

**UNIVERSIDADE FEDERAL DE SANTA MARIA  
CENTRO DE TECNOLOGIA  
PROGRAMA DE PÓS-GRADUAÇÃO EM  
ENGENHARIA DE PRODUÇÃO**

**METADADOS PARA PRESERVAÇÃO E  
SEGURANÇA DO DIÁRIO DE CLASSE  
ELETRÔNICO DA UFSM**

**DISSERTAÇÃO DE MESTRADO**

**Dulce Elaine Saul da Luz**

**Santa Maria, RS, Brasil**

**2011**



# **METADADOS PARA PRESERVAÇÃO E SEGURANÇA DO DIÁRIO DE CLASSE ELETRÔNICO DA UFSM**

**Dulce Elaine Saul da Luz**

Dissertação apresentada ao Curso de Mestrado do Programa de Pós-Graduação em Engenharia de Produção, Área de Concentração em Qualidade e Produtividade, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do grau de **Mestre em Engenharia de Produção**

**Orientador: Prof. Raul Ceretta Nunes**

**Santa Maria, RS, Brasil**

**2011**

L979m Luz, Dulce Elaine Saul da  
Metadados para preservação e segurança do diário de classe eletrônico da  
UFSM / por Dulce Elaine Saul da Luz. – 2011.  
138 p. ; il. ; 30 cm

Orientador: Raul Ceretta Nunes  
Dissertação (mestrado) – Universidade Federal de Santa Maria, Centro de  
Tecnologia, Programa de Pós-Graduação em Engenharia de Produção, RS, 2011

1. Metadados 2. Preservação 3. Segurança da informação 4. Diário de classe  
I. Nunes, Raul Ceretta II. Título.

CDU 651.5

Ficha catalográfica elaborada por Cláudia Terezinha Branco Gallotti – CRB 10/1109  
Biblioteca Central UFSM

---

© 2011

Todos os direitos autorais reservados a Dulce Elaine Saul da Luz. A reprodução de partes ou do todo deste trabalho só poderá ser feita com autorização por escrito do autor.

Endereço: Rua Norizonte Figueiró da Rosa, n.46, Bairro Tomazetti, Santa Maria, RS.  
CEP: 97065-175.

Fone (055) 3211 2223; E-mail: dulcesdaluz@hotmail.com

---

**Universidade Federal de Santa Maria  
Centro de Tecnologia  
Programa de Pós-Graduação em Engenharia de Produção**

A Comissão Examinadora, abaixo assinada,  
aprova a Dissertação de Mestrado

**METADADOS PARA PRESERVAÇÃO E SEGURANÇA DO DIÁRIO  
DE CLASSE ELETRÔNICO DA UFSM**

elaborada por  
**Dulce Elaine Saul da Luz**

como requisito parcial para obtenção do grau de  
**Mestre em Engenharia de Produção**

**COMISSÃO EXAMINADORA:**

**Raul Ceretta Nunes, Dr.**  
(Presidente/Orientador)

**Felipe Martins Müller, Dr (UFSM)**

**Sergio João Limberger, Dr (UFSM)**

Santa Maria, 30 de setembro de 2011.



## DEDICATÓRIA

Dedico esta dissertação, aos meus pais, Guilherme e Erna (*In memoriam*).

Ao meu esposo Isidoro, aos meus filhos Daiani, Danísio e Daniéli

e aos demais familiares com todo meu amor e carinho.





## AGRADECIMENTOS

**A Deus**, por sua companhia perene ao meu lado, pela fé, força e coragem de vencer mais esta etapa da vida, iluminando meu caminho permanentemente.

**Agradecer** é uma atitude e um sentimento que reiteradas vezes envolveram meu ser durante esta caminhada de formação acadêmica. Nas atitudes diárias nem sempre consegui expressar meus agradecimentos a determinadas pessoas no momento certo. Porém, em sentimentos posso afirmar que inúmeras vezes meu coração palpitou em gratidão a muitas pessoas que passaram por mim nesta trajetória. Para essas pessoas, dedico meus sinceros agradecimentos.

Ao meu orientador, professor Raul Ceretta Nunes, agradeço pelo apoio, incentivo, paciência e valiosas sugestões na orientação do estudo, sempre com muita atenção e dedicação, e pela confiança depositada em mim. Também pelos momentos de lazer e confraternização em sua residência, juntamente com sua família e os colegas do grupo de pesquisa.

Aos meus pais (*In memoriam*), o esteio de minha vida, pela maravilhosa criação e estrutura familiar que serviram de base para desenvolver o meu caráter e minha personalidade e, enfim, pelo que sou. Quando ensinaram aos filhos que a verdadeira riqueza não é bens materiais que podem ser perdidos, mas, sim, a riqueza do espírito divino (fé) que é indestrutível e eterna.

À minha família, pelo incentivo nesta investida e nas outras conquistas alcançadas, pelo apoio incondicional. Especialmente ao meu esposo, pelo amor dedicado, compreensão e ajuda no lar e aos meus filhos, pela convivência, carinho, dedicação, presença e amor constante em toda a minha vida acadêmica. Amo vocês!

Aos professores membros da comissão examinadora, pelo aceite do convite e pelas suas contribuições para o aprimoramento do trabalho. À professora Núbia que

sempre torceu pelas minhas conquistas e pela ajuda na tradução do resumo. Aos demais docentes pelo compromisso com a excelência acadêmica e pelas sábias palavras em diversos momentos. Aos colegas servidores técnicos, pelo apoio na secretaria do curso e finalmente aos colegas de turma pela amizade e companheirismo no decorrer do curso.

À UFSM como Instituição, à CPPD meu setor de lotação, pelo apoio institucional e pela oportunidade de eu realizar o curso de Graduação, Pós-Graduação em nível de Especialização e o Mestrado e à PROGRAD, pela receptividade no uso de sua estrutura para o desenvolvimento do projeto.

Aos colegas servidores do DERCA, PROGRAD, DAG, ao Marcos do CPD, pelo auxílio com relação à geração do Diário de Classe, pela disponibilidade nos esclarecimentos das dúvidas, reuniões e discussões sobre o projeto. Em especial, à Débora Flôres por ter auxiliado no projeto, pela amizade e dedicação, ao Nériton e Antão Tadeu, pelo apoio técnico e por serem solidários, ao Cristiano, pelo coleguismo e incentivo, à Jô pela revisão do português, ao Orion pela ajuda no desenho das figuras do DC, aos que participaram das entrevistas e aos bolsistas que auxiliaram durante o período do curso na jornada de trabalho na CPPD.

Enfim, são várias as pessoas, entre colegas, amigos e familiares que presentes ou ausentes, estiveram sempre ao meu lado, partilhando apreensões, dúvidas, certezas e alegrias, que de alguma forma contribuíram para a minha trajetória pessoal e profissional até o presente momento. Espero que cada uma delas também se sinta feliz pelos resultados alcançados.

A TODOS(AS) aqueles(as) que não foram nominados aqui, mas que de alguma forma ou em algum momento desta caminhada, mesmo com pequeno(s) gesto(s) ou palavra(s), contribuíram para a realização desta dissertação e me incentivaram para que as minhas realizações tivessem pleno êxito, meu sincero,

MUITO OBRIGADA E UM ABRAÇO CARINHOSO!

La informática nos enriquece en tiempo  
y hace desaparecer las distancias.  
En cualquier época y mucho más en  
nuestro tiempo ya esto es un tesoro  
que no tiene precio.

(Manuel Vázquez Murillo)



## RESUMO

Dissertação de Mestrado  
Programa de Pós-Graduação em Engenharia de Produção  
Universidade Federal de Santa Maria

### **METADADOS PARA PRESERVAÇÃO E SEGURANÇA DO DIÁRIO DE CLASSE ELETRÔNICO DA UFSM**

AUTORA: Dulce Elaine Saul da Luz

ORIENTADOR: Raul Ceretta Nunes

Data e Local da Defesa: Santa Maria, 30 de setembro de 2011

As instituições públicas de ensino vêm buscando acompanhar os avanços tecnológicos e visam à busca pela evolução na educação que surge de forma crescente no dia-a-dia em seu ambiente organizacional. Esta pesquisa buscou investigar, avaliar e analisar o documento Diário de Classe da Universidade Federal de Santa Maria (UFSM) quanto à gestão, preservação e segurança da informação. A metodologia utilizada foi um estudo exploratório analítico combinado com análise documental a partir de informações encontradas na revisão de literatura, com técnica de estudo de caso. Portanto, foi realizada uma pesquisa bibliográfica, de legislação e de modelos de gestão arquivística de documentos, com abordagem qualitativa. A coleta dos dados foi realizada por meio de reuniões, entrevistas, observação e diagnósticos com os diferentes usuários envolvidos no processo em questão, através dos quais buscou-se verificar os procedimentos e as condições atuais em que se encontram os Diários de Classe nos Departamentos Didáticos. Como resultado, propõe-se um modelo de metadados para o Diário de Classe Eletrônico da UFSM, visando aperfeiçoar a produção, fluxo, armazenamento, acesso, segurança e preservação das informações. O modelo proposto sugere um conjunto de requisitos para gestão informatizada de documentos, indicado na norma e-ARQ Brasil, que especifica todas as atividades e operações técnicas da gestão arquivística de documentos desde a produção, tramitação, utilização e arquivamento até a sua destinação final. Este estudo foi finalizado com o objetivo geral alcançado que é a elaboração do modelo para implantação do Diário de Classe Eletrônico de acordo com a legislação e as políticas arquivísticas da Instituição e do governo, visando à preservação e segurança do DC da UFSM, por longo tempo, através dos metadados definidos para este documento conforme o modelo e-ARQ Brasil, determinando a melhor forma para sua gestão, preservação e segurança.

**Palavras-chave:** Metadados. Preservação. Segurança da Informação. Diário de Classe.



## **ABSTRACT**

Master's Dissertation  
Graduation Program in Production Engineering  
Universidade Federal de Santa Maria

### **METADATA FOR PRESERVATION AND SECURITY OF ELECTRONIC GRADEBOOKS AT UFSM**

AUTHOR: Dulce Elaine Saul da Luz

ADVISER: Raul Ceretta Nunes

Defense Place and Date: Santa Maria, September, 30<sup>th</sup> 2011.

The public education institutions are trying to follow the technological advances and aim to search for the evolution in education that increasingly appears every day in its organizational environment. This research aimed to investigate, evaluate and analyze the document Gradebook at Universidade Federal de Santa Maria (UFSM) in relation to its information management, preservation and security. The methodology used in this study was analytical exploratory combined with the documental analysis from the information in the literature review and, the case study technique. Therefore, we performed a bibliographical research of the legislation and the document archiving management with a qualitative approach. The data collection was performed through meetings, interviews, observation and diagnose with the different users involved in the considered process, where we searched to verify the procedures and the current conditions of the Gradebooks at the Didactic Departments. As a result of this study we suggest a model of metadata for the Electronic Gradebooks in UFSM, aiming to improve the production, flow, storage, access, security and preservation of the information. The proposed model suggests a set of requirements for computerized management of documents, specified in the standard e-ARQ-Brazil, which specifies all the activities and technical operations of the document archiving management from production, processing, use, archiving and final destination. This study was completed with its overall goal reached, which is the development of the model for implementation of Electronic Gradebooks, according to the rules and archival policies of the institution and the government, aiming at the preservation and safety of DC UFSM for a long time through the metadata defined for this document as model, and Brazil-ARQ, determining the best way for their management, preservation and security.

**Key words:** Metadata. Preservation. Information Security. Gradebook.





## LISTA DE FIGURAS

Figura 1 – Estrutura do documento eletrônico .....	29
Figura 2 – Quatro momentos do ciclo de vida da informação considerando os conceitos básicos da segurança e os aspectos complementares .....	40
Figura 3 – Modelo do ambiente SAAI .....	55
Figura 4 – Entidades funcionais do SAAI .....	56
Figura 5 – Obtenção de informação a partir de dados .....	59
Figura 6 – Diário de classe (antigo) .....	74
Figura 7 – Diário de classe (novo) .....	76
Figura 8 – Entidades e seus relacionamentos .....	86



## LISTA DE QUADROS

Quadro 1 – Entidade Documento .....	87
Quadro 2 – Entidade Evento de Gestão .....	88
Quadro 3 – Entidade Classe/Descrição da classe .....	90
Quadro 4 – Entidade Classe/Temporalidade associada à classe.....	91
Quadro 5 – Entidade Agente .....	92
Quadro 6 – Entidade Componente Digital.....	93
Quadro 7 – Entidade Preservação .....	94
Quadro 8 – Entidade Trilha de Auditoria .....	96



## LISTA DE SIGLAS E ABREVIATURAS

AAB – Associação dos Arquivistas Brasileiros  
ABNT – Associação Brasileira de Normas Técnicas  
CCSDS – *Consultive Committee for Space Data Systems*  
CLR – Comissão de Legislação e Regimentos  
CPAD – Comissão Permanente de Avaliação de Documentos  
CPD – Centro de Processamento de Dados  
CPPD – Comissão Permanente de Pessoal Docente  
CTDE – Câmara Técnica de Documentos Eletrônicos  
DAG – Departamento de Arquivo Geral  
DC – Diário de Classe  
DCE – Diário de Classe Eletrônico  
DERCA – Departamento de Registro e Controle Acadêmico  
GED – Gerenciamento Eletrônico de Documentos  
IFEs – Instituição Federal de Ensino Superior  
IDP – Informação Descritiva de Preservação  
ISO – *International Organization for Standardization*  
LDB – Lei de Diretrizes e Bases da Educação Nacional  
PAI – Pacote de Arquivamento de Informação  
PDI – Pacote de Descrição de Informação  
PSI – Pacote de Submissão de Informação  
SAAI – Sistema Aberto de Arquivamento de Informação  
SIE – Sistema de Informação para o Ensino  
SIGAD – Sistemas Informatizados de Gestão Arquivísticas de Documentos  
OAIS – *Open Archival Information System*  
PDI – Plano de Desenvolvimento Institucional 2011-2015 UFSM  
PPGEP – Programa de Pós-Graduação em Engenharia de Produção  
PROGRAD – Pró-Reitoria de Graduação  
TTD – Tabela de Temporalidade e Destinação  
TI – Tecnologia da Informação  
UFSM – Universidade Federal de Santa Maria



## LISTA DE APÊNDICES

Apêndice A – Metadados quadro individual .....	114
Apêndice B – Requisitos para o Diário de Classe Eletrônico .....	130





## LISTA DE ANEXOS

Anexo A – Resolução nº 25, de 27/04/2007 – CONARQ .....	136
Anexo B – Resolução nº 32, de 17/05/2010 – CONARQ .....	138



# SUMÁRIO

<b>1 INTRODUÇÃO .....</b>	<b>17</b>
<b>1.1 Motivação para escolha do tema .....</b>	<b>18</b>
<b>1.2 Delimitação do tema .....</b>	<b>19</b>
<b>1.3 Fundamentos relacionados ao tema .....</b>	<b>20</b>
<b>1.4 Objetivos .....</b>	<b>22</b>
1.4.1 Geral.....	22
1.4.2 Específicos .....	22
<b>1.5 Justificativa.....</b>	<b>23</b>
<b>1.6 Estrutura do trabalho.....</b>	<b>23</b>
<b>2 FUNDAMENTAÇÃO TEÓRICA .....</b>	<b>25</b>
<b>2.1 Arquivística.....</b>	<b>25</b>
<b>2.2. Gestão arquivística de documentos e informação.....</b>	<b>27</b>
2.2.1 Documento eletrônico.....	28
2.2.2 Preservação digital .....	30
<b>2.3 Aspectos de segurança na gestão e preservação de documentos digitais.</b>	<b>34</b>
<b>3 MODELOS DE REFERÊNCIA PARA GESTÃO ARQUIVÍSTICA .....</b>	<b>43</b>
<b>3.1 Modelo e-ARQ Brasil 2009.....</b>	<b>43</b>
3.1.1 Segurança: controle de acesso, trilhas de auditoria e cópias de segurança....	47
3.1.2 Armazenamento .....	50
3.1.3 Preservação .....	51
<b>3.2 Modelo OAIS ou SAAI 2007 .....</b>	<b>52</b>
3.2.1 Aplicabilidade do Modelo.....	53
3.2.2 Informação no OAIS/SAAI.....	59
<b>3.3 Comparação entre os modelos e-ARQ Brasil (2009) e SAAI (2007).....</b>	<b>61</b>
<b>4 METODOLOGIA .....</b>	<b>65</b>
<b>5 O DIÁRIO DE CLASSE NA UFSM.....</b>	<b>69</b>

<b>5.1 Legislação sobre o Diário de Classe.....</b>	<b>69</b>
5.1.1 Contextualização do Diário de Classe na UFSM .....	72
<b>6 PROPOSTA DE MODELO DO DIÁRIO DE CLASSE .....</b>	<b>79</b>
6.1 Requisitos do Sistema .....	79
6.2 Metadados para preservação do Diário de Classe .....	84
6.3 Resultados e discussão .....	97
<b>7 CONCLUSÃO .....</b>	<b>99</b>
7.1 Sugestões para estudos futuros .....	100
<b>REFERÊNCIAS BIBLIOGRÁFICAS.....</b>	<b>101</b>
<b>GLOSSÁRIO.....</b>	<b>109</b>
<b>APÊNDICES .....</b>	<b>113</b>
<b>ANEXOS .....</b>	<b>135</b>

# 1 INTRODUÇÃO

As instituições públicas de ensino vêm buscando acompanhar os avanços tecnológicos e visam à evolução na educação que cresce diariamente em seu ambiente organizacional. Um exemplo é o número de alunos matriculados nos cursos das instituições públicas e conseqüentemente o aumento dos documentos que necessitam de controle.

A pesquisa que originou essa dissertação está voltada para o estudo de caso e ancorada no documento “Diário de Classe da Universidade Federal de Santa Maria (UFSM)”. Foram realizadas a análise de diagnóstico, observação e revisão não só bibliográfica como também da legislação sobre o assunto para a implantação do Diário de Classe Eletrônico nesta Instituição.

O presente estudo constitui-se de uma revisão de literatura sobre o assunto abordando: arquivística, gestão arquivística de documentos e informação, aspectos de segurança na gestão e preservação de documentos digitais, modelos de referência para gestão arquivística e-ARQ Brasil 2009 e SAAI 2007 e a metodologia; do Diário de Classe na UFSM; da proposta de modelo do Diário de Classe; da conclusão e das referências.

Este trabalho pode servir para orientar os arquivistas e outros profissionais quanto à escolha e definição do modelo de requisitos para sistemas informatizados de gestão arquivística de documentos, considerando a preservação compartilhada com a segurança da informação, cada dia mais recorrente na produção documental de uma instituição, seja ela pública ou privada. Desta forma, será divulgado o conhecimento da produção intelectual local, dando segmento na direção da discussão sistematizada que permeia o problema da gestão de documentos eletrônicos, sua preservação e segurança.

É importante e de grande valia para a UFSM, tendo em vista às vantagens que se tem com um modelo de referência arquivístico adequado a realidade do Diário de Classe da UFSM, desde a economia de papel, espaço, mão de obra, tempo e também da ampliação do local de acesso no momento do seu preenchimento.

Para apresentar este modelo, foi elaborado um quadro onde constam as entidades, os metadados e os requisitos referentes ao documento digital Diário de Classe para que possa ser implementado na UFSM.

É importante explicitar que as definições conceituais utilizadas neste estudo encontram-se no glossário.

## **1.1 Motivação para escolha do tema**

A conservação e preservação de documentos é uma disciplina interessante, que desperta atenção dos profissionais da documentação em geral, tanto arquivista como bibliotecário.

Nos últimos anos, na sociedade digital, a segurança da informação torna-se importante para a gestão, preservação e o acesso à informação. Com este trabalho, busca-se alertar que a segurança, mais do que qualquer produto que se possa aplicar, é um processo contínuo e abrangente, com implicações que envolvem toda a área da organização desde à administração até os que executam as operações diárias mais elementares, exigindo um novo olhar sobre os modelos documentais.

Com o avanço emergencial das novas tecnologias e a utilização sem fronteira da Internet, surgem novos elementos, que precisam ser gerenciados como, por exemplo, a possibilidade de gerar e difundir recursos originados em computador, baseados em multimídia digital. Juntamente com isso, surge a possibilidade de digitalizar documentos em suporte papel, documentos sonoros, entre outros.

De acordo com Rodrigues (2003), estes recursos, nascidos digitais e outros não, como cópias de documentos com existência física, conforme com suas características, possuem grandes potencialidades do ponto de vista da difusão e acesso à informação e ao conhecimento, mas existem alguns fatores de risco para a sua sobrevivência à longo prazo: os recursos digitais tornam-se ilegíveis e inacessíveis se os mecanismos de leitura necessários se tornarem obsoletos. Além disto, a fragilidade física dos suportes e a obsolescência tecnológica, entre outras, são barreiras a ultrapassar na preservação digital de longo prazo.

Rodrigues (2003) menciona que de um lado os profissionais lidam com ferramentas eletrônicas que aumentam a capacidade de gerir o conhecimento,

deixando que a difusão da informação se expanda ao maior número de usuários, não só da comunidade local, mas das demais existentes. Por outro lado, têm-se o risco de perder todas as alterações acrescentadas pelo trabalho do profissional, até mesmo os recursos digitais, devido à vulnerabilidade do ambiente e à obsolescência tecnológica.

O sentido do risco de perda é tão grande que ajuda a dar motivação para se dedicar à investigação sobre a gestão, preservação e segurança dos documentos em meio aos recursos digitais à longo prazo, aliado a segurança da informação.

## **1.2 Delimitação do tema**

A presente pesquisa propõe um estudo no Departamento de Registro e Controle Acadêmico (DERCA) da UFSM, a fim de avaliar a situação deficitária que o setor tem com relação aos seus documentos, delimitando o tema à gestão, preservação e acesso com segurança ao documento Diário de Classe.

O tema focalizado no estudo refere-se à gestão e preservação da informação aliada à segurança, sob a perspectiva arquivística, ou seja, pelo gestor de documento e informação.

Considerando esta delimitação, a pesquisa visa propor um modelo de metadados para implantação do Diário de Classe Eletrônico na UFSM, tendo em vista a sua importância como documento de registro e informação, contendo dados sobre a logomarca da UFSM, nome do professor, identificação da disciplina, turma, créditos, carga horária, nome do aluno, matrícula, controle de frequência, matéria lecionada, carga horária, data, código de aprovação, avaliação parcial 1 e 2, média final do aluno, situação e outras informações importantes.

A questão fundamental que originou a presente pesquisa pode estar enunciada como um problema arquivístico que implica na produtividade da Instituição. A deficiência do modelo em papel do Diário de Classe da UFSM está no fato de que há duas aplicações para um mesmo documento. Até 2010, existiam na UFSM, dois modelos de Diário de Classe: um em suporte físico (papel) e outro digital, disponível no programa do SIE, através do Portal do Professor na WEB.

Ambos eram similares e possuíam todos os dados, porém com aplicações diferentes, isto é, uma aplicação gerava as notas e a outra os demais dados.

Portanto, a primeira ideia foi juntar os dois modelos de modo a torná-lo único e eletrônico e, com isso, agilizar, otimizar e potencializar o uso da tecnologia para a implantação do Diário de Classe Eletrônico na UFSM.

### **1.3 Fundamentos relacionados ao tema**

A preocupação com o problema da preservação e conservação das coleções de documentos é tão antiga quanto a sua existência. Conforme Rodrigues (2003, p. 23), “preservar a memória é preservar a identidade cultural; é ligar passado e presente e dessa forma preparar o futuro. Ora, precisamente, é nas bibliotecas e nos arquivos que podemos encontrar uma grande parte dessa memória”.

Atualmente, com o uso das tecnologias na produção e disseminação das informações, uma parte considerável da memória da sociedade encontra-se em meio digital. No entanto, esta sociedade é marcada por uma demanda crescente do volume informacional, dificultando a possibilidade de um tratamento adequado de todas as informações, bem como a segurança em especial com relação ao acesso.

Conseqüentemente, as constantes inovações tecnológicas preocupam e interferem no trabalho do profissional arquivista, pois fica em aberto muitos questionamentos sobre como fazer para gerenciar a informação digital.

Com a tecnologia da informação, o impacto nos arquivos fica evidente no momento em que muitas informações importantes tornam-se inacessíveis em pouco tempo. Portanto, as discussões sobre a preservação dos documentos entram para ordem do dia. Aos profissionais arquivistas e demais envolvidos com a informação, vem aflorando a preocupação com a preservação já na origem dos documentos digitais.

Percebe-se pessoalmente esta preocupação com a preservação dos documentos digitais e também Rondinelli (2002 apud SANTOS et al., 2009 , p. 23), considera que “os documentos eletrônicos exigem mais, uma vez que são constantemente ameaçados pela fragilidade do suporte e pela obsolescência tecnológica”. No meio digital considera-se que o suporte e o conteúdo são



separáveis, mediante a migração contínua de mídia, devido à fragilidade desta e à obsolescência tecnológica, além de possibilitar o aumento da possibilidade de adulteração e a garantia da fidedignidade e autenticidade torna-se bastante complexa e complicada tendo em vista o processo de migração.

Rodrigues (2003) ressalta que nem todos os acervos das bibliotecas ou dos arquivos teriam condições, nem mesmo manifestado interesse, para assegurar a integridade física de todas as espécies que possuem, por isso deveria ser estabelecida, no âmbito da gestão de coleções, uma política de prioridades.

Baseado nesta problemática e a falta de experiência prática na preservação de mídias digitais no Brasil, assim como o acesso no futuro, a discussão sobre o tema preservação digital é considerada fundamental em nosso país.

O e-ARQ Brasil (2009) é uma especificação de requisitos a serem cumpridos pela organização produtora/recebedora de documentos, pelo sistema de gestão arquivística e pelos próprios documentos a fim de garantir sua confiabilidade, autenticidade e acessibilidade; também pode ser usado para orientar a identificação de documentos arquivísticos digitais. Em síntese, ele contém um conjunto de requisitos de segurança que devem integrar qualquer Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD) e compreende mais de noventa requisitos distribuídos em segmentos.

Com relação ao controle de acesso, esta especificação contempla três requisitos: o controle de acesso baseado em papéis de usuário, o controle de usuários por grupo e o de classificação quanto ao grau de sigilo. Os três podem ser combinados, sendo que os de administração de controle de acesso devem ser adaptados a cada tipo ou a uma combinação deles, de acordo com a legislação vigente. Conforme e-ARQ Brasil (2009, p. 87), “esses requisitos não esgotam o tema segurança da informação, pois a segurança integral é sistêmica e abrange não somente a tecnologia, mas também as pessoas, processos e legislação”. Por isso, apresenta os procedimentos e requisitos para serem adotados como cópia de segurança, controle de acesso, classificação da informação quanto ao grau de sigilo e restrição de acesso à informação sensível, trilhas de auditoria, assinaturas digitais, criptografia, marcas d’água digitais, acompanhamento de transferência, autoproteção, e alterar, apagar e truncar documentos arquivísticos digitais. Finalmente, o e-ARQ Brasil compreende grande variedade de requisitos para diferentes esferas de atuação, ramos de atividades e tipos documentais.

No entanto, sozinho o e-ARQ Brasil não abrange todos os requisitos necessários para qualquer organização poder criar, manter e dar acesso a documentos digitais. As organizações possuem exigências legais e regulamentares distintas que devem ser consideradas ao se adotar este modelo. O sucesso da implementação depende de várias decisões, que vão exigir a adoção de uma política arquivística abrangente que vai além de selecionar um *software* ou adotar um já existente. Sabe-se que fica a critério de cada organização a decisão de como adotá-lo, se de forma modular ou completa. Ressalta-se que o presente documento foi elaborado para profissionais das áreas de administração, de arquivologia e de tecnologia da informação, requerendo a interação entre eles para implementar com sucesso.

## **1.4 Objetivos**

### 1.4.1 Objetivo geral

- Investigar o processo para implantação do Diário de Classe Eletrônico de acordo com as políticas arquivísticas e propor um modelo de metadados para sua preservação e segurança.

### 1.4.2 Objetivos específicos

- Analisar e compreender os modelos arquivísticos existentes, enquanto ferramenta tecnológica ou sistema, buscando viabilizar a elaboração do documento em meio eletrônico para uso e armazenamento com segurança.

- Comparar os modelos

- Propor um modelo arquivístico para o Diário de Classe na UFSM, que garanta preservação e segurança.

## **1.5 Justificativa**

A importância deste trabalho surge da necessidade de melhoria para os documentos de uma instituição de ensino. Para proporcionar esta melhoria no arquivo da UFSM, foi preciso propor um modelo arquivístico com metadados adequado à realidade da instituição e as suas políticas.

Em todos os trabalhos acadêmicos, espera-se contribuir com os conhecimentos científicos e empíricos, principalmente no tema proposto, que é considerado multidisciplinar e aborda o estudo de caso na UFSM com relação ao documento Diário de Classe nela utilizado. Devido à importância das informações contidas no mesmo, vislumbra-se torná-lo documento eletrônico, tendo muitas vantagens para a Instituição e usuários, trazendo economia de tempo e espaço, rapidez no acesso, segurança, entre outras.

Esta pesquisa e seu complemento teórico sobre o assunto trará benefícios para todos os profissionais que terão a responsabilidade de gerenciar as organizações arquivísticas com competência, habilidade e conhecimento. O dinamismo com as novas descobertas tecnológicas e o aprimoramento do conhecimento nos faz acreditar que as dificuldades dos dias atuais serão superadas em breve ou no futuro próximo. Em especial, na UFSM, com relação ao gerenciamento dos documentos eletrônicos e suas vantagens.

## **1.6 Estrutura do trabalho**

A apresentação do resultado do estudo está estruturada em sete capítulos, que buscam contemplar os objetivos propostos.

No capítulo dois, está descrita a fundamentação teórica sobre os conteúdos necessários para aprofundar os conhecimentos sobre o tema a ser desenvolvido na dissertação para que os objetivos propostos sejam atingidos.

No capítulo três, estão descritos os modelos e-ARQ Brasil e SAAI, referindo-se à preservação e ao acesso com segurança da informação e a comparação entre os modelos.

A metodologia é apresentada no capítulo quatro, enquanto que o capítulo cinco apresenta o Diário de Classe na UFSM. No sexto é descrita a proposta de modelo do Diário de Classe, bem como os requisitos e os metadados para preservação e segurança;

No capítulo sete, são apresentadas as conclusões da pesquisa e as sugestões para os trabalhos futuros. Por último as referências bibliográficas utilizadas. E no final do trabalho, constam os apêndices com a proposição dos Metadados para o Diário de Classe, o quadro dos requisitos para o DCE e os anexos contendo as Resoluções n. 25/2007 e n. 32/2010 do CONARQ.

## **2 FUNDAMENTAÇÃO TEÓRICA**

Este capítulo apresenta-se os aspectos da literatura que constituem a aporte teórico, baseado em contribuições científicas já elaboradas sobre o tema e que contribuíram para o embasamento do trabalho, referente à preservação e segurança da informação do Diário de Classe da UFSM, com o objetivo de situar o cenário no qual esse estudo desenvolve-se. Os referenciais teóricos utilizados remetem aos seguintes temas: Arquivística, Gestão arquivística de documentos e informação, Documento eletrônico, Preservação digital e Aspectos de segurança na gestão e preservação de documentos digitais.

### **2.1 Arquivística**

De acordo com Rousseau e Couture (1998, p. 55), “a arquivística situa-se no cruzamento de novos contextos culturais, dos novos modos de gestão tal como das novas tecnologias”. A arquivística está passando por um processo de maturação e consolidação de seus princípios, dentre estes os da era digital.

Encontra-se sintomas evidentes da afirmação arquivística em Jenkinson (1992, p. 106-107 apud SILVA et al ., 1998, p. 126): “A verdade arquivística é distinta da verdade histórica, pelo que o arquivista não é, nem deve ser, um historiador. Em sua opinião, o arquivista deve servir, antes de mais, o seu arquivo e só depois o público estudioso.”

De acordo com Silva et al., (1998), na realidade o homem sempre teve a necessidade e a preocupação em deixar registradas as suas ações, decorrente de necessidades imediatas, esse motivo levou-o a estabelecer meios eficazes de conservar os registros para uma posterior utilização dos mesmos.

Rousseau e Couture (1998), dizem que a arquivística pela sua natureza responde às necessidades dos órgãos ou dos indivíduos que criam os documentos, mas é bastante confrontada com os problemas levantados/apontados pela mundialização dos mercados e a definição de novas fronteiras. “A arquivística tem,

pois, como obrigação encontrar solução para estes novos problemas ao mesmo tempo em que aprofunda a sua identidade e mantém a sua coesão” (p. 56). Ainda de acordo com Rousseau e Couture (1998), existem sete funções arquivísticas a considerar: produção, avaliação, aquisição, conservação, classificação, descrição e difusão dos arquivos. Neste estudo, se dará ênfase às funções de avaliação, classificação, conservação/preservação e difusão/acesso.

O processo de avaliação deve considerar a função pela qual foi criado o documento, identificando os valores a ele atribuídos, segundo o seu potencial de uso. O valor primário se refere ao uso administrativo para o órgão, razão primeira da criação do documento o que pressupõe o estabelecimento de prazos de guarda ou retenção anteriores à eliminação ou ao recolhimento para guarda permanente. Relaciona-se ao período de utilidade do documento para cumprimento dos objetivos para os quais o órgão foi criado – administrativos, fiscais, legais e executivos. O valor secundário se refere ao uso para outros fins. A diferença entre os valores pode ser analisada sob dois aspectos: primeiro a prova que contem da organização e do funcionamento do órgão que os produziu e segundo a informação que contem sobre pessoas, entidades, problemas, etc. com que o órgão haja tratado. Schellenberg (2006) afirma que o documento possui valor probatório quando comprova a existência, o funcionamento e as ações da instituição; e o valor informativo quando contém informação essencial sobre matérias com que o órgão lida para fins de estudo ou pesquisa sobre vários assuntos.

Todos os aspectos de um programa de arquivamento visando o controle de documentos dependem de uma boa classificação. Os documentos adequadamente classificados atenderão as necessidades das operações correntes e do órgão com precisão. Portanto, devem ser arranjados de acordo com o uso que eles têm nas unidades administrativas deste órgão. O método de classificação proporciona também a base para a preservação e destruição dos documentos após cumprir aos objetivos das atividades correntes. Schellenberg (2006, p. 84) apresenta três elementos principais a serem considerados na classificação de documentos públicos: a) “ação a que os documentos se referem; b) a estrutura dos órgãos que os produzem e c) o assunto dos documentos”.

Camargo e Bellotto (1996, p. 18-61) definem conservação como “conjunto de procedimentos e medidas destinadas a assegurar a proteção física dos arquivos contra agentes de deterioração” e preservação como “função arquivística destinada

a assegurar as atividades de acondicionamento, armazenamento, conservação e restauração de documentos”.

A difusão é conhecida como atendimento ao público e também acesso, que, conforme Camargo e Bellotto (1996, p. 1-9), definem acesso como “possibilidade de consulta a um arquivo, como resultado de autorização legal”, e atendimento ao público como “função arquivística que consiste em colocar os documentos à disposição dos usuários que os solicitem, dentro de normas estabelecidas”. Portanto, a difusão tem o objetivo de tornar os documentos acessíveis e promover sua consulta, mediante instrumentos como catálogos, guias e outros, que auxiliam o processo de difusão. Pode-se usar o mapa de localização, o qual agiliza a recuperação dos documentos por possuir, detalhadamente, a localização física dos documentos que já estão classificados e arquivados. Este mapa será organizado de forma hierárquica, conforme as especificidades de cada organização, identificando, por exemplo, o número das salas, estantes, gavetas, caixas, entre outros.

Do exposto, identifica-se que os documentos públicos são produtos de ações e subdividem-se, naturalmente, em grupos referentes às ações. Uma ação pode ser considerada em termo de funções, atividades e atos. Cada função é referente às responsabilidades atribuídas a um órgão com a finalidade de atingir os amplos objetivos para os quais foi criado, sendo definida nas leis ou regulamentos que criam o órgão. A arquivística é a ciência que conduz tais ações e funções e nos orienta a uma gestão eficiente de documentos e informações.

## **2. 2 Gestão arquivística de documentos e informação**

A gestão de documentos corresponde ao gerenciamento de todo o ciclo de vida dos documentos de arquivo, iniciando na sua produção, organização, tramitação e uso, completando com sua destinação final (arquivamento), garantindo a eliminação criteriosa dos documentos privados de valor para guarda permanente e a preservação dos que têm valor informativo, probatório ou histórico. De acordo com Camargo e Bellotto (1996, p. 41), gestão de documentos é o “conjunto de medidas e rotinas visando à racionalização e eficiência na criação, tramitação, classificação, uso primário e avaliação de arquivo”. Paes (2004, p. 53), considera gestão de

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

Tradicionalmente, o documento físico, ou apenas documento, é aquele cuja maior característica está na vinculação a um suporte físico. Isto significa que seu conteúdo está unido, de forma inseparável a algo material. Porém, um documento também deve ser enquadrado como “informação registrada, independentemente de suporte ou características”. ARQUIVO NACIONAL ISAD(G) (2000, p. 15), o que reforça a necessidade de desvinculação do conteúdo a um suporte material.

A seguir, discute-se a gestão de documento eletrônico e a preservação digital.

### 2.2.1 Documento eletrônico

Camargo e Bellotto (1996, p. 27-28) definem documento eletrônico como “documentação cujo contexto, registrado em suportes especiais, é acessível apenas por computador”, e documento como “unidade constituída pela informação e seu suporte”. Neste mesmo sentido, Santos (2002, p. 31 e 32) refere que “a definição de documento eletrônico deve deixar claro que ele é um produto de ou conectado a um sistema de computador”.

Observe que o suporte da informação refere-se aos discos rígidos de computadores e mídias de armazenamento de dados onde a informação é escrita, alterada, apagada e copiada durante a rotina.

Um documento eletrônico é constituído pela estrutura lógica, conteúdo e estrutura de apresentação, conforme a citação:

A estrutura lógica especifica a organização de um documento para indicar suas diferentes partes, (títulos de páginas, capítulos e seções), o conteúdo do documento é formado pela informação contida em cada parte (textos, tabelas, equações, imagens, vídeos e som), e a estrutura de apresentação é a forma como o documento aparece na página, sua formatação”. (PROKOPETZ 1998 apud SANTOS, 2002, p. 39).

Adicionalmente é no conteúdo do documento eletrônico que devem estar inseridos os elementos internos requeridos pela análise diplomática para conferir a



autenticidade do documento. Conforme Rondinelli (2002, p. 55), a análise diplomática, consiste em um “processo de abstração e de sistematização cujo objetivo é identificar os atributos essenciais ou “ideais” de um documento e transportá-los para diferentes contextos históricos e documentários”.

Com base nestas delimitações elencadas, documentos eletrônicos são as unidades de registros, acessíveis mediante um equipamento eletrônico. Lembrando da legibilidade por máquina, outras formas de documentos, como aquelas de gravação de som e vídeo, também necessitam o uso de máquinas como meio de acesso ao seu conteúdo informacional, portanto, são entendidas como documentos eletrônicos. Então, a definição de documento eletrônico deve deixar claro que ele é um produto de um sistema de computador, ou conectado a este.

Hoje, com a evolução da tecnologia e o desenvolvimento da Internet, têm-se o documento eletrônico digital e o digitalizado. Documento digital é o “documento codificado em dígitos binários, acessível por meio de sistema computacional” (DICIONÁRIO BRASILEIRO DE TERMINOLOGIA ARQUIVÍSTICA, 2005, p. 75), capaz de ter seus elementos manipulados eletronicamente. Já o documento digitalizado é uma cópia digital de um documento físico existente em outro suporte.

Conforme Santos et al., (2009, p. 26) “o documento digital tem como base três elementos: o *hardware*, o *software* e a informação armazenada em um suporte”, tal como ilustra a figura 1.

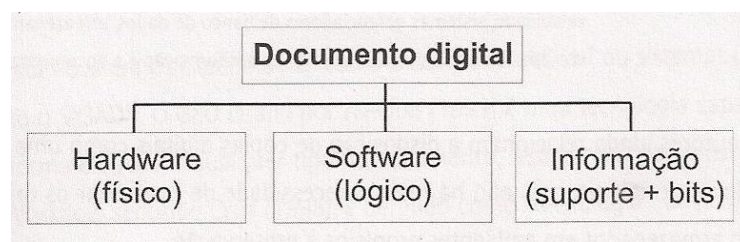


Figura 1 – Estrutura do documento digital

Fonte: Santos et al., 2009

O estudo sobre o documento digital passa pela análise das características do documento físico, para se identificar quais atributos fazem do documento digital a

forma mais utilizada, inclusive no mundo jurídico, atualmente para registro de fatos e se podem ter seus elementos ou efeitos reproduzidos no seu correspondente digital.

A partir da identificação das características envolvidas no documento físico, e constatadas que o documento digital seria uma opção segura, observa-se que motivos levariam ao ensejo, senão uma substituição completa, ou um conforto do uso do físico com relação ao digital. Faz-se necessário a análise do documento digital, para saber se este comporta condições adequadas para ser viável a substituição do documento físico.

Após esta revisão, verifica-se a viabilidade do documento digital, não como um substituto completo do documento físico, mas como uma alternativa válida e capaz de oferecer vantagens quando comparada ao seu correspondente físico.

Conforme Santos et al., (2009), é importante lembrar que a visualização dos documentos digitais dependem diretamente do uso de *software* e computadores, os quais nem sempre estão presentes em todos os lugares e apresentam a tecnologia compatível.

Rodrigues (2003) acredita que o tempo de vida ou a duração dos suportes não seja o fator mais importante para a preservação dos recursos digitais, mas talvez se deva considerar o fator da migração dos dados como um fator relevante, para que o acompanhamento do surgimento das novidades aconteça, e não se corra o risco de ser ultrapassado pela obsolescência dos dispositivos.

### 2.2.2 Preservação digital

Conforme Rodrigues (2003, p. 78), preservação digital é o “conjunto de operações de gestão a empreender, capazes de assegurar a manutenção a longo prazo de uma cadeia de *bytes* e o acesso continuado ao seu conteúdo”.

No momento, as questões relacionadas com a preservação de documentos digitais, mais especificamente, perpassam por diversas estratégias de preservação. Logo, esta subseção aborda a preservação de documentos arquivísticos digitais. Portanto, é necessário destacar que a preocupação reside na preservação de documentos criados em meio digital, constituindo-se numa forma de informação e que precisa atenção quanto aos aspectos de acesso e autenticidade.

Conforme Santos et al., (2009), diante da utilização da tecnologia nas áreas da Ciência da Informação e a tendência cada vez maior de produção de documentos e informações digitais, é importante pesquisar temas relacionados às políticas de preservação, aos formatos físicos e lógicos, aos sistemas gerenciadores, aos processos de migração, de replicação, ao lixo digital, à durabilidade, à confiabilidade, etc.

Visando um projeto que preveja a preservação destes documentos e informações, para não correr o risco de viver numa sociedade sem memória, logo sem parte de sua história, esta preocupação é geral. Santos (2009, p. 23) relata que a *United Nations Educational Scientific and Cultural Organization* (UNESCO), em sua resolução sobre preservação digital, publicada pela Associação dos Arquivistas de São Paulo (ARQ-SP 2001), “considera urgente a necessidade de salvaguardar os patrimônios culturais digitais, garantindo assim o acesso continuado aos conteúdos e a funcionalidade dos registros eletrônicos autênticos em prol da preservação e do acesso aos documentos, para assegurar os direitos dos cidadãos”.

Conforme Santos (2009, p. 23), a preocupação com a preservação digital é relatada por Rondinelli (2002), considerando que “os documentos eletrônicos exigem mais, uma vez que são constantemente ameaçados pela fragilidade do suporte e pela obsolescência tecnológica”. Rondinelli considera que no meio digital o suporte e o conteúdo são separáveis, e esta separação permite a migração continua de mídia, a qual acontece inevitavelmente tendo em vista à fragilidade da mídia e a obsolescência tecnológica. Porém, com a migração, aumenta a possibilidade de adulteração e a garantia da fidedignidade e autenticidade torna-se complexa e dificultada.

Com a possibilidade de sofrer alterações ao longo de sua vida, a preservação envolve vários aspectos a serem considerados na avaliação das informações, lembrando da avaliação e com a idéia de que sendo documentos arquivísticos convencionais ou digitais, representam as atividades que lhes deram origem e mostram um valor que deve ser considerado no ato de sua preservação ou eliminação.

A preservação digital é definida por Ferreira (2006, p. 20) como “o conjunto de actividades ou processos responsáveis por garantir o acesso continuado a longo prazo à informação e restante património cultural existente em formatos digitais”.

Ferreira afirma que a preservação digital consiste na “capacidade de garantir que a informação digital permanece acessível e com qualidades de autenticidade suficientes para que possa ser interpretada no futuro recorrendo a uma plataforma tecnológica diferente da utilizada no momento da sua criação”. Com relação ao longo prazo, há que se tomar cautela, pois a UNESCO considera para o formato digital, o prazo de cinco anos como sendo de longo prazo.

O Dicionário Brasileiro de Terminologia Arquivística (ARQUIVO NACIONAL, 2005, p. 135) apresenta o termo preservação como uma atividade subordinada à conservação que seria a atividade mais abrangente. Preservação é definida então como a “prevenção da deterioração e danos em documentos, por meio de adequado controle ambiental e/ou tratamento físico e/ou químico”.

Ferreira (2006) considera que a preservação digital é muito importante, pois é a atividade responsável por garantir que a comunicação entre um emissor e um receptor é possível, não apenas através do espaço, mas inclusive através do tempo.

De acordo com Camargo e Bellotto (1996, p. 61), a preservação é considerada uma “função arquivística destinada a assegurar as atividades de acondicionamento, conservação, armazenamento e restauração de documentos”, procurando manter os documentos em condições de acesso.

Com relação ao acesso da informação, de acordo com Santos (2002, p. 63), existe “a necessidade de se garantir formas de o arquivista gerenciar os documentos eletrônicos desde sua criação para evitar que eles sejam destruídos por seus produtores, uma vez que tenham cumprido seus objetivos”. Quando se trata de documentos eletrônicos não existe a possibilidade de avaliar e selecionar após ter vencido o prazo de uso pelo produtor.

Entretanto, para a preservação digital, é necessário transformar a informação em metadado, que significa dado sobre dado. Saramago (2004) define metadados como a informação de apoio aos processos associados com a preservação digital de longo prazo. Continuando a autora assevera que:

Os metadados de preservação devem conter informação técnica e administrativa sobre as decisões e ações de preservação, registrar os efeitos das estratégias de conversão de dados, assegurar a autenticidade dos recursos digitais ao longo do tempo, registrar informação acerca de gestão de coleções e de direitos e ainda fornecer informações acerca dos próprios metadados. (SARAMAGO, 2004, p. 3-4).

Conforme Thomaz e Soares (2004, p. 2), a preservação digital é a “capacidade de manter a integridade e a acessibilidade da informação digital por longo prazo”. Esta preservação referida não se limita somente a proteger a informação digital contra o acesso não autorizado, mas, certamente, contra o uso impróprio resultante das más interpretações ou representação da informação vinda dos sistemas computacionais.

No ambiente digital, encontra-se o termo longo prazo; neste contexto entende-se como longo prazo, o tempo determinado de acesso contínuo aos recursos digitais ou a informação armazenada por período indeterminado.

Saramago (2004, p. 1) diz que “os recursos sofrem transformações cujos resultados, nem sempre são fáceis de controlar. Por este motivo deve ser criado um histórico da mudança ao longo do tempo”. Entende-se que, no ambiente digital, o objetivo maior é garantir que sua autenticação e integridade sejam reconstituídas.

De acordo com Santos (2002), diante do relato descrito, observa-se que os arquivistas precisam ter em mente que a finalidade de seu trabalho é acima de tudo, assegurar da melhor maneira possível, a proteção aos documentos, qualquer que seja seu suporte, e também devem garantir o acesso as informações contidas neles. Sem esquecer que é durante a fase corrente que deve ser dado o tratamento adequado para obter a melhor forma de garantir a preservação e a acessibilidade dos documentos no arquivo permanente.

Cunha e Lima (2007), com relação a preservação digital, dizem que existem ações neste sentido, mas ainda não existem consensos sobre as técnicas e metodologias utilizadas, portanto justifica-se a necessidade de abrir novo campo de estudos que produzam contribuições para garantir a acessibilidade e preservação dos objetos digitais para o futuro.

Sobre a preservação de acervos digitais no Brasil, a ação mais significativa foi a reformulação da Câmara Técnica de Documentos Eletrônicos (CTDE), do Conselho Nacional de Arquivo (CONARQ), criado em 1994 e em funcionamento a partir de 2002. Este grupo de trabalho multidisciplinar tem por objetivo “[...] definir e apresentar ao CONARQ, normas, diretrizes e procedimentos técnicos e instrumentos legais sobre gestão arquivística e preservação de documentos digitais, em conformidade com os padrões nacionais e internacionais.” (CONARQ, 2006).

Portanto, as ações de preservação que antes eram voltadas para a conservação e a restauração dos suportes, agora precisam ser determinadas já na

origem do documento, para garantir a preservação da informação em meio digital com segurança e por longo tempo.

Com a tecnologia da informação, o impacto nos arquivos fica evidente no momento em que muitas informações importantes tornam-se incompreensíveis em questão de pouco tempo. Portanto, as discussões sobre a preservação dos documentos entram para ordem do dia. Aos profissionais arquivistas e demais envolvidos com a informação, vem aflorando a preocupação com a preservação já na origem dos documentos digitais.

Baseado na problemática e a falta de experiência prática na preservação de mídias digitais no Brasil, assim como o acesso no futuro, a discussão sobre o tema preservação digital é considerada fundamental em nosso país.

Portanto, observa-se que é importante a questão da preservação digital e a manutenção da autenticidade e da acessibilidade do documento preservado, buscando também a segurança da informação.

### **2.3 Aspectos de segurança na gestão e preservação de documentos digitais**

Considerando a importância da segurança na gestão e preservação do documento, o e-ARQ Brasil 2009 apresenta um conjunto de requisitos para os serviços de segurança recomendado aos documentos digitais. Entre os requisitos estão as cópias de segurança, controle de acesso, classes de sigilo, trilhas de auditoria de sistemas, criptografia para sigilo, assinatura digital e marcas d'água digitais. Os requisitos de identificação, autenticação e trilhas de auditoria são necessários na integração de qualquer Sistema Integrado de Gestão Arquivística de Documentos (SIGAD). As políticas de segurança específicas definirão quanto maior ou menor o rigor do tratamento dos demais requisitos.

Distinguem-se vários tipos de informação necessários ao funcionamento de um SIGAD e elas compreendem os documentos digitais, metadados e informações de controle associadas às camadas de *software* do SIGAD. Todas elas devem ser incluídas nos procedimentos de cópias de segurança.

O objetivo das cópias de segurança é prevenir a perda de informações e garantir a disponibilidade do sistema. Os procedimentos de *backup* devem ser feitos

com regularidade e no mínimo uma cópia deve ser armazenada, de preferência *off-site*.

O controle de acesso trata dos requisitos de identificação e autenticação de usuários, baseado em grupos e em papéis de usuários, e inclui requisitos comuns a qualquer tipo de controle de acesso. A identificação e autenticação de usuários tratam do mapeamento da identidade do usuário legítimo e das permissões dele, após sua autenticação

Com relação ao controle de acesso, este contempla três tipos de requisitos o de controle de acesso baseado em papéis de usuário; de controle de acesso por grupos; e o de classificação quanto ao grau de sigilo. Esses três podem ser combinados, e os requisitos de administração de controle de acesso devem ser adaptados a cada tipo referido antes ou a uma combinação deles, conforme a legislação vigente.

Criptografia é um método de codificação de objetos digitais conforme um código secreto, de maneira que não possam ser apresentados de forma legível ou inteligível numa aplicação, e apenas os usuários autorizados poderão restabelecer sua forma original. Os documentos que necessitam de longo prazo não devem ser armazenados criptografados porque há fatores que põem em risco a criptografia no longo prazo, como o comprometimento, indisponibilidade do portador da chave, obsolescência da mesma e evoluções tecnológicas

Sobre o uso da tecnologia de criptografia, para sigilo ou autenticação, o rigor dos requisitos fica sujeito à legislação vigente e à política de segurança específica. A criptografia é usada como mecanismo de apoio ao controle de acesso reforçando, assim, o sigilo das informações. Já a assinatura digital e certificação digital são necessárias às organizações em que documentos são assinados digitalmente ou para as verificações eletrônicas de autenticidade. Conforme e-ARQ Brasil (2009), esses requisitos não acabam o tema segurança da informação, porque a segurança integral é sistêmica e envolve não só a tecnologia, mas, ao mesmo tempo, as pessoas, processos e legislação.

Conforme e-ARQ Brasil (2009, p. 88): “Usuários acessam dados, metadados e funções via interface do programa”. E a associação entre identidade do usuário e autorizações de acesso é feita durante a identificação e autenticação do usuário na mesma interface do programa, com base nas credenciais de autenticação.

Na implementação do controle de acesso, um SIGAD tem que manter pelo menos esses atributos dos usuários, conforme a política de segurança: identificador do usuário; autorizações de acesso; e credenciais de autenticação.

Controle de acesso por papéis de usuários são funções ou cargos com responsabilidades e autoridades bem determinadas. As operações são as tarefas executadas nos documentos, já as atribuições são as associações entre usuários e papéis. Um usuário pode estar associado a um ou mais papéis e vice-versa. E as permissões constituem garantias aprovadas para efetivação de operações em documentos arquivísticos, somente aplicáveis aos órgãos e entidades em que há controle de acesso por papéis de usuários.

Tendo em vista o acesso com base na classificação quanto ao grau de sigilo e a restrição de acesso à informação sensível, de acordo com e-ARQ Brasil 2009 (p. 91), “a informação sensível pode estar relacionada à honra e à privacidade de pessoas ou a questões estratégicas e de sigilo corporativo”.

Os requisitos flexionam para atender tanto às organizações privadas ou órgãos públicos. Os documentos da administração pública estão sujeitos aos graus de sigilo definidos na legislação vigente.

Conforme o e-ARQ Brasil (2009, p. 93), “a trilha de auditoria consiste num histórico de todas as intervenções, ou tentativas de intervenção, feitas no documento e no próprio SIGAD”. Também é um metadado sobre os documentos arquivísticos digitais e informa sobre sua autenticidade.

O e-ARQ Brasil (2009, p. 96), diz que “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”. E a “Certificação digital é uma técnica, baseada em uma infraestrutura de chaves públicas, de garantia da validade de assinaturas digitais”. O uso de assinaturas digitais e de certificação digital na administração pública foi padronizado e normalizado com a criação da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

Marcas d'água são usadas não só para marcar uma imagem digital com informação sobre sua proveniência e características, como também para proteger a propriedade intelectual, podendo ser suprimida mediante a utilização de um algoritmo ou de uma chave protegida.



Sobre alterar, apagar e truncar documentos arquivísticos digitais, os mesmos completos não podem, em regra, ser alterados e eliminados, exceto no término do seu ciclo de vida num Sistema. A capacidade de apagar documentos tem que ser, rigorosamente, controlada para proteger a integridade desses documentos.

Conforme o e-ARQ Brasil (2009, p. 103), “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”, devendo-se abrigar os documentos, seus metadados, trilhas de auditoria e cópias de segurança. Fisicamente, tais informações residem em dispositivos de armazenamento eletrônicos, magnéticos e ópticos. A arquitetura tecnológica para gerenciá-los deve ser planejada de acordo com a missão e as competências da organização, devendo os equipamentos adequar-se às características *online* ou *offline* das operações.

Quanto à 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”. E a capacidade deverá garantir escalabilidade no armazenamento, permitindo a ampliação permanente dos dispositivos de armazenamento. Com relação à efetividade de armazenamento, esses dispositivos devem suportar métodos de detecção de erros para leitura e escrita de dados. O sistema tem que utilizar técnicas de restauração de dados em caso de falhas; mecanismos de proteção contra escrita, que previnam alterações indevidas e conservam a integridade dos dados armazenados.

Como no caso dos documentos convencionais para o e-ARQ Brasil (2009, p. 106), “a preservação de documentos arquivísticos digitais não é um fim em si mesmo”. Porém possui um propósito que deve ser considerado na definição e implementação das estratégias de preservação, onde a razão para se preservar um documento pode ser seu valor probatório e/ou informativo.

Os documentos gerenciados por um Sistema devem ser preservados durante todo o período previsto, conforme determinado na Tabela de Temporalidade de Documentos (TTD). As características desses documentos demandam atenção específica, sobretudo em relação àqueles que serão mantidos por mais de cinco anos, que já se considera preservação de longo prazo.

Conforme o e-ARQ Brasil (2009, p. 106), “A degradação do suporte e a obsolescência tecnológica são os principais fatores de comprometimento da

preservação dos documentos digitais, porque ameaçam sua autenticidade, integridade e acessibilidade”. Esta degradação é causada por fatores, como a falta de controle de temperatura, umidade, luminosidade, agentes químicos e biológicos agressores, e pela manipulação inadequada ou baixa qualidade do suporte utilizado. Além de respeitar as condições especificadas pela fábrica, é preciso substituir os suportes antes do fim de sua vida útil, essa técnica é conhecida como atualização (*refreshing*). Conforme e-ARQ Brasil (2009, p. 107), a obsolescência tecnológica refere-se a *hardware*, *software* e formatos. “É resultado das mudanças causadas pelo desenvolvimento de novas tecnologias e sua ascensão no mercado”.

No e-ARQ Brasil (2009), as técnicas utilizadas para evitar os riscos provenientes da obsolescência tecnológica são: preservação da tecnologia, com intuito de evitar a necessidade imediata de implementação de novos sistemas; emulação, que é a simulação de determinado *hardware* ou *software*, através de *software*. Assim, permite que um computador moderno, até mais barato e de fácil manutenção, possa executar programas (*software*) antigos, desenvolvidos, originalmente, para outra plataforma. A conversão de dados é empregada quando os formatos tornam-se obsoletos e a migração é migrar para novos sistemas realizados no caso de obsolescência de *hardware*, *software* ou formatos, envolvendo inclusive a conversão de dados. Portanto, as estratégias e procedimentos de preservação devem ser bem definidos, documentados e revisados periodicamente.

Com relação aos aspectos físicos, os suportes têm que ser acondicionados, manipulados e utilizados em condições ambientais compatíveis com sua vida útil prevista, de acordo com as especificações técnicas do fabricante e de entidades isentas, e baseado em estatísticas de uso; aspectos lógicos as cópias de segurança devem ser guardadas em ambientes seguros, em locais distintos de onde se encontra a informação original. Sobre os aspectos gerais, o sistema tem que registrar, em trilhas de auditoria, as operações de preservação realizadas, sendo que o ideal é utilizar suportes de armazenamento e recursos de *hardware* e *software* que sejam maduros, constantes no mercado e disponíveis amplamente.

Segundo a NBR ISO/IEC 27001 (2006, p. 2) segurança da informação é “preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade podem também estar envolvidas”.

A Confidencialidade da informação deve ser protegida conforme o grau de sigilo de seu conteúdo, visando o limite de seu acesso e uso somente às pessoas autorizadas. A Integridade salvaguarda a informação disponibilizada pelo seu proprietário, visando à proteção contra alterações indevidas, intencionais ou acidentais. A Disponibilidade significa que toda informação deve estar acessível e utilizável sob demanda por uma entidade autorizada.

O Não-repúdio visa garantir que o autor não negue ter criado e assinado o documento. Também evita que o emissor ou o receptor neguem a transmissão de uma mensagem, pois, quando se envia uma mensagem, o receptor pode comprovar que o emissor enviou a mensagem. No entanto, quando se recebe uma mensagem, o emissor pode verificar se, de fato, o receptor recebeu a mensagem.

Sêmola (2003, p. 43), define segurança da informação “como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”.

A informação é um ativo que, como qualquer outro ativo importante, é necessária para os negócios de uma organização, e, portanto, necessita ser adequadamente protegida. NBR 17799 (ABNT, 2005, p. IX). Desta forma Camargo e Bellotto (1996, p. 44), definem informação como “todo e qualquer elemento referencial contido num documento”.

Conforme Sêmola (2003), o ciclo de vida da informação é constituído e identificado pelos momentos vividos pela informação que a colocam em risco. Os momentos são vivenciados exatamente quando os ativos físicos, tecnológicos e humanos fazem uso da informação sustentando processos que, por sua vez, mantêm a operação da empresa, seja ela pública ou privada.

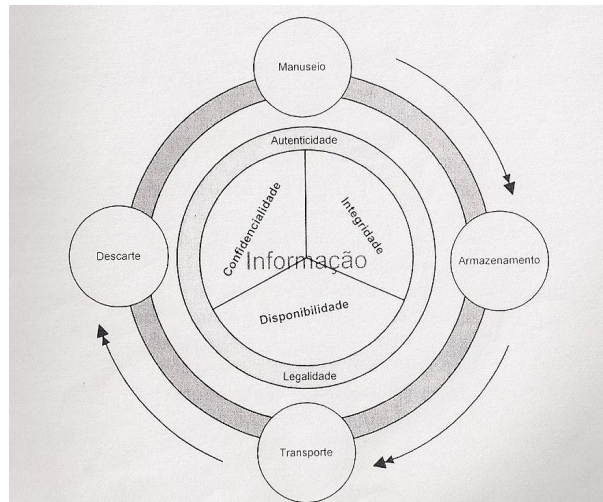


Figura 2 – Quatro momentos do ciclo de vida da informação, considerando os conceitos básicos da segurança e os aspectos complementares.

Fonte: Sêmola 2003

De acordo com Sêmola (2003, p. 9): “Toda informação é influenciada por três propriedades principais: Confidencialidade, Integridade, Disponibilidade, além dos aspectos Autenticidade e Legibilidade que complementam esta influência”, conforme ilustra a figura 2.

A confidencialidade é a propriedade que limita o acesso a informação somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário. A integridade é a propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudança e garantia de seu ciclo de vida (nascimento, manutenção e destruição). E a disponibilidade é a propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

Sêmola (2003) diz que há situações em que a informação é exposta a ameaças que colocam em risco suas propriedades, atingindo a sua segurança, independente da forma como a informação é representada (átomos ou bits), todos os quatro momentos se aplicam. Considerando as prováveis ameaças para a informação esses momentos são o manuseio, o armazenamento, o transporte e o descarte.

O manuseio é o momento em que a informação é criada e manuseada seja ao folhear papéis, ao digitar informações recém-geradas em aplicação Internet, ou ao utilizar sua senha de acesso para autenticação. O armazenamento é o momento em que a informação é armazenada seja em banco de dados compartilhado, uma anotação de papel posteriormente guardada em um arquivo de aço, ou em uma mídia de disquete guardada na gaveta da mesa de trabalho. O transporte é o momento em que a informação é transportada seja ao encaminhar pelo correio eletrônico, ao postar um documento via aparelho de fax, ou ao falar ao telefone uma informação confidencial. E o descarte é o momento em que a informação é descartada seja ao depositar na lixeira da empresa um material impresso, ao eliminar um arquivo eletrônico em seu computador de mesa, ao descartar um CD-ROM usado que falhou na leitura.

Aspectos gerais de controle de acesso são aplicáveis a qualquer organização para conduzir suas funções e atividades, independente do controle de acesso adotado, de acordo com a política de segurança.

Ao finalizar este capítulo relacionado aos aspectos de segurança na gestão e preservação de documentos digitais, se percebe que há vários mecanismos de segurança para os documentos digitais conforme foi descrito anteriormente.

Para atender a preservação digital requerem-se procedimentos específicos e técnicas adequadas para cada tipo de formato e mídia. Com a preservação digital, pretende-se garantir a originalidade dos registros digitais.

Portanto, a preservação a longo prazo de documentos digitais é um assunto complexo, com questões a ser definidas. Cabe ressaltar que apesar da existência de várias estratégias e talvez umas mais viáveis que outras, ainda não há provas conclusivas da eficácia das mesmas para longo prazo, sobretudo no que diz respeito à perda de informação dos documentos digitais.

Para conservar os documentos digitais, as estratégias e procedimentos de preservação devem ser bem determinados, registrados e revisados frequentemente na organização. A falta dessas políticas nos projetos de preservação digital indica a carência de conhecimentos técnicos sobre a importância das estratégias de preservação digital existentes.



## **3 MODELOS DE REFERÊNCIA**

Esse capítulo analisa os modelos de referência e-ARQ Brasil (Seção 3.1) e SAAI (Seção 3.2) para a gestão arquivística. A literatura sobre os modelos (Seções 3.1 e 3.2) demonstra a importância da aplicação de modelos de referência para as organizações como agente de mudanças em prol da preservação e segurança da informação. Após apresenta uma comparação entre os modelos com o objetivo de verificar as diferenças entre eles (Seção 3.3).

### **3.1 Modelo e-ARQ Brasil 2009**

O e-ARQ Brasil (2009) apresenta um Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (SIGAD), elaborado no âmbito da Câmara Técnica de Documentos Eletrônicos (CTDE) do Conselho Nacional de Arquivos (CONARQ).

Este modelo foi desenvolvido, considerando a existência de grande legado de documentos em formato digital, que vêm sendo trabalhado por especialistas de várias áreas. Os mesmos conceituam o documento arquivístico e o documento arquivístico digital para analisar e propor soluções que enfrentam os desafios deste formato.

É importante explicitar as definições estabelecidas pela CTDE no e-ARQ Brasil (2009, p. 8), “o documento arquivístico é produzido e/ou recebido e mantido por pessoa física ou jurídica, no decorrer das suas atividades, qualquer que seja o suporte, e dotado de organicidade”; o documento digital “é a informação registrada, codificada em dígitos binários e acessível por meio de sistema computacional”; o documento arquivístico digital “é tratado e gerenciado como um documento arquivístico, ou seja, incorporado ao sistema de arquivos” e o documento arquivístico convencional “é um documento arquivístico não digital”.

De acordo com e-ARQ Brasil (2009), devem ser considerados os fundamentos da diplomática, da arquivologia, em especial da gestão de documentos

e da tecnologia da informação para fornecer um conjunto de requisitos que seja amplo, rigoroso e de qualidade.

Este modelo especifica os requisitos a serem cumpridos pela organização produtora/recebedora de documentos, pelo sistema de gestão e pelos documentos para garantir sua confidencialidade, autenticidade e sua acessibilidade. Também pode ser usado para orientar a identificação de documentos arquivísticos digitais. E também determina requisitos mínimos para um Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD) e independe da plataforma tecnológica em que for desenvolvido e/ou implantado. O SIGAD deve gerenciar ao mesmo tempo os documentos digitais e os convencionais. Nos documentos convencionais, o sistema registra unicamente as referências sobre os documentos, já nos documentos digitais, a captura, o armazenamento e o acesso são feitos por meio do SIGAD.

Os requisitos dirigem-se aos que fazem uso de sistemas informatizados como parte do seu trabalho rotineiro de produzir, receber, armazenar e acessar documentos arquivísticos. No SIGAD está incluído um sistema de protocolo informatizado entre outras funções da gestão de documentos.

O e-ARQ Brasil (2009) especifica as atividades e operações técnicas da gestão arquivística de documentos, iniciando na produção, tramitação, utilização e arquivamento até a sua destinação final. Essas atividades poderão ser cumpridas pelo SIGAD, desde que desenvolvido conforme a norma e seus requisitos apresentados, que conferirá credibilidade à produção e à manutenção de documentos arquivísticos.

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 destes (e-ARQ Brasil, 2009, p. 9).

O sucesso dele dependerá, essencialmente, da implementação prévia de um programa de gestão arquivística de documentos.

O e-ARQ Brasil (2009, p. 9) refere que a produção de documentos digitais levou à criação do SIGAD. E para se assegurar que documentos arquivísticos digitais sejam confiáveis e autênticos e possam ser preservados com suas características, “é fundamental que os sistemas referidos incorporem os conceitos arquivísticos e suas implicações no gerenciamento dos documentos digitais”.



Conforme o e-ARQ Brasil (2009, p. 10), 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)”. Define também que o sistema de informação é o “conjunto organizado de políticas, procedimentos, pessoas, equipamentos e programas computacionais que produzem, processam, armazenam e provêem acesso à informação proveniente de fontes internas e externas para apoiar o desempenho das atividades da organização”. A Gestão arquivística de documentos é o “conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento dos documentos em fase corrente e intermediária, visando sua eliminação ou recolhimento para guarda permanente”. Na sequência, o e-ARQ Brasil conceitua que o Sistema de gestão arquivística de documentos é o “conjunto de procedimentos e operações técnicas, cuja interação permite a eficiência e a eficácia da gestão arquivística de documentos”.

Continuando as definições, o e-ARQ Brasil (2009, p.10) conceitua que GED é o “conjunto de tecnologias utilizadas para organização da informação não estruturada de um órgão ou entidade, que pode ser dividido em funcionalidades como: captura, gerenciamento, armazenamento e distribuição”. Informação não estruturada é aquela que não está armazenada em banco de dados, exemplo: mensagem de correio eletrônico, arquivo de texto, imagem ou som, etc. “O GED pode englobar tecnologias de digitalização, automação de fluxos de trabalho (*workflow*), processamento de formulários, indexação, gestão de documentos, repositórios, entre outras”.

A literatura sobre GED distingue as 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.

Conforme e-ARQ Brasil, (2009, p. 10), o SIGAD é um “conjunto de procedimentos e operações técnicas que visam o controle do ciclo de vida dos documentos, desde a produção até a destinação final, seguindo os princípios da gestão arquivística de documentos e apoiado em um sistema informatizado”. Ele tem que ser capaz de manter a relação orgânica entre os documentos e de garantir a confiabilidade, a autenticidade e o acesso, ao longo do tempo, aos documentos

arquivísticos, ou seja, seu valor como fonte de prova das atividades do órgão produtor. É também aplicável em sistemas híbridos.

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” (e-ARQ Brasil, 2009, p.11).

Sobre os documentos digitais, um SIGAD deve abranger todos os tipos de documentos arquivísticos digitais do órgão ou entidade, como os textos, imagens fixas e em movimento, gravações sonoras, mensagens de correio eletrônico, páginas *web*, bases de dados.

Baseado nestas definições pode-se tecer as seguintes considerações: Um sistema de informação abarca todas as fontes de informação existentes na organização, incluindo o sistema de gestão arquivística de documentos, biblioteca, centro de documentação, serviço de comunicação, entre outros; um GED trata os documentos de maneira compartimentada, enquanto o SIGAD parte de uma concepção orgânica, qual seja, a de que os documentos possuem uma inter-relação que reflete as atividades da instituição que os criou. É diferente do SIGAD, o GED nem sempre incorpora o conceito arquivístico de ciclo de vida dos documentos e, conforme e-ARQ Brasil (2009, p. 11), “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”.

De acordo com e-ARQ Brasil (2009), o SIGAD possui requisitos característicos como captura, armazenamento, indexação e recuperação de todos os tipos de documentos arquivísticos, de todos os componentes digitais deste documento como uma unidade complexa; 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; integração entre documentos digitais e convencionais; foco na manutenção da autenticidade dos documentos; avaliação e seleção dos documentos para recolhimento e preservação daqueles considerados de valor permanente; aplicação de tabela de temporalidade e destinação de

documentos; transferência e recolhimento dos documentos por meio de uma função de exportação e gestão de preservação dos documentos.

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

Conforme o e-ARQ Brasil (2009), o SIGAD deve prever controles de acesso e procedimentos de segurança que garantam a integridade dos documentos. Entre esses procedimentos, destacam-se o uso de controles técnicos e programáticos, diferenciando tipos de documentos, perfis de usuários e características de acesso aos dados e a manutenção de trilhas de auditoria e de rotinas de cópias de segurança. Deve-se levar em conta exigências e procedimentos de segurança da infraestrutura das instalações.

Sobre o controle de acesso o sistema precisa controlar o acesso a documentos por usuário e/ou grupos de usuários. No mínimo o controle de acesso deve garantir as funções de restrição de acesso aos documentos; exibição dos documentos, criptografados ou não, e dos metadados, bem como, uso e intervenção nos documentos somente pelos usuários autorizados.

De acordo com e-ARQ Brasil (2009, p. 40) “os documentos também devem ser analisados com relação às precauções de segurança, ou seja, se são considerados ostensivos ou sigilosos”. Nesse caso, existem regras, normas e legislação que estabelecem diferentes razões e graus de sigilo a serem atribuídos a cada documento, além de definirem as autoridades competentes para fazê-lo.

Conforme e-ARQ Brasil (2009, p. 41), “os documentos relativos ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, como os dossiês funcionais e prontuários médicos, estão sujeitos a restrições de acesso, conforme legislação específica”. O sistema de gestão arquivística deve impedir que usuários não autorizados acessem os documentos sigilosos, previstos em lei, bem como àqueles tidos como originalmente sigilosos. O acesso aos metadados sigilosos depende de regulamentação interna do órgão. E o monitoramento e mapeamento das permissões de acesso devem ser um processo contínuo em todos os sistemas de gestão arquivística de documentos.

O modelo e-ARQ Brasil (2009) afirma que a utilização dos documentos pelos usuários deve ser registrado pelo sistema nos seus respectivos metadados e inclui: a identificação da permissão de acesso dos usuários; a identificação da precaução de segurança e da categoria de sigilo dos documentos; a garantia de que somente os indivíduos autorizados tenham acesso esses documentos sigilosos; o registro de todos os acessos, as tentativas de acesso e o uso dos documentos em todo o processo com identificação de usuário, data hora, e até estação de trabalho se possível e revisão periódica das classificações de acesso a fim de garantir sua atualização.

O e-ARQ Brasil (2009, p. 41) diz que “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 e dos documentos produzidos.

Conforme e-ARQ Brasil (2009, p. 41-42), “a trilha de auditoria é o conjunto de informações registradas que permite o rastreamento de intervenções ou tentativas de intervenção no documento arquivístico digital ou no SIGAD”. A trilha deve registrar o movimento e o uso dos documentos arquivísticos dentro de um SIGAD, informando quem operou, a data e a hora, e as ações realizadas. A mesma tem o objetivo de fornecer informações sobre a aplicação das políticas e regras da gestão arquivística de documentos do órgão/entidade, e serve para: “identificar os autores de cada operação realizada nos documentos; prevenir a perda de documentos; monitorar todas as operações realizadas no SIGAD e garantir a segurança e a integridade do SIGAD”.

Este modelo esclarece que nos procedimentos que exijam prazo a ser cumprido pelo órgão ou entidade, devem ser implementadas ações de rastreamento, de forma que determine os passos a serem dados em resposta às atividades ou ações registradas no documento; atribuir a uma pessoa a responsabilidade por cada ação e registrar a data em que uma ação deve ser executada e a data em que ocorreu.

Com relação às cópias de segurança, o SIGAD deve prever controles para proporcionar a salvaguarda regular dos documentos arquivísticos e dos seus metadados. Também deve poder recuperá-los rapidamente em caso de perda devido a sinistro, falhas no sistema, contingência, quebra de segurança ou

degradação do suporte. Esses mecanismos devem seguir a política de segurança da informação da organização.

O modelo e-ARQ Brasil (2009, p. 42) normatiza que “em sistemas de gestão arquivística de documentos convencionais, pode-se prever a reprodução de documentos em outros suportes como medida de segurança, como, por exemplo, pelos processos de microfilmagem e digitalização”. Nestes sistemas, o SIGAD deve prover meios de realização de cópias de segurança becape (*backup*). Esse processo consiste na realização de cópias periódicas das informações com o propósito de restauração posterior, em caso de perda devido a falhas de *software*, *hardware* ou mesmo de acidentes. O processo reverso ao *backup* é a restauração (*restore*), que consiste em recuperar as informações para o ambiente de produção do SIGAD em um estado consistente. No e-ARQ Brasil (2009, p. 42) “como o objetivo é restaurar o sistema em caso de falhas, as informações não são armazenadas por períodos muito longos (normalmente, até um ano)”. Desse modo, o procedimento de cópias de segurança não pode ser confundido com uma estratégia de preservação de longo prazo.

Sobre à segurança da infraestrutura, o e-ARQ Brasil (2009, p. 42) afirma que “a natureza das medidas de segurança da infraestrutura de instalações do acervo digital diz respeito a requisitos operacionais e não é muito diferente daquela do acervo convencional”. Essas medidas devem considerar esses 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 controlada, e fornecimento estável de energia elétrica. Deve haver controle contínuo para verificar se essas condições estão sendo atendidas:

- equipamentos contra incêndio devem estar presentes em toda a área de instalação e de acordo com as normas de segurança estabelecidas;
- os equipamentos contra incêndio devem ser verificados periodicamente e substituídos antes do término da vida útil prevista;
- o órgão ou entidade tem que prever instalações adequadas de para-raios, com procedimentos de manutenção periódica, seguindo a legislação e as normas técnicas estabelecidas;
- a área reservada à instalação do SIGAD deve ser compartimentada, com o objetivo de controlar o acesso às informações;
- as salas de computadores servidores são de uso exclusivo de pessoal autorizado e devem ter controle eletrônico de acesso;
- para acesso a áreas de segurança, identificações e credenciais de segurança têm de estar de acordo com as atribuições individuais e as regras de segurança do órgão ou entidade (e-ARQ Brasil 2009, p. 43).

### 3.1.2 Armazenamento

Conforme e-ARQ Brasil (2009, p. 43), “as considerações e ações relativas ao armazenamento dos documentos arquivísticos convencionais e digitais permeiam todo o seu ciclo de vida”. Esse armazenamento deve garantir a autenticidade e o acesso aos documentos pelo tempo estipulado na TTD. Documentos de valor permanente, independente do formato, requerem um armazenamento criterioso desde o momento da sua produção, para garantir sua preservação no longo prazo.

Num cenário híbrido devem-se considerar requisitos de armazenamento que atendam igualmente às necessidades desses dois tipos de documentos. As condições de armazenamento têm de levar em conta o volume e as propriedades físicas dos documentos. Devem ser projetadas considerando também a proteção contra acesso não autorizado e perdas por destruição, furto e sinistro.

De acordo e-ARQ Brasil (2009, p. 43-45), 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 especificar as mudanças ocorridas nos sistemas e nos formatos dos documentos.

Os fatores mais importantes selecionados das opções de armazenamento são: volume e estimativa de crescimento dos documentos – este fator deve ser levado em conta para se avaliar a capacidade de armazenamento; segurança dos documentos – as instalações de armazenamento correspondentes aos depósitos, arquivos, e computadores, deverão prever a limitação de acesso aos documentos; características físicas do suporte e do ambiente – fatores como tipo de suporte, peso, grau de contaminação do documento e do ambiente, temperatura e umidade influenciam a adequação das condições de armazenamento; frequência de uso – o uso mais ou menos freqüente dos documentos deve ser levado em conta na seleção das opções de armazenamento; custo relativo das opções de armazenamento dos documentos – além do custo dos dispositivos de armazenamento, devem ser considerados, para sua manipulação, os valores dos equipamentos e do *software* de controle. Pelo previsível alto custo, pode-se considerar a possibilidade de terceirização do armazenamento.

Os documentos digitais são armazenados em dispositivos eletrônicos, magnéticos e ópticos. Conforme o e-ARQ Brasil (2009, p. 44), “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; e memória terciária”. A memória primária é essencial a qualquer sistema computacional. É nela que *software* e dados são armazenados durante a execução. Representam essa classe as memórias RAM (*random access memory*), extremamente rápidas. A memória secundária apresenta volume maior de armazenamento que a primária, sendo, porém, mais lenta e não é volátil. São os discos rígidos magnéticos (*hard disk*, HD), que podem ser usados isolados ou combinados em *disk arrays*. A memória terciária compreende fitas magnéticas, discos ópticos e outros. No uso, incluem armazenamento do acervo digital e cópias de segurança, também denominada mídias de armazenamento. As memórias secundárias e terciárias são adequadas ao armazenamento.

### 3.1.3 Preservação

Quanto à preservação, os documentos arquivísticos têm de se manter acessíveis e utilizáveis pelo tempo que for necessário, garantindo, dessa forma, sua longevidade, funcionalidade e acesso contínuo.

O e-ARQ Brasil (2009) salienta que devem ser asseguradas as características dos documentos, tais como autenticidade e acessibilidade, pela adoção de estratégias institucionais e técnicas proativas de produção e preservação que garantam sua perenidade. As estratégias necessárias são estabelecidas por uma política de preservação.

O e-ARQ Brasil (2009, p. 45), afirma que, tradicionalmente, a preservação de documentos arquivísticos concentra-se na obtenção da estabilidade do suporte da informação. Nos documentos convencionais, conteúdo e suporte estão intrinsecamente ligados, de modo que a manutenção do suporte garante a preservação do documento. Já nos documentos digitais, o foco da preservação é a manutenção do acesso, que pode implicar mudança de suporte e formato, bem como atualização do ambiente tecnológico. “A fragilidade do suporte digital e a

obsolescência tecnológica de *hardware*, *software* e formato exigem intervenções periódicas”.

De acordo e-ARQ Brasil (2009), as estratégias de preservação devem ser selecionadas com base na sua capacidade de manter as características desses documentos e na avaliação custo-benefício. Ainda se inclui monitoramento e controle ambiental, restrições de acesso, cuidados no manuseio direto e obtenção de suportes e materiais mais duráveis. Especificamente, nos documentos digitais, essas estratégias incluem a prevenção da obsolescência tecnológica e de danos físicos ao suporte, por meio de procedimentos de migração, como atualização (*refreshing*) e conversão. Há outras técnicas utilizadas na preservação de documentos digitais que são emulação, encapsulamento e preservação da tecnologia. A adoção de formatos digitais abertos configura-se, adicionalmente, como medida de preservação recomendável e necessária.

Qualquer estratégia de preservação adotada é preciso documentar os procedimentos e as estruturas de metadados. O desenvolvimento de novas tecnologias pode tornar disponíveis outros procedimentos para preservar documentos digitais por longos períodos.

No e-ARQ Brasil, (2009, p. 46), “as estratégias de preservação de documentos digitais e dos respectivos metadados devem ser formuladas e integradas ao SIGAD desde a fase de elaboração do projeto do sistema”. Dessa forma, será possível garantir o uso e o acesso aos documentos digitais durante todo o período previsto para sua guarda.

### **3.2 O modelo SAAI 2007**

O grande crescimento dos recursos computacionais, espaço internet e conectividade originaram um progresso no número de comunidades e organizações que disponibilizam informação digital em todas as áreas, para facilitar o uso destas tecnologias pelas pessoas, onde esses espaços satisfazem condições de acessibilidade a todos.

Atualmente, transações entre qualquer tipo de organizações são dirigidas usando, como meio de transmissão, o recurso digital, ao invés do tradicional papel.



Estas inovações causam grandes problemas no que tange à preservação de informação digital e para algumas organizações que, no seu planejamento de formação não foram desenhadas para desempenhar a tarefa de gerenciar a informação, ou seja, tratar da catalogação e registro da mesma.

Os especialistas da área que trabalham com informação em formatos digitais estão preparando normas necessárias para armazenar e compartilhar de modo adequado esses materiais, bem como, buscam a formulação de políticas institucionais de preservação para os documentos em formato digital, para que estes continuem a serem utilizados, em longo prazo, como fontes de informações confiáveis.

O modelo para repositórios de metadados de preservação bastante usado atualmente é o modelo de referência *Open Archival Information System* (OAIS), publicado pelo *Consultive Committee for Space Data Systems* (CCSDS) da ISO (*International Organization for Standardization*) como padrão em junho de 2003. ABNT adotou o padrão ISSO também para o Brasil lançando em 2007 a Norma NBR 15472, onde o OAIS foi traduzido como Sistema Aberto de Arquivamento de Informação (SAAI). A NBR 15472 define um modelo de referência em alto nível para organizações e pessoas que tem informação e precisam de uma preservação de longo prazo, bem como para as organizações que adquirem tais informações. No restante do texto, vai ser usado a denominação SAAI e não OAIS.

### 3.2.1 Aplicabilidade do modelo

Esse modelo pode ser aplicado a qualquer arquivo, mas ele é de interesse para as organizações com responsabilidade de tornar a informação disponível por longo prazo e também para aquelas organizações e indivíduos que produzem informação passível de preservação longa e aos interessados em obter informações desses arquivos. Conforme a Norma NBR 15472 (ABNT, 2007, p. VII). “Implementações reais podem agrupar ou desdobrar as funcionalidades de forma diferente”. O modelo de referência SAAI não define, ou exige um método específico de implementação desses conceitos.

Segundo Arellano (2004), originalmente era aplicado apenas para informações digitais obtidas de observações de ambientes espaciais e da Terra. Atualmente é aplicável a qualquer tipo de arquivo digital e compatível com os sistemas baseados no protocolo do mesmo. Um arquivo baseado no SAAI significa considerar os arquivos como organizações de pessoas e sistemas, que aceitaram a responsabilidade de preservar a informação e torná-la disponível da melhor forma, para obter boa comunicação e produtividade entre as diferentes comunidades.

Conforme a NBR 15472 (ABNT, 2007), o modelo SAAI possui várias responsabilidades, e entre elas identificam-se as mínimas que devem ser assumidas; embora nem todas sejam aplicadas a todos os SAAI. Aqui se destacam as essenciais para que uma organização possa operar este modelo:

- a) negociar com o produtor sobre a aceitação adequada de informações vinda do mesmo como, por exemplo, os critérios: tipo, assunto, fonte, originalidade, mídias, etc.;
- b) obter controle suficiente da informação fornecida para garantir a preservação de longo prazo, exemplo: propriedade do objeto físico x propriedade intelectual, acordo de transferência, etc.;
- c) determinar, por si mesmo ou em conjunto com outros parceiros, quais devem ser as designadas comunidades e, portanto, capacitadas a entenderem a informação fornecida;
- d) assegurar que a informação a ser preservada seja compreensível aos usuários de forma independente, ou seja, sem auxílio ou assistência dos especialistas que produzem a informação;
- e) seguir políticas e procedimentos documentados que garantam que a informação seja preservada contra todas as contingências, e possibilitar que a informação seja disseminada como cópia autêntica do original ou rastreável até o original e;
- f) tornar a informação preservada disponível para a designada Comunidade.

O SAAI é um modelo de referência ISO – *International Organization for Standardization*; de longo prazo e aberto. “Abrir no SAAI” significa que é usado para dizer que a presente recomendação e as futuras relacionadas com normas são desenvolvidas em fóruns abertos, e isso não implica que o acesso ao arquivo é ilimitado, e com garantias de confiabilidade.

O modelo de referência tem como propósito importante facilitar uma compreensão mais ampla do que é necessário para preservar e acessar informação por longo prazo. É também reconhecido como o trabalho conceitual mais relevante de um sistema voltado para a preservação digital.

No esquema conceitual do SAAI, atuam quatro entidades que são: o produtor, a administração, o consumidor e o arquivo propriamente dito.

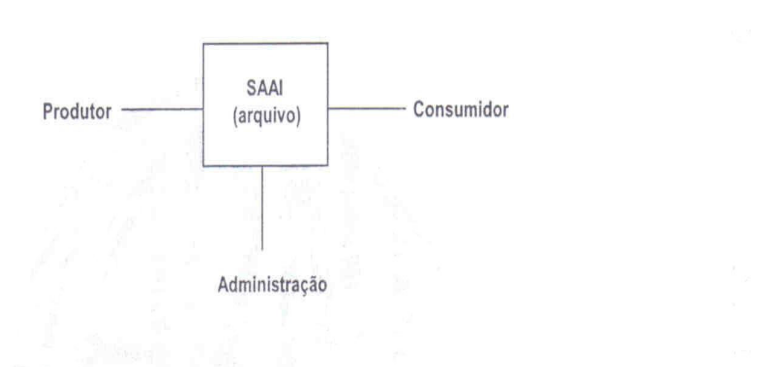


Figura 3 – Modelo do ambiente SAAI

Fonte: ABNT NBR 15472:2007

Os produtores são pessoas ou sistemas clientes que fornecem a informação a ser preservada. A administração é a entidade responsável que contém os serviços e funções necessárias para controlar o funcionamento das outras entradas e o estabelecimento das políticas gerais dentro de um domínio maior de políticas para o sistema de arquivo. Os consumidores são pessoas ou sistemas-cliente que interagem com os serviços do SAAI, preservando informações de interesse e capazes de compreender a informação preservada e acessar essa informação e o arquivo que é o próprio órgão.

Este modelo, a partir dessas entidades, é desdobrado em seis entidades funcionais e interfaces associadas, no entanto, somente os fluxos principais de informação estão representados a seguir.

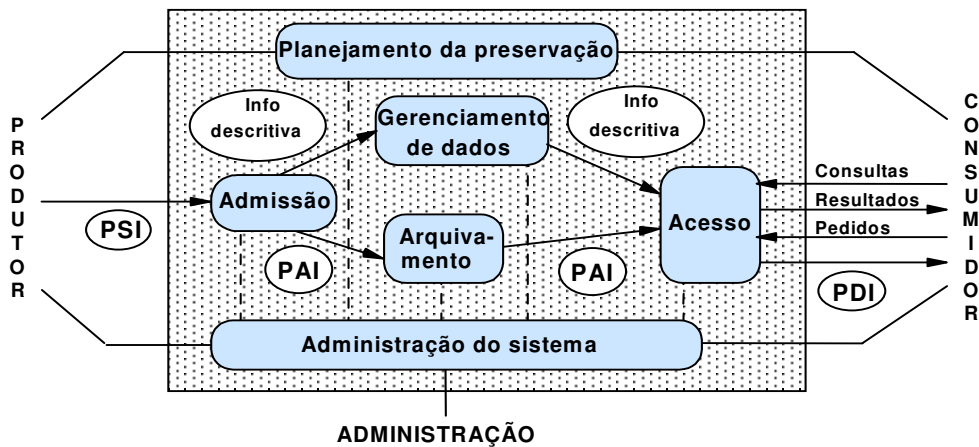


Figura 4 – Entidades funcionais do SAAI

Fonte: ABNT NBR 15472:200

Conforme a NBR 15472 (ABNT, 2007), a entidade **Admissão** é responsável pela aceitação de Pacotes de Submissão de Informação (PSI) dos produtores (ou de componentes internos sob controle da administração do sistema) e preparação dos conteúdos para arquivamento e gerenciamento. Os processos desta entidade envolvem receber PSI, verificar a qualidade dos PSI, gerar os Pacotes de Arquivamento de Informação (PAI), de acordo com a formatação de dados e padrões de documentação, extrair informação descritiva dos PAI para inclusão no banco de dados e coordenar as atualizações nas entidades arquivamento e gerenciamento de dados.

A entidade **Arquivamento** oferece serviços e processos para arquivar, manter e recuperar PAI. Estas responsabilidades envolvem receber PAI da entidade admissão e adicioná-los na área permanente conforme os critérios, gerenciar a hierarquia da área de armazenamento, renovar as mídias, executar rotinas de verificação de erro, oferecer capacidade de recuperação de desastre e fornecer cópias de PAI solicitado à entidade acesso para atender pedidos.

A entidade **Gerenciamento de Dados** oferece serviços e processos necessários para incluir, manter e acessar tanto a informação descritiva, que identifica e documentam os conteúdos do arquivo, quanto os dados administrativos usados para gerenciá-lo. Os processos desta entidade envolvem administrar as funções do banco de dados (manter as definições de esquemas e de visões e a

integridade referencial), executar atualizações (carrega nova informação descritiva ou dados administrativos do arquivo), processar as consultas sobre os dados de gerenciamento para gerar resultados e produzir relatórios.

A entidade **Administração do Sistema** gerencia a rotina operacional do arquivo como um todo. Suas funções incluem solicitar e negociar acordos de submissão com produtores, auditar submissões para garantir que atendem aos padrões e manter o gerenciamento da configuração do *hardware* e *software* do sistema. Oferece processos de Engenharia de sistema para monitorar e melhorar as operações e inventariar, emitir relatórios e atualizar os conteúdos por meio de migração/atualização de seus conteúdos. É responsável também por estabelecer e manter os padrões e políticas do arquivo, fornecer apoio ao cliente e ativar solicitações pendentes.

A entidade **Planejamento de Preservação** oferece serviço e processo para monitorar o ambiente e fornecer recomendações para garantir que a informação armazenada permaneça acessível por longo prazo à comunidade/alvo, mesmo que o ambiente computacional original torne-se obsoleto. Suas funções envolvem avaliar os conteúdos do arquivo e recomendar periodicamente atualizações da informação arquivada para migrar os conteúdos e desenvolver recomendações para padrões e políticas do arquivo e monitorar as mudanças no ambiente tecnológico, nas demandas de serviço e na base de conhecimento da comunidade/alvo. Esta entidade projeta gabaritos de PI e oferece assistência e revisão de projeto para adaptar esses gabaritos em PSI e PAI para submissões específicas. É responsável pelo desenvolvimento de planos detalhados de migração, protótipos de *software* e planos de teste para permitir a implementação das metas de migração da entidade Administração do Sistema.

A entidade **Acesso** oferece serviços e processos para apoiar os consumidores na determinação da existência, descrição, localização e disponibilidade da informação armazenada e permitir que os consumidores solicitem e recebam produtos de informação. Suas funções incluem comunicar com os consumidores para receber solicitações, aplicar controles para limitar o acesso à informação especificamente protegida, coordenar a execução de solicitações, para que se completem com sucesso, gerar respostas (pacotes de disseminação de informação, resultados, relatórios) e entregar as respostas aos consumidores.

Além das entidades descritas, as aplicações da computação assumem serviços comuns que servem de apoio, tais como comunicação entre processos, serviços de nome, alocação de memória temporária, tratamento de exceção, segurança e serviços de diretório, devem estar disponíveis e esses serviços constituem outra entidade funcional neste modelo; mas, como é muito extensa e para maior clareza, não foi apresentada na figura 4.

Sobre a aplicação do OAIS, a autora Innarelli refere que:

A aplicação do OAIS em arquivos consiste na organização de pessoas e sistemas, tendo como responsabilidade a preservação e o acesso da informação a comunidade interessada e como foco principal a informação digital, as formas primárias de armazenamento e suporte da informação para os materiais de arquivos digitais e físicos (INNARELLI, 2006, p. 10).

No esquema do SAAI, está incluído um modelo de informação para inserção dos metadados de preservação.

No modelo, objeto físico e objeto digital podem ser referenciados juntos como objetos de dados. Eles são interpretados pela combinação da base de conhecimento da comunidade e a informação de representação associada ao objeto de dados. O objeto de dados pode ser complementado com informação de representação, para ser bem entendido pela comunidade alvo.

Conforme Ferreira (2006), o modelo de referência SAAI constitui um ponto de partida para a discussão sobre a necessidade de criar um conjunto de elementos de metainformação capazes de dar suporte às atividades relacionadas com a preservação digital. Após isso, diversas instituições vieram propor modelos de metadados de preservação que refletem as necessidades individuais dos projetos em que estão ou estiveram envolvidas. O mesmo autor assevera que:

A metainformação de preservação tem como objetivo descrever e documentar os processos e actividades relacionadas com a preservação de materiais digitais. Ou seja, a metainformação de preservação é responsável por reunir, junto ao material custodiado, informação detalhada sobre a sua proveniência, autenticidade actividades de preservação, ambiente tecnológico e condicionantes legais (FERREIRA 2006, p. 54).

Em 2002, o consórcio Online Computer Library Center e Research Libraries Group (OCLC/RLG) consolidou este conhecimento acumulado num único documento onde se enumeraram as diversas classes de informações que deverão estar presentes num esquema de metainformação de preservação.

### 3.2.2 Informação no SAAI

Uma definição clara de informação é fundamental para preservação da informação no SAAI; para informação digital significa que o SAAI deve identificar claramente os *bits* e a Representação da Informação que se aplica a esses *bits*.

A Informação de Representação existe de duas formas: objeto físico, como por exemplo: rocha lunar e objeto digital, onde o exemplo é seqüência de *bits*.

Conforme a NBR 15472 (ABNT, 2007), a informação é qualquer forma de conhecimento passível de intercâmbio, esta informação é representada por meio de algum tipo de dado, exemplo a informação em um livro impresso é característico que é expresso por caracteres observáveis e combinados com o conhecimento da linguagem utilizada são convertidos em informações mais significativas. Se o receptor não entende inglês em sua base de conhecimento, precisará de um dicionário, tradutor ou um formato compreensível por seu conhecimento.

A Base de Conhecimento é uma pessoa ou sistema que possui um conjunto de informações que permite que compreendam a informação recebida.

A interpretação do Objeto de Dados é como uma informação significativa pela designada Comunidade, sendo obtida por meio da combinação da base de conhecimento dessa comunidade e a informação de representação associada ao Objeto de Dado.

Pode-se dizer de modo geral que o dado interpretado, usando sua Informação de Representação, produz informação chamada de Objeto de Informação, conforme a figura a seguir.

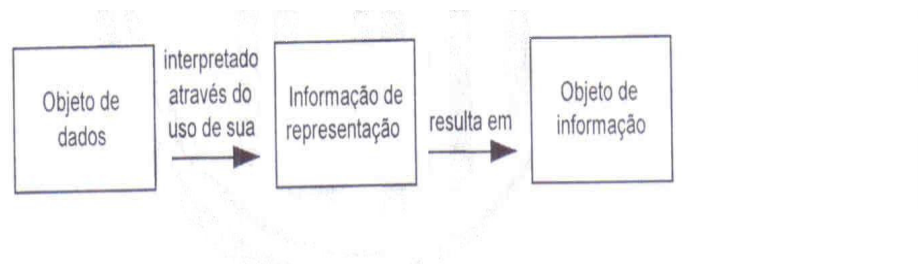


Figura 5 – Obtenção de informação a partir de dados

Para um Objeto de Informação ser preservado com sucesso é crítico para um SAAI identificar e compreender claramente o Objeto de Dados e a sua Informação de Representação. Isto é um desafio importante para a preservação digital, porque conforme a Norma deve tomar a decisão em manter a informação de representação ou manter uma quantidade maior de consumidores com conhecimento menos especializado. “Ao longo do tempo, a evolução da base de conhecimento da comunidade/alvo pode exigir atualizações da informação de representação para continuar garantido o entendimento” NBR 15472 (ABNT, 2007, p. 10).

A NBR 15472 (ABNT, 2007, p. 43) define o pacote de informação como: “A estrutura conceitual que apóia a preservação por longo prazo de informação é o pacote de informação”. Um pacote de informação é um recipiente conceitual de dois tipos de informação:

- a) informação de Conteúdo é a informação original da preservação, consistindo no Objeto de Dados de conteúdo, isto é, os *bits* e a sua Informação de Representação associada. O pacote resultante pode ser encontrado pela informação descritiva. O conteúdo da informação é que é a informação a qual é o objetivo inicial da preservação. A informação de Empacotamento é a informação usada para juntar e identificar os componentes de um Pacote de Informação de conteúdo à IDP e a informação Descritiva é aquela informação usada pelo gerenciamento de dados para apoiar os processos de localização, ordenação e recuperação de informação de conteúdo de interesse do usuário;
- b) informação de Descrição de Preservação aplica-se à informação de conteúdo necessária para preservar de forma adequada a Informação de Conteúdo à qual está associada, garantindo sua identificação e entendendo o ambiente em que o conteúdo informação foi criado. Dividem-se em quatro tipos as informações de preservação que são os seguintes:
  - Proveniência – descreve a fonte da informação de conteúdo, quem teve sua custódia desde sua origem e seu histórico, inclusive os de processamento;
  - Contexto – descreve a informação de conteúdo e relaciona-se com as informações fora do pacote de informação. Podendo descrever porque a



informação de conteúdo foi produzida e como se relaciona com objeto de informação de conteúdo disponível;

- Referência – fornece um ou mais sistemas de identificação, que permite que a informação de conteúdo seja identificada de forma única, exemplo a identificação no sistema; identificação global ou descrição do recurso e;
- Permanência ou fixidez – fornece proteção à informação de conteúdo contra a alteração não documentada.

### **3.3 Comparação entre os modelos e-ARQ Brasil (2009) e SAAI (2007)**

Esta seção realiza uma comparação do modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-ARQ Brasil 2009) com o Sistema Aberto de Arquivamento de Informação (SAAI 2007).

O e-ARQ Brasil (2009, p.12), “deve ser utilizado para desenvolver um sistema informatizado ou para avaliar um já existente, cuja atividade principal seja a gestão arquivística de documentos”. Ele é aplicável aos sistemas que produzem e mantêm somente documentos digitais e aos que compreendem documentos digitais e convencionais. Para os documentos convencionais, o sistema inclui apenas o registro das referências nos metadados, e para os digitais o sistema inclui os próprios documentos. Desta forma, o e-ARQ pode ser utilizado no setor público ou privado de qualquer esfera e âmbito de atuação, servindo para diferentes tipos de documentos arquivísticos. 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.

Já o modelo SAAI aplica-se a qualquer arquivo, mas mais especificamente as organizações com responsabilidade de tornar a informação preservada e disponível por longo prazo. Ele não especifica um projeto ou uma implementação. Pode agrupar ou desdobrar as funcionalidades de forma diferente. O termo aberto significa que, atualmente e no futuro, as recomendações e padrões relacionados

sejam desenvolvidos em fóruns abertos. É um sistema encarregado de preservar por longo prazo e manter o acesso à informação digital de qualquer natureza.

Apesar de o modelo SAAI reconhecer os dois tipos de objetos (físico e digital), sua atenção está voltada para o objeto digital. Diferentemente, no e-ARQ Brasil (2009, p. 12), os objetivos do SIGAD são: “orientar a implantação da gestão arquivística de documentos arquivísticos digitais e não digitais; fornecer especificações técnicas e funcionais, além de metadados”, com a finalidade de orientar a aquisição e/ou a especificação e o desenvolvimento de sistemas informatizados de gestão arquivística de documentos. Neste sentido, o e-ARQ é mais amplo do que o SAAI.

Da norma, observa-se que o principal objetivo do modelo SAAI (2009, p. 8) “é possibilitar maior compreensão daquilo que é necessário para preservar e acessar informação por longo prazo”. Neste sentido, o SAAI define um sistema que executa funções de preservação e de acesso à informação por longo tempo e oferece linguagem padronizada para a comunidade/alvo, conforme seus requisitos.

Observa-se também que enquanto o e-ARQ Brasil está dividido em 14 classes que se desdobram com descrições bem específicas, o SAAI admite apenas seis entidades que agrupam os seus requisitos de forma genérica.

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. Ele pode ser utilizado para desenvolver um sistema informatizado ou para avaliar um já existente e também em sistemas que possuem documentos digitais e convencionais, porém para os documentos digitais os registros incluem apenas as referências nos metadados, já no caso dos documentos digitais o sistema consta dos próprios documentos. Destina-se aos documentos relativos às atividades-meio e às atividades-fim da organização e não se restringe a um ramo de atividade específica.

As seis entidades funcionais SAAI gerenciam o fluxo de informação entre os produtores e o arquivo e entre o arquivo e os consumidores. Em conjunto, identificam os processos-chave, típicos da maioria dos arquivos dedicados a preservação de informação digital. O arquivo digital deverá provavelmente conter componentes funcionais similares aqueles descritos, embora cada implementação específica tenha suas peculiaridades.

Os dois modelos visam à preservação e o acesso aos documentos digitais produzidos por organizações públicas, privadas ou outras. Mas o e-ARQ Brasil foca a gestão como um todo e o SAAI visa mais a preservação digital por longo tempo em repositório. Infere-se assim que ambos os modelos e seus sistemas atendem bem as demandas que surgiram com a evolução tecnológica e os novos suportes em que se encontram as informações, possibilitando assim a preservação, a autenticidade, e o acesso às informações com segurança. Porém, o e-ARQ Brasil foca a gestão arquivística como um todo e o SAAI visa à preservação digital por longo tempo em repositório digital.

Considerando as similaridades entre os modelos e o regulamento que foi elaborado pela CTDE do CONARQ, que recomenda através da Resolução n. 25/2007-CONARQ a adoção do Modelo e-ARQ pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos – SINAR, ao qual a UFSM faz parte, adotou-se para este trabalho o modelo de requisitos e-ARQ Brasil, que é mais amplo e atende as expectativas da UFSM.



## 4 METODOLOGIA

Nesse capítulo, será abordada a metodologia utilizada na pesquisa, sendo descritos os métodos, técnicas e abordagem de pesquisa, bem como a forma de coleta, observação e análise de dados.

As escolhas para o desenvolvimento deste trabalho são de fundamental importância, pois servirão de base para uma implementação eficiente do Diário de Classe da UFSM. Pretende-se, com este estudo, também apresentar uma contribuição teórico/prática para a gestão, preservação e segurança da informação nos documentos arquivísticos digitais por meio da análise de mecanismos e subsídios existentes.

Esta pesquisa é de natureza aplicada, objetivando gerar conhecimento para aplicação prática dirigida à solução de problemas específicos. É de abordagem qualitativa e, conforme Minayo (2003), responde a questões muito particulares; e nas ciências sociais se preocupa com um nível de realidade que não pode ser quantificado. É descritiva, portanto, os pesquisadores tendem a analisar seus dados indutivamente, o processo e seu significado são os focos principais de abordagens.

Com relação à pesquisa qualitativa, Poupart et al., (2010, p. 130), afirma que “entretanto, ela é, a maior parte do tempo, completa em si mesma, e não tem obrigatoriamente necessidade de ser continuada por outros pesquisadores, por meio de outras técnicas”.

Nas palavras de Charmaz (2009, p. 10): “refiro-me aos materiais com os quais trabalhamos como “dados” e não como materiais ou relatos, pois a pesquisa qualitativa ocupa um lugar na investigação científica por seus próprios méritos”. Segundo ela (2009), esses dados são construídos por meio das nossas observações, das interações e dos materiais reunidos sobre o tópico ou o ambiente. Estudam-se experiências e os eventos empíricos, seguindo as nossas intuições e idéias analíticas potenciais sobre os mesmos.

Minayo (2003, p. 22) afirma que “o conjunto de dados quantitativos e qualificativos, porém não se opõem. Ao contrário se complementam, pois a realidade abrangida por eles interage dinamicamente excluindo qualquer dicotomia”.

Tendo em vista os objetivos propostos, foi realizado estudo exploratório analítico, combinado com análise documental, a partir de informações encontradas nas revisões de literaturas disponíveis em livros, artigos, legislação e outros referentes ao assunto disponibilizado na Internet.

O método exploratório proporciona maior familiaridade com o problema, tornando-o mais explícito a construção de hipóteses. Conforme Gil (2002, p. 45), “têm como objetivo principal o aprimoramento de idéias ou a descoberta de intuições”. Seu planejamento é flexível, de modo que possibilita a consideração dos vários aspectos relativos ao fato estudado. Sobre o assunto, Minayo (2003, p. 26) afirma que “seu foco fundamental é a construção do projeto de investigação”.

Charmaz (2009, p. 31) diz que “a flexibilidade da pesquisa qualitativa permite ao pesquisador seguir as indicações que vão surgindo”. Os métodos da teoria fundamentada aumentam essa flexibilidade e, portanto, oferecem mais foco ao pesquisador do que outros métodos.

Para Marconi e Lakatos (2005), a pesquisa bibliográfica tem a finalidade de colocar o pesquisador para o contato direto com tudo aquilo que já foi escrito sobre um determinado tema, permitindo a definição de linhas de ação para abordar o assunto e gerar novas idéias para discussão.

A pesquisa bibliográfica abrangeu as leituras recomendadas nas disciplinas cursadas no Programa de Pós-Graduação em Engenharia de Produção (PPGEP), também pelo professor Orientador e obras relevantes na área de Arquivologia e Segurança da Informação, modelos de referência e-ARQ Brasil e OAIS (Open Archive Information System) – SAAI, para gestão arquivística de documentos, legislação do Conselho Nacional de Arquivos (CONARQ) e outras como a Lei de Diretrizes e Bases (LDB), o Estatuto e o Regimento Geral da UFSM, principalmente no que se refere ao Diário de Classe. Foram consultadas produções acadêmicas como artigos, dissertações e teses. O recurso da Internet foi utilizado para verificar os sítios do Arquivo Nacional, Associação Arquivística Brasileira (AAB), UFSM, CONARQ, Conselho Internacional de Arquivos (CIA) entre outros e para troca de mensagens eletrônicas.

A análise documental, como técnica de pesquisa de dados qualitativos, foi utilizada para complementar as informações obtidas por outros meios e também para identificar informações factuais nos documentos relacionados a questões ou hipóteses de interesse. Esta técnica traz vantagens como o fato dos documentos

constituírem pontos estáveis e ser de baixo custo onde requer apenas tempo e atenção na análise. Conforme Minayo (2003, p. 26), “essa etapa combina entrevistas, observação, levantamento de material documental, bibliográfico, instrucional, etc.”. Poupart et al., (2010, p. 140) confirma que “desejando vivamente recolher o máximo de informações pertinentes, os pesquisadores combinam, usualmente, várias dessas técnicas”.

De acordo com Glaser (2002 apud CHARMAZ 2009, p. 33), “tudo são dados. Sim, tudo o que você descobre no(s) ambiente(s) de pesquisa ou sobre o seu tema de pesquisa pode servir como dados”. Porém, eles variam na qualidade, na relevância dos interesses emergentes e na utilidade para a interpretação. Os pesquisadores variam em relação à suas capacidades de discernimento de dados úteis e nas e eficácias para registrá-los.

A primeira etapa, do estudo teve como objetivo a pesquisa bibliográfica; após a pesquisa da legislação sobre o Diário de Classe e a partir do momento em que esta foi realizada surgiu a idéia/necessidade de sugerir uma proposta de alteração no Regimento Geral da UFSM, com relação ao documento Diário de Classe (frequência e nota), a qual foi aceita pela Pró-Reitoria de Graduação (PROGRAD) e encaminhada ao Conselho Universitário para apreciação e aprovação.

Na segunda etapa foi realizado um estudo dos padrões e normas, nacionais e internacionais, de metadados para gestão documental, sendo priorizadas as funções de gestão, preservação e difusão dos documentos com segurança, objetivando desenvolver um modelo conceitual de metadados e requisitos do sistema de arquivo, para trazer a gestão, preservação e segurança da informação ao documento Diário de Classe.

Após analisados o e-ARQ Brasil – Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos e o Modelo de Referência OAIS (Open Archive Information System)/SAAI, adotou-se o modelo de requisitos e-ARQ Brasil 2009, baseado no regulamento que foi elaborado pela Câmara Técnica de Documentos Eletrônicos do Conselho Nacional de Arquivos – CONARQ, que recomenda através da Resolução n. 25, de 27 de abril de 2007/CONARQ, a adoção do Modelo pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos – SINAR, ao qual a UFSM faz parte.

Foram utilizados, nesta pesquisa, fontes primárias e bibliográficas e um diagnóstico realizado por meio de apontamentos de reuniões, observação direta,

visitas e entrevistas. Conforme Minayo (2003), o trabalho de campo que consiste no recorte empírico da construção teórica elaborada no momento.

As consultas de fontes primárias, sobre a origem, produção, geração e preservação do Diário de Classe foram realizadas no Departamento de Arquivo Geral (DAG), Pró-Reitoria de Graduação (PROGRAD), Departamento de Registro e Controle Acadêmico (DERCA) e em alguns Departamentos Didáticos, todos pertencentes à UFSM.

Na terceira etapa iniciaram as reuniões com o DERCA e o Centro de Processamento de Dados (CPD) para investigar a origem/geração deste documento tendo os questionamentos iniciais: A produção onde ocorre? Quem é o responsável pelo preenchimento e pelo armazenamento? Bem como diagnosticar os problemas existentes no modelo atual. A partir do conhecimento da realidade que envolve o Diário de Classe, procurou-se possíveis alternativas como forma de solução e melhoria para propor um modelo, visando sua gestão, preservação e acesso com segurança das informações.

A quarta etapa, visou à coleta de informações referentes ao documento onde foram realizadas visitas e entrevistas com alguns secretários nas secretarias dos Departamentos Didáticos, para obter mais informações sobre o Diário e observar como está o arquivamento, a conservação/preservação e a segurança dos mesmos.

Finalmente, foram determinados os metadados para o documento Diário de Classe, conforme os requisitos do modelo e-ARQ Brasil a fim de propor um modelo eletrônico para o Diário de Classe da UFSM. Foi especificado cada elemento e seus relacionamentos conforme o modelo sugerido e também foi elaborado um quadro com todos os itens recomendados para o Diário de Classe, em apenso.



## **5 O DIÁRIO DE CLASSE NA UFSM**

Este capítulo apresenta uma análise e discussão sobre a legislação e a utilização do Diário de Classe na UFSM. Para isso, foram utilizadas as informações coletadas durante a pesquisa e analisada a legislação e os modelos de referência.

### **5.1 Legislação sobre o Diário de Classe**

A Universidade Federal de Santa Maria (UFSM), com sede na cidade de Santa Maria, Estado do Rio Grande do Sul, criada pela Lei n. 3834-C, de 14 de dezembro de 1960, é uma Instituição Federal de Ensino Superior (IFEs), constituída como autarquia educacional de regime especial e vinculada ao Ministério da Educação.

Em seu Estatuto (1996, p. 4) define-se que “a organização e o funcionamento da Universidade reger-se-á pela legislação federal pertinente e pelas disposições constantes dos documentos legais”, possibilitando assim a legislação sobre o Diário de Classe.

A saber, têm-se as seguintes legislações: a Lei n. 9.394, Diretrizes e Bases da Educação Nacional, promulgada em 20 de dezembro de 1996; o Estatuto, que regulamenta a estrutura e formulações básicas; o Regimento Geral, que regula, a partir do Estatuto, todos os aspectos comuns da vida universitária; os Regimentos complementares do Regimento Geral, quanto às características próprias dos Órgãos e das Unidades Universitárias; e as Resoluções dos Conselhos Universitários e de Ensino, Pesquisa e Extensão. Nesta legislação, nenhuma referência foi feita ao Diário de Classe.

Por outro lado, a partir do conhecimento do documento Diário de Classe e pesquisa sobre o mesmo, pode-se definir diário de classe como instrumento de registro de atividades relativas ao processo ensino-aprendizagem, contendo informações essenciais sobre a frequência, desempenho dos alunos, conteúdo lecionado e também o registro da frequência do professor.

Responsáveis pelos registros escolares, os estados costumam regular o preenchimento dos registros. Conforme o Decreto n. 18.590, de 18 de março de 1987, publicado no Diário Oficial n. 14.534, de 19 de março de 1987, parte I, página 4, do Estado do Ceará – Fortaleza, que dispõe sobre registro de presença e dá outras providências, em seu art. 3º, § 10: “os professores farão o registro de presença no diário de classe”. Como não poderia deixar de ser, entende-se que o professor é o responsável pelo preenchimento do Diário de Classe ou seu substituto legal.

Assegurados o registro da frequência e do aproveitamento do aluno, na forma do regulamento, a disponibilização desses dados fica a critério da instituição escolar bem como sua guarda no Arquivo da unidade escolar.

Baseado na autonomia universitária, consta no Regimento Geral da UFSM (1988), publicado no Diário Oficial da União, de 02/01/1989, na seção II – Dos Departamentos, no art. 90, que ao Departamento Didático compete: no item I – (p. 29) “elaborar seus planos de trabalho e a parte que lhe competir no plano geral de atividades da Universidade”. Define-se que no art. 91, item IV, aos chefes dos Departamentos Didáticos incumbe entre outros “coordenar e supervisionar as atividades do departamento e suas dependências” bem como item X “examinar, decidindo em primeira instância, as questões suscitadas pelos corpos docente, discente e administrativo”, e no item XXIV – (p. 30) “cumprir e fazer cumprir as disposições do Estatuto e dos Regimentos, as decisões dos órgãos deliberativos da Universidade e da legislação concernente ao ensino”.

Continuando neste regimento, na Seção IV – Da matrícula, no art. 124, (p. 37) “Haverá dois tipos fundamentais de matrícula: matrícula por disciplina e matrícula no Curso/Trancamento Total”.

Na sequência, no art. 125 – (p. 37): “a matrícula será feita semestralmente junto à Coordenação do Curso nos períodos estabelecidos no Calendário Escolar devidamente aprovado no CEPE”.

E a seguir, no art. 128 – (p. 37): “semestralmente será publicado, através do DERCA/PROGRAD, o Guia de Matrícula contendo: a) informações gerais e procedimentos para realização das matrículas; b) normativas gerais de matrícula; c) informações gerais sobre o Sistema Acadêmico”.

Na seção V – Da frequência, no art. 129 – (p. 37): “a frequência às aulas teóricas, aulas práticas, seminários e qualquer outra atividade escolar é obrigatória e permitida somente a alunos regularmente matriculados”.

No § 1º, (p. 37), “a aprovação em qualquer disciplina somente será concedida ao aluno que obtiver no mínimo 75% de frequência às atividades escolares desta disciplina”; § 2º, “Compete ao professor ministrante da disciplina verificar a situação de frequência dos alunos”; e no § 3º, (p. 38) “Será vedada a prestação de Avaliação Final (Exame de Recuperação) na disciplina ao aluno que não alcançar frequência mínima exigida de 75%”.

A Lei Nº. 9.394, de dezembro de 1996, publicada no Diário Oficial Nº. 248, Seção 1, p. 27833 a 27841, de 23/12/1996. Estabelece as Diretrizes e Bases da Educação Nacional (LDB). Da Educação Superior no capítulo IV, no art. 47, § 3º, (p. 27838) diz que: “É obrigatória a frequência de aluno e professores, salvo nos programas de educação à distância”.

BRANDÃO (2005), no artigo 47, o § 3º, define claramente sobre a frequência por se tratar de uma questão fundamental de qualquer ensino presencial, ou seja, a obrigatoriedade da frequência de alunos e professores aos seus cursos, com exceção dos programas de educação à distância que por sua natureza não exigem frequência.

Na continuação da Lei 9.394, art. 53, estabelece que: “No exercício de sua autonomia são asseguradas às atribuições às universidades sem prejuízo de outras”. Entre elas no item V – (p. 27838) “Elaborar e reformar os seus estatutos e regimentos em consonância com as normas gerais atinentes”

Esta LDB em vigor não é detalhista, ela dá liberdade para as escolas, para os sistemas de ensino dos municípios, dos estados e para as Universidades, fixando normas gerais.

A UFSM é uma IFEs que possui sua estrutura e na mesma constam as Unidades de Ensino, com seus respectivos Departamentos Didáticos, e a maneira de registrar a frequência dos alunos, o desempenho e o conteúdo é no instrumento/formulário Diário de Classe, embora não esteja previsto em nenhum regulamento.

A Lei n. 10.172, de 09 de janeiro de 2001, publicada no Diário Oficial n. 7, de 10/01/2001, aprova o Plano Nacional de Educação e dá outras providências, com duração de dez anos. No capítulo B – Educação Superior – 4.3 Objetivos e Metas no

item 5 (p. 10) “Assegurar efetiva autonomia didática, científica, administrativa e de gestão financeira para as universidades públicas”.

No Ministério da Educação – Conselho Nacional de Educação tramitam processos para serem homologados, mas se tratando de frequência, ou seja, abono de faltas aos estudantes que se ausentem regularmente dos horários de aulas devido a convicções religiosas, este é independente de homologação, porque o Conselho Federal de Educação tratou de salvaguardar a obrigatoriedade da frequência no percentual de 75%, não permitindo abono de faltas. Processo publicado no DOU N.º. 10, S.1, p. 29, de 15/05/2007.

Conforme as orientações constantes no *site* do MEC/SESU – Secretaria de Educação Superior sobre o assunto, há no art. 47, § 3º da Lei de Diretrizes e Bases da Educação Nacional (LDB) n.º. 9.393, de 20 de dezembro de 1996, orientações sobre frequência, sendo obrigatória tanto para alunos como para professores, salvo nos programas de educação à distância, que regem por outras disposições. Não existe legalmente abono de faltas. É admitida para a aprovação, a frequência mínima de 75% (setenta e cinco por cento) da frequência total às aulas e demais atividades escolares, em conformidade com o disposto na Resolução n. 4, de 16 de setembro de 1986, do extinto Conselho Federal de Educação.

A Lei n. 6.202, de 17 de abril de 1975, publicada no Diário Oficial da União de 17/04/1975: atribui à estudante em estado de gestação o regime de exercícios domiciliares instituído pelo Decreto-lei n.º. 1.044, de 21/10/1969, art. 1º, “A partir do oitavo mês de gestação e durante três meses a estudante em estado de gravidez ficará assistida pelo regime de exercícios domiciliares”. Parágrafo único, o período de afastamento é determinado mediante atestado médico a ser apresentado à direção da escola. No art. 2º, parágrafo único, “é assegurado às estudantes em estado de gravidez o direito à prestação dos exames finais”.

Após esta revisão da legislação pesquisada, destaca-se a Portaria n. 78, de 04 de fevereiro de 2009, do Secretário de Estado de Educação do Distrito Federal, que considera vários itens para o processo de implantação do diário de classe, por meio eletrônico, na Rede Pública do Ensino do Distrito Federal e resolve legislar conforme a determinação desta. A mesma encontra-se no site descrito a seguir, bem como orientações para Diário Eletrônico no SIGE – Solução Integrada de Gestão Educacional. O sistema de preenchimento digital de diários de classe está disponível

na página da *Web* de cada instituição educacional do Distrito Federal e pode ser acessada no *sítio* da SEDF. <http://www.se.df.gov.br/>

Ao finalizar o levantamento referente à legislação consultada, salienta-se que a UFSM não definia oficialmente o Diário de Classe nos seus documentos legislativos.

### 5.1.1 Contextualização do Diário de Classe na UFSM

O Diário de Classe é um instrumento semestral de acompanhamento e registro do desempenho e da frequência dos alunos, do registro do conteúdo ministrado, data e professor responsável pela disciplina, no decorrer do curso.

Este documento é um valioso instrumento pedagógico que, no dia-a-dia escolar, auxilia a sistematização, organização e análise da aprendizagem dos alunos e do trabalho realizado pelo professor. Em resumo, é um instrumento de acompanhamento semestral e registro do desempenho dos alunos no processo educacional.

Para a UFSM, ele visa guiar a ação pedagógica no que diz respeito aos registros e avaliação das melhorias e dificuldades apresentadas pelos alunos no processo de construção do conhecimento. Esta avaliação é uma referência pedagógica para o programa do professor, adotada como marco de aprendizagem das disciplinas e áreas do conhecimento.

O mesmo é elaborado pelo Sistema Integrado de Ensino (SIE) e gerado no Portal do Professor via *Web*, no momento em que o professor responsável pela disciplina acessar e começar a digitar as informações solicitadas no mesmo, o qual fica a disposição do professor da disciplina durante o semestre letivo e vai ser finalizado somente quando ele estiver com todas as informações digitadas e encerrar o semestre conforme o Calendário Acadêmico.

Este documento é produzido no decorrer das atividades docentes, portanto contém informações de interesse público. O Diário de Classe tradicional da UFSM possui quatro seções: na primeira, consta a logomarca da Instituição, nome do documento e informações de datas importantes; na segunda seção, a identificação

da disciplina, turma, créditos, curso, nome do aluno, número da matrícula entre outros; na terceira, o controle de frequência, dia mês e na contra capa consta o código de aprovação, avaliação entre outras informações.

Atualmente, o professor tem que manter o Diário de Classe em ordem e atualizado, sem emendas e rasuras, registrando diariamente a frequência dos alunos e as informações sobre o trabalho realizado em sala de aula. Porém, no decorrer da pesquisa, verificou-se que nem sempre estes procedimentos são adotados.

A seguir são descritos os trâmites dos Diários de Classe:

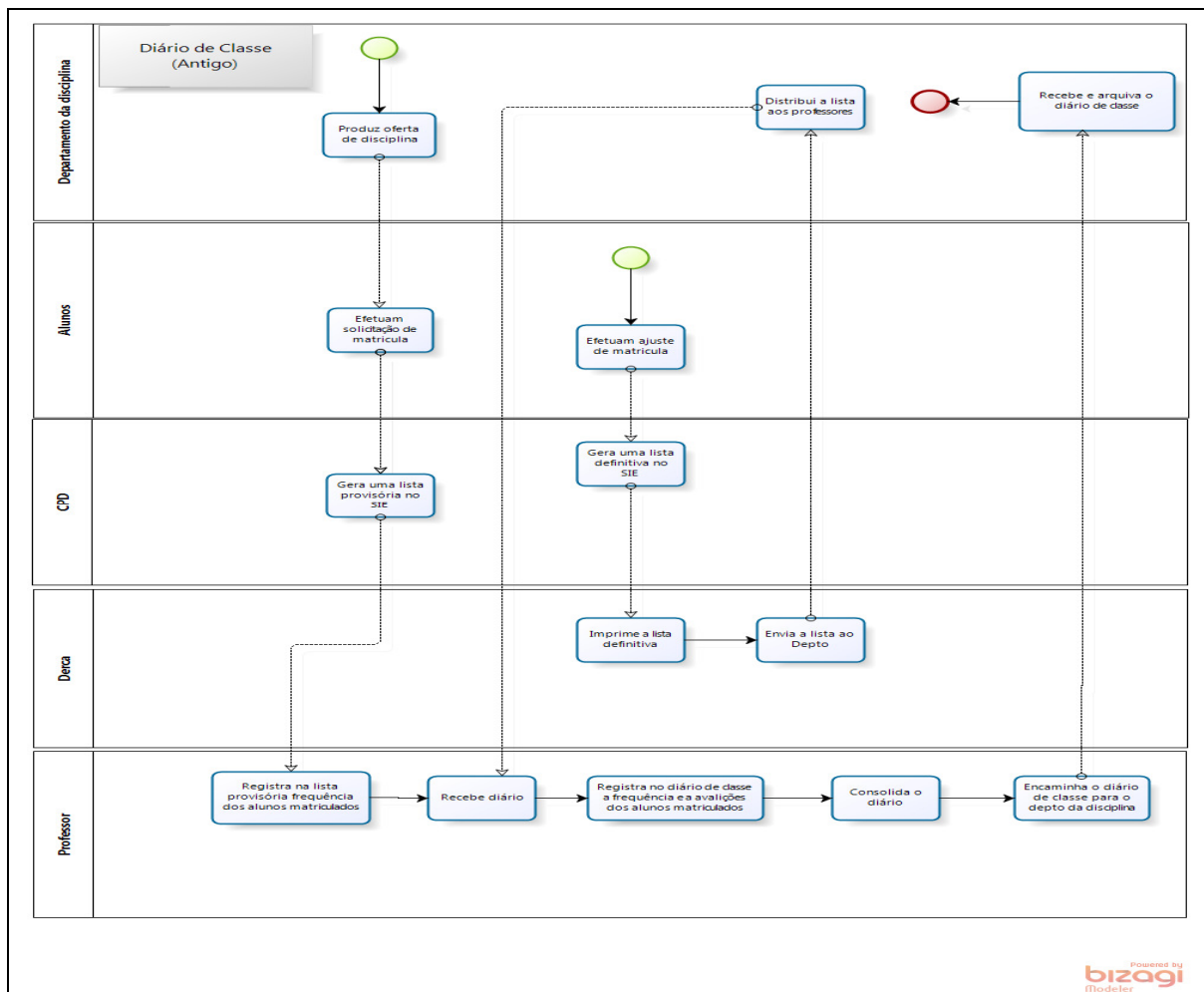


Figura 6 – Fluxo do Diário de Classe (Antigo)

Fonte: PROGRAD/UFSM

O trâmite do Diário de Classe tradicional acontecia no início do semestre, em duas etapas complementares: a primeira a partir do momento em que o Departamento Didático produzia a oferta da disciplina. Na sequência quando os alunos efetuavam a solicitação de matrícula. Depois era gerada uma lista provisória no SIE por meio do banco de dados gerenciado no CPD em conformidade com o DERCA e após o Professor registrava na lista provisória a frequência dos alunos matriculados.

Na segunda etapa, acontecia o ajuste da matrícula pelo aluno via Web sendo, então, gerada uma lista definitiva no SIE pelo CPD, e o DERCA imprimia a lista definitiva em folha A3 e enviava ao Departamento Didático que distribuía aos professores para registrar a frequência e avaliações dos alunos matriculados consolidando assim o Diário de Classe, após assinado entregando-o no Departamento Didático respectivo para arquivo.

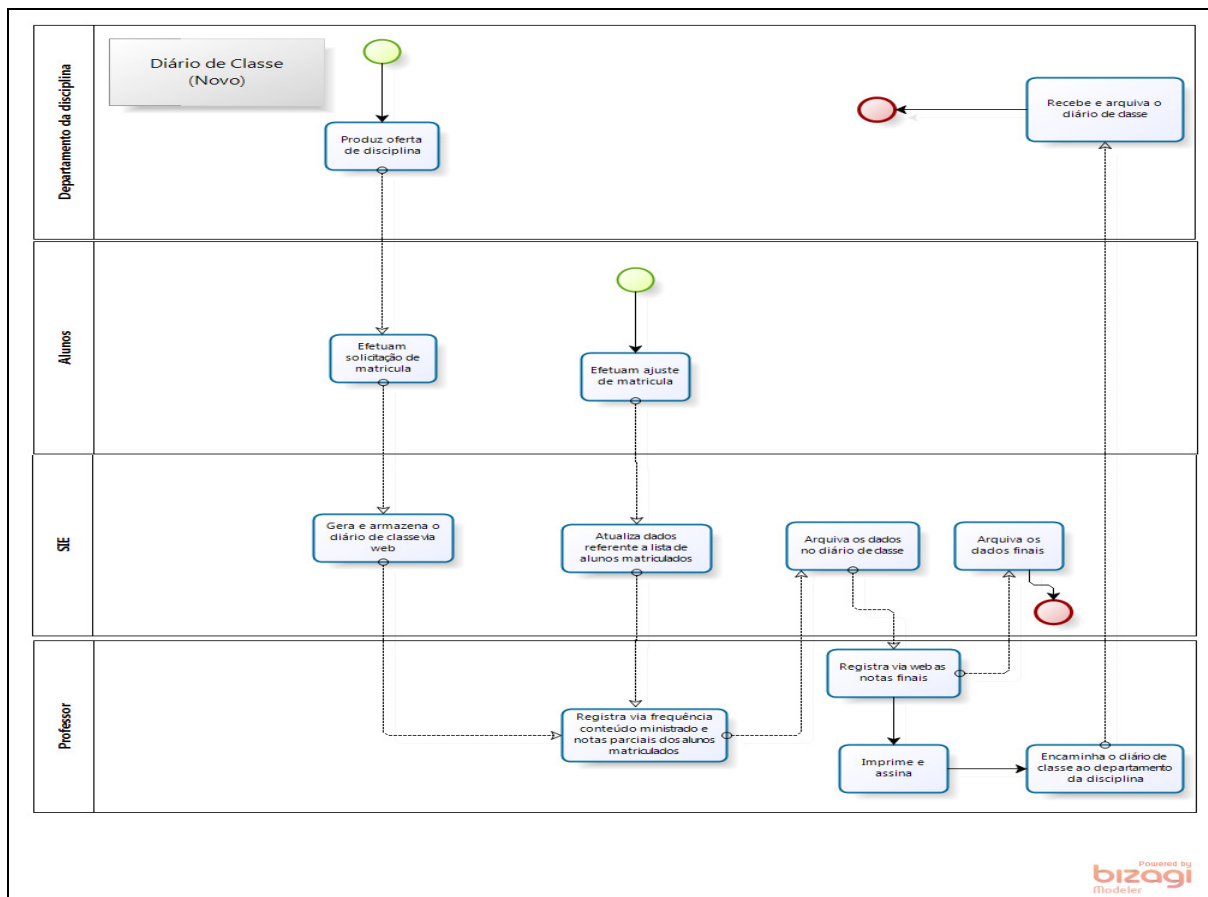


Figura 7 – Fluxo do Diário de Classe (Novo)

Fonte: PROGRAD/UFSM

O trâmite do Diário de Classe eletrônico acontece no início do semestre, em duas etapas complementares a partir de quando o Departamento Didático produz a oferta da disciplina e, na sequência, quando os alunos efetuam a solicitação de matrícula, após o documento é armazenado no banco de dados via Web.

Após, os alunos efetuam o ajuste de matrícula, e o SIE atualiza os dados e disponibiliza para o professor registrar no portal do professor, via Web, a frequência, conteúdo ministrado e notas parciais das avaliações dos alunos matriculados. Após os dados do Diário de Classe são armazenados durante o período letivo definido no Calendário Acadêmico, sendo que os professores podem registrar via Web as notas finais que ficam armazenadas para arquivo no banco de dados do SIE, que é organizado e mantido no CPD. A partir deste procedimento, é gerado um arquivo em



PDF, impresso em folha A4 e assinado pelo professor que posteriormente entrega no Departamento Didático respectivo para arquivo.

Conforme Paes (2004), junto com essas tarefas, o arquivamento, deve ser realizado com todo cuidado e atenção, uma vez que o futuro da documentação de uma instituição dependerá do bom ou do mau tratamento que foi dispensado aos documentos em sua fase corrente.

O arquivo em PDF, após o encerramento do semestre letivo, será impresso em folha A4 e assinado pelo professor responsável da disciplina para guarda permanente no arquivo do departamento didático respectivo e, além da guarda física em papel, os dados serão armazenados no Banco de Dados da UFSM, em dois locais diferentes, porém dentro da Instituição. Os mesmos são acessados com segurança e preservação garantidos em meio digital, tendo em vista o *backup* semanal e o acesso somente por usuários autorizados. Além de possuir seus metadados associados no armazenamento.

O Diário de Classe Eletrônico vai estar disponível para consulta após o encerramento do mesmo, com mecanismos de busca através da turma, disciplina, semestre/ano, identificador e professor da disciplina.

A responsabilidade pela guarda permanente, consulta e requerimentos de aluno ou interessado, solicitando algo sobre o Diário de Classe depois dele gerado é do respectivo Departamento e as consultas disponibilizadas serão efetuadas somente no documento impresso (papel).



## **6 PROPOSTA DE MODELO DO DIÁRIO DE CLASSE**

Este estudo tem como objetivo propor um modelo arquivístico para geração, preservação e acesso com segurança ao Diário de Classe (DC) da Universidade Federal de Santa Maria (UFSM).

Para o desenvolvimento deste modelo, foram analisados os modelos: Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-ARQ Brasil) e o Sistema Aberto de Arquivamento de Informação (SAAI). Esta proposta foi elaborada com base no e-ARQ Brasil, onde constam os requisitos para sistemas informatizados de gestão arquivística de documentos.

Este capítulo apresenta a proposta de como deve funcionar um sistema, de acordo com as normativas, para atender a elaboração, gestão e preservação do Diário de Classe Eletrônico. O capítulo divide-se em duas seções, sendo a primeira destinada aos requisitos que o sistema deve atender, e a segunda aos padrões de metadados para a preservação do documento arquivístico digital.

### **6.1 Requisitos do sistema**

Para que um documento arquivístico seja efetivamente eletrônico, e adquira as características de autenticidade e confiabilidade, devem ser adotados alguns requisitos no sistema, de maneira a assegurar a gestão, preservação e acesso com segurança. Os requisitos flexionam para atender tanto às organizações privadas como órgãos públicos. No entanto, os documentos da administração pública estão sujeitos a algumas normativas específicas. Os requisitos designados para o Diário de Classe são para definir como deve funcionar o sistema, e porque devem ser utilizados.

Desta forma, após estudo e análise do e-ARQ Brasil, foram definidos quais os requisitos da norma que devem ser implementados no gerenciamento e armazenamento do Diário de Classe pelo Sistema da UFSM. Tais requisitos estão dispostos resumidamente no Apêndice B e discutidos a seguir. Salienta-se que

alguns requisitos desta norma não foram contemplados porque não são aplicáveis no gerenciamento deste tipo documental.

Neste sentido, a elaboração do Diário de Classe, em meio eletrônico, deve atender primeiramente para a questão do formato e armazenamento onde serão registradas as informações. Assim, no momento em que o Diário de Classe for finalizado, e todo seu conteúdo lançado, deverá ser gerado e armazenado um arquivo em Portable Document Format (PDF). Este formato está sendo utilizado como padrão de documentos digitais por órgãos oficiais, devido à melhor garantia na integridade do conteúdo informacional. O PDF tem uma melhor compactação, tornando os arquivos mais leves, além de possuir compatibilidade com diversos sistemas operacionais do mercado.

A identificação arquivística deste arquivo em PDF deve estar sempre associada às suas características definidas na gestão Documental. Os documentos arquivísticos são organizados logicamente por um instrumento chamado “plano de classificação”, que deve constituir a análise central do sistema. Neste plano de classificação arquivística, são hierarquizadas classes e subclasses, e nessas estão vinculados os documentos. O Diário de Classe se caracteriza como um documento arquivístico, portanto deve estar associado a uma classificação arquivística e vinculado hierarquicamente aos níveis de classificação. Para identificar suas características arquivísticas, o sistema deve atribuir automaticamente ao documento um identificador da classe e subclasse. O Diário de Classe deve incorporar os metadados predefinidos da classe a qual pertence, sendo necessária a atualização automática quando houver alteração nesses metadados.

Deve haver a possibilidade de reclassificação do Diário de Classe, somente por usuário autorizado. Porém, devem-se manter os registros da posição anterior. Essa reclassificação deve ser acompanhada por uma justificativa.

Ainda enquanto característica arquivística, a temporalidade do Diário de Classe, que define o seu prazo de guarda, deve estar associada à temporalidade da classe a que pertence. Esta associação deve ser realizada automaticamente no momento da produção, através da classe onde o documento foi inserido. Conforme a legislação analisada nesta pesquisa, para o Diário de Classe a temporalidade será sempre guarda permanente. O sistema deve permitir a alteração nos prazos de guarda somente por usuários autorizados, mantendo um histórico das alterações realizadas.

O sistema também tem que definir a estrutura dos procedimentos de gestão e ser capaz de operacionalizar as regras estabelecidas pelo sistema de gestão arquivística de documentos.

Já, para a identificação do arquivo PDF no sistema, desde a captura até sua destinação final, deverá ser gerado no momento da produção um número padronizado para cada Diário de Classe, chamado identificador único. O formato e a estruturação deste número devem ser definidos no momento da configuração do sistema.

Através deste identificador, o sistema irá indicar o *status* do documento, se é uma minuta, ou se é a versão original. Este controle de versões deve ser registrado em metadados específicos, e o sistema deve atribuir a cada documento, no momento da captura, um código de manutenção de integridade baseado em criptografia.

O sistema deve poder inserir automaticamente metadados já previstos e permitir a entrada de outros metadados por usuários autorizados. Também deve ser permitida a inserção de novos metadados após o documento já gerado, bem como o registro e associação quando houver mais de uma versão do Diário de Classe (no caso de alguma alteração de conteúdo, em que gera outro original).

Neste contexto, para o controle da segurança das informações, os principais requisitos necessários para serem adotados visando à integridade e preservação do conteúdo contido nos Diários de Classe, são as cópias de segurança, controle de acesso, trilhas de auditoria de sistemas e autenticação digital.

Dentre os requisitos citados, os de identificação, autenticação e trilhas de auditoria são necessários na integração de qualquer sistema. Os demais requisitos serão definidos de acordo com as políticas específicas de segurança, quanto maior ou menor o rigor no tratamento dos documentos.

Portanto, no sistema de autenticação digital é que as transações efetuadas por meio de diversos canais eletrônicos de atendimento garantem a autenticidade (originalidade) e permitem a recuperação e validação dos documentos a partir da autenticação única, segura e não sujeita a fraudes.

Para cópias de segurança, os *backups* devem conter além do conteúdo do documento original, todos os metadados e padrões do sistema. Devem-se ter cópias de segurança, prevendo testes de restauração, e *backups* em dois locais diferentes e fisicamente distantes. Os backups devem ser agendados automaticamente.

O controle de acesso deve ser realizado por meio do sistema, com identificação e autenticação de usuários, baseando-se em grupos e em papéis de usuários. A identificação e autenticação de usuários tratam do mapeamento da identidade do usuário legítimo e das permissões dele, após sua autenticação. No caso do Diário de Classe, somente serão usuários autorizados por meio de login e senha, os professores responsáveis pelas disciplinas, os chefes de Departamentos Didáticos que ofertam as disciplinas e os administradores que utilizam o sistema e as informações referentes ao documento. No entanto, após a criação do documento, não será utilizado grau de sigilo para o acesso às informações, devendo o interessado solicitar o documento ao responsável que é o Departamento Didático.

Ao implementar o controle de acesso para o Diário de Classe, visando à segurança das informações, o sistema tem que manter associados os atributos dos usuários, como o identificador do usuário; as autorizações de acesso; e credenciais de autenticação. É necessário exigir que o usuário esteja devidamente identificado antes de iniciar qualquer operação no sistema que dependa de autorização, a alteração das credenciais de autenticação (usuário e senha) só poderá ser efetuada pelo administrador, e em conformidade com a política de segurança.

Os aspectos gerais de controle de acesso são aplicáveis a qualquer organização para conduzir suas funções e atividades, independente do modelo de controle adotado, conforme a política de segurança. Deve ser permitido acesso às funções do sistema somente aos usuários autorizados e sob controle rigoroso da administração do sistema, a fim de proteger a autenticidade dos documentos arquivísticos digitais. Para isso, o sistema implementa alterações ou revogações dos atributos de segurança de usuários e de documentos digitais.

Conforme o e-ARQ Brasil (2009), o controle de acesso por papéis de usuários são funções ou cargos com responsabilidades e autoridades bem definidas. Operações são as tarefas executadas nos documentos. Atribuições de usuários são as associações entre os dois. Um usuário pode estar associado a um ou mais papéis e ao contrário. E as permissões constituem garantias aprovadas para efetivação de operações arquivísticas. Somente aplicáveis aos órgãos e entidades em que há controle de acesso por papéis de usuários.

É importante salientar que, para o Diário de Classe, foi adotada a “Trilha de Auditoria”, na qual são registradas todas as alterações que ocorrem no documento depois de gerado, quem e o que alterou e a data da alteração do documento. Essas

trilhas de auditoria devem ser copiadas frequentemente, prevendo armazenamento pelo menos em um lugar *off-site*.

Por conseguinte, o sistema tem que assegurar que as informações da trilha de auditoria estejam disponíveis para inspeção, a fim de que uma ocorrência específica possa ser identificada e todas as informações correspondentes sejam claras e compreensíveis. Além disso, deve possuir mecanismos para realização de buscas nos eventos das trilhas de auditoria e ser capaz de impedir qualquer modificação na trilha de auditoria.

O Diário de Classe deve estar preparado ainda para ser exportado (dentro ou fora da Instituição) para outro sistema, juntamente com seus metadados que nunca devem se dissociar do documento. Já para a apresentação, visualização e impressão, o sistema deve salvar em PDF conforme visto anteriormente, mantendo assim as características estruturais de *layout*. Deve-se manter o formato do documento no momento da impressão, poder visualizar e imprimir todos os metadados resultantes de uma pesquisa do documento e deve estar acessível simultaneamente para mais de um usuário, permitindo ao administrador imprimir o conteúdo deste junto com metadados pré-selecionados.

No que tange o armazenamento, a escolha de dispositivos devem ser revista sempre que a evolução tecnológica indicar mudanças importantes. As atividades de migração devem ser efetivadas, preventivamente, sempre que se torne evidente ou previsível a obsolescência do padrão corrente. O sistema tem que possuir capacidade de armazenamento suficiente para acomodação de todos os documentos e suas cópias de segurança, além da verificação periódica dos suportes de armazenamento.

Com relação aos aspectos físicos, os suportes de armazenamento do sistema têm que ser acondicionados, manipulados e utilizados em condições ambientais compatíveis com sua vida útil prevista e/ou pretendida, de acordo com as especificações técnicas do fabricante e de entidades isenta, e com base em estatísticas de uso.

Quanto à efetividade de armazenamento, o sistema tem que utilizar técnicas de restauração de dados em caso de falhas; mecanismos de proteção contra escrita, que previnam alterações indevidas e mantenham a integridade dos dados armazenados.

A partir de falha ou descontinuidade do sistema, quando a recuperação automática não for possível, o sistema tem que ser capaz de entrar em modo de manutenção, no qual é oferecida a possibilidade de restaurar o sistema para um estado seguro. Nesta restauração o sistema deve ser capaz de garantir a recuperação de perdas ocorridas, inclusive dos documentos de transações mais recentes.

Por conseguinte, a preservação do Diário de Classe, enquanto documento arquivístico, de caráter histórico e probatório se dará com o conjunto de requisitos adotados no sistema. Todavia, os procedimentos específicos de preservação do Diário de Classe realizados no sistema, deverão ser registrados e gerenciados através de metadados.

Neste sentido, apresenta-se na próxima seção uma estrutura de metadados visando contribuir com a segurança e preservação dos dados contidos no Diário de Classe.

## **6.2 Metadados para preservação do Diário de Classe**

Os documentos são mais acessíveis de usar e administrar se algo a respeito deles é conhecido, como o autor, data, assunto, etc. Estas informações podem ser inferidas rapidamente com um olhar a um documento em papel. No caso dos documentos digitais estas informações são fornecidas através de metadados.

Em âmbito nacional, as normas brasileiras para sistemas de gestão eletrônica de documentos foram estabelecidas em 2004, através da Resolução n. 20 do CONARQ que “dispõe sobre a inserção dos documentos digitais em programas de gestão arquivística de documentos dos órgãos e entidades integrantes do Sistema Nacional de Arquivos” (BRASIL, 2004), que estabelece o seguinte sobre os metadados: “Os metadados são informações estruturadas e codificadas que descrevem e permitem gerenciar, compreender, preservar e acessar os documentos digitais ao longo do tempo” (BRASIL, 2004, § 3º).

Os metadados referem-se à identificação e contexto documental, que correspondem ao identificador único, instituição produtora, nomes, assunto, datas, local, código de classificação, tipologia documental, temporalidade, destinação entre



outros e o contexto tecnológico que diz respeito ao formato e tamanho de arquivo, dependências de *hardware* e *software*, tipos de mídias e localização física do documento. Neste trabalho, os metadados para o Diário de Classe estão especificados no quadro individual dos metadados incluído no Apêndice A.

Baseando-se nos dois modelos pesquisados (e-ARQ e SAAI) e na Resolução n. 25/2007 – CONARQ, que recomenda a adoção do Modelo e-ARQ Brasil pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos – SINAR, ao qual a UFSM faz parte, e a Resolução n. 32, de 17 de maio de 2010/CONARQ, que dispõe sobre a inserção dos metadados na parte II do Modelo referido, verificou-se a possibilidade de utilizar essa legislação e a norma e-ARQ Brasil para implementar o Diário de Classe da UFSM.

Deste modo, optou-se pela norma e-ARQ Brasil para desenvolver um modelo conceitual de metadados e requisitos do sistema de arquivo, para trazer a gestão, preservação e segurança da informação ao documento DC considerado pertinente para a proposta em questão. O quadro de metadados, que se encontra no Apêndice A, caracteriza o documento arquivístico de acordo com a legislação e políticas arquivísticas referentes aos documentos da Instituição, compreendendo a identificação de documentos e formatos, e as ações que gerenciam seu ciclo de vida. O aproveitamento de elementos de esquemas similares já consagrados por órgãos nacionais e internacionais, visam assegurar a interoperabilidade dos sistemas, bem como assegurar o armazenamento das informações do DC da UFSM que não havia no SIE e agora está sendo implementado no diário eletrônico.

Os metadados do DC da UFSM foram definidos para as entidades: documento, evento de gestão, classe, agente, componente digital, evento de preservação e trilha de auditoria. O modelo conceitual de elementos de metadados propostos ao documento DC da UFSM foi elaborado em quadros que detalham cada entidade e seus elementos, e pode ser observado no Apêndice A. A figura 8 apresenta as entidades do modelo proposto.

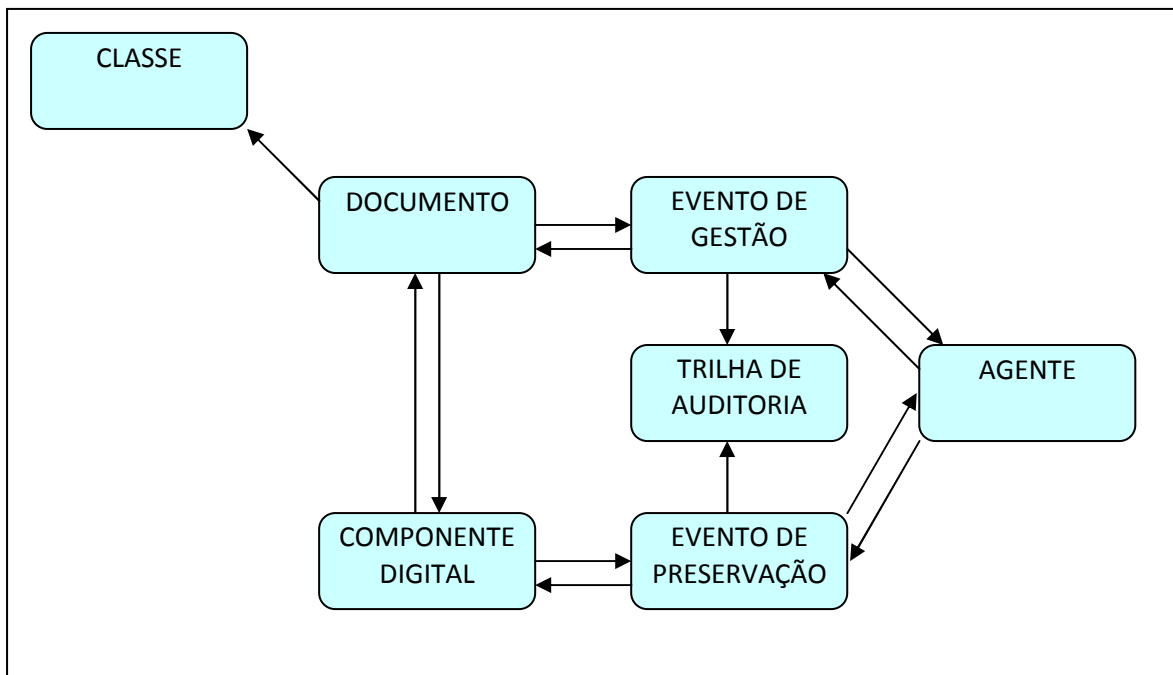


Figura 8 – Entidades e seus relacionamentos

Fonte: Modelos de requisitos para sistemas informatizados de gestão arquivística de documentos e-ARQ Brasil (2009) - adaptado.

A descrição dos elementos mais relevantes para o DC é realizada a seguir e as descrições dos demais se encontram no quadro individual Apêndice A.

Entende-se que a entidade **Documento** refere-se aos documentos arquivísticos que são gerenciados pelo sistema. Neste caso, o DC vai ser caracterizado como um destes documentos. Nesta entidade, são atribuídos os elementos suficientes à identificação e descrição do mesmo, tais como: a disciplina, a turma, o professor, o ano e o semestre. Para simplificação, apenas os itens com (\*) são os descritos no texto. Os demais são descritos apenas no quadro individual apêndice A.

Identificador do documento*
Tipo de meio*
Status*
Identificador de versão
Título
Descrição*
Assunto
Autor*
Destinatário
Originador*
Redator
Procedência
Identificador do componente digital
Gênero
Espécie
Tipo
Relação com outros documentos
Níveis de acesso
Data da produção
Classe
Destinação prevista
Prazo de guarda
Localização

Quadro 1 – Entidade Documento

Fonte: Autora

O Identificador do documento é único e atribuído ao mesmo no ato de sua captura, por meio do sistema com o objetivo de identificá-lo de forma unívoca para que o Sistema possa gerenciá-lo. Pode ser um elemento simples e conter um componente de localização. Deve ser gerado, preferencialmente, de forma automática pelo sistema, seguindo as normas específicas da Instituição.

O Tipo do meio é digital, cujo objetivo é identificar se o documento é digital, não digital ou híbrido, visando controlar as relações entre os ambientes e o monitoramento de preservação. No documento DC o tipo do meio é digital.

O *Status* é original e identifica o grau de formalização do documento e as relações existentes entre os originais, as minutas e as cópias, mantendo o controle sobre a disposição de cópias. Para o DC o *Status* será sempre o original.

A Descrição, como o próprio nome diz, descreve o documento; e, no caso do DC, é um documento oficial da UFSM, utilizado para controle da frequência e

aproveitamento dos alunos, além do registro do conteúdo ministrado. Ele é gerado nos departamentos didáticos, sob a responsabilidade do(s) professor(es) de cada disciplina e identifica o conteúdo do documento e facilita a pesquisa. Cada instituição vai fixar critérios e modelos de elementos para elaborá-la.

O Autor é caracterizado e identificado pelo Nome e Siape dos Docentes responsáveis pela disciplina no caso do DC. Identifica o autor do documento e fornece informação sobre o contexto de produção e demonstra a autenticidade do documento, indicando o responsável direto pela sua produção.

O Originador é o responsável designado com login pela geração do documento, para o DC o originador é o docente, o mesmo consegue identificar a origem do documento, fornece informação sobre a produção do documento e demonstra a autenticidade deste, indicando o responsável legal pela emissão do DC, é usado quando o nome dele for diferente do autor ou redator.

Durante o ciclo de vida do documento, ocorre uma série de eventos, que devem ser registrados no sistema, através da entidade **Evento de Gestão** que se relaciona com o documento e com o agente responsável pela ação. Cada documento arquivístico está relacionado com mais de um evento de gestão. O evento de gestão se define com as ações de gestão que ocorrem nos documentos arquivísticos durante seu ciclo de vida, como a captura, tramitação, recolhimento entre outros. No entanto, é por meio da captura que o DC será inserido no sistema e a partir da inserção, considerado um documento arquivístico digital. Essa captura se dará no momento em que o DC já estiver finalizado pelos professores responsáveis de cada disciplina, e ter originado um arquivo em formato PDF. A partir deste momento, serão preenchidos todos os elementos de metadados relativos a este documento.

Captura*
Tramitação*
Transferência*
Recolhimento*
Classificação_sigilo
Desclassificação_sigilo
Reclassificação_sigilo

Quadro 2 – Entidade Evento de Gestão

Fonte: Autora

A **Captura** descreve a captura do documento, registra a identificação do documento, data/hora da captura e o responsável pela mesma. No DC vai ocorrer após sua finalização pelo docente responsável.

A **Tramitação** é o registro da tramitação do documento como a identificação dele, data/hora de transmissão, remetente, data/hora do recebimento, destinatário, situação do trâmite. No DC vai ficar registrado na trilha de auditoria.

A **Transferência** é o registro do procedimento de transferência de documentos como a data/hora de envio, de recebimento, destinatário, método utilizado, responsável pela transferência e pelo recebimento, localização do suporte anterior e atual, identifica o lote, número do termo de transferência. Para o DC vai ocorrer após o docente responsável finalizar o documento.

O **Recolhimento** é o registro do procedimento de recolhimento dos documentos com objetivo de registrar informações como a data/hora de envio, de recebimento, destinatário, método utilizado, responsável pelo recolhimento, localização e suporte anterior e atual, identificação do lote, número do termo de recolhimento. Para o DC este vai ocorrer após cinco anos que é o prazo final para recolhimento.

A entidade **Classe** compreende as informações arquivísticas a respeito da temporalidade e da destinação prevista para os documentos dessa classe, e refere-se aos níveis de agregação do plano de classificação.

O plano de classificação define a organização dos documentos ordenados pelo órgão, e estruturado de forma hierárquica constituído por classes, subclasses, grupos e subgrupos, e a partir desses níveis de agregação têm-se a unidade de arquivamento e o item documental. O DC é um item documental que pertence ao plano de classificação, podendo ser identificado por códigos. A gestão de documentos é executada a partir da aplicação deste plano nos documentos, sendo a espinha dorsal de um sistema. Assim, quando um requisito trata da classe, consideram-se todos os níveis do plano de classificação e cada uma delas pode conter outras classes a ela subordinada, unidades de arquivamento e ou documentos arquivísticos.

Todas as alterações ocorridas no plano de classificação devem ficar registradas nos metadados da classe. As mesmas estão relacionadas aos documentos arquivísticos nelas classificados, sendo que todo documento deve ser relacionado a uma classe no momento da sua captura para o sistema.

O tipo documental DC consta no plano de classificação da UFSM e está classificado no grupo Departamento Didático, na classe Apoio ao Ensino e subclasse Atividade Docente.

A tabela de temporalidade e destinação determinam os prazos de guarda previstos nas fases corrente e intermediária e a destinação final dos documentos de uma classe. A cada classe que permite classificar unidades de arquivamento ou documentos arquivísticos, aplicam-se uma temporalidade e uma destinação.

Conforme a minuta da Tabela de Temporalidade de Documentos das Unidades Universitárias, elaborada pela equipe de arquivistas do Departamento de Arquivo Geral da UFSM, o prazo de guarda deste tipo documental é de cinco anos no arquivo corrente, e posterior guarda permanente.

Classe_nome*
Classe_código
Classe_subordinação*
Registro de abertura*
Reativação de classe
Registro de mudança de nome de classe
Registro de deslocamento de classe
Registro de extinção
Indicador de classe ativa/inativa

Quadro 3 – Entidade Classe/Descrição da classe

Fonte: Autora

A **Classe\_nome** é a divisão de um plano de classificação referindo-se às classes, subclasses, grupos e subgrupos. O DC está na classe Apoio de Ensino e subclasse Atividades Docente.

A **Classe\_subordinação** registra a subordinação na hierarquia do plano, o DC está no Grupo: Centro de Ensino; Sub-grupo: Departamento Didático e Classe: Apoio de Ensino. Estas informações auxiliam o acompanhamento no decorrer das mudanças das ações em relação à classificação arquivística.

O **Registro de abertura** é o primeiro registro do cadastro com data/hora e responsável. Serve para auxiliar no acompanhamento das ações relacionadas à classificação arquivística.

Classe_código
Prazo de guarda na fase corrente*
Evento que determina a contagem do prazo de guarda na fase corrente
Prazo de guarda na fase intermediária*
Evento que determina a contagem do prazo de guarda na fase intermediária
Destinação final*
Registro de alteração
Observações

Quadro 4 – Entidade Classe/Temporalidade associada à classe

Fonte: Autora

**Prazo de guarda na fase corrente** para o DC será durante o semestre letivo.

**Prazo de guarda na fase intermediária** para o DC será de cinco anos.

**Destinação final** para o DC será a guarda permanente. Estas informações auxiliam o acompanhamento nas mudanças das ações em relação à avaliação e a classificação arquivística.

A entidade **Agente** refere-se aos usuários que acessam o sistema, e relacionam-se com o documento DC, seja como Autor, Redator, DERCA, Professor do Departamento, do Curso ou responsável por algum evento de gestão ou preservação. Os metadados de identificação e as credenciais para acesso e autenticação no sistema são registrados na trilha de auditoria.

Nome*
Identificador*
Autorização de acesso*
Credenciais de autenticação
Relação*
Status do agente*

Quadro 5 – Entidade Agente

Fonte: Autora

**Nome** é o nome do agente que tem poder de utilização do agente responsável pela operação no DC, auxiliando na garantia da autenticidade e acesso.

**Identificador** do agente é o número do SIAPE que concede poder de utilização do agente responsável pela operação no DC e auxilia na garantia da autenticidade e acesso.

**Autorização de acesso** é o nível de restrição de acesso (uso e intervenção) aos documentos e operações do sistema. E o poder de utilização deste agente responsável pela operação no DC vai auxiliar na garantia da autenticidade e acesso.

**Relação** faz o relacionamento entre o usuário a papéis ou grupo (funções). Neste caso, tem o papel e o poder de utilização do agente responsável pela operação. No DC, é auxiliar na garantia da autenticidade e acesso.

**Status do agente** indica se o agente está ativo ou inativo no Sistema o qual é o responsável pela operação no DC e auxilia na garantia da autenticidade e acesso.

A entidade **Componente Digital** refere-se aos objetos digitais que compõem o documento arquivístico digital e são os arquivos de computadores com as informações de conteúdos, forma e composição necessária à apresentação do documento. As ações de preservação são obtidas nesses componentes. Cada documento está relacionado a um ou mais componentes, e um componente pode conter informações referentes a um ou mais documentos servindo para agrupar se houver mais de um DC. Eventos de preservação acontecem nos componentes digitais permitindo o acesso contínuo ao longo tempo, e devem ser registrados pelo sistema. Cada componente está integrado a uma série de eventos de preservação.



Identificador do componente digital*
Características técnicas*
Formato de arquivo*
Armazenamento*
Ambiente de hardware
Ambiente de software
Relacionamento*
Fixidade*

Quadro 6 – Entidade Componente Digital

Fonte: Autora

O **Identificador do componente digital** é a designação usada para identificar os componentes digitais que integram o documento, vai identificar que o DC é um documento único.

**Características técnicas** são as propriedades técnicas de um componente digital, aplicáveis à maioria dos formatos, como o nível de composição, tamanho, *software* de criação e inibidores. Elas fornecem informações para apoiar ações de acesso, manutenção e preservação.

**Formato de arquivo** identifica o formato de arquivo do componente digital, para o DC vai ser o formato PDF. Assim conhecer o referido formato é essencial para o planejamento e implementação das ações de preservação.

**Armazenamento** são informações sobre a localização e o suporte do componente digital, e os recursos necessários para armazenamento permanente. Localiza-se o componente digital no armazenamento. E o suporte em que o componente digital está armazenado ajuda o monitoramento das ações de preservação. O DC vai possuir o armazenamento e pode usar a migração sempre que for necessário.

**Relacionamento** é o registro das relações de um componente digital com outros componentes digitais ou com documento. Para o documento DC, esta relação vai ser entre as versões e, se caso ocorrer alterações, gerará outro DC.

**Fixidade** corresponde às informações utilizadas para verificar se o componente digital sofreu mudanças não documentadas. Faz a verificação do componente digital para saber se foi alterado de forma não documentada/autorizada, comprometendo sua autenticidade. A fixidade corresponde à ação adotada para preservação fidedigna do CD.

Entidade **Evento de Preservação** se refere às ações de preservação efetuadas nos documentos arquivísticos digitais, como a migração, compressão, validação e decifração. Este evento relaciona-se com o componente digital e com o agente responsável pela sua ação.

Validação de assinatura digital*
Verificação de fixidade*
Migração*
Replicação*
Verificação de vírus*
Validação

Quadro 7 – Entidade Evento de Preservação

Fonte: Autora

**Validação de assinatura digital** é o registro de validação da assinatura digital de um documento de acordo com o certificado digital deste. Registra a identificação e data da validação, agente responsável pela validação e resultados da validação. Em função de não haver uma assinatura digital, o DC vai ser produzido em PDF e assinado, porque não há uma certificação digital, tem-se a assinatura autenticada que serve apenas para garantir que o documento é o que diz ser, mas não garante que foi o professor designado que fez o documento. De qualquer forma, pode-se garantir que o DC atualmente é autêntico.

**Verificação de fixidade** é o registro desta verificação de um documento para verificar se os recursos utilizados para garantir a fixidade não foram corrompidos. Registra informações como o tipo de recurso de autenticação, identificação e data da verificação, agente responsável pela verificação e resultados da verificação. Para o DC resulta no controle de sua autenticidade.

**Migração** é o registro de procedimento de migração de documento, onde registra a identificação da migração, data da migração, agente responsável pela migração, resultado e conseqüências da migração. Ela é indispensável para a preservação e segurança do DC, fazendo com que possa migrar antes que aconteça a obsolescência tecnológica ou outro motivo.

**Replicação** é o registro de procedimento de replicação de documento, onde registra informações como a identificação e data da replicação, agente responsável pela replicação e consequências dessa replicação.

**Verificação de vírus** é o registro da verificação de vírus no documento e registra informações como a identificação e data da verificação, agente responsável pela verificação e detalhes da verificação.

O modelo e-ARQ Brasil contém vários requisitos para as diferentes esferas de atuação, atividades e tipos documentais, mas sozinho não abrange todos os requisitos necessários para qualquer órgão poder criar, administrar e dar acesso aos documentos digitais. As organizações e ou instituições possuem exigências legais e regulamentares diferenciadas que devem se considerar ao adotar este modelo.

Portanto, deixa a critério da organização a decisão de como adotá-lo, de forma modular ou completa. Ai reside às vantagens do modelo por deixar livre a escolha, devido às necessidades e normatização de cada organização. Para o Diário de classe será implementado de forma modular, tendo em vista suas particularidades, normas e políticas arquivísticas da Instituição. Ressalta-se ainda que foi elaborado para profissionais das áreas de Administração, Arquivo e Tecnologia da Informação, requerendo a interação entre eles para que a implementação seja bem sucedida. Baseado neste contexto e na necessidade do modelo pretendido, adotou-se a Trilha de Auditoria e entende sendo uma das entidades para o Diário de Classe da UFSM.

**Trilha de auditoria** é o conjunto de informações registradas que permitem o rastreamento de operações incluindo o retroagir no documento arquivístico digital e no sistema. Esta deve registrar o movimento e o uso dos documentos dentro de um sistema, informando quem operou, a data e hora da captura, reclassificação e outras ações realizadas. Tem o objetivo de informar sobre a autenticidade do documento e fornecer informações sobre o cumprimento das políticas e regras da gestão de documentos arquivísticos do órgão. Conforme o modelo de requisitos para sistemas informatizados de gestão arquivística de documentos e-ARQ Brasil, a definição da trilha de auditoria é a seguinte:

A trilha de auditoria consiste num histórico de todas as intervenções, ou tentativas de intervenção, feitas no documento e no próprio SIGAD. Nesse sentido, é também um metadado sobre os documentos arquivísticos digitais e informa sobre sua autenticidade (e-ARQ BRASIL 2009, p. 93).

A trilha de auditoria deverá ter o conteúdo fixo sem poder sofrer alterações, e o sistema deve permitir consulta **somente para leitura** e apenas ao auditor e administrador do sistema. A exportação será efetuada somente pelos administradores autorizados e somente administradores autorizados e acompanhado pelo auditor podem conferir o conjunto de eventos auditáveis e seus atributos.

Histórico da Intervenção*
---------------------------

#### Quadro 8 – Entidade Trilha de Auditoria

Fonte: Autora

**Histórico da Intervenção** registra o histórico de todas as intervenções, ou tentativas de intervenção, feitas no documento e no próprio Sistema. A trilha de auditoria consiste num histórico de todas as intervenções, ou tentativas, feitas no documento e no Sistema. Informa sobre a autenticidade do documento. Para o DC vai servir para registrar todas as alterações, quando e quem alterou o documento durante o período em que o aluno permaneceu na UFSM.

Considerando a importância documental do DC, o modelo sugerido agrega valor por garantir a sua preservação e acesso com segurança, tendo em vista a possibilidade de preservação por longo tempo em meio digital. Os metadados proporcionam vantagens como: possibilitar o armazenamento e administração de uma grande quantidade de dados com economia de espaço, garantindo segurança, autenticidade e principalmente acesso rápido pelos usuários. Além disso, possibilitam transparência quanto a origem, história e qualidade da informação por meio dos metadados.

Finalmente, pode-se afirmar que os metadados exercem a função básica de promover as informações sobre o documento digital sustentando o processo de gestão, recuperação e reprodução. São fundamentais para redução de riscos de deterioração a que estão sujeitas as informações e a ampliação das oportunidades de sobrevivência da informação digital. Servem como uma ferramenta que melhora significativamente o trabalho na área dos dados e de grande importância para os usuários do sistema que irão tratar do DCE da UFSM, desde a criação até a destinação final.

### 6.3 Resultados e discussão

Neste capítulo, foram apresentados os resultados da pesquisa através da verificação dos objetivos, demonstrando que estes foram alcançados.

O modelo e-ARQ Brasil possui mais de trezentos requisitos recomendados para utilização na gestão arquivística de documentos no sistema. Para o DC, foram escolhidos mais de noventa requisitos do total, que contém a norma e entende-se que os demais não são usáveis para o documento DC, porque a proposta é exclusiva para este documento. Salienta-se que com os requisitos selecionados e associados ao DC, torna-se um documento arquivístico eletrônico autêntico e com condições de ser gerado, administrado, migrado e preservado em meio digital.

Este modelo determina noventa e cinco elementos de metadados para as seis entidades. Deste foram definidos mais de sessenta elementos para o DC da UFSM de modo a torná-lo eletrônico e com todas as prerrogativas necessárias para integrar-se no sistema informatizado de gestão arquivística da UFSM. Foi adotada a trilha de auditoria para o DC e entende-se a mesma como uma entidade e metadados, que vão registrar toda e qualquer alteração no documento, portanto, vai ter um histórico completo do DC.

Após a leitura da legislação e com o uso do documento Diário de Classe na UFSM, contendo várias informações como a logomarca, nome do aluno, frequência, matéria lecionada, carga horária, avaliação e outras informações importantes, percebeu-se como é omissa, na legislação, o local e a forma de registro dessas informações, já que, conforme a legislação, a frequência é obrigatória.

Tendo em vista a autonomia da Universidade e o processo de encaminhamento da versão final da Atualização do Regimento Geral da UFSM pela Pró-Reitoria de Planejamento (PROPLAN) ao Conselho Universitário (CONSU), a Pró-Reitoria de Graduação (PROGRAD) propôs alterações no Artigo 129, do mesmo, com a seguinte redação na Seção V – Da Frequência, no Artigo 108, § 2º, onde se lê: Compete ao professor ministrante da disciplina verificar a **situação de frequência dos alunos**, acrescentar “**e registrá-la no documento Diário de Classe**”. Na seção VI – Art. 112, onde se lê: Durante os períodos letivos serão feitas duas avaliações parciais, sendo que os resultados deverão ser **encaminhados, posteriormente, ao DERCA para registro**, substituir por, “**registrados pelo**

**professor ministrante da disciplina no documento Diário de Classe**". Após ter transcorrido o tempo necessário para discussão do assunto, e possíveis novas sugestões por parte da comunidade universitária e tendo o processo tramitado por todas as instâncias administrativas necessárias, a Comissão de Legislação e Regimentos elaborou o Parecer nº. 031/2011 – CLR através do qual o Conselho Universitário aprovou a Atualização do Regimento Geral da UFSM, na Sessão nº. 722, realizada em 15/04/2011, com as alterações sugeridas. Vale comentar que as sugestões acima foram contempladas com a aprovação e justificam-se pelo uso e valor das informações contidas no documento arquivístico Diário de Classe.

Além da mudança na legislação para o Diário de Classe da UFSM, o DC começou a ser produzido exclusivamente por meio do Portal do Professor via WEB a partir do primeiro semestre de dois mil e onze. Aumentando a sustentabilidade institucional de acordo com o Plano de Desenvolvimento Institucional (PDI) 2011-2015 UFSM. Desde então não há mais a impressão do DC na folha A3. Com este procedimento foram obtidas vantagens como o tempo no preenchimento, mão de obra e espaço físico reduzidos, entre outros. Após a produção da versão eletrônica, versado em folha A4 é produzida para guarda permanente. Sendo garantida sua preservação por meio de *backup* e manutenção da versão física em locais distintos.

Neste contexto, a pesquisa indica que o Diário de Classe possui os requisitos e metadados conforme o modelo e-ARQ Brasil, que podem garantir sua gestão, preservação e acesso com segurança por longo prazo, a partir de sua implementação no Sistema.

Quando esta proposta for implementada e avaliada, o bom funcionamento e suas vantagens servirão de ponto de partida para a Instituição tornar outros documentos de sua criação em meio eletrônico, bem como servir de exemplo como documento arquivístico digital integrante do Sistema adaptado às políticas arquivísticas da UFSM e normatizado conforme o modelo e-ARQ Brasil, para outras instituições e ou organizações.

## 7 CONCLUSÃO

Este trabalho foi importante para o desenvolvimento geral do DERCA e DAG da UFSM, e poderá ser continuamente aperfeiçoado, conseguindo, assim, diminuir, consideravelmente, o risco da perda de documentos, de tempo e também de espaço físico, além de garantir a agilidade na recuperação da informação e a segurança no acesso da mesma.

Visando compreender e identificar modelos arquivísticos como ferramenta tecnológica ou sistema e viabilizar a elaboração de documento em meio eletrônico para uso e armazenamento com segurança, foram estudados modelos de referência. Optou-se pelo modelo e-ARQ Brasil, para elaborar um modelo com requisitos e metadados para o Diário de Classe da UFSM, conforme contém o quadro individual Apêndice A, pois este modelo atende tanto objetos digitais como físicos e é recomendado para adoção nas instituições públicas.

Desta forma, foi proposto um modelo arquivístico para o DC que garanta preservação e segurança, tendo em vista a relevância das informações deste documento e seus metadados para preservação por longo prazo com segurança conforme as normas e políticas da Instituição.

A elaboração do modelo para implantação do Diário de Classe Eletrônico alinhado a legislação e as políticas arquivísticas da Instituição e do governo, juntamente com um conjunto de metadados definidos para este documento com base no modelo e-ARQ Brasil, possibilita sua gestão, preservação e segurança por longo tempo. Considera-se que a concretização do modelo é um processo **pioneiro** de melhoria, pois a necessidade de implantar este projeto na UFSM é evidente e com esta implementação, o arquivo será mais seguro e com muitas vantagens para os Departamentos envolvidos, bem como para a UFSM como um todo.

Considerando-se a implantação do modelo no Sistema, pode-se concluir que a Instituição poderá identificar à necessidade de realizar o mesmo trabalho em outros documentos de sua criação. Esse foi o ponto alvo fundamental, que em curto ou médio prazo, poderá resultar na maturidade, não só de um único documento como o Diário de Classe, mas também de outros documentos da UFSM.

Em vista do exposto, acredita-se que este estudo possa colaborar com os profissionais das áreas de Arquivística, Administração e Tecnologia da Informação, com as contribuições proporcionadas no que se refere aos requisitos e metadados para um modelo informatizado de gestão arquivística de documentos.

### **7.1 Sugestões para estudos futuros**

O modelo de requisitos e-ARQ Brasil pode ser adotado por qualquer outra instituição pública ou privada independente de sua localização, porte ou área de atuação. É de extrema importância o acompanhamento das ações e cada etapa deve ser questionada e executada conforme descrito para que não haja riscos.

Na UFSM, o Diário de Classe tradicional, ou seja, em folha A3, impresso e utilizado há muito tempo (como uma herança antiga), pôde ser abolido com a implementação do Diário de Classe Eletrônico. Isso se justifica pela agilização no processo de registro, armazenamento e recuperação das informações, além da diminuição do gasto excessivo de impressão em papel que chega a, mais ou menos 6 mil formulários por semestre, mão-de-obra e também do espaço físico no arquivo.

O Diário de Classe Eletrônico, para ser implementado, necessita ter as suas normativas de utilização descritas no Regimento Geral da Instituição, conforme está. Mas deverá conter claramente os procedimentos complementares e regulamentação de uso. Portanto, sugere-se a criação de uma regulação específica para este fim.

Quando houver um Repositório Digital na Instituição, para gerenciar os documentos digitais de acordo com a legislação e políticas arquivísticas estabelecidas, o Diário de Classe é um documento que reúne as condições mínimas necessárias para ser gerenciado eletronicamente, mantendo sua preservação e acesso com segurança não só no SIE, mas no repositório também.

A partir deste trabalho, sugere-se que sejam realizados outros trabalhos de pesquisa científica sobre a gestão, preservação e segurança das informações criadas, armazenadas e manipuladas no sistema pelas organizações, em especial na UFSM.



## REFERÊNCIAS BIBLIOGRÁFICAS

ARELLANO Miguel Angel. Artigo: **Preservação de documentos digitais**. Ci. Inf., Brasília. V. 33, n. 2, p. 15-27, maio/ago. 2004. Disponível em: <<http://revista.ibict.br/index.php/ciinf/article/download/305/271>>. Acesso em: 20 out. 2009.

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

\_\_\_\_\_. **Dicionário brasileiro de terminologia arquivística**. Rio de Janeiro: Arquivo Nacional, 2005, 232 p. Publicações Técnicas, nº 51. Disponível em: <[www.portal.arquivonacional.gov.br/...](http://www.portal.arquivonacional.gov.br/)> Acesso em: 20 jul. 2010.

\_\_\_\_\_. **ISAD (G) Norma Geral Internacional de Descrição Arquivística: Adotada pelo comitê de Normas de Descrição, Estocolmo, Suécia, 1999 [Versão brasileira preparada por grupo de trabalho do Arquivo Nacional]**. 2ª Ed. Madrid: Subdirección General de los Archivos Estatales, 2000, 128p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001**. Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. Primeira Edição 31/03/2006 – Válida a partir de 30/04/2006.

\_\_\_\_\_. **NBR 15472**. Sistemas espaciais de dados e informações – Modelo de referência para um sistema aberto de arquivamento de informação (SAAI). Assunto. Referência ABNT NBR 15472:2007. Elaboração ABNT/CB-08. Rio de Janeiro. 2007, 95 p. Primeira Edição 09/04/2007 – Válida a partir de 09/05/2007.

BRAGA, Gilda Maria; PINHEIRO, Lena Vânia Ribeiro. Desafios do impresso ao digital: questões contemporâneas de informação e conhecimento. In:\_\_\_\_\_. **Informação em ciência, tecnologia e inovação: configurações institucionais e mediações tecnológicas**. (Orgs.). Brasília: Ibict: Unesco, 2009. Cap.15, p. 407-427.

BRANDÃO, Carlos da Fonseca. **LDB: passo a passo: Lei de Diretrizes e Bases da Educação Nacional (Lei nº 9.394/96)**. 2 ed. Atual. São Paulo: Editora Avercamp, 2005.

BRASIL – Arquivo Nacional. **Resolução n. 25, de 27 de abril de 2007**. Dispõe sobre a adoção do Modelo para Sistemas Informatizados de Gestão Arquivística de

Documentos e-ARQ Brasil. Diário Oficial da União – Seção 1, Nº 81, de 27/04/2007, (p.14-15).

BRASIL. **Decreto n. 18.580, de 18 de março de 1987.** Dispõe sobre o registro semanal de aulas e dá outras providências. Diário Oficial do Estado do Ceará. Fortaleza, 19 mar. 1987.

BRASIL, Conselho Nacional de Arquivos. **Resolução N. 20 de 16 de junho de 2004.** Disponível em: <<http://www.arquivonacional.gov.br/conarq/leis/downl.htm>>. Acesso em: 11 nov. 2010.

\_\_\_\_\_. **Resolução n. 25, de 27 de abril de 2007.** Publicado no Diário Oficial da União, edição n. 81, de 27/04/2007 – Seção 1. Disponível em: <[www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm](http://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm)> Acesso em: 20 jul. 2010.

\_\_\_\_\_. **Resolução n. 32, de 17 de maio de 2010.** Publicado no Diário Oficial da União, edição n. 93, de 18/05/2010 – Seção 1. Disponível em: <[www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm](http://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm)> Acesso em: 11 abr. 2011.

\_\_\_\_\_. Câmara Técnica de Documentos Eletrônicos. MODELO DE REQUISITOS PARA. SISTEMAS INFORMATIZADOS DE. GESTÃO ARQUIVÍSTICA DE DOCUMENTOS **e-ARQ Brasil. 2009.** Disponível em: <[www.conarq.arquivonacional.gov.br/media/.../earqmet/earqbrasilv1.1.pdf](http://www.conarq.arquivonacional.gov.br/media/.../earqmet/earqbrasilv1.1.pdf)> Acesso em: 10 maio 2010.

BRASIL – **Constituição:** República Federativa do Brasil. Brasília: Senado Federal, centro gráfico, 1988.

BRASIL. Decreto n. 5.773, de 09 de maio de 2006. Dispõe sobre o exercício das funções de regulação, supervisão e avaliação de instituições de educação superior e cursos superiores de graduação e seqüenciais no sistema federal de ensino. **Diário Oficial da União**, Brasília, DF, 10 maio 2006. n. 88, Seção 1, p. 6-10. Disponível em: <<http://www.in.gov.br>>. Acesso em: 2 jun. 2010.

BRASIL. Lei n. 6.202, de 17 de abril de 1975. Atribui à estudante em estado de gestação o regime de exercícios domiciliares instituído pelo Decreto-lei n. 1.044, de 1969, e da outras providências. **Diário Oficial da União**, Brasília, DF, 17 abril 1975. Disponível em: <<http://www.in.gov.br>>. Acesso em: 2 jun. 2010.

BRASIL. Lei n. 9.394, de 20 de dezembro de 1996. Estabelece as Diretrizes e Bases da Educação Nacional. **Diário Oficial da União** n. 248, de 23/12/1996. S.I, p.27833 a 27841. <<http://www.in.gov.br>>. Acesso em: 1 jun. 2010

BRASIL. Lei n. 10.172, de 09 de janeiro de 2001. Aprova o Plano Nacional de Educação e dá outras providências. **Diário Oficial da União**, Brasília, DF, 10 jan. 2001. n. 7, Seção I, p. 1-21.

BRASIL. Lei n. 11.788, de 25 de setembro de 2008, Dispõe sobre o estágio de estudantes; altera a redação do art. 428 da Consolidação das Leis do Trabalho – CLT, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, e a Lei nº 9.394, de 20 de dezembro de 1996; revoga as Leis nºs 6.494, de 7 de dezembro de 1977, e 8.859, de 23 de março de 1994, o parágrafo único do art. 82 da Lei nº 9.394, de 20 de dezembro de 1996, e o art. 6º da Medida Provisória nº 2.164-41, de 24 de agosto de 2001; e dá outras providências. **Diário Oficial da União**, Brasília, DF, 26 set. 2008. n. 187, Seção 1, p. 3-4. Seção 1, p. 6-10.  
Disponível em: <<http://www.in.gov.br>>. Acesso em: 1 jun. 2010.

CAMARGO, Ana Maria de Almeida; BELLOTTO, Heloísa Liberalli. **Dicionário de terminologia arquivística**. São Paulo: Associação dos Arquivistas Brasileiros – Núcleo Regional de São Paulo: Secretaria de Estado da Cultura, 1996.

CHARMAZ, Kathy. **A Construção da Teoria Fundamentada**: guia prático para análise qualitativa / tradução Joice Elias Costa. Porto Alegre: Artmed, 2009. 272 p.

CONSELHO ESTADUAL DE EDUCAÇÃO. Deliberação CEE n. 239/99. Regulamenta o arquivamento de documentos escolares em instituições de educação básica do Sistema Estadual. Conclusão do plenário em 04/05/1999. Rio de Janeiro. Disponível em: <[http://www.cee.rj.gov.br/coletanea/d236\\_245.pdf](http://www.cee.rj.gov.br/coletanea/d236_245.pdf)>. Acesso em: 07 jun. 2010.

CONSELHO NACIONAL DE EDUCAÇÃO (Brasil). Resolução n. 4, de 16 de setembro de 1986. Dispõe sobre o mínimo de frequência obrigatória nos cursos superiores. **Diário Oficial da União**, Brasília. Disponível em: <<http://portal.in.gov.br/>> Acesso em: 1 jun. 2010.

\_\_\_\_\_. Resolução CNE/CES n. 1, de 03 de abril de 2001. Estabelece normas para o funcionamento de cursos de pós-graduação. **Diário Oficial da União**, de 09/04/2001, S.I, p.12. Alterada pela Resolução n. 24 de 18/12/2002 e Resolução n. 1, de 08/06/2007.

CUNHA, Jaqueline de Araújo; LIMA, Marcos Galindo. **Preservação Digital**: o estado da arte. In: Encontro Nacional de Pesquisa em Ciência da Informação, 8, 28-31 out. 2007, Salvador. Anais do VIII ENANCIB. Salvador: UFBA/PPGCI; Ancib, 2007. Disponível em: <<http://www.enancib.ppgci.ufba.br/artigos/GT--043.pdf>>. Acesso em: 14 jul. 2010.

FERREIRA, Miguel. **Introdução à preservação digital**: conceitos, estratégias e actuais consensos. Guimarães, Portugal: Escola de Engenharia da Universidade do Minho, 2006. Disponível em: <<https://repositorium.sdum.uminho.pt/bitstream/1822/5820/1/livro.pdf>>. Acesso em: 07 nov. 2008.

GIL, A. C. **Como Elaborar Projetos de Pesquisa**. 4ª ed. São Paulo: Atlas, 2002. 176 p.

INNARELLI, Humberto Celeste. **Preservação de Documentos Digitais**: confiabilidade de mídias CD-ROM e CD-R. 2006. 147 p. Dissertação (Mestrado Engenharia Mecânica). Faculdade de Engenharia Mecânica, Universidade Estadual de Campinas, Campinas. 2006. Disponível em: <<http://libdigi.unicamp.br/document?code=vtls000384479>>. Acesso em: 14 jul. 2010.

LACERDA Edson Alves; ALMEIDA Lânia Márcia de. **Sistemas Informatizados de Gestão Arquivística de Documentos. 2008** – SIGAD's dos órgãos da Administração. Pública Federal face aos requisitos do e-ARQ Brasil. Disponível em: <<http://bdjur.stj.gov.br/xmlui/handle/2011/20645>>. Acesso em: 23 mar. 2010. Artigo.

LAUREANO, Marcos Aurelio Pchek. **Gestão de Segurança da Informação**. 2005. Disponível em: <[www.mlaureano.org/aulas\\_material/gst/apostila\\_versao\\_20.pdf](http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf)>. Acesso em: 16 abr. 2010. Artigo.

MARCONI, M. de A.; LAKATOS, E. M. **Fundamentos de Metodologia Científica**. 6ª ed. São Paulo: Atlas. 2005. 315 p.

MÁRDERO ARELLANO, Miguel Ángel - **Preservação de documentos digitais. Preservação de documentos digitais**. Doutorando em ciência da informação. Disponível em: <[www.scribd.com/.../MARDERO-ARELLANO-Miguel-Angel-Preservacao-de-documentos-digitais](http://www.scribd.com/.../MARDERO-ARELLANO-Miguel-Angel-Preservacao-de-documentos-digitais)>. Acesso em: 24 fev. 2010. Artigo.

MINAYO, Maria Cecília de Souza (Org.); DESLANDES, Suely Ferreira; CRUZ NETO, Otavio; GOMES, Romeu. **Pesquisa Social**: teoria, método e criatividade. 22. Ed. Petrópolis: Editora Vozes, 2003. 80 p.

MURILLO, Manuel Vázquez. **Política de la administración de documentos y archivos**. Impreso em Argentina, agosto 2003.

Orientação Diário Eletrônico. SIGE–Solução Integrada de Gestão Educacional. Diários de classe – **Preenchimento Digital**. Brasília, fev. 2009. Disponível em: <<http://www.se.df.gov.br/sites/400/412/00000057.pdf>>. Acesso em: 12 jun. 2010.

PAES, Marilena Leite. **Arquivo**: teoria e prática. 3ª edição ver. ampl. Rio de Janeiro. Editora FGV, 2004. 228 p.

Portaria n. 78, de 04 de fevereiro de 2009. Implantação do Diário de classe, por meio eletrônico. **DODF Nº 26, 5 fev. 2009** – Disponível em: <<http://www.ufsm.br>>. Acesso em: 12 jun. 2010.

POUPART, Jean; DESLAURIERS, Jean-Pierre; GROULX, Lionel-H.; LAPERRIÈRE, Anne; MAYER, Robert; PIRES, Álvaro P. **A Pesquisa Qualitativa**: enfoques epistemológicos e metodológicos / tradução de Anna Cristina Arantes Nasser. 2ª Ed. Petrópolis, Rio de Janeiro: Vozes, 2010. (Coleção Sociologia).

RODRIGUES, Maria de Lurdes Tainha Saramago (2003) – **Preservação digital de longo prazo**: estado da arte e boas práticas em repositórios digitais. 2003. Lisboa, s.n., 145 p. (Tese de Mestrado em Estudos de Informação e Bibliotecas Digitais).

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

ROUSSEAU, Jean-Yves; COUTURE, Carol. **Os Fundamentos da Disciplina Arquivística**. Publicações Dom Quixote – Lisboa 1998.

SANTOS, Vanderlei Batista dos. **Gestão de documentos eletrônicos**: uma visão arquivística. 1ª, Ed, Brasília: ABARQ, 2002.

SANTOS, Vanderlei Batista dos; INNARELLI, Humberto Celeste; SOUSA, Renato Tarciso Barbosa de. **Arquivística**: temas contemporâneos: classificação, preservação digital e gestão do conhecimento. 3ª ed. Distrito Federal. SENAC, 2009.

SARAMAGO, Maria de Lurdes. **Metadados para preservação digital e aplicação do modelo OAIS**. In: Congresso Nacional de Bibliotecários, Arquivistas e Documentalistas, 8, 2004, Estoril, Portugal. Disponível em: <<http://badinfo.apbad.pt/congresso8/comm2.pdf>>. Acesso em: 13 nov. 2008.

SCHELLENBERGER, Theodore R. **Arquivos Modernos: princípios e técnicas**. 6ª edição Rio de Janeiro Editora FGV, 2006. 388 p.

SÊMOLA, Marcos. **Gestão da segurança da informação: visão executiva da segurança da informação: aplicada ao Security Officer e Módulo Security Solutions S.A.** – Rio de Janeiro: Elsevier, 2003 – 10ª reimpressão.

SILVA, Armando Malheiro da; RIBEIRO Fernanda; RAMOS Júlio; REAL Manuel Luís. Arquivística – **Teoria e Prática de uma Ciência da informação**. Volume 1. 1998. Edições Afrontamento e Acabamento: Rainho & Neves, Lda. Santa Maria da feira. Junho de 1999.

SÍNTESE de pareceres n. 1, publicado no **Diário Oficial da União** n. 10, seção 1, p.29 de 15/01/2007. Parecer independente de homologação e ... . Consulta sobre abono de falta. Disponível em: <[www.padmachado.g12.br/fapem/arquivos/.../](http://www.padmachado.g12.br/fapem/arquivos/.../)>. Acesso em: 12 jun. 2010.

SOUSA, Renato Tarciso Barbosa de. **As bases do processo classificatório na Arquivística: um debate metodológico**. São Paulo: Arq-SP, 2002. (Scripta 2).

THOMAZ, Katia P.; SOARES, Antonio José. A preservação digital e o modelo Open Archival Information System (OAIS). **DataGramZero – Revista de Ciência da Informação**, v.5, n.1, fev. 2004. Disponível em: <[http://dici.ibict.br/archive/00000342/01/A\\_preservacao\\_digital\\_e\\_o\\_modelo\\_de\\_referencia\\_Open\\_Arcival\\_System.pdf](http://dici.ibict.br/archive/00000342/01/A_preservacao_digital_e_o_modelo_de_referencia_Open_Arcival_System.pdf)>. Acesso em: 10 out. 2008.

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO. **Resolução n. 431/2007**. Ementa: Aprova o regimento do Diário de Classe, dos procedimentos e orientações para elaboração, execução e preenchimento. Aprovada em 19 nov.2007. Secretaria Geral dos Conselhos da Administração Superior Conselho de Ensino, Pesquisa e Extensão. Disponível em: <[www.uag.ufrpe.br/](http://www.uag.ufrpe.br/)>. Acesso em: 10 jun. 2010.

UNIVERSIDADE FEDERAL DE SANTA MARIA. **Estatuto da UFSM** (Adaptado de acordo com a Lei nº 9.394/96, Diretrizes e Bases da Educação Nacional. Promulgada em 20.12.1996). Disponível em: <<http://www.ufsm.br>>. Acesso em: 2 jun. 2010.

\_\_\_\_\_. **Regimento Geral da UFSM** – 1988 – Diário Oficial, de 02 de janeiro de 1989. Disponível em: <<http://www.ufsm.br>>. Acesso em: 2 jun. 2010.

\_\_\_\_\_. **Atualização do Regimento Geral da UFSM** – 2011. Parecer n. 031/2011 – CLR, aprovado na Seção n. 722 do Conselho Universitário, em 15/04/2011.

\_\_\_\_\_. **Plano de Desenvolvimento Institucional 2011-2015 UFSM**. Parecer n. 082/2011 – CLR, aprovado na Seção n. 725 do Conselho Universitário, em 22/06/2011.





## GLOSSÁRIO

**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.

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

**Administrador** – Responsável por manter o ambiente operacional do sistema.

**Anexo** – Um objeto digital que segue junto com a mensagem de correio eletrônico ou com um fluxo de trabalho.

**Armazenamento** – Guarda de documentos digitais em dispositivos de memória não volátil. 2 Guarda de documentos arquivísticos em local apropriado.

**Arquivamento** – 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.

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

**Base de dados** – Conjunto de dados estruturados, com as respectivas regras de acesso, formatação e validação, e administrados por um Sistema Gerenciador de Banco de Dados (SGBD).

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

**Ciclo vital dos documentos** – Sucessivas fases por que passam os documentos arquivísticos, de sua produção à guarda permanente ou eliminação.

**Classe** – Primeira divisão de um plano de classificação ou de um código de classificação.

**Classificação** – Análise e identificação do conteúdo de documentos, seleção da categoria de assunto sob a qual sejam recuperados, podendo-se-lhes atribuir códigos.

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

**Confiabilidade** – Credibilidade de um documento arquivístico enquanto afirmação de um fato.

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

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

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

**Documento** – Unidade de registro de informações, qualquer que seja o suporte ou formato.

**Documento digital** – Informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional.

**Documento eletrônico** – Informação registrada, codificada em forma analógica ou em dígitos binários, acessível e interpretável por meio de equipamento eletrônico.

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

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

**Gestão de documentos** – Conjunto de procedimentos e operações técnicas que engloba a produção, a tramitação, a utilização, a avaliação e o arquivamento em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente. (Lei nº 8.159, de 1991, art. 3).

**Gestor** – Responsável pelo gerenciamento das regras de negócio do sistema. Cabe ao gestor, entre outras atividades, a criação de usuários e atribuição de privilégios.

**Hardware** – Conjunto dos componentes físicos necessários à operação de um sistema computacional.

**Identificador único** – Código gerado automaticamente que identifica o dossiê, processo ou item documental de maneira a distingui-lo dos demais.

**Informação** – Elemento referencial, noção, idéia ou mensagem contida num documento.

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

**Metadado** – Informação que descreve e contextualiza o dado.

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

**Minuta** – Versão preliminar de documento sujeita a aprovação

**Original** – Primeiro documento completo e efetivo.

**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.

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

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

**Recolhimento** – Entrada de documentos em arquivos permanentes.

**Sistema de informação** – Conjunto organizado de políticas, procedimentos, pessoas, equipamentos e programas computacionais que produzem, processam, armazenam e provêem acesso à informação.

**Software** – Ver programa de computador .

**Suporte** – Base física sobre a qual a informação é registrada.

**Tramitação** – Curso do documento desde a sua produção ou recepção até o cumprimento de sua função administrativa. Também chamado movimentação ou trâmite.

**Transferência** – Passagem de documentos do arquivo corrente para o arquivo intermediário.

**Usuário autorizado** – Aquele que possui níveis de acesso diferenciados atribuídos pelo gestor.

**Versão** – Uma ou mais variantes de um mesmo documento.

**Via original** – Primeiro documento completo e efetivo.



## **APÊNDICES**

## Apêndice A – Metadados quadro individual

Para um melhor entendimento do quadro coloca-se os seguintes conceitos para esclarecimento sobre o documento Diário de Classe e outros.

**Definição:** O Diário de Classe é um documento oficial da UFSM, utilizado para controle da frequência e aproveitamento dos alunos, além do registro do conteúdo ministrado.

**Palavras-chave:** frequência, aproveitamento e conteúdo ministrado.

**Entidade:** Abrange as informações e ações que nela ocorrem;

**Elemento:** Indicação do nome atribuído ao metadado;

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

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

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

<b>ENTIDADE DOCUMENTO</b>	
Elemento	<b>Identificador do documento</b>
Definição	Identificador único atribuído ao documento no ato de sua captura (Interno do sistema).
Objetivo	Identificar de forma unívoca o documento para que o Sistema possa gerenciá-lo.
Requisitos que atendem à Gestão do Diário	1.6.2 / 3.1.5 / 3.1.7 / 3.1.9 / 5.2.6 / 6.8.3
Elemento	<b>Tipo de meio</b>
Definição	Digital.
Objetivo	Identificar se o documento é digital, não digital ou híbrido para controlar as relações entre os meios e o monitoramento de preservação.
Requisitos que atendem à Gestão do Diário	3.4 / 4.3.13
Elemento	<b>Status</b>
Definição	Original

Objetivo	Identificar o grau de formalização do documento e as relações existentes entre os originais, as minutas e as cópias. Manter um controle sobre a disposição de cópias.
Requisitos que atendem à Gestão do Diário	2.2.1 / 2.2.4
Elemento	<b>Identificador de versão</b>
Definição	Identificação da versão do documento
Objetivo	Identificar a versão do documento e estabelecer a relação entre as versões anteriores e posteriores.
Requisitos que atendem à Gestão do Diário	2.2.2 / 3.1.5 / 3.1.18
Elemento	<b>Título</b>
Definição	Diário de Classe.
Objetivo	Identificar o documento e servir como elemento de acesso ao documento
Requisitos que atendem à Gestão do Diário	3.1.5 / 5.2.6
Elemento	<b>Descrição</b>
Definição	O Diário de Classe é um documento oficial da UFSM, utilizado para controle da frequência e aproveitamento dos alunos, além do registro do conteúdo ministrado. Ele é gerado nos departamentos didáticos, sob a responsabilidade do(s) professor(es) de cada disciplina.
Objetivo	Identificar o conteúdo do documento e facilitar a pesquisa.
Requisitos que atendem à Gestão do Diário	3.1.5 / 3.1.11
Elemento	<b>Assunto</b>
Definição	Frequência, aproveitamento, disciplina e conteúdo ministrado
Objetivo	Referir de forma sucinta o teor geral do documento.
Requisitos que atendem à Gestão do Diário	3.1.5 / 3.1.11/ 3.2.11 / 5.2.6

Elemento	<b>Autor</b>
Definição	Nome e Siape dos Docentes responsáveis pela disciplina.
Objetivo	Identificar o autor do documento. Fornecer informação sobre o contexto de produção do documento. Demonstrar a autenticidade de um documento, indicando o responsável direto pela sua produção.
Requisitos que atendem à Gestão do Diário	3.1.5 / 5.2.6
Elemento	<b>Destinatário</b>
Definição	Todos os envolvidos
Objetivo	Identificar o destinatário do documento. Fornecer informação sobre o contexto de produção do documento. Demonstrar a autenticidade de um documento, indicando a quem ele é dirigido.
Requisito que atende à Gestão do Diário	3.1.5
Elemento	<b>Originador</b>
Definição	Docente responsável pela geração do Diário de Classe
Objetivo	Identificar o originador do documento. Fornecer informação sobre o contexto de produção do documento. Demonstrar a autenticidade de um documento, indicando o responsável legal pela sua emissão.
Requisitos que atendem à Gestão do Diário	3.1.5 / 5.2.6
Elemento	<b>Redator</b>
Definição	Responsável (eis) pela elaboração do conteúdo do documento. (log de redação).
Objetivo	Identificar o redator do documento. Fornecer informação sobre o contexto de produção do documento. Demonstrar a autenticidade de um documento, indicando o responsável pela articulação do seu conteúdo.
Requisitos que atendem à	3.1.5 / 5.2.6 / 1.1.65



Gestão do Diário	
Elemento	<b>Procedência</b>
Definição	UFMS – Departamento ou Curso da disciplina.
Objetivo	Apóia a administração das unidades de protocolo e outras unidades de registro arquivístico. Apóia a presunção de autenticidade de um documento, indicando a procedência do seu registro. Facilitar a pesquisa.
Requisitos que atendem à Gestão do Diário	1.1.5.3 / 3.1.6 / 5.2.6
Elemento	<b>Identificador do componente digital</b>
Definição	Identificador dos componentes digitais do sistema que integram o documento.
Objetivo	Estabelecer a relação entre o documento e os componentes digitais necessários para apresentá-lo.
Requisitos que atendem à Gestão do Diário	3.1.7 / 3.1.9 / 3.1.21
Elemento	<b>Gênero</b>
Definição	Textual.
Objetivo	Monitorar os diversos gêneros documentais de um acervo para fins de gestão arquivística. Facilitar a pesquisa.
Requisito que atende à Gestão do Diário	3.1.5
Elemento	<b>Espécie</b>
Definição	Diário.
Objetivo	Complementar a descrição do documento. Facilitar a pesquisa.
Requisito que atende à Gestão do Diário	3.1.5
Elemento	<b>Tipo</b>
Definição	Diário de Classe.
Objetivo	Complementar a descrição do documento ou a identificação

	do título. Permite a pesquisa limitada a um determinado tipo.
Requisito que atende à Gestão do Diário	3.1.5
<b>Relação com outros documentos</b>	
Elemento	<b>Relação com outros documentos</b>
Definição	Registro das relações significantes de um documento com outro, ou seja, relação no sistema entre as versões, ou até mesmo a relação com o papel.
Objetivo	Tornar explícito o relacionamento e facilitar o processamento automático e o gerenciamento arquivístico. Demonstrar a organicidade dos documentos.
Requisitos que atendem à Gestão do Diário	3.1.5 / 3.1.10 / 1.1.21
<b>Níveis de acesso</b>	
Elemento	<b>Níveis de acesso</b>
Definição	Os docentes da disciplina, chefes de Departamento/Curso e DERCA.
Objetivo	Garantir o acesso somente a pessoas autorizadas.
Requisitos que atendem à Gestão do Diário	3.1.5 / 6.3.1
<b>Data da produção</b>	
Elemento	<b>Data da produção</b>
Definição	Data, hora e local de quando for gerado.
Objetivo	Indicar local e data em que foi produzido o documento.
Requisitos que atendem à Gestão do Diário	1.3.1 / 3.1.5 / 3.3.1 / 5.2.6
<b>Classe</b>	
Elemento	<b>Classe</b>
Definição	Apoio de Ensino
Objetivo	Identificar a localização intelectual do documento no âmbito da estrutura orgânica ou funcional.
Requisitos que atendem à Gestão do Diário	1.2.1 / 1.5.3 / 3.1.5 / 3.1.10 / 5.2.6
<b>Destinação prevista</b>	
Elemento	<b>Destinação prevista</b>

Definição	Recolhimento.
Objetivo	Apoiar o controle do ciclo de vida do documento.
Requisitos que atendem à Gestão do Diário	1.5.3 / 4.2.1 / 4.2.4
<b>Elemento</b>	
Definição	<b>Prazo de guarda</b>
Objetivo	Guarda permanente.
Objetivo	Apoiar o controle do ciclo de vida do documento. Servir de prova.
Requisitos que atendem à Gestão do Diário	1.5.3 / 3.1.5 / 4.1.2 / 4.2.4
<b>Elemento</b>	
Definição	<b>Localização</b>
Objetivo	Base de dados do CPD-UFSM.
Objetivo	Permitir a localização dos documentos em qualquer mídia. Monitorar o armazenamento de documentos.
Requisitos que atendem à Gestão do Diário	1.1.6.5 / 3.1.5 / 3.4.1 / 3.4.2
<b>ENTIDADE EVENTO DE GESTÃO</b>	
Elemento	<b>Captura</b>
Definição	Descreve a captura do documento.
Objetivo	Registrar informações tais como: identificação do documento, data/hora da captura, responsável pela captura.
Requisitos que atendem à Gestão do Diário	3.1.5 / 3.1.6 / 2.2.1 / 3.3.1 / 3.4.1 / 6.4.1
<b>Elemento</b>	
Definição	<b>Tramitação</b>
Objetivo	Registro da tramitação do documento.
Objetivo	Registrar informações tais como: identificação do documento, data/hora de transmissão, remetente, data/hora do recebimento, destinatário, situação do trâmite.
Requisitos que atendem à Gestão do Diário	3.1.5 / 2.1.20
<b>Elemento</b>	
Definição	<b>Transferência</b>

Definição	Registro do procedimento de transferência de documentos.
Objetivo	Registrar informações tais como: data/hora de envio, data/hora de recebimento, destinatário, método utilizado, responsável pela transferência, responsável pelo recebimento, localização/suporte anterior, localização/suporte atual, identificação do lote, número do termo de transferência.
Requisitos que atendem à Gestão do Diário	4.1.4 / 6.8.3
<b>Elemento</b>	
<b>Recolhimento</b>	
Definição	Registro do procedimento de recolhimento dos documentos.
Objetivo	Registrar informações tais como: data/hora de envio, data/hora de recebimento, destinatário, método utilizado, responsável pelo recolhimento, localização/ suporte anterior, localização/suporte atual, identificação do lote, número do termo de recolhimento.
Requisito que atende à Gestão do Diário	4.1.4
<b>Elemento</b>	
<b>Classificação_sigilo</b>	
Definição	Registro do procedimento de classificação de sigilo.
Objetivo	Registrar informações referentes à classificação de grau de sigilo, tais como: grau de sigilo, data/hora da classificação, responsável pela classificação.
Requisitos que atendem à Gestão do Diário	1.6.8 / 6.3
<b>Elemento</b>	
<b>Desclassificação_sigilo</b>	
Definição	Registro do procedimento de desclassificação de sigilo.
Objetivo	Registrar informações referentes à desclassificação do grau de sigilo, tais como: grau de sigilo, data/hora da desclassificação, responsável pela classificação.
Requisitos que atendem à Gestão do Diário	6.3
<b>Elemento</b>	
<b>Reclassificação_sigilo</b>	

Definição	Registro do procedimento de reclassificação de sigilo.
Objetivo	Registrar informações referentes à reclassificação do grau de sigilo, tais como: data/hora da reclassificação, responsável pela reclassificação e justificativa.
Requisitos que atendem à Gestão do Diário	Ver seção 6.3
<b>ENTIDADE CLASSE</b>	
<b>Descrição da classe</b>	
Elemento	<b>Classe_nome</b>
Definição	Apoio de Ensino.
Objetivo	Estas informações auxiliam o acompanhamento nas mudanças das ações em relação à classificação arquivística.
Requisito que atende à Gestão do Diário	1.1.11
Elemento	<b>Classe_código</b>
Definição	Ainda não foi definido.
Objetivo	Estas informações auxiliam o acompanhamento nas mudanças das ações em relação à classificação arquivística.
Requisito que atende à Gestão do Diário	1.1.11
Elemento	<b>Classe_subordinação</b>
Definição	Grupo: Centro de Ensino; Sub-grupo: Departamento Didático Classe: Apoio de Ensino.
Objetivo	Estas informações auxiliam o acompanhamento nas mudanças das ações em relação à classificação arquivística.
Requisito que atende à Gestão do Diário	1.1.13
Elemento	<b>Registro de abertura</b>
Definição	Primeiro registro será o do cadastro, registrará data, hora e responsável.
Objetivo	Estas informações auxiliam o acompanhamento nas mudanças das ações em relação à classificação arquivística.

Requisito que atende à Gestão do Diário	1.1.4
<b>Reativação de classe</b>	
Definição	Registro da data, hora e responsável.
Objetivo	Estas informações auxiliam o acompanhamento nas mudanças das ações em relação à classificação arquivística.
Requisito que atende à Gestão do Diário	1.1.4
<b>Registro de mudança de nome de classe</b>	
Definição	Registro da data, hora e responsável.
Objetivo	Estas informações auxiliam o acompanhamento nas mudanças das ações em relação à classificação arquivística.
Requisito que atende à Gestão do Diário	1.1.4
<b>Registro de deslocamento de classe</b>	
Definição	Registro da data, hora e responsável.
Objetivo	Estas informações auxiliam o acompanhamento nas mudanças das ações em relação à classificação arquivística.
Requisito que atende à Gestão do Diário	1.1.4
<b>Registro de extinção</b>	
Definição	Registro da data, hora e responsável.
Objetivo	Estas informações auxiliam o acompanhamento nas mudanças das ações em relação à classificação arquivística.
Requisito que atende à Gestão do Diário	1.1.4

Elemento	<b>Indicador de classe ativa/inativa</b>
Definição	Registro da data, hora e responsável.
Objetivo	Estas informações auxiliam o acompanhamento nas mudanças das ações em relação à classificação arquivística.
Requisito que atende à	1.1.4

Gestão do Diário	
<b>Temporalidade associada à classe</b>	
Elemento	<b>Classe_código</b>
Definição	Ainda não foi definido.
Objetivo	Estas informações auxiliam o acompanhamento nas mudanças das ações em relação à avaliação e a classificação arquivística.
Requisito que atende à Gestão do Diário	4.1.3
<b>Prazo de guarda na fase corrente</b>	
Elemento	<b>Prazo de guarda na fase corrente</b>
Definição	Durante o semestre letivo
Objetivo	Estas informações auxiliam o acompanhamento nas mudanças das ações em relação à avaliação e a classificação arquivística.
Requisito que atende à Gestão do Diário	4.1.3
<b>Evento que determina a contagem do prazo de guarda na fase corrente</b>	
Elemento	<b>Evento que determina a contagem do prazo de guarda na fase corrente</b>
Definição	Momento em que o Diário de Classe é gerado.
Objetivo	Estas informações auxiliam o acompanhamento nas mudanças das ações em relação à avaliação e a classificação arquivística.
Requisito que atende à Gestão do Diário	4.1.3
<b>Prazo de guarda na fase intermediária</b>	
Elemento	<b>Prazo de guarda na fase intermediária</b>
Definição	Cinco anos
Objetivo	Estas informações auxiliam o acompanhamento nas mudanças das ações em relação à avaliação e a classificação arquivística.
Requisito que atende à Gestão do Diário	4.1.3

Elemento	<b>Evento que determina a contagem do prazo de guarda na fase intermediária</b>
Definição	Final do semestre letivo subsequente à produção do Diário de Classe.
Objetivo	Estas informações auxiliam o acompanhamento nas mudanças das ações em relação à avaliação e a classificação arquivística.
Requisito que atendem à Gestão do Diário	4.1.3
<b>Destinação final</b>	
Elemento	<b>Destinação final</b>
Definição	Guarda permanente.
Objetivo	Estas informações auxiliam o acompanhamento nas mudanças das ações em relação à avaliação e a classificação arquivística.
Requisito que atende à Gestão do Diário	4.1.3
<b>Registro de alteração</b>	
Elemento	<b>Registro de alteração</b>
Definição	Registro detalhado das alterações.
Objetivo	Registrar informações tais como: data/hora da alteração, responsável, identificador da classe que teve prazo ou destinação alterada, descrição da alteração (incluindo o prazo/destinação anterior).
Requisitos que atendem à Gestão do Diário	4.1.7 / 4.1.8 / 4.1.9
<b>Observações</b>	
Elemento	<b>Observações</b>
Definição	Informações adicionais.
Objetivo	Informações complementares como: previsão de conversão de suporte, legislação relativa à justificativa de prazos.
Requisito que atende à Gestão do Diário	4.1.3
<b>ENTIDADE AGENTE</b>	
Elemento	<b>Nome</b>



Definição	Nome do agente.
Objetivo	Poder de utilização do agente responsável pela operação no Diário e auxiliar na garantia da autenticidade e acesso.
Requisito que atende à Gestão do Diário	6.2.1
Elemento	<b>Identificador</b>
Definição	Siape do agente.
Objetivo	Poder de utilização do agente responsável pela operação no Diário e auxiliar na garantia da autenticidade e acesso.
Requisitos que atendem à Gestão do Diário	6.2.1 / 6.2.3
Elemento	<b>Autorização de acesso</b>
Definição	Nível de restrição de acesso (uso e intervenção) aos documentos e operações do sistema.
Objetivo	Poder de utilização do agente responsável pela operação no Diário e auxiliar na garantia da autenticidade e acesso.
Requisitos que atendem à Gestão do Diário	6.2.1 / 6.2.3 / 6.2.8
Elemento	<b>Credenciais de autenticação</b>
Definição	Autentica o usuário no Sistema. Pode ser: senha.
Objetivo	Poder de utilização do agente responsável pela operação no Diário e auxiliar na garantia da autenticidade e acesso.
Requisitos que atendem à Gestão do Diário	6.2.1 / 6.2.4
Elemento	<b>Relação</b>
Definição	Relaciona o usuário ao seu papel (funções). <ul style="list-style-type: none"> <li>• tem papel</li> </ul>
Objetivo	Poder de utilização do agente responsável pela operação no Diário e auxiliar na garantia da autenticidade e acesso.
Requisitos que atendem à Gestão do Diário	6.2.11 / 6.2.15

Elemento	<b>Status do agente</b>
Definição	Indica se o agente está ativo ou inativo no Sistema.
Objetivo	Poder de utilização do agente responsável pela operação no Diário e auxiliar na garantia da autenticidade e acesso.
Requisito que atende à Gestão do Diário	6.2.1
<b>ENTIDADE COMPONENTE DIGITAL</b>	
Elemento	<b>Identificador do componente digital</b>
Definição	Designação usada para identificar os componentes digitais que integram o documento.
Objetivo	Identificar que o Diário de Classe é um documento único.
Requisito que atende à Gestão do Diário	3.1.21
Elemento	<b>Características técnicas</b>
Definição	Propriedades técnicas de um componente digital, aplicáveis à maioria dos formatos, tais como: nível de composição, tamanho, software de criação e inibidores.
Objetivo	Fornecer informações para apoiar ações de acesso, manutenção e preservação.
Requisitos que atendem à Gestão do Diário	Seção 8 (Preservação)
Elemento	<b>Formato de arquivo</b>
Definição	PDF.
Objetivo	Conhecer o formato de arquivo do componente digital é essencial para planejamento e implementação das ações de preservação.
Requisitos que atendem à Gestão do Diário	3.5
Elemento	<b>Armazenamento</b>
Definição	Informações sobre a localização e o suporte do componente digital, bem como os recursos necessários para

	armazenamento permanente.
Objetivo	Localizar o componente digital no armazenamento. E o suporte em que o componente digital está armazenado ajudam o monitoramento das ações de preservação.
Requisito que atende à Gestão do Diário	6.1.7
<b>Elemento</b>	
<b>Ambiente de <i>software</i></b>	
Definição	Informações sobre o ambiente de <i>software</i> necessário para apresentar e/ou usar os componentes digitais, incluindo a aplicação e o sistema operacional.
Objetivo	Informar o ambiente de <i>software</i> necessário para uso.
Requisitos que atendem à Gestão do Diário	Seção 8 (Preservação)
<b>Elemento</b>	
<b>Ambiente de <i>hardware</i></b>	
Definição	Informações sobre os componentes de <i>hardware</i> necessário para operar o software referenciado em 5.6, incluindo periféricos.
Objetivo	Informar o ambiente de <i>hardware</i> necessário para operação.
Requisitos que atendem à Gestão do Diário	Seção 8 (Preservação)
<b>Relação com outros componentes digitais</b>	
<b>Relacionamento</b>	
Definição	Relacionamento entre as versões de um mesmo Diário de Classe.
Objetivo	Explicitar o relacionamento entre componentes digitais para possibilitar o processamento e acesso aos documentos e identificar os tipos de relação (estrutural ou de derivação). Alguns documentos são formados por diversos componentes digitais relacionados, (relações estruturais). Outros podem ser armazenados de formas diferentes, como, documento máster e documento derivado, ou o original e cópias de <i>backup</i> (relações de derivação).
Requisitos que atendem à	Seção 8 (Preservação)

Gestão do Diário	
<b>Elemento</b>	<b>Fixidade</b>
Definição	Informações utilizadas para verificar se o componente digital sofreu mudanças não documentadas.
Objetivo	Verificar se o componente digital foi alterado de forma não documentada/autorizada, comprometendo sua autenticidade.
Requisitos que atendem à Gestão do Diário	6.5.3 / 6.5.4 / 6.6.3 / 6.6.6 / Seção 8 (Preservação)
<b>ENTIDADE EVENTO DE PRESERVAÇÃO</b>	
<b>Elemento</b>	<b>Validação de assinatura digital</b>
Definição	Registro de validação da assinatura digital de um documento de acordo com o certificado digital deste.
Objetivo	Registrar informações tais como: identificação da validação, data da validação, agente responsável pela validação e resultados da validação.
Requisitos que atendem à Gestão do Diário	6.5.1 / 6.5.4 / 6.5.5 / 8.3.1 / 8.3.6
<b>Elemento</b>	<b>Verificação de fixidade</b>
Definição	Registro da verificação de fixidade de um documento, ou seja, se os recursos utilizados para garantir a fixidade não foram corrompidos.
Objetivo	Registrar informações como: tipo de recurso de autenticação, identificação da verificação, data da verificação, agente responsável pela verificação e resultados da verificação.
Requisitos que atendem à Gestão do Diário	6.5.5 / 6.7.2 / 8.2.6 / 8.3.1 / 8.3.6
<b>Elemento</b>	<b>Migração</b>
Definição	Registro de procedimento de migração de documento.
Objetivo	Registrar informações tais como: identificação da migração, data da migração, agente responsável pela migração, resultado e conseqüências da migração.
Requisitos que atendem à	3.1.5 / 8.3.1 / 8.3.6

Gestão do Diário	
Elemento	<b>Replicação</b>
Definição	Registro de procedimento de replicação de documento.
Objetivo	Registrar informações tais como: identificação da replicação, data da replicação, agente responsável pela replicação e conseqüências da replicação.
Requisitos que atendem à Gestão do Diário	6.10.7 / 8.3.1 / 8.3.6
Elemento	<b>Verificação de vírus</b>
Definição	Registro de verificação de vírus no documento.
Objetivo	Registrar informações tais como: identificação da verificação, data da verificação, agente responsável pela verificação e detalhes da verificação.
Requisitos que atendem à Gestão do Diário	6.9.1 / 8.3.1 / 8.3.6
Elemento	<b>Validação</b>
Definição	Registro de validação de documento.
Objetivo	Registrar informações tais como: identificação da validação, data da validação, agente responsável pela validação e detalhes da validação.
Requisitos que atendem à Gestão do Diário	7.3.1 / 7.3.2 / 7.3.4 / 7.3.5
<b>ENTIDADE TRILHA DE AUDITORIA</b>	
Elemento	<b>Histórico da Intervenção</b>
Definição	Registrar o histórico de todas as intervenções, ou tentativas de intervenção, feitas no documento e no próprio Sistema.
Objetivo	A trilha de auditoria consiste num histórico de todas as intervenções, ou tentativas, feitas no documento e no próprio Sistema. Informar sobre autenticidade do documento.
Requisitos que atendem à Gestão do Diário	6.4.1 / 6.4.2 / 6.4.3 / 6.4.4 / 6.4.5 / 6.4.6 / 6.4.7

## Apêndice B – Requisitos para o diário de classe eletrônico

### O DIÁRIO DEVE:

Ref.	Requisitos
1.1.1 / 1.1.11	Possuir identificado no sistema a sua classificação arquivística, através de um identificador da classe e subclasse.
1.1.19	A classificação deve ser automática, somente na classe/subclasse autorizada.
1.1.24 / 1.1.25 / 4.2.8	O diário deve incorporar os metadados e temporalidades predefinidos da classe a qual pertence, sendo necessária a atualização automática quando houverem alterações nesses metadados ou temporalidade.
4.1.2	A temporalidade do Diário deve estar associada à temporalidade da classe a qual ele está vinculado, e associado automaticamente no momento da produção.
4.1.6	Expressar o prazo de guarda em n° de anos.
4.1.8 / 4.1.9 / 4.2.7	O sistema deve permitir a alteração nos prazos de guarda somente por usuários autorizados, mantendo um histórico das alterações.
1.1.27 / 1.1.28 / 1.1.29	Deve haver a possibilidade de reclassificação do Diário, somente por usuário autorizado. Porém, deve-se manter os registros da posição anterior. Essa reclassificação deve ser acompanhada por uma justificativa.
1.1.31	O diário deve possuir como metadado a sua data de produção.
1.1.32	O encerramento e geração do Diário devem ser realizado somente por usuário autorizado e identificado.
1.1.33	Garantir a consulta dos Diários apenas por usuários autorizados.
1.1.37	A relação hierárquica do Diário e da sua classe deve ser sempre mantida.
1.1.65	O sistema deve registrar trilhas de auditoria de toda e qualquer alteração nos metadados do Diário.
2.2.1	O Diário deve apresentar seu <i>Status</i> atual, se é minuta ou original.
2.2.4 / 3.1.7 / 3.1.8 / 3.1.10 / 5.2.5	O sistema tem que manter o identificador único do documento e o controle de versões tem que ser registrado em metadados específicos. Identificador único do Diário (ver 3.1.9)
3.1.5 / 3.1.6	O Diário deve manter associado os metadados: <ul style="list-style-type: none"> <li>- nome do arquivo</li> <li>- n° identificador</li> <li>- data de produção</li> <li>- data e hora de transmissão e recebimento</li> <li>- data e hora da captura</li> <li>- título ou descrição abreviada</li> <li>- classificação de acordo com o plano</li> <li>- prazo de guarda</li> <li>- autor</li> <li>- redator</li> <li>- originador</li> <li>- destinatário</li> <li>- setor responsável</li> <li>- indicação de anotações/ anexos/versão</li> <li>- restrição de acesso</li> <li>- registro das migrações e data de ocorrência</li> </ul> OPCIONAIS: <ul style="list-style-type: none"> <li>- associação a documentos diferentes</li> </ul>

	- formato e software - templates (estrutura)
3.1.11	Ver lista de assuntos do governo (e-ping)
3.1.12 / 3.1.13	Somente usuários autorizados podem inserir e alterar metadados ao Diário, sendo obrigatório o registro de trilha de auditoria das alterações.
3.1.15 / 3.1.16	O sistema pode inserir automaticamente metadados já previstos, e permitir a entrada de outros metadados por usuários autorizados.
3.1.17	Deve ser permitida a inserção de novos metadados após o Diário já gerado. Ex. data e hora de mudança de suporte ou formato.
3.1.18	Permitir o registro e associação quando houver mais de uma versão do Diário (no caso de alguma alteração de conteúdo, em que gera-se outro original)
3.6.1 / 3.6.2 / 3.6.3	Definir a estrutura dos procedimentos de gestão (quem pode e quem faz o que).
4.3.1	O Diário deve estar preparado para ser exportado para outro sistema, juntamente com seus metadados.
4.3.3 / 4.3.11	Os metadados nunca devem se dissociar do Diário.
5.2.3	Deve poder-se realizar pesquisas no conteúdo dos metadados.
5.2.6	Deve-se poder pesquisar no mínimo com: - identificador - título - assunto - datas - procedência / interessado - autor / redator / originador - planos de classificação
5.3.7	Salvar em PDF justamente para manter as características estruturais de layout.
5.3.9	Deve-se manter o formato do Diário no momento da impressão.
5.3.12	Deve-se poder visualizar e imprimir os metadados do Diário.
5.3.19	O Diário deve estar acessível simultaneamente para mais de um usuário.
5.3.20	Pode permitir ao administrador imprimir o conteúdo do Diário junto com metadados pré-selecionados.
6.1.1	Os <i>backups</i> devem conter além do conteúdo do documento original, todos os metadados e padrões do sistema.
6.1.2 / 6.1.4	Deve-se ter cópias de segurança, prevendo testes de restauração, e <i>backups</i> em 2 locais diferentes e fisicamente distantes.
6.1.5	Os backups devem ser agendados automaticamente.
6.1.6	Dispor de autenticação digital das cópias se segurança, garantindo a integridade dos dados e a identificação do responsável pelo procedimento.
6.1.9	Trilhas de auditoria devem ser copiadas freqüentemente, prevendo armazenamento pelo menos em um lugar <i>off-site</i> .
6.2.1	Ao implementar o controle de acesso tem que manter pelo menos os seguintes atributos dos usuários, de acordo com a política de segurança: - identificador do usuário; - autorização de acesso; - credenciais de autenticação. Ex. senha, chave criptográfica e outros.
6.2.2	Exigir que o usuário esteja devidamente identificado e autenticado antes de iniciar qualquer operação no sistema.
6.2.3	Garantir que os valores dos atributos de segurança e controle de acesso, associados ao usuário, estejam dentro de conjuntos de valores válidos.
6.2.4	Alterar as credenciais de autenticação só pelo usuário proprietário ou pelo administrador, com a anuência do proprietário e em conformidade com a

	política de segurança.
6.2.5	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.
6.2.6	Se o usuário solicitar o acesso ou pesquisa de um documento arquivístico, volume ou dossiê/processo específico a que não tenha direito de acesso, um Sistema Integrado de Gestão Arquivística de Documentos (SIGAD) deve fornecer a seguinte resposta (estabelecida durante a configuração): Não mostrar qualquer informação do documento, nem indicar a sua existência.
6.2.8	Um SIGAD deve implementar, imediatamente, alterações ou revogações dos atributos de segurança de usuários e de documentos digitais.
6.2.16	Um SIGAD tem que usar os seguintes atributos dos documentos digitais ao implementar a política de controle de acesso por papéis: <ul style="list-style-type: none"> <li>· identificação do documento digital;</li> <li>· operações permitidas aos vários papéis de usuários, sobre as classes ou unidades de arquivamento a que o documento pertence.</li> </ul>
6.4.1	Um SIGAD tem que ser capaz de registrar, na trilha de auditoria, informações acerca das ações a seguir: <ul style="list-style-type: none"> <li>· data e hora da captura de todos os documentos;</li> <li>· responsável pela captura;</li> <li>· reclassificação, desclassificação ou redução do grau de sigilo de um documento ou dossiê/processo, com a classificação inicial e final.</li> <li>· qualquer alteração na tabela de temporalidade e destinação de documentos;</li> <li>· qualquer ação de reavaliação de documentos;</li> <li>· qualquer alteração nos metadados associados a classes, dossiês/ processos ou documentos;</li> <li>· data e hora de produção, aditamento e eliminação de metadados;</li> <li>· alterações efetuadas nas permissões de acesso que afetem um dossiê/processo, documento ou usuário;</li> <li>· ações de exportação e importação envolvendo os documentos;</li> <li>· tentativas de exportação (inclusive para <i>backup</i>) e importação (inclusive <i>restore</i>);</li> <li>· usuário, data e hora de acesso ou tentativa de acesso a documentos e ao SIGAD;</li> <li>· tentativas de acesso negado a qualquer documento;</li> <li>· ações de eliminação de qualquer documento e seus metadados;</li> <li>· infrações cometidas contra mecanismos de controle de acesso;</li> <li>· mudanças no relógio gerador de carimbos de tempo;</li> <li>· todas as ações administrativas sobre os atributos de segurança (papéis, grupos, permissões etc.);</li> <li>· todas as ações administrativas sobre dados de usuários (cadastro, ativação, bloqueio, atualização de dados e permissões, troca de senha etc.);</li> <li>· todos os eventos de administração e manutenção das trilhas de auditoria (alarmes, cópias, configuração de parâmetros etc.).</li> </ul>
6.4.4	Um SIGAD tem que assegurar que as informações da trilha de auditoria estejam disponíveis para inspeção, a fim de que uma ocorrência específica possa ser identificada e todas as informações correspondentes sejam claras e compreensíveis.
6.4.5	Um SIGAD deve possuir mecanismos para realização de buscas nos eventos das trilhas de auditoria. Para facilitar a visualização do relatório, os resultados podem ser apresentados de modo ordenado, mas essa ordenação não pode alterar os dados incluídos na trilha.
6.4.6	Um SIGAD tem que ser capaz de impedir qualquer modificação na trilha de



	auditoria.
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. <i>Todas as outras operações estarão bloqueadas até a liberação pelo administrador.</i>
6.5.1	Um SIGAD deve ser capaz de garantir a origem e a integridade dos documentos com assinatura digital.
6.5.3	Um SIGAD tem que ser capaz de verificar a validade da assinatura digital no momento da captura do documento.
6.5.5	Um SIGAD deve ser capaz de armazenar, juntamente com o documento, as informações de certificação a seguir: <ul style="list-style-type: none"> <li>· assinatura digital;</li> <li>· certificado digital (cadeia de certificação) usado na verificação da assinatura;</li> <li>· lista de certificados revogados (LCR). 6.5.6</li> </ul>
6.9.1	Um SIGAD deve fazer a verificação de vírus ou pragas antes da efetivação da captura.
6.9.2	Um SIGAD deve ter dispositivos e procedimentos que reduzam a possibilidade de erros, falhas e descontinuidades no seu funcionamento, capazes de causar danos ou perdas aos documentos arquivísticos digitais.
6.9.3	Após falha ou descontinuidade do sistema, quando a recuperação automática não for possível, um SIGAD tem que ser capaz de entrar em modo de manutenção, no qual é oferecida a possibilidade de restaurar o sistema para um estado seguro. <i>Na restauração ao estado seguro, um SIGAD deve ser capaz de garantir a recuperação de perdas ocorridas, inclusive dos documentos de transações mais recentes</i>
6.9.4	Um SIGAD deve garantir que os dados de segurança, quando replicados, sejam consistentes. <i>Permissões de controle de acesso, chaves criptográficas e parâmetros de algoritmos criptográficos são exemplos de dados de segurança.</i>
6.9.9	Um SIGAD pode atribuir a cada documento, no momento da captura, um código de manutenção de integridade baseado em criptografia robusta.
6.10.4	Em caso de erro na inserção de metadados, o administrador terá que corrigi-lo, e o SIGAD tem que registrar essa ação na trilha de auditoria.
6.10.5	Um SIGAD tem que permitir a um usuário autorizado fazer um extrato (cópia truncada) de um documento, com o objetivo de não alterar o original.
6.10.7	Quando uma cópia truncada é produzida, um SIGAD tem que registrar essa ação nos metadados do documento, incluindo, pelo menos, data, hora, motivo e quem a produziu.
7.1.2	A escolha de dispositivos tem que ser revista sempre que a evolução tecnológica indicar mudanças importantes.
7.1.3	Atividades de migração têm que ser efetivadas, preventivamente, sempre que se torne patente ou previsível a obsolescência do padrão corrente.
7.2.1	Um SIGAD tem que possuir capacidade de armazenamento suficiente para acomodação de todos os documentos e suas cópias de segurança. <i>Para grandes volumes de dados, é conveniente o uso de dispositivos com maior capacidade unitária de armazenamento, a fim de reduzir a sobrecarga operacional.</i>
7.3.2	Um SIGAD tem que utilizar técnicas de restauração de dados em caso de falhas.
7.3.3	Um SIGAD tem que utilizar mecanismos de proteção contra escrita, que previnam alterações indevidas e mantenham a integridade dos dados armazenados.
7.3.4	A infraestrutura de um SIGAD deve prever o uso de técnicas para garantir

	<p>maior confiabilidade e desempenho. As técnicas recomendadas incluem:</p> <ul style="list-style-type: none"> <li>· espelhamento (<i>mirroring</i>) nas memórias secundárias para maior confiabilidade;</li> <li>· partição de dados (<i>data stripping</i>) nas memórias secundárias para maior desempenho.</li> </ul>
7.3.5	A integridade dos dispositivos de armazenamento tem que ser, periodicamente, verificada.
8.1.1	<p>Os suportes de armazenamento de um SIGAD têm que ser acondicionados, manipulados e utilizados em condições ambientais compatíveis com sua vida útil prevista e/ou pretendida, de acordo com as especificações técnicas do fabricante e de entidades isentas, e com base em estatísticas de uso.</p> <p><i>A vida útil pretendida de um suporte pode ser menor que sua vida útil prevista, o que permite condições ambientais mais flexíveis.</i></p>
8.2.1	<p>Um SIGAD tem que manter cópias de segurança.</p> <p><i>As cópias de segurança devem ser guardadas em ambientes seguros, em locais diferentes de onde se encontra a informação original.</i></p>
8.2.3	Um SIGAD tem que permitir a substituição dos dados armazenados que apresentarem erros.
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.
8.2.6	Um SIGAD deve manter um histórico dos resultados da verificação periódica dos dados armazenados.
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.
8.3.1	Um SIGAD tem que registrar, em trilhas de auditoria, as operações de preservação realizadas.
8.3.6	Um SIGAD tem que gerir metadados relativos à preservação dos documentos e seus respectivos componentes.
10.1.2	Um SIGAD tem que estar de acordo com a legislação e as normas específicas para gestão e acesso de documentos arquivísticos
11.1.3	<p>O sistema de ajuda <i>on-line</i> fornecido pelo SIGAD deve ser vinculado à função ou tarefa executada, em todo o sistema.</p> <p><i>Exemplo: Se o usuário estiver executando uma operação de edição, uma vez acionada a ajuda, ela deve remeter ao tópico de ajuda sobre edição.</i></p>
11.1.23	Um SIGAD deve fornecer a usuários finais e administradores funções intuitivas e fáceis de usar, que requeiram poucas ações para completar uma tarefa padrão.
13.1.1	Um SIGAD tem que se adequar ao grau de disponibilidade estabelecido pela organização.

## **ANEXOS**

**ANEXO A – Resolução nº 25, de 27 de abril de 2007.**

CASA CIVIL  
SECRETARIA EXECUTIVA  
ARQUIVO NACIONAL  
CONSELHO NACIONAL DE ARQUIVOS

**RESOLUÇÃO Nº. 25, DE 27 DE ABRIL DE 2007**

Dispõe sobre a adoção do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR.

**O PRESIDENTE DO CONSELHO NACIONAL DE ARQUIVOS - CONARQ**, no uso de suas atribuições, previstas no item IX do art. 23 de seu Regimento Interno, aprovado pela Portaria nº. 5, da Casa Civil da Presidência da República, de 7 de fevereiro de 2002, e de conformidade com a deliberação do Plenário em sua 43ª reunião ordinária, realizada no dia 04 de dezembro de 2006, e

Considerando que o Conselho Nacional de Arquivos tem por finalidade definir a política nacional de arquivos públicos e privados e exercer orientação normativa visando à gestão documental e à proteção especial aos documentos de arquivo, independente da forma ou do suporte em que a informação está registrada;

Considerando que a gestão arquivística de documentos, independente da forma ou do suporte adotados, tem por objetivo garantir a produção, a manutenção, a preservação de documentos arquivísticos confiáveis, autênticos e compreensíveis, bem como o acesso a estes;

Considerando que as organizações públicas e privadas e os cidadãos vêm cada vez mais produzindo documentos arquivísticos exclusivamente em formato digital e que governos, organizações e cidadãos dependem do documento digital como fonte de prova e informação, bem como de garantia de direitos;

Considerando que o artigo 3º da Resolução do CONARQ nº 20, de 16 de julho de 2004, prevê a implantação de um sistema informatizado de gestão arquivística de documentos, com a especificação de requisitos e de metadados para garantir a integridade e a acessibilidade de longo prazo dos documentos arquivísticos;

**RESOLVE:**

Art. 1º Recomendar aos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR a adoção do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil, Versão 1.0, aprovado na 43ª reunião plenária do CONARQ, realizada no dia 4 de dezembro de 2006, de que trata esta Resolução, disponibilizada em pdf na página web do CONARQ, [www.conarq.arquivonacional.gov.br](http://www.conarq.arquivonacional.gov.br).

§1º Considera-se gestão arquivística de documentos o conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento de documentos em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente.

§2º Consideram-se requisitos o 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, bem como seu acesso.

§3º Considera-se sistema informatizado de gestão arquivística de documentos o sistema desenvolvido para produzir, receber, armazenar, dar acesso e destinar documentos arquivísticos em ambiente eletrônico.

Art. 2º O e-ARQ Brasil tem por objetivo orientar a implantação da gestão arquivística de documentos, fornecer especificações técnicas e funcionais, bem como metadados para orientar a aquisição e/ou desenvolvimento de sistemas informatizados, independentes da plataforma tecnológica em que forem desenvolvidos e/ou implantados, referidos no parágrafo 3º do art. 3º da Resolução nº 20, de 16 de julho de 2004.

Parágrafo único. Os metadados mencionados no caput desse artigo serão incluídos na próxima versão. (Incluídos pela Resolução nº 32)

Art. 3º O e-ARQ Brasil é aplicável para os sistemas que produzem e mantêm somente documentos digitais ou para sistemas que compreendem documentos digitais e convencionais ao mesmo tempo.

§1º Para documentos convencionais o sistema inclui apenas o registro das referências nos metadados.

§2º Para documentos digitais, o sistema inclui os próprios documentos.

Art. 4º O CONARQ, por intermédio de sua Câmara Técnica de Documentos Eletrônicos, poderá subsidiar os órgãos e entidades integrantes do SINAR na aplicação do e-ARQ Brasil.

Art. 5º Caberá ao CONARQ, por intermédio de sua Câmara Técnica de Documentos Eletrônicos, proceder à atualização periódica do e-ARQ Brasil.

Art. 6º Esta Resolução entra em vigor na data de sua publicação.

**JAIME ANTUNES DA SILVA**  
Presidente do CONARQ

[Publicado no Diário Oficial da União, Edição nº 81, de 27 de abril de 2007 - Seção 1]

## **ANEXO B – Resolução nº 32, de 17 de maio de 2010**

**CASA CIVIL  
SECRETARIA EXECUTIVA  
ARQUIVO NACIONAL  
CONSELHO NACIONAL DE ARQUIVOS**

### **RESOLUÇÃO Nº 32, DE 17 DE MAIO DE 2010**

**Dispõe sobre a inserção dos Metadados na Parte II do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil**

**O PRESIDENTE DO CONSELHO NACIONAL DE ARQUIVOS - CONARQ**, no uso de suas atribuições, previstas no item IX do art. 23 de seu Regimento Interno, aprovado pela Portaria nº 5, da Casa Civil da Presidência da República, de 7 de fevereiro de 2002, em cumprimento do art. 2º, parágrafo único, da Resolução do CONARQ nº 25, de 27 de abril de 2007, e de conformidade com a deliberação do Plenário em sua 55ª reunião ordinária, realizada no dia 15 de dezembro de 2009, **RESOLVE**:

**Art. 1º** Aprovar a inserção dos Metadados na Parte II do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil, prevista pelo art. 2º, parágrafo único, da Resolução do CONARQ nº 25, de 2007.

**Art. 2º** O Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil, em sua versão 1.1, será publicado e disponibilizado no sítio do CONARQ em: <http://www.conarq.arquivonacional.gov.br> .

**Art. 3º** Esta Resolução entra em vigor na data de sua publicação.

**JAIME ANTUNES DA SILVA**  
Presidente do CONARQ

[Publicado no Diário Oficial da União, Edição nº 93, de 18 de maio de 2010 - Seção 1]