o reenvio de dados de autenticação e segurança de um usuário, sem conhecimento deste. O evento deve ser registrado nas trilhas, cancelando a comunicação com o sistema remoto/usuário e considerando o usuário fora do sistema.	AD
6.9.9	Um SIGAD pode atribuir a cada documento, no momento da captura, um código de manutenção de integridade baseado em criptografia robusta.	F

6.10 Alterar, Apagar e Truncar Documentos Arquivísticos Digitais

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

- Eliminação definitiva;

- Retenção, acompanhada de uma anotação nos metadados do documento arquivístico, informando que o mesmo 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 de disponibilizar documentos arquivísticos que contêm informações sigilosas (seja em conseqüência de legislação sobre proteção de dados, seja por questões de segurança, ou de segredo comercial, etc). Por esse motivo, aos administradores têm que ser dado o poder de retirar a informação sensível, sem afetar o documento arquivístico correspondente. Esse processo é chamado de truncamento, ou de corte, e o SIGAD armazena o documento original e a cópia truncada, chamada de "extrato".

Referência	Requisito	Obrig
6.10.1	Um SIGAD tem que permitir, a um administrador autorizado a anulação da 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
6.10.2	Um SIGAD, para evitar erros irrecuperáveis, deve inibir a eliminação (permanente ou lógica) de grupos ou lotes de documentos fora do processo regular de eliminação previsto na Tabela de Temporalidade e Destinação de documentos.	AD
6.10.3	Em casos excepcionais, o administrador tem que ser autorizado a apagar ou corrigir dossiês/processos, volumes e documentos. Nesses casos, 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 os mesmos forem eliminados; ▪ Garantir que nenhum documento seja eliminado, se tal ação resultar na alteração a outro documento arquivístico; ▪ Informar ao 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
6.10.4	No caso de erro na inserção de metadados, o administrador terá que corrigi-lo e o SIGAD terá que registrar essa ação na trilha de auditoria.	O
6.10.5	Um SIGAD tem que permitir a um usuário autorizado fazer um extrato (cópia truncada) de um documento, com o objetivo de truncá-lo sem alterar o original.	O

Referência	Requisito	Obrig
6.10.6	Um SIGAD deve dispor de funções de ocultação de informação sigilosa contida na cópia truncada do documento, permitindo o seguinte: ▪ 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 de áudio, caso existam. Se o SGAE não fornecer diretamente esses recursos, tem que permitir que outros pacotes de *software* os proporcionem. *É essencial que quando os recursos para truncar documento forem empregados, nenhuma informação retirada ou ocultada seja passível de visualização na cópia truncada, na tela, nem quando impressa ou reproduzida por meios audiovisuais, independentemente da utilização de quaisquer recursos, tais como rotação, variação focal ou qualquer outra manipulação.*	AD
6.10.7	Quando uma cópia truncada é produzida, um SIGAD tem que registrar essa ação nos metadados do documento, incluindo pelo menos a data, a hora, o motivo, e quem a produziu.	O
6.10.8	Um SIGAD pode solicitar a quem produziu a cópia truncada que a inclua em um dossiê/processo.	F
6.10.9	Um SIGAD deve registrar uma referência cruzada a uma cópia truncada nos mesmos dossiês/processos, pastas e documentos em que se encontra o documento original.	AD
6.10.10	Um SIGAD tem que armazenar na trilha de auditoria qualquer alteração efetuada para satisfazer os requisitos desta seção.	O

7 ARMAZENAMENTO

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

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

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

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

7.1 Durabilidade

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

Referência	Requisito	Obrig
7.1.1	Um SIGAD deve utilizar preferencialmente dispositivos e padrões de armazenamento maduros, estáveis no mercado e amplamente disponíveis. *Um SIGAD deve utilizar preferencialmente padrões abertos de armazenamento (como exemplo: ISO 9660:1999 – definição do formato de sistema de arquivos para CD-Rom.).* *A escolha dos dispositivos de armazenamento deve contemplar padrões estáveis de mercado e fornecedores consolidados.*	AD
7.1.2	A escolha de dispositivos têm que ser periodicamente revista sempre que a evolução tecnológica indicar mudanças importantes.	O
7.1.3	Atividades de migração têm que ser efetivadas preventivamente sempre que se torne patente ou previsível a obsolescência do padrão corrente.	O

Referência	Requisito	Obrig
7.1.4	Para as memórias secundárias, um SIGAD tem que manter registro de MTBF (*Mean Time Between Failure*)[45], bem como as datas de sua aquisição.	O
7.1.5	Para as memórias secundárias e terciárias, um SIGAD tem que fazer o gerenciamento das mídias por meio do registro de durabilidade prevista, data de aquisição e histórico de utilização. *Informações técnicas sobre previsibilidade de duração de mídias referidas em 7.1.3 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
7.1.6	Para as memórias secundárias e terciárias, um SIGAD deve manter estatísticas da durabilidade efetivamente observada.	AD
7.1.7	No caso de uso de fitas magnéticas, o mecanismo de *backup* provido pelo SIGAD deve proporcionar meios para que o item 8.2.6 possa ser implementado automaticamente, integrado à ação do *backup*.	AD
7.1.8	O acesso às informações armazenadas em memória terciária deve ser efetuado preferencialmente mediante uso de rede de dados. *O objetivo é minimizar acesso físico às mídias, visando diminuição do desgaste. A manipulação direta das mídias deverá ser restrita a administradores do sistema e não aos usuários comuns.*	AD
7.1.9	Quando se proceder à eliminação de documentos, as memórias de suporte têm que ser devidamente "sanitizadas", isto é, ter suas informações efetivamente indisponibilizadas. *Este requisito aplica-se principalmente às memórias secundária e terciária, pela sua característica não volátil. As informações devem ser eliminadas de forma irreversível, incluindo, no caso de memória terciária, a possibilidade de destruição física das mídias.*	O

7.2 Capacidade

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

Referência	Requisito	Obrig
7.2.1	Um SIGAD tem que possuir capacidade de armazenamento suficiente para acomodação de todos os documentos, suas cópias de segurança.	O

[45] MTBF – (*Mean Time Between Failure*). Tempo médio entre falhas. É um valor relativo ao período médio entre falhas de um sistema ou dispositivo e que permite a avaliação de sua confiabilidade ou vida útil.

Referência	Requisito	Obrig
	Para grandes volumes de dado, é conveniente o uso de dispositivos com maior capacidade unitária de armazenamento, a fim de reduzir a sobrecarga operacional.	
7.2.2	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 de 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
7.2.3	Um SIGAD deve permitir ao administrador configurar os limites de capacidade de armazenamento dos diversos dispositivos.	AD
7.2.4	Um SIGAD deve oferecer ao administrador facilidades para a monitoração da capacidade de armazenamento. *Esse controle indica, por exemplo, capacidade utilizada, capacidade disponível e taxa de ocupação. Tais informações são úteis para subsidiar ações de expansão em tempo hábil.*	AD
7.2.5	Um SIGAD deve informar automaticamente ao administrador quando os dispositivos de armazenamento *on-line* atingirem níveis críticos de ocupação.	AD
7.2.6	Um SIGAD deve manter estatísticas de taxa de crescimento de utilização de memória secundária e terciária para informar ao administrador previsões de exaustão de recursos. *Este tipo de estimativa possibilita ao administrador antecipar ações de expansão antes que a utilização atinja níveis críticos.*	AD

7.3 Efetividade de armazenamento

Referência	Requisito	Obrig
7.3.1	Os dispositivos de armazenamento de um SIGAD devem suportar métodos de detecção de erros para leitura e escrita de dados.	AD
7.3.2	Um SIGAD tem que utilizar técnicas de restauração de dados em caso de falhas.	O
7.3.3	Um SIGAD tem que utilizar mecanismos de proteção contra escrita, que previnam alterações indevidas e mantenham a integridade dos dados armazenados.	O

7.3.4	A infra-estrutura de um SIGAD deve prever 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
7.3.5	A integridade dos dispositivos de armazenamento tem que ser periodicamente verificada.	O

8 PRESERVAÇÃO

Exatamente como no caso dos documentos convencionais, a preservação de documentos arquivísticos digitais não é um fim em si mesmo. Antes, possui um propósito que deve ser considerado na definição e na implementação das estratégias de preservação. A razão para preservação de 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 de tempo previsto para sua guarda, conforme determinado na tabela de temporalidade e destinação de documentos. Ressalte-se que as características desses documentos demandam atenção específica, principalmente naqueles que serão mantidos por mais de cinco anos, o que, nesse contexto, já é considerado de longo prazo.

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

A degradação do suporte é causada por fatores como falta de controle de temperatura, umidade, luminosidade, agentes químicos e biológicos agressores, bem como manipulação inadequada ou 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 rejuvenescimento (*refreshing*).

No que diz respeito à obsolescência tecnológica, refere-se tanto a *hardware* quanto 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 (disco óptico, fita magnética, por exemplo), unidades de disco, unidades de fita magnética ou os próprios 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 somente 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 bastante freqüentes. O *software* podem ser simplesmente descontinuados, substituídos por outros equivalentes, supostamente melhores, ou ainda ter sua versão atualizada para correção de *bugs* ou acréscimo de novas funcionalidades. É importante notar que os fornecedores de *software* deixam de prestar suporte a versões mais antigas de seus produtos.

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

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

. preservação da tecnologia: evita a necessidade imediata de implementação de novos sistemas. Porém, as necessidades de manutenção e integração com outros

sistemas podem apresentar problemas ao longo do tempo. A preservação do *hardware*, em especial, é uma alternativa cara, mesmo nas situações em que o *hardware* é compartilhado entre mais de um usuário. Além disso, essa alternativa não é exeqüível a longo prazo, uma vez que o *hardware* pode ser danificado de forma irreversível, ficando completamente indisponível.

. emulação: é a simulação de um determinado *hardware* ou *software* através de *software*. Permite que um computador moderno, possivelmente mais barato e de fácil manutenção, possa executar programas (*software*) antigos desenvolvidos originalmente para outra plataforma. Para evitar possíveis perdas de informação e funcionalidades, deve ser realizada com bastante rigor. A probabilidade de ocorrência de perdas de informações e funcionalidades aumenta à medida que são utilizadas diversas camadas de emulação, como resultado da aplicação dessa técnica repetidas vezes.

. conversão de dados: é empregada quando os formatos se tornam obsoletos. Os dados em formatos antigos são convertidos para novos formatos, apoiados em *hardware* e *software* mais atuais. Esse processo não está isento de problemas, podendo resultar em perdas de informações e funcionalidades. A conversão de dados também pode ser utilizada para reduzir a quantidade de formatos utilizados e, conseqüentemente, de sistemas a serem mantidos e gerenciados, de modo a facilitar as ações de preservação.

. migração: a migração para novos sistemas é realizada no caso de obsolescência de *hardware*, *software* ou formatos. Envolve, inclusive, a conversão de dados. Pode abranger uma grande quantidade de elementos – *hardware*, *software* e formatos – e, dessa forma, apresentar uma maior complexidade para ser planejada e executada. Apesar disso, mostra-se como uma alternativa interessante para acompanhamento das mudanças decorrentes da evolução tecnológica. A migração, assim como a emulação e a conversão de dados, apresenta riscos quanto à integridade e à funcionalidade dos documentos arquivísticos digitais, por isso, deve ser realizada de modo criterioso e sistemático.

Embora os problemas de degradação dos suportes e obsolescência tecnológica possam ser contornados com conhecimento técnico e uso de técnicas de preservação, sua resolução pode ser muito dispendiosa. Por isso, as preocupações com preservação devem existir desde a concepção do SIGAD e a escolha de sua base tecnológica. De uma forma geral, recomenda-se o uso de suportes de alta qualidade e que tenham uma vida útil prevista adequada para os propósitos de preservação, o monitoramento contínuo dos avanços tecnológicos e da degradação do suporte, a adoção de formatos abertos e a busca por soluções independentes de *hardware*, *software* e fornecedor.

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

Nesta seção, não se pretende apresentar procedimentos de preservação preestabelecidos ou argumentar em favor de uma técnica específica. Os requisitos foram organizados em aspectos físicos, lógicos e gerais. Levando em conta esses aspectos, cada organização deve desenvolver e implementar sua própria estratégia de preservação de documentos arquivísticos digitais da forma mais adequada à sua realidade e de acordo com as diretrizes fornecidas pela instituição arquivística em sua devida esfera de competência.

8.1 Aspectos físicos

Referência	Requisito	Obrig
8.1.1	Os suportes de armazenamento de um SIGAD têm que ser acondicionados, manipulados e utilizados em condições ambientais compatíveis com sua vida útil prevista e/ou pretendida, dentro das especificações técnicas de seu 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	Um SIGAD deve permitir ao administrador especificar a vida útil prevista/pretendida dos suportes.	AD
8.1.3	Um SIGAD tem que permitir o controle da vida útil dos suportes para auxiliar no processo de rejuvenescimento.	O
8.1.4	Um SIGAD deve informar automaticamente quais são os suportes que se encontram próximos do fim de sua vida útil.	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 local diferente de onde se encontra a informação original.*	O
8.2.2	Um SIGAD tem que possuir funcionalidades para a verificação periódica dos dados armazenados, visando à detecção de possíveis erros. *Nesse caso, recomenda-se o uso de um checksum robusto, ou seja, que permita a constatação da integridade dos dados e seja seguro quanto a fraudes.*	O
8.2.3	Um SIGAD tem que permitir a substituição dos dados armazenados que apresentarem erros.	O
8.2.4	Um SIGAD pode permitir a correção dos erros detectados nos dados armazenados. *Nesse contexto, a correção de erros refere-se à restauração de dados corrompidos.*	F
8.2.5	Um SIGAD deve informar os resultados da verificação periódica dos dados armazenados, incluindo os erros detectados, bem como as substituições e as correções de dados realizadas.	AD
8.2.6	Um SIGAD deve manter um histórico dos resultados da verificação periódica dos dados armazenados.	AD
8.2.7	Ações de preservação têm que ser efetivadas sempre que se torne patente ou previsível a obsolescência da tecnologia utilizada pelo SIGAD.	O

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

9 FUNÇÕES ADMINISTRATIVAS

Referência	Requisito	Obrig
9.1.1	Um SIGAD tem que permitir que os administradores, de uma maneira controlada e sem esforço excessivo, recuperem, visualizem e reconfigurem os parâmetros do sistema e os atributos dos usuários.	O
9.1.2	Um SIGAD tem que fornecer relatórios flexíveis para o administrador gerenciar os documentos e seu uso, que apresentem 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; ▪ relatórios de atividades por usuário.	O
9.1.3	Um SIGAD tem que prover documentação cobrindo aspectos de administração do sistema. A documentação deve incluir todas as informações necessárias para o correto gerenciamento do sistema.	O

10 CONFORMIDADE COM A LEGISLAÇÃO E REGULAMENTAÇÕES

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

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

[46] Para obter informações sobre legislação arquivística brasileira, consulte Serviços ao Público, opção Legislação Arquivística, disponível em: <http://www.arquivonacional.gov.br.>

11 USABILIDADE

Projetar um sistema de *software* com boa usabilidade[47] significa concentrar esforços para produção de um sistema que proporcione facilidade do uso, através de suporte para realização de tarefas simples, diretas e objetivas, que apóiem 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 um 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. Usabilidade depende diretamente das tarefas específicas que os usuários realizam por meio do sistema, bem como do nível de conhecimento do sistema pelos usuários envolvidos.

As recomendações para uma boa usabilidade estão associadas ao contexto operacional do sistema, aos diferentes tipos de usuários, tarefas, ambientes físicos e organizacionais. Quando da elaboração da descrição das características de um SIGAD, deve-se levar em consideração: facilidade de utilização da interface, tipos de usuários, facilidade na execução de tarefas, uso de equipamentos adequados, ergonomia, ambiente e contexto de uso.

Referência	Requisito	Obrig
11.1.1	Um SIGAD deve possuir documentação completa, clara, inteligível e organizada para instalação e uso do *software*.	AD
11.1.2	Um SIGAD deve possuir sistema de ajuda *on-line*.	AD
11.1.3	O sistema de ajuda o*n-line* fornecido pelo SIGAD deve ser vinculado à função ou tarefa executada, em todo o sistema. *Exemplo:* *Quando se está executando uma operação de edição, uma vez acionada a ajuda, ela deve remeter para o tópico de ajuda da edição.*	AD
11.1.4	Um SIGAD deve permitir a personalização de conteúdo de ajuda *on-line* por adição de texto ou edição do texto existente. *Exemplo: O responsável pela administração do conteúdo da ajuda pode adicionar esclarecimentos ou alterar o conteúdo das descrições, de modo a facilitar o entendimento das funções.*	AD
11.1.5	Toda mensagem de erro produzida pelo SIGAD deve ser clara e significativa, de modo a permitir que o usuário possa recuperar-se do erro ou cancelar a operação.	AD

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

Referência	Requisito	Obrig
11.1.6	A interface de um SIGAD deve seguir 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 alguma legislação específica do estado/município/órgão federal), bem como a utilização 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 instituições arquivísticas interessadas em criar ou redefinir seus sítios.*	AD
11.1.7	O SIGAD deve empregar um conjunto simples e consistente de regras de interface, privilegiando a facilidade de aprendizado de operação pelos seus usuários. *O uso de um conjunto de regras consistentes com o ambiente operacional em que o SIGAD será executado permite que ele apresente menus, comandos e outras facilidades consistentes em toda aplicação.* *Essas regras de interface, quando compatíveis com outras aplicações principais já instaladas, levam à padronização da terminologia utilizada para funções, rótulos e ações consistente em toda a aplicação.*	AD
11.1.8	A interface de visualização dos documentos arquivísticos deve fornecer o recurso de arrastar e soltar, se apropriado no ambiente operacional do SIGAD.	AD
11.1.9	O SIGAD deve permitir que a sua estrutura de classes e dossiês/processos possa ser visualizada em diferentes formas de apresentação.	AD
11.1.10	Deve ser possível personalizar a interface gráfica com o usuário de um SIGAD. A personalização deve incluir pelo menos as seguintes possibilidades: ▪ conteúdos de menus; ▪ formatos de telas; ▪ utilização de teclas de função; ▪ alteração de cores, fontes e tamanhos de fontes em telas e janelas; ▪ avisos sonoros.	AD
11.1.11	Sempre que um SIGAD utilizar janelas *pop-up* e barras de ferramentas, deve-se permitir ao usuário a possibilidade de configuração e de habilitar/desabilitar esse tipo de recurso. *Porém, de forma a não infringir a recomendação de uso de um conjunto simples e consistente de regras de interface.*	AD
11.1.12	Sempre que um SIGAD permitir o uso de janelas, ele deve permitir sua movimentação, redimensionamento e gravação das modificações da aparência, de forma a permitir a personalização por perfil de usuário.	AD

Referência	Requisito	Obrig
11.1.13	Um SIGAD deve permitir a seleção de avisos sonoros e a personalização de tom e volume, bem como a gravação dessas escolhas no perfil do usuário.	AD
11.1.14	Um SIGAD deve permitir a gravação de opções *default* para entrada de dados de configuração: ▪ valores de variáveis definidas pelo usuário; ▪ valores iguais aos de um item anterior; ▪ valores que possam ser selecionados de 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
11.1.15	A interface de um SIGAD com usuário deve ser apropriada para adaptações e personalizações que permitam a sua utilização por usuários com necessidades especiais. Essas adaptações e personalizações devem ser compatíveis com *software* especializado que possa vir a ser acoplado (por exemplo, leitores de telas 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[48].* *É desejável que o padrão seguido possa ser verificado através da aplicação de uma validação manual ou automática, de preferência visando à obtenção de certificação de acessibilidade.*	AD
11.1.16	Um SIGAD deve permitir a realização de transações ou tarefas mais freqüentemente executadas com um pequeno número de iterações (por exemplo, cliques de mouse) e sem mudanças excessivas de contexto.	AD
11.1.17	Um SIGAD deve estar fortemente integrado com o 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
11.1.18	No caso de integração do SIGAD com o sistema de correio eletrônico, deve ser possível fazer referências a documentos arquivísticos sem necessidade de envio de cópias adicionais.	AD

[48] *Exemplos:* **e-MAG** - Modelo de Acessibilidade de Governo Eletrônico, disponível em: < http://www.governoeletronico.gov.br/governoeletronico/index.wsp>; **Decreto nº 5.296**, de 02 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>; **Guia de Validação – SERPRO,** disponível em: **<**http://www.serpro.gov.br/acessibilidade/g_validacao.php>; **W3C - HTML Validation Service,** disponível em: **<**http://validator.w3c.org>.

Referência	Requisito	Obrig
11.1.19	Um SIGAD deve possuir integração com o sistema padrão de edição de documentos, de modo que possa fazer uso da facilidade de gravação.	AD
11.1.20	Um SIGAD pode fornecer recursos que possibilitem o reconhecimento óptico de caracteres (como por exemplo, *Optical Character Recognition – OCR e Intelligent Character Recognition - ICR*) quando for necessária a introdução de metadados a partir de imagens de documentos impressos, ou etiquetas identificadoras de documentos.	F
11.1.21	Um SIGAD deve permitir a definição e utilização de referências cruzadas entre documentos arquivísticos digitais correlacionados, permitindo uma fácil navegação entre eles, inclusive com uso de *hyperlinks*.	AD
11.1.22	Um SIGAD deve disponibilizar pelo menos dois papéis de acesso diferenciados, um para usuário final e outro para administrador de sistema.	AD
11.1.23	Um SIGAD deve fornecer para os usuários finais e administradores funções intuitivas e fáceis de usar, que requeiram poucas ações para completar uma tarefa padrão. Particularmente em operação normal, um SIGAD deve ser capaz de: ▪ capturar e declarar um documento arquivístico com, no máximo, três cliques de mouse ou acionamentos de teclas; ▪ 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 teclas. ▪ apresentar os metadados de um documento arquivístico com no máximo, três cliques de mouse ou acionamentos de teclas.	AD
11.1.24	Um SIGAD deve restringir o acesso às funcionalidades administrativas impossibilitando sua visualização ao 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 restrito pela configuração de menus que não as apresentam ao usuário sem permissão para executá-las.*	O
11.1.25	Um SIGAD deve levar em consideração as condições de operação como ruído, luminosidade, necessidade de rapidez na conclusão da tarefa, necessidades específicas para dispositivos móveis, ambiente *desktop/Web* e necessidades de instalação automática, para configurar as formas de interação com o usuário. *Exemplo:* *Não se deve utilizar menus audíveis em ambientes que apresentam alto volume de ruídos na proximidade dos terminais de usuários.*	AD

12 INTEROPERABILIDADE

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

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

Por interoperabilidade, entende-se:"Intercâmbio coerente de informações e serviços entre sistemas. A interoperabilidade deve possibilitar a substituição de qualquer componente ou produto usado nos pontos de interligação por outro de especificação similar, sem comprometimento das funcionalidades do sistema"[49]. Isto se faz através do uso de regras e padrões de comunicação.

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

Referência	Requisito	Obrig
12.1.1	Um SIGAD deve ser capaz de interoperar com outros SIGADs, 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
12.1.2	Um SIGAD deve ser capaz de interoperar com outros sistemas através de padrões abertos de interoperabilidade. *Por exemplo, padrões abertos como os estabelecidos pela e-PING, XML e Dublin Core.*	AD
12.1.3	Um SIGAD tem que aplicar os requisitos de segurança descritos neste documento para executar operações de interoperabilidade. *Isso é fundamental para que as operações, feitas em ambiente com interoperabilidade, não afetem a integridade dos documentos e impossibilitem acessos não autorizados.*	O

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

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

13 DISPONIBILIDADE

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

Os requisitos de disponibilidade devem ser especificados pelo administrador do SIGAD de acordo o nível de serviço a ser fornecido. Por exemplo, os períodos previstos de atendimento ("8x5" indica 8 horas por dia útil. "24x7" indica atendimento contínuo), bem como 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
13.1.1	Um SIGAD tem que se adequar ao grau de disponibilidade estabelecido pela organização.	O

14 DESEMPENHO E ESCALABILIDADE

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

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

Esses acréscimos de *hardware* podem se dar acrescentando-se mais *hosts* (escalabilidade horizontal) ou mais memória RAM e poder de processamento aos *hosts* existentes (escalabilidade vertical).

Referência	Requisito	Obrig
14.1.1	Um SIGAD deve manter estatísticas dos tempos de atendimento, discriminados por tipo de operação.	AD
14.1.2	Um SIGAD deve ser expansível até comportar um número máximo preestabelecido de usuários simultâneos, provendo continuidade efetiva de serviços.	AD
14.1.3	Um SIGAD deve 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 a mudanças planejadas da organização, sem causar grandes sobrecargas de administração.*	O
14.1.4	Um SIGAD deve ser escalável, a fim de permitir adaptação a organizações de diferentes tamanhos e complexidades.	AD
14.1.5	Um SIGAD deve fornecer evidências do grau de escalabilidade ao longo do tempo. Avaliações quantitativas devem incluir: ▪ O número máximo de *sites* remotos suportados com desempenho adequado. ▪ O tamanho máximo do repositório, expresso em Gigabytes ou Terabytes, que pode ser suportado com desempenho adequado. ▪ O número máximo de usuários simultâneos que possam ser atendidos com desempenho adequado. ▪ A sobrecarga administrativa prevista para um período de cinco anos, permitindo crescimento do número de usuários e da quantidade de registros. ▪ A quantidade de reconfigurações e de indisponibilidades previstas para um período de cinco anos, permitindo o crescimento do número de usuários e da quantidade de registros.	AD

Referência	Requisito	Obrig
	▪ A quantidade de reconfigurações e de indisponibilidades previstas para um período de cinco anos, permitindo mudanças substanciais na estrutura da organização, mudanças nos esquemas de classificação e mudanças na administração de usuários.	

Metadados

Em estudo.

Será incluído na próxima versão.

Anexo 1 - Glossário

AC

Ver: Autoridade Certificadora

Acervo

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

Acessibilidade

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

Ver também: Acesso

Acesso

Direito, oportunidade ou meios de encontrar, recuperar e usar a informação.

Ver também: Acessibilidade; classificação (2); credencial de segurança.

Anotação

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

AR

Ver: Autoridade de registro

Armazenamento

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

Arquivamento

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

Arquivo

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

Ver também: Arquivo digital.

Arquivo digital

Conjunto de bits que formam uma unidade lógica interpretável por computador e armazenada em suporte apropriado.

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 seja o mesmo signatário; 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: Certificado digital; criptografia; Assinatura eletrônica

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

Autenticação

Atestação de que um documento é verdadeiro ou que uma cópia reproduz fielmente o original, de acordo com as normas legais de validação.

Ver também: Autenticidade; certificado de autenticidade

Autenticidade

Qualidade de um documento ser o que diz ser, independente de se tratar de minuta, original ou cópia, e que é livre de adulterações ou qualquer outro tipo de corrupção.

Ver também: Autenticação; certificado de autenticidade

Autoridade Certificadora (AC)

Organização que emite certificados digitais obedecendo às práticas definidas na Infra-estrutura de Chaves-Públicas - ICP.

Ver também: Certificado digital; chave privada; chave pública; ICP

Autoridade de Registro (AR)

Organização que distribui certificados digitais aos usuários finais mediante processo de identificação estabelecido nas práticas definidas na Infra-estrutura de Chaves-Públicas - ICP.

Ver também: Certificado digital; chave privada; chave pública; ICP

Avaliação

Processo de análise de documentos, que estabelece os prazos de guarda e a destinação, de acordo com os valores que lhes são atribuídos.

Banco de dados

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

Ver também: Base de dados

Base de dados

Conjunto de dados de mesma natureza, tais como catálogo de registros bibliográficos, dados sobre funcionários de uma empresa, que podem ser gerenciados por um software SGBD – Sistema Gerenciador de Banco de Dados.

Ver também: Banco de dados

Blog

Sítio na internet onde são publicados conteúdos pessoais, como notícias, pensamentos, comentários e filosofias, atualizados periodicamente. Normalmente refletem o ponto de vista de seu criador e permitem aos leitores inserirem comentários. Forma reduzida do termo *weblog*.

Captura

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

Ver também: Arquivamento; classificação; registro

Categoria de sigilo

Ver: Grau de sigilo

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

Documento emitido e assinado digitalmente por uma autoridade certificadora, que contém dados que identificam seu titular e o relaciona à sua respectiva chave-pública.

Ver também: Assinatura digital; chave privada; chave pública

Chat

Espaço virtual de comunicação que permite que duas ou mais pessoas dialoguem entre si *online* mediante troca de mensagens enviadas e recebidas com o auxílio de computadores interligados em redes locais ou remotas. O texto de uma sessão de chat pode ser armazenado para consulta posterior.

Chave privada

Chave matemática formada por uma seqüência 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 descriptografar aqueles criptografados com a chave pública correspondente.

Ver também: Assinatura digital; certificado digital; chave pública

Chave pública

Chave matemática formada por uma seqüência de dígitos, usada para criptografia assimétrica e criada em conjunto com a chave privada correspondente, disponibilizada publicamente por certificado digital, e utilizada para verificar assinaturas digitais. Também pode ser usada para criptografar mensagens ou arquivos a serem descriptografados com a chave privada correspondente.

Ver também: Assinatura digital; certificado digital; chave privada

Ciclo vital dos documentos

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

Classificação

1. Análise e identificação do conteúdo de documentos, seleção do descritor sob o qual o documento será recuperado, podendo-se-lhe atribuir um código. 2. Atribuição a documentos, ou às informações neles contidas, de graus de sigilo, conforme legislação específica. Também chamada "classificação de segurança".

Ver também: Código de classificação; grau de sigilo; plano de classificação

Código de classificação

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

Ver também: Classificação; plano de classificação

Confiabilidade

Capacidade de o documento sustentar os fatos a que se refere. Para tanto há que ser dotado de completeza, ser criado pela autoridade competente e ter seus procedimentos de criação bem controlados.

Ver também: Completeza

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 conseqüências. (I) *Completeness.*

Ver também: Elemento intrínseco; elemento extrínseco; confiabilidade

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 documental; contexto jurídico-administrativo; contexto de procedimentos; contexto de proveniência; contexto tecnológico

Contexto documental

Refere-se a código de classificação, guias, índices e outros instrumentos que situam o documento dentro do conjunto a que pertence, ou seja, ao fundo.

Ver também: Contexto; contexto jurídico-administrativo; contexto de procedimentos; contexto de proveniência; contexto tecnológico

Contexto jurídico-administrativo

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

Ver também: Contexto documental; contexto de procedimentos; contexto de proveniência; contexto tecnológico.

Contexto de procedimentos

Refere-se a normas internas que regulam a criação, tramitação, uso e arquivamento dos documentos da instituição.

Ver também: Contexto documental; contexto jurídico-administrativo; contexto de proveniência; contexto tecnológico

Contexto de proveniência

Refere-se a organogramas, regimentos e regulamentos internos que identificam a instituição produtora de documentos.

Ver também: Contexto documental; contexto jurídico-administrativo; contexto de procedimentos; contexto tecnológico

Contexto tecnológico

Refere-se ao ambiente tecnológico (*hardware, software* e padrões) que envolve o documento.

Ver também: Contexto documental; contexto jurídico-administrativo; contexto de

procedimentos; contexto de proveniência

Controle de versão

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

Ver também: Identificador único

Conversão

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

Ver também: Migração; rejuvenescimento; reformatação

Cópia

Resultado da reprodução de um documento.

Ver também: Reprodução

Correio eletrônico

Sistema usado para criar, transmitir e receber mensagens e outros documentos digitais por meio de redes de computadores.

Ver também: Mensagem eletrônica

Credencial de segurança

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

Criptografia

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

Ver também: Assinatura digital; chave privada; chave pública; criptografia assimétrica; criptografia simétrica; ICP

Criptografia assimétrica

Método de criptografia que utiliza um par de chaves diferentes entre si, que se relacionam matematicamente por meio de um algoritmo, de forma que o texto cifrado por uma chave, apenas seja decifrado pela outra do mesmo par. As duas chaves envolvidas na criptografia assimétrica são denominadas chave pública e chave privada. (ITI)

Ver também: Chave privada; chave pública; criptografia simétrica

Criptografia de chave pública

Ver: Criptografia assimétrica

Criptografia simétrica

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

Ver também: Criptografia assimétrica

Custódia

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

Dado

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

Ver também: Metadados

Destinação

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

Ver também: Eliminação; recolhimento

***Digital Object Identifier* (DOI)**

Ver: DOI

Digitalização

Processo de conversão de um documento em qualquer suporte ou formato para o formato digital, por meio de dispositivo apropriado.

Documento

Informação registrada, qualquer que seja o formato ou suporte.

Ver também: Documento digital; documento eletrônico; suporte

Documento arquivístico

Documento produzido e/ou recebido por uma pessoa física ou jurídica, no decorrer das suas atividades, qualquer que seja o suporte, e dotado de organicidade. (I) *Record*

Ver também: Organicidade

Documento arquivístico digital

Documento arquivístico codificado em dígitos binários, produzido, tramitado e armazenado por sistema computacional. São exemplos de documentos arquivísticos digitais: textos, imagens fixas, imagens em movimento, gravações sonoras, mensagens de correio eletrônico, páginas web, bases de dados, dentre outras possibilidades de um vasto repertório de diversidade crescente.

Ver também: Autenticidade; completeza; elemento extrínseco; elemento

intrínseco; confiabilidade; organicidade.

Documento digital

Informação registrada, codificada em dígitos binários, acessível por meio de sistema computacional.

Documento eletrônico

Informação registrada, codificada em forma analógica ou em dígitos binários, acessível por meio de um equipamento eletrônico.

DOI

Sistema para identificação persistente de objetos digitais em redes, bem como para o intercâmbio de informações sobre propriedade intelectual desses objetos. Marca registrada da DOI Foundation (http://www.doi.org). Abreviatura de Digital Object Identifier.

Dossiê

Conjunto de documentos relacionados entre si por ação, evento, pessoa, lugar, projeto, que constitui uma unidade.

Ver também: Dossiê híbrido; processo

Dossiê híbrido

Dossiê constituído por documentos digitais e não digitais. Por exemplo: projetos arquitetônicos que apresentam a descrição em papel e as plantas em disco óptico.

Ver também: Processo híbrido

E-mail

Ver: Correio eletrônico

Elemento extrínseco

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

Ver também: Documento arquivístico; elemento intrínseco

Elemento intrínseco

Atributo que caracteriza a forma interna do documento arquivístico. Exemplo: autor, destinário, data, local, assinatura, assunto e outros.

Ver também: Documento arquivístico; elemento extrínseco

Eliminação

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

Emulação

Utilização de recursos computacionais que fazem uma tecnologia funcionar com as características de outra, aceitando as mesmas entradas e produzindo as mesmas saídas.

Exportação

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

Ver também: Conversão

Forma documental

Regras de representação que permitem que o conteúdo de um documento arquivístico seja comunicado. A forma documental se constitui de elementos extrínsecos e intrínsecos. (I) *documentary form*

Ver também: Elemento extrínseco*;* elemento intrínseco

Formato de arquivo

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

Formato de caractere

Especificação padronizada de como traduzir uma seqüência de bits em caracteres (letras, números, sinais gráficos e de pontuação), por exemplo: ASCII, Unicode e EBCDIC.

Gestão arquivística de documentos

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

Ver também: Sistema de gestão arquivística de documentos; sistema informatizado de gestão arquivística de documentos

Grau de sigilo

Gradação de sigilo atribuída a um documento ou parte dele em razão da natureza de seu conteúdo e com o objetivo de limitar sua divulgação a quem tenha necessidade de conhecer.

Hardware

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

Hipertexto

Forma de estruturação de documentos que permite a leitura por meio de enlaces *(hiperlinks)* que possibilitam a conexão direta entre os diversos itens de um documento e/ou deste para outros. (I) *Hipertext*.

Hipermídia

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

ICP

Ver: Infra-estrutura de Chaves Públicas

Identificador único

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

Ver também: Controle de versão; registro

Informação

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

Infra-estrutura de Chaves Públicas (ICP)

É um 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 composta pela Autoridade Certificadora Raiz - AC Raiz, pelas demais Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR.

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

Integridade

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

Item documental

A menor unidade arquivística intelectualmente indivisível.

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 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*

Mensagem eletrônica

Documento digital criado ou recebido via um sistema de correio eletrônico, incluindo anexos que possam ser transmitidos com a mensagem.

Metadados

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

Mídia

Ver: Suporte

Migração

Conjunto de procedimentos e técnicas para assegurar a capacidade dos objetos digitais serem acessados face 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. A migração pode ocorrer por **conversão**, por **rejuvenescimento** ou por **reformatação**.

Ver também: Acessibilidade; conversão; objeto digital; reformatação; rejuvenescimento

Minuta

Versão preliminar de documento sujeita à aprovação.

Objeto digital

Arquivo digital que, além de seu conteúdo, possui identificador único e metadados associados. É composto de: 1. objeto físico – é o objeto digital enquanto fenômeno físico que registra as codificações lógicas dos bits nos suportes. Por exemplo, no suporte magnético o objeto físico é a seqüência do estado de polaridades (negativa e positiva); nos suportes ópticos é a seqüência de estados de translucidez (transparência e opacidade); 2. objeto lógico – é o objeto digital enquanto conjunto de seqüências de bits, que constitui a base dos objetos conceituais; 3. objeto conceitual - é o objeto digital que se apresenta de maneira compreensível para o usuário, por exemplo, o documento visualizado na tela do computador.

Ver também: Arquivo digital

OCR

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

***Optical Character Recognition* (OCR)**

Ver: OCR

Organicidade

Atributo essencial para se considerar que um determinado conjunto de documentos é um arquivo. A organicidade de um arquivo expressa as relações que os documentos guardam entre si ao refletirem, na sua totalidade, as funções e atividades da pessoa ou organização que os produziu. (I) *Archival bond*; (F) *organicité*; (E) *organicidad*.

Ver também: Documento arquivístico

Original

Primeiro documento completo e efetivo.

Patrimônio digital

Conjunto de objetos digitais que possuem valor suficiente para serem conservados a fim de que possam ser consultados e utilizados no futuro.

Ver também: Objeto digital

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.

Ver também: Classificação; código de classificação

Preservação digital

Ações destinadas a manter a integridade e a acessibilidade dos objetos digitais ao longo do tempo. Devem alcançar todas as características essenciais do objeto digital: físicas, lógicas e conceituais.

Ver também: Migração; rejuvenescimento

Processo

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

Ver também: Dossiê; processo hibrido

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: dossiê híbrido

Programa de computador

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

***RDF Site Summary* (RSS)**

Ver: RSS

Recolhimento

Entrada de documentos em arquivos permanentes.

Recuperação da informação

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

Reformatação

1. técnica de migração que consiste na mudança da forma de apresentação de um documento para fins de acesso ou manutenção dos dados, por exemplo: impressão ou transformação de documentos digitais em microfilme (tecnologia COM) ou transferência dos documentos de um sistema computacional para uma mídia móvel (tecnologia COLD). 2. Apagar todos os dados de uma unidade de armazenamento. (I) *Reformatting*

Ver também: Conversão; migração; rejuvenescimento

Registro

É o 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: Identificador único

Rejuvenescimento

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

Ver também: Conversão; migração; reformatação

Reprodução

Processo de geração de uma cópia. (I) *Reproduction*.

Ver também: Cópia

Rich Site Summary (RSS)

Ver: RSS

RSS

Acrônimo para Really Simple Syndication, Rich Site Summary ou ainda RDF Site Summary. Formato baseado em XML que permite a distribuição de listas de hiperlinks com notícias ou outros tipos de informação.

Sistema de informação

Conjunto organizado de políticas, procedimentos, pessoas, equipamentos e programas computacionais que produzem, processam, armazenam e proveêm acesso à informação. (I) *Information systems*.

Sistema informatizado de gestão arquivística de documentos

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

Ver também: Gestão arquivística de documentos; captura

Sistema de gestão arquivística de documentos

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

Ver também: Gestão arquivística de documentos; Sistema informatizado de gestão arquivística de documentos

Sistema operacional

Programa de computador que controla a execução de aplicativos e outros programas, alocação de recursos e demais operações de um sistema computacional. (I) *operating system*; (F) *système d'exploitation*; (E) *sistema operativo*; (P) sistema operativo.

Software

Ver: Programa de computador

Suporte

Base física sobre a qual a informação é registrada. (I) *Medium, storage medium*.

Ver também: Documento

Tramitação

Curso do documento desde a sua produção ou recepção até o cumprimento de sua função administrativa. Também referido como trâmite ou movimentação.

Transferência

Passagem de documentos do arquivo corrente para o arquivo intermediário.

Trilha de auditoria

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

Valor primário

Valor atribuído aos documentos em função do interesse que possam ter para a entidade produtora, levando-se em conta a sua utilidade para fins administrativos, legais e fiscais.

Valor secundário

Valor atribuído aos documentos em função do interesse que possam ter para a entidade produtora e outros usuários, tendo em vista a sua utilidade para fins diferentes daqueles para os quais foram originalmente produzidos.

Versão

Uma ou mais variantes de um mesmo documento. (I) *Version.*

Ver também: Minuta; controle de versão

Referências

ARQUIVO NACIONAL (Brasil). Conselho Nacional de Arquivos. **Classificação, temporalidade e destinação de documentos de arquivo relativos às atividades-meio da administração pública**. Rio de Janeiro: Arquivo Nacional, 2001. 156p.

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

AUSTRALIAN STANDARD **Records management**. Part 1: general. AS ISO 15489.1 - 2002.

AUSTRALIAN STANDARD **Records management**. Part 2: guidelines. AS ISO 15489.2 – 2002.

BRASIL. Ministério da Defesa. Marinha do Brasil. **Normas sobre documentação administrativa e arquivamento na Marinha – NODAM**. Brasília: Secretaria-Geral da Marinha, 2000.

CONSELHO INTERNACIONAL DE ARQUIVOS. Comitê de arquivos correntes em ambiente electrônico. **Documentos de arquivo electrônicos**: manual para arquivistas. ICA, Estudo nº 16. 2005. Disponível em: <http://www.ica.org/biblio.php?pdocid=285> Acesso em: 08 ago 2006.

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

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

DURANTI, Luciana, The InterPARES Project. In: **Authentic Records in the Electronic Age**. Vancouver: University of British Columbia, 2000.

DURANTI, Luciana. **The long-term preservation of the authentic electronic records:** findings of the InterPARES project. [S. l.]: L. Duranti Ed., 2005.

DURANTI, Luciana; 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. 118p. (Studies 10).

INDOLFO, Ana Celeste, CASCARDO, Ana Maria, OLIVEIRA, Maria Izabel, COSTA, Mônica Medrado e CAUVILLE, Verone Gonçalves. **Gestão de Documentos: conceitos e procedimentos básicos**. Rio de Janeiro: Arquivo Nacional, 1993. 49 p. (Série Publicações Técnicas nº 47).

INDOLFO, Ana Celeste. **Curso de gestão de documentos**. Rio de Janeiro, 2004.

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

INTERNATIONAL COUNCIL ON ARCHIVES. Committee on Electronic Records. **Guide for managing electronic records from an archival perspective**. Paris: International Council on Archives. 1997. 55p. (Studies 8).

The International Research on Permanent Authentic Records in Electronic Systems (InterPARES). **Interpares 2 Project**. Disponível em: <http://www.interpares.org/>. Acesso em: 4 ago 2006.

NATIONAL ARCHIVES & RECORDS ADMINISTRATION (US). **Disposition of federal records: a records management handbook**. Washington: National Archives & Records Administration, 2000 (web edition of 1997 printed publication). Disponível em: <http://www.archives.gov/records_management/publications/disposition_of_federal_records>. Acesso em: 7 jan 2004.

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (United States). **Electronic Records Management Initiative**. Disponível em: <http://www.archives.gov/records-mgmt/initiatives/erm-overview.html>. Acesso em: 08 ago 2006.

PUBLIC RECORD OFFICE (United Kingdom). **Management, appraisal and preservation of electronic records guidelines**. Disponível em: <http://www.nationalarchives.gov.uk/electronicrecords/advice/guidelines.htm>. Acesso em: 08 ago 2006.

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

ROUSSEAU, Jean-Yves e COUTURE, Carol: **Os Fundamentos da Disciplina Arquivística**. Lisboa, Publicações D. Quixote, 1994.

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

THE NATIONAL ARCHIVES OF ENGLAND, WALES AND THE UNITED KINGDOM. **Requirements for electronic records management systems: 1: Functional requirements -** 2002 revision: final revision. Kew:The Archives, 2002.

UNESCO. División de la Sociedad de la Información. **Directrices para la preservación del patrimonio digital**. Preparado por la Biblioteca Nacional de Australia. Canberra: Biblioteca Nacional de Austrália, 2002. 176p. Disponível em: http://unesdoc.unesco.org/ulis/cgi-bin/ulis.pl?database=ged&req=2&by=3&sc1=1&look=new&sc2=1&text_p=inc&text=Directrices+para+la+preservaci%F3n+del+patrimonio+digital&submit=GO>. Acesso em: 08 ago 2006.

UNESCO. División de la Sociedad de la Información. **Directrices para la preservación del patrimonio digital**. Preparado por la Biblioteca Nacional de Australia. Canberra: Biblioteca Nacional de Austrália, 2002. 176p. Disponível em: http://unesdoc.unesco.org/ulis/cgi-bin/ulis.pl?database=ged&req=2&by=3&sc1=1&look=new&sc2=1&text_p=inc&text=Directrices+para+la+preservaci%F3n+del+patrimonio+digital&submit=GO>. Acesso em: 08 ago 2006.

UNITED STATES. Department of Defense. **Design criteria standard for electronic records management *software* applications:** DOD 5015.2-STD. Washington: The Department, 2002. 57 p.