



UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS HUMANAS E SOCIAIS
ESCOLA DE ARQUIVOLOGIA

THAYANE CARVALHO SILVA DE MORAES

GESTÃO DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS: Análise do Sistema
Alfresco

RIO DE JANEIRO

2018

THAYANE CARVALHO SILVA DE MORAES

GESTÃO DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS: ANÁLISE DO SISTEMA
ALFRESCO

Trabalho de conclusão de cursos apresentado à
Escola de Arquivologia, como requisito para obtenção
do Grau de Bacharel em Arquivologia.
Orientadora: Prof^a. Brenda Couto de Brito Rocco

Rio de Janeiro

2018

C827 Carvalho Silva de Moraes, Thayane
GESTÃO DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS:
ANÁLISE DO SISTEMA ALFRESCO / Thayane Carvalho
Silva de Moraes. -- Rio de Janeiro, 2018.
57

Orientadora: Brenda Couto de Brito Rocco.
Trabalho de Conclusão de Curso (Graduação) -
Universidade Federal do Estado do Rio de Janeiro,
Graduação em Arquivologia, 2018.

1. Gestão arquivística de documentos. 2. Sistema
Alfresco. 3. Arquivos digitais. 4. e-Arq Brasil. I.
Couto de Brito Rocco, Brenda, orient. II. Título.

THAYANE CARVALHO SILVA DE MORAES

GESTÃO DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS: ANÁLISE DO SISTEMA
ALFRESCO

Trabalho de conclusão de curso apresentado à Escola de
Arquivologia como requisito para obtenção do Grau de
Bacharel em Arquivologia.

Aprovado em:

BANCA EXAMINADORA

Orientadora: Me. Brenda Couto de Brito Rocco

Prof. Dr. Eliezer Pires da Silva

Prof.^a Dr.^a Priscila Ribeiro Gomes

AGRADECIMENTOS

À Deus em primeiro lugar, por me direcionar desde o início da graduação até finalmente concluir uma etapa tão importante da minha vida.

Aos meus queridos pais Felisberto Cardoso e Ester Carvalho que sempre me incentivaram e me deram força para não desistir e por me proporcionarem toda a base e estrutura que me possibilitaram chegar até aqui.

Ao meu marido amado Léonard Moraes que foi o meu maior suporte sempre acreditando em mim e tornando a minha vida mais leve e alegre ao longo desses anos de graduação.

As minhas irmãs Pamela e Thais por serem grandes inspirações de força de vontade e dedicação sempre me cobrando mas também apoiando.

À minha orientadora Brenda Rocco pela paciência e direcionamento.

Aos professores Eliezer Pires e Priscila Gomes por aceitarem analisar e avaliar esse trabalho

RESUMO

MORAES, Thayane Carvalho Silva de. Gestão de Documentos Arquivísticos Digitais: Análise do Sistema Alfresco. 2018. Trabalho de Conclusão de Curso (Bacharel em Arquivologia). Universidade Federal do Estado do Rio de Janeiro. Rio de Janeiro.

A partir de levantamentos literários arquivísticos sobre Gestão de Documentos Arquivísticos Digitais, foi possível analisar os procedimentos para a implantação do Sistema Alfresco, visando à adequação desse sistema livre disponível no mercado aos requisitos do e-ARQ Brasil 2011. O uso de estratégias de preservação para documentos digitais é prioritário, porque sem elas não seria possível existir uma garantia de acesso, autenticidade e confiabilidade dos documentos a longo prazo. É necessário que se chame a atenção para esta questão devido ao avanço tecnológico que diariamente nos desafia a entender e nos tornar participantes desta nova realidade. A gestão arquivística de documentos digitais é estudada já há algumas décadas, porém as mudanças tecnológicas se dão em um ritmo extremamente acelerado, fazendo com que muitas vezes seja indagado como seria possível acompanhar toda essa mudança constante, desta forma a análise do sistema Alfresco permitiu uma visão real da possibilidade desse sistema ser implementado e gerir conforme as regulamentações do e-Arq Brasil e CONARQ, contribuindo para que gestão de documentos arquivísticos digitais não seja falho mas sim um fato.

Palavras-Chave: Gestão de documentos arquivísticos digitais. E-Arq Brasil. Sistema Alfresco

ABSTRACT

From archival literary surveys on Digital Records Management, it was possible to analyze the procedures for the implementation of the Alfresco System, aiming at the adaptation of this free system available in the market to the requirements of e-ARQ Brazil 2011. The use of preservation strategies for digital documents is a priority because without them a guarantee of long-term access, authenticity and reliability would not be possible. It is necessary to draw attention to this issue due to the technological advance that daily challenges us to understand and become participants in this new reality. The record management of digital documents has been studied for a few decades, but technological changes occur at an extremely rapid pace, making it very often asked how it would be possible to keep up with all this constant change, in this way the Alfresco system analysis allowed a real vision of the possibility of this system being implemented and managed according to the regulations of e-Arq Brasil and CONARQ, contributing to the management of digital archival documents is not a flaw but a fact.

Key words: Management records. E-Arq Brasil. Alfresco System

SUMÁRIO

1. INTRODUÇÃO	10
2. CONCEITOS FUNDAMENTAIS DA ARQUIVOLOGIA	14
2.1. CONCEITO DE ARQUIVO.....	15
2.2. CONCEITO DE DOCUMENTO ARQUIVÍSTICO.....	18
2.3. CONCEITO DE DOCUMENTO ARQUIVÍSTICO DIGITAL.....	20
2.4. CONCEITO DE GESTÃO DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS ..	22
3. SISTEMA INFORMATIZADO DE GESTÃO ARQUIVÍSTICA DE DOCUMENTOS (SIGAD)	26
4. SISTEMA ALFRESCO COM BASE NO e-ARQ BRASIL	29
5. CONSIDERAÇÕES FINAIS	33
REFERÊNCIAS	34
ANEXO	37

1. INTRODUÇÃO

A denominada era da informação trouxe uma nova realidade, as TIC's, que se equivalem de meios técnicos para o tratamento da informação auxiliando a comunicação, em qualquer condição de transmissão de informações, culminando no surgimento de novos desafios para os profissionais de arquivo que trabalham em unidades de informação e centros de informação, sendo eles públicos ou privados. E para que ele, o arquivista contemporâneo, se adapte a essa nova realidade é preciso preparo para tratar a informação como um todo, seja ela no ambiente digital ou analógico e estando ela em qualquer suporte. A chave para enfrentar essa nova realidade, está na capacitação, que sugere aprendizado.

Podemos entender que no século passado, a inovação das tecnologias de informação e comunicação (TIC's), proporcionou um novo meio de produção e registro das funções trazendo inúmeros impactos que, atingiram diversas áreas sociais como as atividades de indivíduos, instituições e governos que, por sua vez sofreram mudanças ao realizarem seus registros em meios eletrônicos e principalmente em formatos digitais. Devido ao aumento da produção de documentos arquivísticos digitais, é possível verificar algumas mudanças na forma de realizar gestão documental.

Trabalhando em arquivos, é possível analisar o cunho dinâmico e vivo de seus documentos devido ao seu conteúdo retratar as atividades, rotinas de pessoas físicas e jurídicas além de refletirem as mudanças geradas pela tecnologia.

Ao deparar-se com o caráter do arquivo, o arquivista deve analisar e se preparar para utilizar todos os meios cabíveis para que ele continue dinâmico, onde facilmente consegue-se recuperar, as informações que sejam confiáveis, precisas e completas. Infelizmente, ainda hoje mesmo com grande avanço das TIC's, é possível verificar a relutância de alguns profissionais de arquivologia frente à esse cenário apresentado pelas novas tecnologias.

Em virtude do crescimento de documentos arquivísticos digitais e o desafio em sua manutenção muito deve ser feito para evitar as implicações que a má gestão pode ocasionar no que diz respeito à preservação e ao acesso a longo prazo.

Dessa forma, o Conselho Nacional de Arquivos (CONARQ) publicou em 2005, a Carta para a Preservação do Patrimônio Arquivístico Digital¹, onde há a consideração de que o patrimônio arquivístico digital se encontra em perigo de desaparecimento e risco de falta de confiabilidade, além de apontar que sua preservação em benefício das gerações atuais e futuras é uma preocupação urgente no mundo inteiro.

Segundo o Observatório de documentos digitais², 57% das Instituições Federais de Ensino Superior (IFES) produzem documentos arquivísticos digitais na instituição, porém apenas 2% estão de acordo com as normas do e-Arq Brasil. Entretanto a porcentagem que mais impacta é de que 89% das instituições não possuem um repositório arquivístico digital confiável (RDC-Arq). A partir desses números é possível concluir que a gestão arquivística de documentos em ambiente digital é falha, pois nem todas as etapas são concluídas para que efetivamente se realize a gestão, embora documentos arquivísticos digitais continuem sendo produzidos diariamente, o que fatalmente irá comprometer a acessibilidade desses documentos, mesmo que não imediatamente, mas a médio e longo prazo.

O uso de estratégias de preservação para documentos digitais é prioritário, porque sem elas não seria possível existir uma garantia de acesso, autenticidade e confiabilidade dos documentos a longo prazo. É necessário que se chame a atenção para esta questão devido ao avanço tecnológico que diariamente nos desafia a entender e nos tornar participantes desta nova realidade.

A gestão arquivística de documentos digitais é estudada já há algumas décadas, porém as mudanças tecnológicas se dão em um ritmo extremamente acelerado, fazendo com que muitas vezes seja indagado como seria possível acompanhar toda essa mudança constante.

Diferentemente dos documentos analógicos, onde conservação se dá a partir de um local com condicionamento adequado para que aquele documento, mantendo a estabilidade do seu suporte, tenha acesso a longo prazo, no âmbito digital a necessidade é de se realizar constantemente transferências para outros suportes ou

¹A Carta para a Preservação do Patrimônio Arquivístico Digital encontra-se disponível online em: http://conarg.arquivonacional.gov.br/images/publicacoes_textos/Carta_preservacao.pdf.

²A idealização do observatório de documentos digitais surgiu como um desdobramento do Grupo de Pesquisa do CNPq-UFSM: Gestão Eletrônica de Documentos Arquivísticos – GED/A (grupo este que desenvolve pesquisas voltadas à gestão arquivística de documentos digitais e preservação digital), e volta suas ações para o monitoramento dos aspectos tecnológicos, estruturais, organizacionais, e até mesmo culturais que os documentos digitais suscitam às instituições públicas.

conversão para outros tipos de formatos e sistemas, onde se possa garantir a legitimidade, autenticidade e estabilidade do documento em questão. Diante dessa preocupação relevante de produzir, manter e preservar documentos que sejam confiáveis, autênticos e acessíveis é que se faz necessário a implementação de um sistema que irá gerir esses documentos desde sua produção até a sua destinação final.

O presente trabalho tem como objetivo investigar o sistema de conteúdo digital multi plataforma e de código aberto chamado Alfresco, para analisar se o mesmo pode realizar a gestão arquivística de documentos digitais, que possibilita o acesso a longo prazo da memória digital, onde é possível mostrar a autenticidade, acessibilidade e preservação dos documentos ali arquivados. O questionamento que irá nortear a pesquisa será: “É possível realizar a gestão de documentos arquivísticos em ambiente digital, utilizando o sistema Alfresco?”. Buscar-se-á apresentar esse sistema como um mecanismo para gestão de documentos arquivísticos digitais e uma ferramenta de grande valor para o arquivista.

Nessa direção, a presente pesquisa irá analisar o sistema Alfresco, identificando seus aspectos relevantes, como a acessibilidade e modos de pesquisa, com base no modelo de requisitos para sistemas informatizados de gestão arquivística de documentos, o e-Arq Brasil. Tendo em vista, uma melhor compreensão será explorando o Sistema Informatizado de Gestão Arquivística de Documentos, SIGAD.

A escolha de analisar o sistema Alfresco permitirá uma visão real da possibilidade desse sistema ser implementado e gerir conforme as regulamentações do e-Arq Brasil e CONARQ, contribuindo para que gestão de documentos arquivísticos digitais não seja falho, mas sim um fato. Além disso, irá nortear a problemática de como realizar gestão em documentos arquivísticos em meio digital.

O presente projeto de pesquisa se valerá de um estudo bibliográfico e documental além da análise que será realizada ao sistema Alfresco, à luz do e-Arq Brasil que definirá as normas e procedimentos que deverão ser analisadas no sistema, e a partir desse estudo será fornecido os dados necessários para que a pesquisa se norteie. O estudo em questão situa-se na área de arquivologia, com enfoque interdisciplinar, desenvolvido em duas partes. A primeira parte será a leitura ao manual do sistema Alfresco e do e-Arq Brasil, possibilitando o conhecimento teórico do objeto que se deseja estudar.

A segunda parte irá verificar a usabilidade do sistema que será alvo do estudo e sua possibilidade de ser implementada atendendo às necessidades de acesso e recuperação de dados indexados, conservando seus recursos informacionais. A metodologia utilizada será de natureza qualitativa constituindo em uma investigação teórica para a aplicação prática e imediata.

Além desta introdução, o presente trabalho apresenta quatro capítulos. Com base em revisão de literatura, o segundo capítulo tem como base conceituar os objetos de estudo da arquivologia, trazendo clareza e definição desses temas. Em seguida, no capítulo três foi feita uma breve contextualização sobre o Sistema Informatizado de Gestão Arquivística de Documentos - SIGAD. O quarto capítulo propõe-se analisar o sistema Alfresco se baseando no e-Arq Brasil, verificando se o mesmo pode realizar a gestão arquivística de documentos digitais. O quinto e último capítulo apresenta as reflexões finais acerca da análise feita.

2. CONCEITOS FUNDAMENTAIS DA ARQUIVOLOGIA

Para melhor compreensão do que será abordado nesse trabalho, alguns conceitos e definições relacionados à Arquivologia serão abordados nesse primeiro capítulo, fornecendo suporte e orientação para o estudo de gestão arquivística de documentos digitais.

A fim de conceituar a arquivologia o Dicionário Brasileiro de Terminologia Arquivística (DIBRATE) afirma que ela é uma:

“Disciplina que estuda as funções do arquivo e os princípios e técnicas a serem observados na produção, organização, guarda, preservação e utilização dos arquivos. Também chamada arquivística.” (ARQUIVO NACIONAL, 2005, p. 37).

Segundo a Base de Dados de Terminologia do projeto *International Research on Permanent Authentic Records on Electronic Systems - InterPARES 3*³, arquivologia é definida como “Conceitos, princípios e metodologias que orientam o tratamento de arquivos.” (INTERPARES 3,2012)

O fazer arquivístico é uma prática antiga, originada na civilização grega segundo Schellenberg afirma que "Os arquivos como instituição, provavelmente, tiveram origem na antiga civilização grega. Entre os séculos V e IV a.c. quando os atenienses guardavam seus documentos de valor no templo da mãe dos deuses, isto é, no Metroon". (SCHELLENBERG, 2006, p. 25)

Mas, somente com a publicação do Manual dos Arquivistas Holandeses em 1898 é que a Arquivologia teve seu marco como área do conhecimento.

“Pode-se afirmar que a Arquivística, ou Arquivologia, é uma área de construção teórica recente. [...] O ponto alto do período foi a publicação, no final do século, do manual conhecido no Brasil como Manual dos arquivistas holandeses (1898). Este livro, que apresenta princípios e regras sobre como organizar um arquivo, serviu por anos como uma das bases para a organização de arquivos nos moldes modernos propostos pela história positivista.”(BARROS, 2015, p.13)

³ Pesquisa internacional sobre registros autênticos permanentes em sistemas eletrônicos acesse em: http://www.interpares.org/ip3/ip3_index.cfm?team=4

A partir da publicação do Manual dos Arquivistas Holandeses, o avanço teórico da arquivística, consolidando princípios e conceitos da área.

2.1. CONCEITO DE ARQUIVO

A representatividade dos arquivos ao longo da história se restringia apenas as instituições arquivísticas, pelo interesse europeu em basear sua memória nacional, através do registro e da guarda do patrimônio histórico/cultural, de forma que o mesmo contribuísse para que uma identidade própria fosse então estabelecida.

Através dos milênios, os arquivos têm representado, alternada e cumulativamente, os arsenais da administração, do direito, da história, da cultura e da informação. A razão pela qual eles puderam servir a tantas finalidades é que os materiais arquivísticos, ou registros documentais, representam um tipo de conhecimento único: gerados ou recebidos no curso das atividades pessoais ou institucionais, como seus instrumentos e subprodutos, os registros documentais são as provas primordiais para as suposições ou conclusões relativas a essas atividades e às situações que elas contribuíram para criar, eliminar, manter ou modificar. (DURANTI, 1994, p.50)

Para Duarte existe um dualismo entre os conceitos de documento, como arquivo e informação, afirmando que uma informação não pode se sobrepor em detrimento de outra.

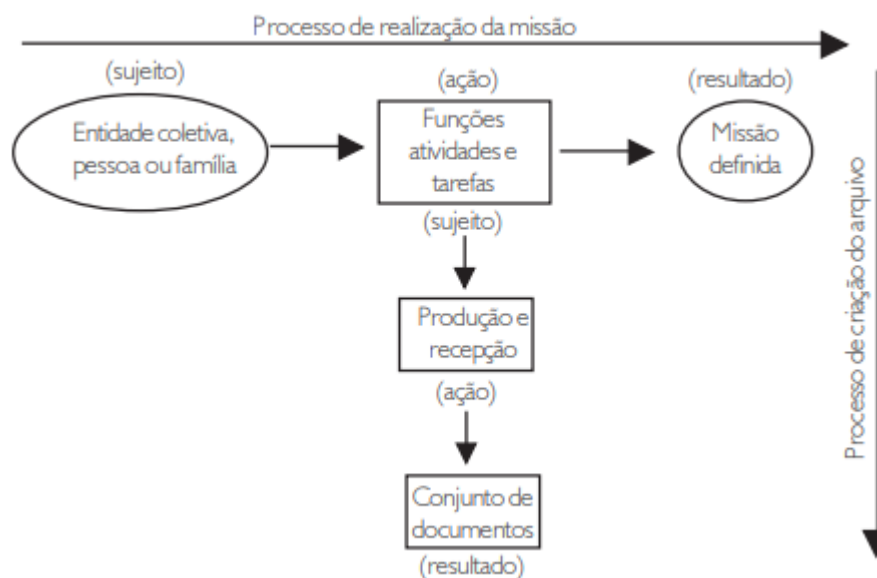
Quando se fala de arquivo, associam-se a ele conceitos de documentos e de informação. Essa é a base para o entendimento de seu contexto. Não importa o tipo de informação que foi gerado e não se pode depreciar um dado informacional em detrimento de outro. No final, ter-se-á concebido um documento de arquivo, que deverá receber tratamento a partir dos mecanismos que lhe facilitem o acesso e a recuperação da informação guardada e por ele contextualizada. (DUARTE, 2007, p.144)

De acordo com o Dicionário Brasileiro de Terminologia Arquivística (DIBRATE) arquivo é: “Conjunto de documentos produzidos e acumulados por uma entidade coletiva, pública ou privada, pessoa ou família, no desempenho de suas atividades, independentemente da natureza do suporte.” (ARQUIVO NACIONAL, 2005, p. 27).

Através da definição acima é possível notar que o arquivo pode ser pessoal ou institucional, além de ser criado a partir da necessidade que pessoas (físicas ou jurídicas) têm de documentar fatos que possam comprovar as atividades que elas desenvolveram ao longo de suas vidas.

A fim de ilustrar melhor esse conceito, Rodrigues disponibiliza essa figura explicativa, onde esquematicamente encontramos:

Figura 1 – Esquema de criação de arquivo



Fonte: RODRIGUES, Ana Marcia Lutterbach, 2006, p.105

De acordo com a autora a ação, descrita no esquema se refere a:

O que é ação, no processo de realização da missão, passa a ser o sujeito no processo de criação do arquivo. O arquivo é, então, o resultado de dois processos integrados. O processo de produção e recepção de documentos resulta do processo de realização da missão. Na perspectiva jenkisoniana, essa concepção do que é arquivo, ancorada na origem dos documentos, torna-se referência para o tratamento do arquivo em suas três fases. (RODRIGUES, 2006, p.105)

Outra interpretação sobre arquivos vem de A. C. Rodrigues (2005) no qual é discutido por ela o tratamento dos arquivos.

[...] Os arquivos conservam registros de ações e de fatos como prova da gestão que os produziu, dos quais são produtos naturais. [...] o arquivo se forma por um processo de acumulação natural, o que significa dizer que tem o atributo especial de ser um conjunto orgânico e estruturado, onde seu conteúdo e significado só podem ser compreendidos na medida em que se

possa ligar o documento ao seu contexto mais amplo de produção, às origens funcionais. (A. C. RODRIGUES, 2005, p. 5)

Entretanto, arquivo pode ser definido também como um lugar de guarda dos documentos que foram produzidos e também como uma instituição. Segundo o projeto InterPARES 3, arquivo pode ser definido como:

[documentos arquivísticos] Conjunto de documentos produzidos ou recebidos por uma pessoa física ou jurídica ou organização na condução de seus negócios, e preservados.

[lugar] Lugar onde são mantidos documentos arquivísticos selecionados para preservação permanente;

[instituição] Uma agência ou instituição responsável pela preservação e comunicação de documentos arquivísticos selecionados para preservação permanente. (InterPARES 3, 2012)

O manual dos arquivistas holandeses conceitua arquivo como:

Conjunto de documentos escritos, desenhos e material impresso, recebidos ou produzidos oficialmente por determinado órgão administrativo ou por um de seus funcionários, na medida em que tais documentos se destinavam a permanecer na custódia desse órgão ou funcionário (ASSOCIAÇÃO DOS ARQUIVISTAS HOLANDESES, 1973, p. 13).

Outra definição de arquivo é apresentada por Duchein que diz:

“Conjuntos de documentos de qualquer natureza, reunidos organicamente e automaticamente por um corpo administrativo, uma pessoa física ou jurídica, em razão de suas funções ou de sua atividade.”(DUCHEIN, 1986, p.17)

O conceito de arquivo também foi definido pela Associação Brasileira de Normas Técnicas (ABNT) – NBR 9578, onde é afirmado que arquivo é:

Designação genérica de um conjunto de documentos produzidos e recebidos por uma pessoa física ou jurídica, pública ou privada, caracterizado pela natureza orgânica de sua acumulação e conservado por essas pessoas ou por seus sucessores, para fins de prova ou informação. De acordo com a natureza do suporte, o arquivo terá a qualificação respectiva, como, por exemplo: arquivo audiovisual, fotográfico, iconográfico, de microformas, informático. (ABNT NBR 9578, 1986, p. 2).

De acordo com SCHELLENBERG, a palavra grega para arquivo é *archives* sendo definida segundo o *Oxford English Dictionary* como:

- a) “Lugar onde são guardados os documentos públicos e outros documentos de importância”; e
- b) “Registro histórico ou documento assim preservado.”

Muitas definições são apresentadas nesse capítulo e isso nos tem serventia, pois reforça que não existe uma definição que seja única e absoluta, essas definições indicam que elas estão baseadas em diferentes práticas arquivísticas, administrativas e jurídicas.

2.2. CONCEITO DE DOCUMENTO ARQUIVÍSTICO

O projeto InterPARES, define documento arquivístico como um “Documento elaborado ou recebido no curso de uma atividade prática como instrumento ou resultado de tal atividade, e retido para ação ou referência.”(INTERPARES 3, 2012)

O documento arquivístico possui características que o diferencia de outros materiais e ao mesmo tempo identifica-o como documento arquivístico.

Da mesma forma a Câmara Técnica de Documentos Eletrônicos (CTDE) define documento arquivístico como “Documento produzido (elaborado ou recebido), no curso de uma atividade prática, como instrumento ou resultado de tal atividade, e retido para ação ou referência” (CONSELHO NACIONAL DE ARQUIVOS, 2014, p.18).

Nas duas definições acima não é especificado claramente se o tipo de suporte influencia no conceito de documento arquivístico, por outro lado, Schellenberg conceitua documento arquivístico, aproximando-se da Arquivística moderna considerando que *records* é aquele que foi concebido ou usado ao longo de um processo administrativo:

Todos os livros, papéis, mapas, fotografias e outras espécies documentárias, independentemente de sua apresentação física ou características, expedidos ou recebidos por qualquer entidade pública ou privada no exercício de seus encargos legais ou em função das suas atividades e preservados ou depositados para preservação por aquela

entidade ou por seus legítimos sucessores como prova de suas funções, sua política, decisões, métodos, operações ou outras atividades, ou em virtude do valor informativo dos dados neles contidos. (SCHELLENBERG, 2002 p. 41)

No trecho acima, Schellenberg descarta a ideia de documento arquivístico ser produzido por pessoa física, apenas reconhece aqueles que são produzidas por instituições públicas ou privadas no exercício de suas atividades.

Duranti, leva em consideração dois pontos chave que determinam o valor probatório e informativo dos documentos arquivísticos, esses atestam ações e transações, dependendo sua veracidade das formas de criação e preservação dos mesmos. Desta forma, ela descreve características de documentos arquivísticos no quesito integridade que são imparcialidade, autenticidade, naturalidade, inter-relacionamento e unicidade.

Imparcialidade caracteriza as razões pelas quais o documento foi produzido e as circunstâncias que foi criado assegura que ele é parte legítima.

Os registros são inerentemente verdadeiros. Assim, os documentos fornecem provas originais porque constituem uma parte real do corpus dos fatos, do caso. Isto porque trazem uma promessa de fidelidade aos fatos e ações que manifestam e para cuja realização contribui. (DURANTI, 1994, p.51)

Autenticidade é a capacidade de se provar que o documento é realmente aquilo que se diz ser.

Os documentos são autênticos porque são criados tendo-se em mente a necessidade de agir através deles, são mantidos com garantias para futuras ações ou para informação, e são definitivamente separados para preservação, tacitamente julgados dignos de serem conservados por ser criador ou legítimo sucessor como testemunho escrito de suas atividades no passado. Assim, os documentos são autênticos porque são criados, mantidos e conservados sob custódia de acordo com procedimentos regulares que podem ser comprovados (DURANTI, 1994, p.51)

Naturalidade é a forma como se dá a acumulação dos documentos no decorrer das atividades da fonte geradora.

Essa naturalidade diz respeito à maneira como os documentos se acumulam no curso das transações de acordo com as necessidades de matéria em pauta: eles não são coletados artificialmente, como os objetos de um museu [...], mas acumulados naturalmente nos escritórios em função dos objetivos práticos da administração. O fato de os documentos não

serem concebidos fora dos requisitos da atividade práticas, isto é, de se acumularem de maneira contínua e progressiva, como sedimentos de estratificações geológicas, os dota de um elemento de coesão espontânea, ainda que estruturada. (DURANTI, 1994, p.52).

Inter-relacionamento, pois o documento é transversal.

Esse inter-relacionamento é devido ao fato de que os documentos estabelecem relações no decorrer do andamento das transações e de acordo com suas necessidades. Cada documento está intimamente relacionado com outros tanto dentro quanto fora do grupo no qual está preservado e [...] seu significado depende dessas relações. As relações entre os documentos, e entre eles e as transações das quais são resultantes, estabelecem o axioma de que um único documento não pode se constituir em testemunho suficiente do curso de fatos e atos passados: os documentos são interdependentes no que toca a seu significado e sua capacidade comprobatória. (DURANTI, 1994, p.52).

Unicidade é devido ao fato de cada documento é único e desempenha um papel único dentro do universo documental em que esta inserido.

A unicidade provém do fato de que cada registro documental assume um lugar único na estrutura documental do grupo ao qual pertence e no universo documental. Cópias de um registro podem existir em um mesmo grupo ou em outros grupos, mas cada cópia é única em seu lugar, porque o complexo das suas relações com outros registros é sempre único. (DURANTI, 1994, p.52).

Segundo Duranti essas características citadas acima servem como análise dos registros documentais como método básico pelo qual é possível alcançar a compreensão do passado tanto imediato quanto histórico, sendo os propósitos administrativos ou culturais.

2.3. CONCEITO DE DOCUMENTO ARQUIVÍSTICO DIGITAL

Segundo o Glossário da Câmara Técnica de Documentos Eletrônicos (CTDE), do Conselho Nacional de Arquivos (CONARQ) a definição de documento arquivístico digital é “Documento digital reconhecido e tratado como um documento arquivístico” (CONSELHO NACIONAL DE ARQUIVOS, 2014, p.18). Desta forma, a CTDE leva em consideração que o documento arquivístico digital tem as características de

documento arquivístico e deve ser reconhecido e tratado como igual. Assim sendo, ele possui informação registrada, porém com a diferença de ser codificada em dígitos binários, acessível e interpretável por meio de um sistema computacional, possuindo os elementos constitutivos suficientes para servir de prova das atividades de determinada instituição.

De acordo com Rondinelli (2011, p.227) para entender o conceito de documento arquivístico digital é necessário que se identifique as características de um documento arquivístico, que são: forma fixa, conteúdo estável, relação orgânica, contexto identificável e ação. A forma fixa de um documento arquivístico digital é definido pelo projeto *International Research on Permanent Authentic Records on Electronic Systems - InterPARES* como a “Qualidade de um documento arquivístico que assegura a mesma aparência ou apresentação documental cada vez que o documento é recuperado” (INTERPARES 2, 2006).

O conteúdo estável é definido como:

“A característica de um documento arquivístico que torna a informação e os dados nele contidos imutáveis e exige que eventuais mudanças sejam feitas por meio do acréscimo de atualizações ou da produção de uma nova versão” (INTERPARES 2, 2006).

A definição de relação orgânica segundo Rondinelli (2011, p. 228) é:

Uma característica eminentemente arquivística e que se encontra implícita no conceito de documento arquivístico, na medida em que, de acordo com esse conceito, os documentos se constituem em registros de atividades e, conseqüentemente, mantêm um vínculo inextricável entre si. No caso do documento arquivístico digital, essa vinculação se dá entre documentos dentro e fora do sistema, isto é, nos chamados ambientes híbridos os quais se caracterizam por abranger documentos digitais e não digitais ao mesmo tempo. (DURANTI; THIBODEAU, 2008 apud RONDINELLI, 2011, p. 228).

E para o contexto identificável Rondinelli (2011, p. 228) define como “Uma hierarquia de estruturas fora do documento arquivístico na qual se dá sua produção e gestão” (DURANTI; THIBODEAU, 2008 apud RONDINELLI, 2011, p. 228). E na ação, Rondinelli (2011, p. 228) usa como definição “O fato do documento arquivístico participar ou simplesmente apoiar uma ação, significando que sua produção pode ser obrigatória ou facultativa” (DURANTI; THIBODEAU, 2008 apud RONDINELLI, 2011, p. 228).

Assim como o documento arquivístico, o documento arquivístico digital deve prover as mesmas características mesmo estando em ambiente digital.

2.4. CONCEITO DE GESTÃO DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS

Nos últimos anos, vários projetos desenvolvidos nos Estados Unidos, Canadá, Europa e Austrália cooperaram na revisão de conceitos arquivísticos, definição de normas de gestão bem como na especificação de requisitos funcionais, além de metadados para sistemas de gestão arquivística de documentos.

Porém no Brasil, a gestão arquivística de documentos só recebeu amparo legal a partir da criação da Lei nº 8.159, de 8 de janeiro de 1991 – Lei de Arquivos - e do Decreto nº 4.073, de 3 de janeiro de 2002, ambos regulamentam a gestão de documentos para a Administração Pública Federal. A Lei nº 8.159, também deu origem ao Conselho Nacional de Arquivos, que é responsável pela definição da política nacional de arquivos públicos e privados além de executar orientação normativa, colocando em prática a gestão documental e a proteção especial aos documentos de arquivo.

Em seu Modelo de requisitos para sistemas informatizados de gestão arquivística de documentos, o e-ARQ Brasil destaca que:

A gestão arquivística de documentos compreende a responsabilidade dos órgãos produtores e das instituições arquivísticas em assegurar que a documentação produzida seja o registro fiel das suas atividades e que os documentos permanentes sejam devidamente recolhidos às instituições arquivísticas. (CONARQ, 2006, p.15)

O Glossário da CTDE define sistema de gestão arquivística de documentos como um “Conjunto de procedimentos e operações técnicas cuja interação permite a eficiência e a eficácia da gestão arquivística de documentos” (CONSELHO NACIONAL DE ARQUIVO, 2014, p.32).

Para o e-ARQ Brasil, a gestão arquivística de documentos é definido como:

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. (CONSELHO NACIONAL DE ARQUIVOS, 2011, p.10).

Um dos pilares da gestão arquivística de documentos é a teoria das três idades e de acordo com essa teoria, os documentos passam por três idades, que são corrente, intermediária e permanente.

Corrente: refere-se aos documentos que estão em curso, isto é, tramitando ou que foram arquivados, mas que são objeto de consultas frequentes; eles são conservados nos locais onde foram produzidos sob a responsabilidade do órgão produtor;

Intermediária: refere-se aos documentos que não são mais de uso corrente mas que, por conservarem ainda algum interesse administrativo, aguardam, no arquivo intermediário, o cumprimento do prazo estabelecido em tabela de temporalidade e destinação para serem eliminados ou recolhidos ao arquivo permanente.

Permanente: refere-se aos documentos que devem ser definitivamente preservados devido a seu valor histórico, probatório ou informativo. (e-ARQ Brasil, 2006, p.16)

A gestão de documentos implica, basicamente, em acompanhar todo o ciclo dos documentos produzidos por uma instituição ou por uma pessoa ao longo de suas atividades, obtendo uma redução da massa documental produzida, determinando os documentos que devem ser conservados a curto, médio e longo prazo resultando em eficiência e economia, tanto de tempo como de espaço.

A Carta de Preservação do Patrimônio Arquivístico Digital⁴ elaborada pela CTDE com o apoio da Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO) e aprovada pelo CONARQ, aborda sobre o armazenamento e a preservação, dois pontos fundamentais da gestão de documentos arquivísticos digitais.

Sobre o armazenamento ela diz:

A tecnologia digital é comprovadamente um meio mais frágil e mais instável de armazenamento, comparado com os meios convencionais de registrar informações, tendo um impacto profundo sobre a gestão dos documentos digitais no presente para que se tenha garantia de acesso no futuro. (CONSELHO NACIONAL DE ARQUIVOS, 2004, p.3)

E sobre preservação afirma:

⁴A Carta de Preservação do Patrimônio Arquivístico Digital é uma orientação normativa, visando à gestão documental e à proteção especial aos documentos de arquivo, independente do suporte em que a informação está registrada. Ela foi aprovada pelo CONARQ em 6 de Julho de 2004.

A preservação de documentos digitais pressupõe uma constante atualização de suporte e de formato, além de estratégias para possibilitar a recuperação das informações, que passam pela preservação da plataforma de hardware e software em que foram criados, pela migração ou pela emulação. Estas são algumas iniciativas que vêm sendo tomadas, mas que não são ainda respostas definitivas para o problema da preservação de longo prazo. Não há soluções únicas e todas elas exigem investimento financeiro elevado e contínuo em infra-estrutura tecnológica, pesquisa científica aplicada e capacitação de recursos humanos. (CONSELHO NACIONAL DE ARQUIVOS, 2004, p.3)

E revela a eficácia de um documento arquivístico que requer ações arquivística incorporadas em todo o ciclo de vida desse documento desde antes de sua criação, garantindo a sua disponibilidade futura.

A eficácia de um documento arquivístico depende da qualidade e do rigor dos procedimentos de produção e manutenção realizados pelas organizações produtoras de documentos. Entretanto, como a informação em formato digital é extremamente suscetível à degradação física e à obsolescência tecnológica - de *hardware*, *software* e formatos -, essas novas facilidades trazem consequências e desafios percucientes para assegurar sua integridade e acessibilidade. A preservação dos documentos digitais requer ações arquivísticas, a serem incorporadas em todo o seu ciclo de vida, antes mesmo de terem sido criados, incluindo as etapas de planejamento e concepção de sistemas eletrônicos, a fim de que não haja perda nem adulteração dos registros. Somente desta forma se garantirá que esses documentos permaneçam disponíveis, recuperáveis e compreensíveis pelo tempo que se fizer necessário.(CONSELHO NACIONAL DE ARQUIVOS, 2004, p.2)

Quando há a implementação da gestão de documentos é necessário um planejamento onde os objetivos a serem alcançados sejam de interesse para a maioria dos profissionais que trabalham naquela determinada instituição, apresentando as vantagens da realização da gestão arquivística dos documentos digitais. Entretanto é neste ponto onde se encontra a maior dificuldade, pois na maioria das vezes há uma relutância às mudanças propostas na gestão. É neste momento em que o arquivista necessita ir para além de sua formação técnica e se utilizar do seu conhecer natural às relações interpessoais, mostrando pacientemente a importância e relevância da gestão arquivística de documentos digitais.

O documento digital apresenta especificidades que podem comprometer sua autenticidade, uma vez que é suscetível à degradação física dos seus suportes, à obsolescência tecnológica de *hardware*, *software* e de formatos e a intervenções não autorizadas, que podem ocasionar adulteração e

destruição. Somente com procedimentos de gestão arquivística é possível assegurar a autenticidade dos documentos arquivísticos digitais. (e-ARQ Brasil, 2006, p.17)

Para que se tenha de forma assegurada a autenticidade de documentos arquivísticos digitais, é imprescindível que seja realizada uma gestão arquivística. Essa fornecerá todo o respaldo necessário para que os documentos cumpram a sua finalidade e futuramente sirvam como prova comprobatória das informações contidas neles.

De forma sucinta, a gestão arquivística de documentos tem por objetivo o gerenciamento de todo o ciclo de vida dos documentos, desde sua produção, tramitação, uso, avaliação, arquivamento até a sua destinação. Sendo essa gestão feita desde a criação do documento permeando toda a sua trajetória dentro da instituição (pessoa jurídica) ou cumprindo sua função no dia a dia (pessoa física), certamente esse documento arquivístico não perderá o seu valor.

3. SISTEMA INFORMATIZADO DE GESTÃO ARQUIVÍSTICA DE DOCUMENTOS (SIGAD)

Neste capítulo será apresentado o Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD) para que desta forma seja possível nortear a nossa pesquisa e análise futura do Sistema Alfresco, com base no que será exposto nesse capítulo sobre o assunto.

O conceito de SIGAD foi definido recentemente, pelo CONARQ, frente às novas tecnologias e formas de fazer arquivístico que tornaram mais complexas as formas de guarda, conservação e preservação de documentos, principalmente aqueles que são nato-digitais, tendo por objetivo difundir as informações para além da era presente mostrando que essa ciência não se tornou obsoleta com o avanço tecnológico.

Segundo o CONARQ, que conceituou SIGAD em 2011 o termo significa:

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. (CONSELHO NACIONAL DE ARQUIVOS, 2011, p. 10).

Além disso, o CONARQ afirma que para um SIGAD ter sucesso é extremamente necessária à implementação prévia de um programa de gestão arquivística de documentos. Sendo também aplicável nesse programa de gestão sistemas híbridos que contemplem documentos convencionais e digitais.

Conforme foi observado na citação acima, o SIGAD abrange documentos arquivísticos convencionais (analógicos) e documentos arquivísticos digitais, se valendo de ações como registro das referências dos documentos convencionais e digitais, podendo incluir imagens digitalizadas, captura, armazenamento, controle de versões, controle de prazos de guarda e destinação desses documentos, promoção do acesso e preservação aos documentos arquivísticos digitais e não digitais que sejam autênticos e confiáveis.

O Sistema de Arquivos – SIARQ⁵ da Universidade Federal de Juiz de Fora cita algumas características arquivísticas importantes de um SIGAD que são:

Captura, armazenamento, indexação e recuperação de todos os tipos de documentos arquivísticos e de todos os componentes digitais do documento arquivístico, como, por exemplo, um relatório com os anexos em diferentes arquivos;
Integração entre documentos digitais e não digitais;
Gestão dos documentos a partir do plano de classificação;
Avaliação dos documentos e aplicação da tabela de temporalidade e destinação para recolhimento e preservação dos que tenham valor permanente;
Exportação dos documentos para transferência e recolhimento;
Armazenamento seguro para garantir a autenticidade dos documentos;
Instrumentos para gestão de estratégias de preservação dos documentos;
Implementação de metadados⁶ para descrever os contextos documentais:
[a] juricoadministrativo; [b] de proveniência; [c] de procedimentos; [d] documental;
[e] tecnológico. (SISTEMA DE ARQUIVOS/UFJF, 2009)

As fases de atuação do SIGAD são a corrente e intermediária de documentos e também fundamenta procedimentos de preservação conforme disposto no art. 8º, §§ 1º e 2º, da Lei n.º 8.159, de 8 de janeiro de 1991:

Consideram-se documentos correntes aqueles em curso ou que, mesmo sem movimentação, constituam objeto de consultas frequentes; e consideram-se documentos intermediários aqueles que, não sendo de uso corrente nos órgãos produtores, por razões de interesse administrativo, aguardam a sua eliminação ou recolhimento para guarda permanente. (CONSELHO NACIONAL DE ARQUIVOS, 2011, p.1)

De acordo com o CONARQ, o foco do SIGAD é dar o controle total do ciclo de vida do documento, desde a sua criação ou captura, independentemente do sistema ou da ferramenta que possa ter produzido, chegando até a sua destinação final, seja a eliminação ou recolhimento a fase permanente seguindo os padrões e procedimentos da gestão arquivística de documentos.

⁵ O SIARQ/UFJF é o conjunto de objetivos, princípios, diretrizes e programas propostos pelo Arquivo Central e que busca a integração dos diversos arquivos dos órgãos e unidades da UFJF de forma a garantir a gestão unificada de seus documentos arquivísticos.

⁶ Metadados são dados que se referem a outros dados. São dados estruturados e codificados que com o objetivo de descrever e permitir encontrar, gerenciar, compreender ou preservar outros dados ao longo do tempo. (CONSELHO NACIONAL DE ARQUIVOS, 2004, p.11)

Assim como a eliminação de documentos não digitais, dispõe de leis e normas que regulamentam o descarte, da mesma maneira acontece com a eliminação de um SIGAD, conforme expresso na Lei 8.159:

A eliminação de documentos produzidos por instituições públicas e de caráter público será realizada mediante autorização da instituição arquivística pública, na sua específica esfera de competência; e os documentos de valor permanente são inalienáveis e imprescritíveis. (CONSELHO NACIONAL DE ARQUIVOS, 2011, p.2)

O SIGAD, também deve ter a capacidade de manter a relação orgânica entre os documentos garantindo sua confiabilidade, acesso e autenticidade, em longo prazo, aos documentos arquivísticos.

As operações feitas pelo SIGAD garantem o acesso e a preservação a médio e longo prazo de documentos digitais e não digitais.

Abaixo são apresentados os requisitos arquivísticos que caracterizam um SIGAD, de acordo com o CONARQ.

Captura, armazenamento, indexação e recuperação de todos os tipos de documentos arquivísticos;
Captura, armazenamento, indexação e recuperação de todos os componentes digitais do documento arquivístico como uma unidade complexa;
Gestão dos documentos a partir do plano de classificação para manter a relação orgânica entre os documentos;
Implementação de metadados associados aos documentos para descrever os contextos desses mesmos documentos (jurídico-administrativo, de proveniência, de procedimentos, documental e tecnológico);
Integração entre documentos digitais e convencionais;
Foco na manutenção da autenticidade dos documentos;
Avaliação e seleção dos documentos para recolhimento e preservação daqueles considerados de valor permanente;
Aplicação de tabela de temporalidade e destinação de documentos;
Transferência e recolhimento dos documentos por meio de uma função de exportação;
gestão de preservação dos documentos. (CONARQ,2011, p.11-12)

A partir dessas características acima apresentadas, será possível aplicar ao Sistema Alfresco e analisar se o sistema é um SIGAD e se o mesmo encontra-se em conformidade com os requisitos do e-ARQ Brasil.

4. SISTEMA ALFRESCO COM BASE NO e-ARQ BRASIL

A Alfresco Software, Inc. ("Alfresco") é uma empresa de software de código aberto voltada para o avanço do fluxo de negócios digitais, esta sediada nos Estados Unidos em San Mateo e, também na Europa, em Maidenhead, Reino Unido.

Alfresco é um software de gestão de conteúdo empresarial que funciona nos sistemas Windows e Linux. Ele foi criado para ser uma alternativa de alta qualidade e custo acessível para o usuário, estando no mercado desde 2005 e já foram realizadas algumas versões, atualmente rodando na versão 4.3, desenvolvido em Java.

As principais funções desse software são gerenciamento de arquivos, colaboração e conteúdo web, direcionados para gestão de documentos.

A seguir será iniciada a análise comparativa do software Alfresco, com os requisitos designados no e-Arq Brasil onde será possível verificar se é possível realizar gestão de documentos com esse software.

O modelo de requisitos para Sistema Informatizados de Gestão Arquivística de Documentos - e-Arq Brasil, é dividido em duas partes, nosso foco será na Parte II onde são descritos 14 especificações sobre os aspectos de funcionalidade que um SIGAD precisa ter. As 14 especificações que serão analisadas são: Organização dos documentos arquivísticos: plano de classificação e manutenção dos documentos; Tramitação e fluxo de trabalho; Captura; Avaliação e destinação; Pesquisa, localização e apresentação dos documentos; Segurança; Armazenamento; Preservação; Funções administrativas; Funções administrativas; Conformidade com a legislação e regulamentações; Usabilidade; Interoperabilidade; Disponibilidade; Desempenho e escalabilidade.

Os 232 requisitos obrigatórios do e-Arq Brasil se encontram disponíveis no Anexo 1, para melhor compreensão dos itens que foram analisados e que serão abordados nesse capítulo.

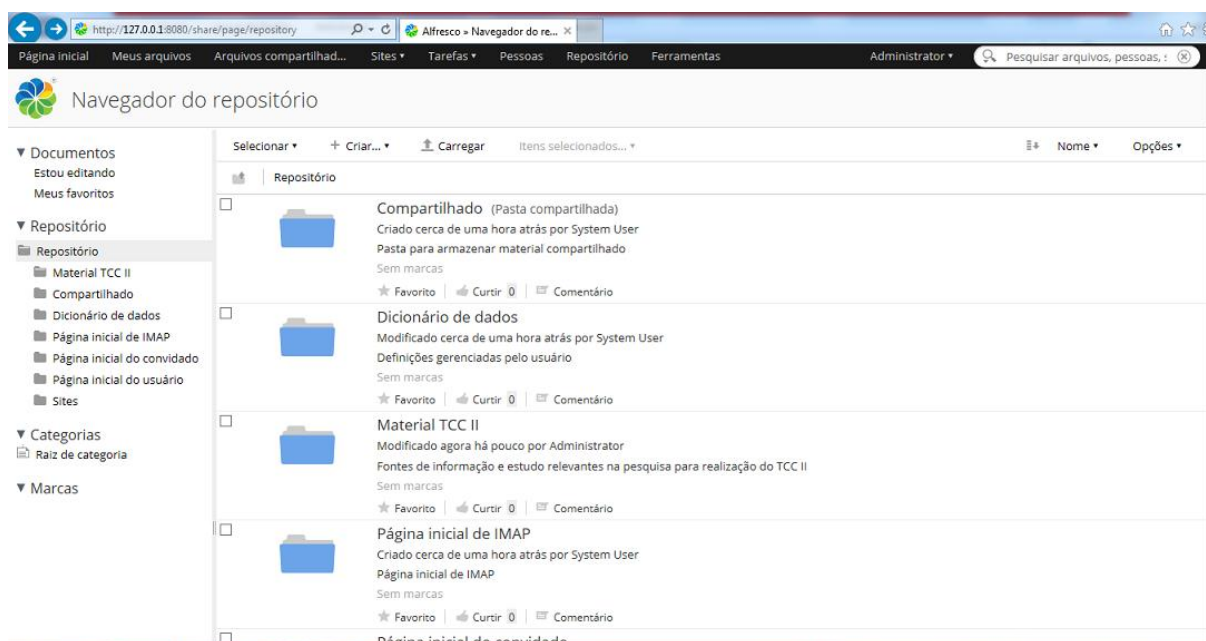
A análise foi realizada com o uso da versão grátis do software Alfresco (limitada), leitura de manuais e minicursos realizados na internet. O software é complexo e com muitas opções de gerenciamento de documentos, porém somente

com um treinamento adequado seria possível avaliar quais requisitos do e-Arq Brasil poderiam ter sido ajustados.

A partir do resultado encontrado na análise foi possível observar que o software Alfresco funciona como um repositório de documentos e alguns processos da gestão documental podem ser vistos na sua interface e proposta de funcionalidade, mas não cabe chamar o software de um SIGAD. Os números que serão apresentados revelam que um pouco menos da metade dos requisitos considerados obrigatórios para o e-Arq, encontram-se disponíveis no software, outros poucos cumprem parcialmente os requisitos, mas a grande maioria não atende às obrigatoriedades propostas pelo órgão competente no Brasil.

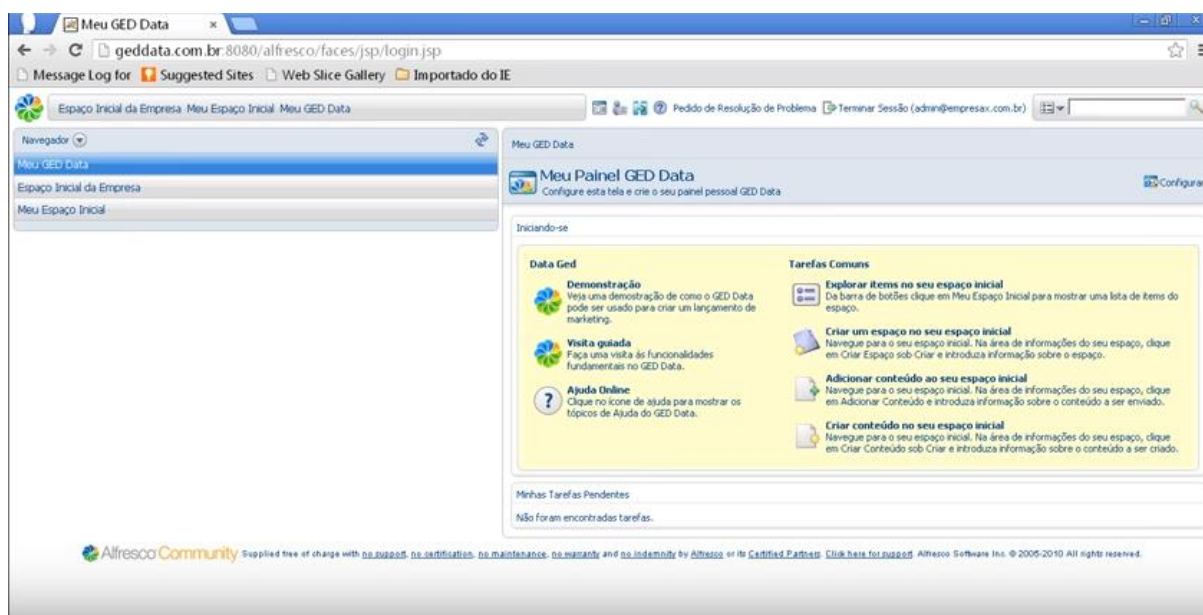
O software apresenta duas interfaces diferentes, uma para versão grátis e outra para versão paga, conforme verificado nas duas figuras abaixo:

Figura 2 – Captura de tela do Alfresco (versão grátis)



Fonte: Site eletrônico do Alfresco

Figura 3 – Captura de tela do Alfresco (versão paga)



Fonte: Site eletrônico do GEDDATA

Inicialmente é possível analisar as diferenças de interface, na (Figura 3) pode-se observar uma diversidade maior de opções de informações e funções que não são proporcionadas aos usuários da interface apresentada na (Figura 2).

Dos 232 requisitos obrigatórios das 14 especificações do e-Arq Brasil, 96 requisitos estavam cumprindo com as obrigatoriedades do órgão, 129 requisitos não estavam em conformidade e apenas 7 requisitos cumpriam parcialmente a exigência.

Sobre os 96 requisitos que estavam em conformidade é importante assinalar que se encontraram em sua maioria na especificação 1 que diz respeito a Organização dos documentos arquivísticos: Plano de classificação e manutenção dos documentos, é possível então concluir que o software tem como prioridade a organização e classificação dos documentos inseridos para que se obtenha uma rápida recuperação, utilizando instrumentos de busca disponibilizados pela aplicação, facilitando e atraindo novos usuários que desejam apenas ter um repositório organizado e funcional.

Os 129 requisitos que não estavam em conformidade, muitos foram identificados dessa forma devido a falta de conteúdo disponível na versão utilizada

do software e também a falta de conteúdo nos manuais sobre a especificação em questão. Foram dessa forma encontrados em sua grande maioria na especificação 6 - Segurança. Um fator interessante analisado nessa pesquisa sobre a especificação de segurança foi o fato de o usuário poder optar por incluir seus documentos em servidores nas nuvens (cloud server), facilitando o acesso e o compartilhamento de documentos entre usuários da mesma empresa. Isso também justifica o fato de ter mais requisitos não atendidos nessa especificação.

Os 7 requisitos parcialmente em conformidade com o e-Arq Brasil, estavam em sua maioria na especificação 1 - Organização dos documentos arquivísticos: Plano de classificação e manutenção dos documentos, devido a alguns requisitos terem tópicos muito específicos e por isso o software não atendia a todos os tópicos descritos.

Deste modo, pode-se concluir que o software Alfresco não pode ser considerado um SIGAD, pois o mesmo não realiza a gestão arquivística de documentos, conforme conceituado nos capítulos anteriores dessa pesquisa. O Alfresco pode servir como uma opção de repositório digital por ter mais semelhança com os aspectos de um sistema de informação que serve para armazenar, preservar, organizar e disseminar informações, utilizando-se de um software.

5. CONSIDERAÇÕES FINAIS

Essa pesquisa se originou na busca por compreender se o software Alfresco poderia ser utilizado como um SIGAD. Procurou-se verificar cada especificação obrigatória que o e-Arq Brasil instituiu para que se tenha um sistema que realiza todas as práticas arquivísticas para a realização de uma verdadeira gestão arquivística de documentos.

Os dados comparativos coletados nessa pesquisa identificam aspectos no que diz respeito a necessidade de criar um software que atenda aos requisitos das especificações fornecidas pelo e-Arq Brasil, para que a gestão arquivística de documentos possa ter seu espaço em ambiente digital.

É de fundamental importância que tenha-se um olhar mais atento as novas formas de desenvolver a prática arquivística, pois em pleno século 21 onde a maior parte dos registros são feitos através do uso de tecnologia, onde utiliza-se mais o digital do que o analógico, ainda temos tanta resistência em utilizar recursos digitais ao nosso favor.

A gestão arquivística de documentos é essencial para a garantia de efetividade da produção, administração, manutenção e destinação de documentos, e se ela for realizada de forma a integrar documentos em diferentes suportes, através de um sistema informatizado seguro aumentará sua eficácia na recuperação e principalmente na preservação desses documentos.

A partir do estudo do software Alfresco, ainda pouco utilizado no Brasil, é possível imaginar a despadronização que deve existir nas Instituições públicas e privadas, onde softwares como o Alfresco são utilizados para realizar a gestão, muito embora o mesmo não se enquadra na maior parte das especificações do e-Arq Brasil.

É preciso que ferramentas comecem a ser desenvolvidas, de acordo com os critérios do e-Arq, para que o profissional arquivista não perca o seu espaço, por não se adequar as novas tecnologias e formas de gerir a documentação que tem sido produzida nessa era.

REFERÊNCIAS

ARQUIVO NACIONAL. **Dicionário Brasileiro de Terminologia Arquivística – DIBRATE**. Rio de Janeiro, 2005. Disponível em: <http://www.conarq.arquivonacional.gov.br/publicacoes-2/26-dicionario-brasileiro-de-terminologia-arquivistica-dibrate.html>. Acessado em: 23 Jun, 2018

ARQUIVO NACIONAL. **Manual de arranjo e descrição de Arquivos**. Rio de Janeiro: Arquivo Nacional, 1973.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 9578: Arquivos: — Terminologia**. In: _____. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 1986.

BARROS, THB. Introdução. In: **Uma trajetória da Arquivística a partir da Análise do Discurso: inflexões histórico-conceituais** [online]. São Paulo: Editora UNESP; São Paulo: Cultura Acadêmica, 2015, pp. 13-26

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **Carta para a Preservação do Patrimônio Arquivístico Digital**. Rio de Janeiro, 2004. Disponível em: http://conarq.arquivonacional.gov.br/images/publicacoes_textos/Carta_preservacao.pdf Acessado em: 04 Jun, 2018

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **Glossário**. Rio de Janeiro, 2014. Disponível em: http://www.conarq.arquivonacional.gov.br/images/ctde/Glossario/2014ctdeglossario_v6_public.pdf. Acesso em: 15 Set, 2018

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **Modelo de requisitos para sistemas informatizados de gestão arquivística de documentos: e-ARQ Brasil**. Rio de Janeiro, 2011.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **Orientação Técnica n.º 1 Abril / 2011**. Rio de Janeiro. Disponível em:

http://www.conarq.gov.br/images/ctde/Orientacoes/Orientacao_tecnica_1.pdf.

Acessado em: 17, Out, 2018.

DUCHEIN, M. **O respeito aos fundos em arquivística: princípios teóricos e problemas práticos**. Arquivo & Administração. Rio de Janeiro, v.10-14, n.1, p. 14-33, abr. 1982/ago.1996.

DUARTE, Zeny. **Arquivo e arquivista: conceituação e perfil profissional**. Porto, 2006-2007. Disponível em: <http://ler.letras.up.pt/uploads/ficheiros/6624.pdf> .
Acessado em: 17, Out, 2018.

DURANTI, Luciana. **Registros documentais contemporâneos. Estudos Históricos**, Rio de Janeiro, v.7, n.13, 1994, p.50-54

INTERPARES. **Projeto InterPARES 2**. [S.l.: s.n.], 2006. Disponível em: http://www.interpares.org/ip2/display_file.cfm?doc=ip2_preserver_guidelines_booklet--portuguese.pdf. Acesso em: 23 Set, 2018

INTERPARES. **Projeto InterPARES 3**. [S.l.: s.n.], 2012. Disponível em: http://interpares.org/ip3/ip3_terminology_db.cfm?team=15. Acesso em: 14 Out, 2018

OBSERVATÓRIO DE DOCUMENTOS DIGITAIS. **Gestão e preservação de documentos nas IFES**. 2017. Disponível em: <https://observatoriodedocumentosdigitais.wordpress.com/gestao-e-preservacao-de-documentos-nas-ifes/> Acessado em: 04 Jun, 2018

PAES, Marilena Leite. **Arquivo: teoria e prática**. Rio de Janeiro: Editora FGV, 1986.

RODRIGUES, Ana Célia. **Manual de tipologia documental: um instrumento de gestão para arquivos municipais brasileiros**. In: CONGRESSO NACIONAL DE ARQUIVOLOGIA, 1. Brasília, 2005

RODRIGUES, Ana Marcia Lutterbach, **A teoria dos arquivos e a gestão de documentos**. Perspect. ciênc. inf., Belo Horizonte, v.11 n.1, p. 102-117, jan./abr. 2006. Disponível em: <http://www.scielo.br/pdf/pci/v11n1/v11n1a09> Acessado em: 16 Out, 2018

RONDINELLI, Rosely Cury. **Gerenciamento arquivístico de documentos eletrônicos**. 4ª edição, Rio de Janeiro: FGV, 2005. p.55

RONDINELLI, Rosely Cury. **O conceito de documento arquivístico frente à realidade digital: uma revisitação necessária**. 2011. Tese (Programa de Pós-Graduação em Ciência da Informação) - Universidade Federal Fluminense, Niterói, 2011. Disponível em:

https://www.siarq.unicamp.br/siarq/images/siarq/publicacoes/preservacao_digital/tese_rondinelli.pdf Acesso em: 23 Set, 2018

SCHELLENBERG, Theodore R. **Arquivos Modernos: princípios e técnicas**. 6ª edição, Rio de Janeiro: FGV, 2006

SISTEMA DE ARQUIVOS DA UNIVERSIDADE FEDERAL DE JUIZ DE FORA. **O que é um SIGAD?** 2009. Disponível em:

<http://www.ufjf.br/siarqsis/files/2009/06/oqehsigad.pdf> Acessado em: 16 Out, 2018

ANEXO 1 – Quadro de análise do sistema Alfresco com base nos requisitos das especificações do e-Arq Brasil

1. Organização dos documentos arquivísticos: Plano de classificação e manutenção dos documentos	
1.1 Configuração e administração do plano de classificação no SIGAD	
Requisitos	Conformidade e-Arq Brasil
1.1.1 Um SIGAD tem que incluir e ser compatível com o plano de classificação do órgão ou entidade.	EC
1.1.2 Um SIGAD tem que garantir a criação de classes, subclasses, grupos e subgrupos nos níveis do plano de classificação de acordo com o método de codificação adotado.	EC
1.1.3 Um SIGAD tem que permitir a usuários autorizados acrescentar novas classes sempre que necessário.	EC
1.1.4 Um SIGAD tem que registrar a data de abertura de uma nova classe no respectivo metadado.	EC
1.1.5 Um SIGAD tem que registrar a mudança de nome de uma classe já existente no respectivo metadado.	EC
1.1.6 Um SIGAD tem que permitir o deslocamento de uma classe inteira, incluídas as subclasses, grupo, subgrupos e documentos nela classificados, para outro ponto do plano de classificação. Nesse caso, é necessário fazer o registro do deslocamento nos metadados do plano de classificação.	EC
1.1.7 Um SIGAD deve permitir que usuários autorizados tornem inativa uma classe em que não sejam mais classificados documentos.	EC
1.1.8 Um SIGAD tem que permitir que um usuário autorizado apague uma classe inativa.	EC
1.1.9 Um SIGAD tem que impedir a eliminação de uma classe que tenha documentos nela classificados. Essa eliminação pode ocorrer a partir do momento em que todos os documentos ali classificados tenham sido recolhidos ou eliminados, e seus metadados apagados, ou que esses documentos tenham sido reclassificados.	EC
1.1.10 Um SIGAD tem que permitir a associação de metadados às classes, conforme estabelecido no padrão de metadados, e deve restringir a inclusão e alteração desses mesmos metadados somente a usuários autorizados.	EC
1.1.11 Um SIGAD tem que disponibilizar pelo menos dois mecanismos de atribuição de identificadores a classes do plano de classificação, prevendo a possibilidade de se utilizar ambos, separadamente ou em conjunto, na mesma aplicação: <ul style="list-style-type: none"> • atribuição de um código numérico ou alfanumérico; • atribuição de um termo que identifique cada classe. 	EC
1.1.13 Um SIGAD tem que utilizar o termo completo para identificar uma classe. Entende-se por termo completo toda a hierarquia referente àquela classe.	EC
1.1.14 Um SIGAD tem que assegurar que os termos completos, que identificam cada classe, sejam únicos no plano de classificação.	EC

1.1.17 Um SIGAD tem que prover funcionalidades para elaboração de relatórios de apoio à gestão do plano de classificação, incluindo a capacidade de: <ul style="list-style-type: none"> • gerar relatório completo do plano de classificação; • gerar relatório parcial do plano de classificação a partir de um ponto determinado na hierarquia; • gerar relatório dos documentos ou dossiês/processos classificados em uma ou mais classes do plano de classificação; • gerar relatório de documentos classificados por unidade administrativa. 	EC
1.2 Classificação e metadados das unidades de arquivamento	
1.2.1 Um SIGAD tem que permitir a classificação das unidades de arquivamento somente nas classes autorizadas. Ver requisito 1.1.12	EC
1.2.2 Um SIGAD tem que permitir a classificação de um número ilimitado de unidades de arquivamento dentro de uma classe.	NC
1.2.3 Um SIGAD tem que utilizar o termo completo da classe para identificar uma unidade de arquivamento, tal como especificado no item 1.1.13.	EC
1.2.4 Um SIGAD tem que permitir a associação de metadados às unidades de arquivamento e deve restringir a inclusão e alteração desses metadados a usuários autorizados	EC
1.2.5 Um SIGAD tem que associar os metadados das unidades de arquivamento conforme estabelecido no padrão de metadados.	EC
1.2.6 Um SIGAD tem que permitir que uma nova unidade de arquivamento herde, da classe em que foi classificada, alguns metadados predefinidos. Exemplos desta herança são prazos de guarda previstos na tabela de temporalidade e destinação e restrição de acesso	PC
1.2.9 Um SIGAD tem que permitir que uma unidade de arquivamento e seus respectivos volumes e/ou documentos sejam reclassificados por um usuário autorizado e que todos os documentos já inseridos permaneçam nas unidades de arquivamento e nos volumes que estão sendo transferidos, mantendo a relação entre documentos, volumes e unidades de arquivamento	EC
1.3 Gerenciamento dos dossiês/processos	
1.3.1 Um SIGAD tem que registrar nos metadados as datas de abertura e de encerramento do dossiê/processo.	EC
1.3.2 Um SIGAD tem que permitir que um dossiê/processo seja encerrado por meio de procedimentos regulamentares e somente por usuários autorizados.	EC
1.3.3 Um SIGAD tem que permitir a consulta aos dossiês/processos já encerrados por usuários autorizados.	EC
1.3.4 Um SIGAD tem que impedir o acréscimo de novos documentos a dossiês/ processos já encerrados.	EC
1.3.6 Um SIGAD tem que impedir sempre a eliminação de uma unidade de arquivamento digital ou de qualquer parte de seu conteúdo, a não ser quando estiver de acordo com a tabela de temporalidade e destinação de documentos.	NC
1.3.7 Um SIGAD tem que garantir sempre a integridade da relação hierárquica entre classe, dossiê/processo, volume e documento, e entre classe, pasta e documento, independentemente de atividades de manutenção, ações do usuário ou falha de componentes do sistema.	NC
1.4 Requisitos adicionais para o gerenciamento de processos	

1.4.1 Um SIGAD tem que prever a formação/autuação de processos por usuário autorizado conforme estabelecido em legislação específica.	NC
1.4.3 Um SIGAD tem que prever que os documentos integrantes do processo digital recebam numeração sequencial sem falhas, não se admitindo que documentos diferentes recebam a mesma numeração.	EC
1.4.4 Um SIGAD tem que controlar a renumeração dos documentos integrantes de um processo digital.	NC
1.4.5 Um SIGAD tem que prever procedimentos para juntada de processos segundo a legislação específica na devida esfera e âmbito de competência. A juntada pode ser por anexação ou apensação. Este procedimento deve ser registrado nos metadados do processo.	EC
1.4.6 Um SIGAD tem que prever procedimentos para desapensação de processos segundo a legislação específica na devida esfera e âmbito de competência. Esse procedimento deve ser registrado nos metadados do processo.	EC
1.4.7 Um SIGAD tem que prever procedimentos para desentranhamento de documentos integrantes de um processo, segundo norma específica na devida esfera e âmbito de competência. Esse procedimento deve ser registrado nos metadados do processo.	EC
1.4.8 Um SIGAD tem que prever procedimentos para desmembramento de documentos integrantes de um processo, segundo norma específica na devida esfera e âmbito de competência. Esse procedimento deve ser registrado nos metadados do processo.	EC
1.4.9 Um SIGAD tem que prever o encerramento dos processos incluídos seus volumes e metadados.	NC
1.4.10 Um SIGAD tem que prever o desarquivamento para reativação dos processos, por usuário autorizado e obedecendo a procedimentos legais e administrativos	NC
1.5 Volumes: abertura, encerramento e metadados	
1.5.3 Um SIGAD tem que permitir que um volume herde, automaticamente, do dossiê/processo ao qual pertence, alguns metadados predefinidos, como, por exemplo, procedência, classes e temporalidade	EC
1.5.4 Um SIGAD tem que permitir a abertura de volumes para qualquer dossiê/processo que não esteja encerrado.	EC
1.5.6 Um SIGAD tem que assegurar que um volume conterá somente documentos. Não é permitido que um volume contenha outro volume ou outro dossiê/processo.	NC
1.5.7 Um SIGAD tem que permitir que um volume seja encerrado por meio de procedimentos regulamentares e apenas por usuários autorizados.	EC
1.5.8 Um SIGAD tem que assegurar que, ao ser aberto um novo volume, o precedente seja automaticamente encerrado. Apenas o volume produzido mais recentemente pode estar aberto; os demais volumes existentes no dossiê/processo têm que estar fechados.	NC
1.5.9 Um SIGAD tem que impedir a reabertura, para acréscimo de documentos, de um volume já encerrado	NC
1.6 Gerenciamento de documentos e processos/dossiês arquivísticos convencionais e híbridos	
1.6.1 Um SIGAD tem que capturar documentos ou dossiês/processos convencionais e gerenciá-los da mesma forma que os digitais.	EC
1.6.2 Um SIGAD tem que ser capaz de gerenciar a parte convencional e a parte digital integrantes de dossiês/processos híbridos, associando-as com o mesmo número identificador atribuído pelo sistema e o mesmo título, além de indicar que se trata de um documento arquivístico híbrido.	EC

1.6.3 Um SIGAD tem que permitir que um conjunto específico de metadados seja configurado para os documentos ou dossiês/processos convencionais e incluir informações sobre o local de arquivamento.	EC
1.6.4 Um SIGAD tem que dispor de mecanismos para acompanhar a movimentação do documento arquivístico convencional, de forma que fique evidente para o usuário a localização atual do documento.	EC
1.6.5 Um SIGAD tem que ser capaz de oferecer ao usuário funcionalidades para solicitar ou reservar a consulta a um documento arquivístico convencional, enviando uma mensagem para o detentor atual do documento ou para o administrador.	NC
1.6.7 Um SIGAD tem que assegurar que a recuperação de um documento ou dossiê/processo híbrido permita, igualmente, a recuperação dos metadados da parte digital e da convencional.	PC
1.6.8 Sempre que os documentos ou dossiês/processos híbridos estiverem classificados quanto ao grau de sigilo, um SIGAD tem que garantir que a parte convencional e a parte digital correspondente recebam a mesma classificação de sigilo.	PC
1.6.9 Um SIGAD tem que poder registrar na trilha de auditoria todas as alterações efetuadas nos metadados dos documentos ou dossiês/ processos convencionais e híbridos.	EC
2. Tramitação e fluxo de trabalho	
2.1 Controle do fluxo de trabalho	
2.1.1 Um recurso de fluxo de trabalho de um SIGAD tem que fornecer os passos necessários para o cumprimento de trâmites preestabelecidos ou aleatórios. Nesse caso, cada passo significa o deslocamento de um documento ou dossiê/ processo de um participante para outro, a fim de serem objeto de ações.	EC
2.1.2 Um SIGAD tem que ter capacidade, sem limitações, de estabelecer o número necessário de trâmites nos fluxos de trabalho.	EC
2.1.3 O fluxo de trabalho de um SIGAD tem que disponibilizar uma função para avisar um participante do fluxo de que um documento lhe foi enviado, especificando a ação necessária.	EC
2.1.5 O recurso de fluxo de trabalho de um SIGAD tem que permitir que fluxos de trabalho pré-programados sejam definidos, alterados e mantidos exclusivamente por usuário autorizado.	EC
2.1.7 Um recurso de fluxo de trabalho de um SIGAD tem que registrar na trilha de auditoria todas as alterações ocorridas neste fluxo.	EC
2.1.8 Um recurso de fluxo de trabalho de um SIGAD tem que registrar a tramitação de um documento a fim de que os usuários possam conhecer a situação de cada um no processo.	EC
2.1.12 Um recurso de fluxo de trabalho de um SIGAD tem que fornecer um histórico de movimentação dos documentos. O histórico de movimentação corresponde a um conjunto de metadados de datas de entrada e saída, nomes de responsáveis, título do documento, providências etc.	EC
2.1.14 Um recurso de fluxo de trabalho de um SIGAD tem que incluir processamento condicional, isto é, permitir que um fluxo de trabalho seja suspenso para aguardar a chegada de um documento e prossiga automaticamente quando este é recebido.	EC
2.1.16 Um recurso de fluxo de trabalho de um SIGAD tem que reconhecer indivíduos e grupos de trabalho como participantes.	EC

2.1.19 Um recurso de fluxo de trabalho de um SIGAD tem que fornecer meios de elaboração de relatórios completos para permitir que gestores monitorem a tramitação dos documentos e o desempenho dos participantes	EC
2.1.20 Um recurso de fluxo de trabalho de um SIGAD tem que registrar a tramitação de um documento em seus metadados. Os metadados referentes à tramitação devem registrar data e hora de envio e recebimento, e a identificação do usuário.	EC
2.2 Controle de versões e do status do documento	
2.2.1 Um recurso de fluxo de trabalho de um SIGAD tem que ser capaz de registrar o status de transmissão do documento, ou seja, se é minuta, original ou cópia.	EC
2.2.2 Um SIGAD tem que ser capaz de controlar as diversas versões de um documento que está tramitando.	EC
2.2.3 Um SIGAD tem que ser capaz de associar e relacionar as diversas versões de um documento.	EC
2.2.4 Um SIGAD tem que manter o identificador único do documento, e o controle de versões tem que ser registrado em metadados específicos.	EC
3. Captura	
3.1 Procedimentos gerais	
3.1.1 A captura tem que garantir a execução das seguintes funções: <ul style="list-style-type: none"> • registrar e gerenciar todos os documentos convencionais; • registrar e gerenciar todos os documentos digitais, independentemente do contexto tecnológico; • classificar todos os documentos de acordo com o plano ou código de classificação; • controlar e validar a introdução de metadados 	EC
3.1.2 Um SIGAD tem que ser capaz de capturar documentos digitais das formas a seguir: <ul style="list-style-type: none"> • captura de documentos produzidos dentro do SIGAD; • captura de documento individual produzido em arquivo digital fora do SIGAD; • captura de documento individual produzido em workflow ou em outros sistemas integrados ao SIGAD; • captura de documentos em lote 	EC
3.1.4 Um SIGAD tem que aceitar o conteúdo do documento, bem como as informações que definem sua aparência, mantendo as associações entre os vários objetos digitais que compõem o documento, isto é, anexos e links de hipertexto	EC

<p>3.1.5 Um SIGAD tem que permitir a inserção de todos os metadados obrigatórios e opcionais definidos na sua configuração e garantir que se mantenham associados ao documento. Os metadados obrigatórios são:</p> <ul style="list-style-type: none"> • nome do arquivo digital; • número identificador atribuído pelo sistema; • data de produção; • data e hora de transmissão e recebimento; • data e hora da captura; • título ou descrição abreviada; • classificação de acordo com o plano ou código de classificação; • prazos de guarda; • autor (pessoa física ou jurídica); • redator (se diferente do autor); • originador; • destinatário (e respectivo cargo); • nome do setor responsável pela execução da ação contida no documento; • indicação de anotação; • indicação de anexos; • indicação de versão; • restrição de acesso; <p>• registro das migrações e data em que ocorreram. Os metadados opcionais se referem a informações mais detalhadas sobre o documento, tais como:</p> <ul style="list-style-type: none"> • espécie/tipo/gênero documental; • associações a documentos diferentes que podem estar relacionados pelo fato de registrarem a mesma atividade ou se referirem à mesma pessoa ou situação; • formato e software (nome e versão) em que o documento foi produzido ou capturado; • máscaras de formatação (templates) necessárias para interpretar a estrutura do documento; • assunto/descritor (diferentes do já estabelecido no código de classificação); • localização física; e • outros que se julgarem necessários. 	PC
<p>3.1.6 Um SIGAD tem que prever a inserção dos metadados obrigatórios, previstos em legislação específica na devida esfera e âmbito de competência, no momento da captura de processos</p>	EC
<p>3.1.7 Um SIGAD tem que ser capaz de atribuir um número identificador a cada dossiê/processo e documento capturado, que serve para identificá-lo desde o momento da captura até sua destinação final no SIGAD.</p>	NC
<p>3.1.8 O formato do número identificador atribuído pelo sistema deve ser definido no momento da configuração do SIGAD. O identificador pode ser numérico ou alfanumérico, ou pode incluir os identificadores encadeados das entidades superiores no ramo apropriado da hierarquia.</p>	NC

3.1.9 Num SIGAD, o número identificador atribuído pelo sistema tem que: <ul style="list-style-type: none"> • ser gerado automaticamente, sendo vedada sua introdução manual e alteração posterior; ou • ser atribuído pelo usuário e validado pelo sistema antes de ser aceito. Uma opção seria gerar o número identificador automaticamente, mas, nesse caso, ocultando-o do usuário e permitindo a este introduzir uma sequência não necessariamente única como um “identificador”. O usuário empregaria essa sequência como um identificador, mas o SIGAD a consideraria um metadado pesquisável, definido pelo usuário. 	NC
3.1.10 Um SIGAD tem que prever a adoção da numeração única de processos e/ou documentos oficiais de acordo com a legislação específica a fim de garantir a integridade do número atribuído ao processo e/ou documento na unidade protocolizadora de origem.	NC
3.1.12 Um SIGAD tem que garantir que os metadados associados a um documento sejam inseridos somente por usuários autorizados.	EC
3.1.13 Um SIGAD tem que garantir que os metadados associados a um documento sejam alterados somente por administradores e usuários autorizados e devidamente registrados em trilhas de auditoria.	EC
3.1.16 Um SIGAD tem que garantir a visualização do registro de entrada do documento no sistema com todos os metadados inseridos automaticamente e os demais a serem atribuídos pelo usuário.	EC
3.1.17 Um SIGAD tem que garantir a inserção de outros metadados após a captura.	EC
3.1.18 Sempre que um documento tiver mais de uma versão, o SIGAD tem que permitir que os usuários selecionem pelo menos uma das seguintes ações: <ul style="list-style-type: none"> • registrar todas as versões do documento como um só documento arquivístico; • registrar uma única versão do documento como um documento arquivístico; • registrar cada uma das versões do documento, separadamente, como um documento arquivístico. 	EC
3.1.21 No caso de documentos ou dossiês/processos constituídos por mais de um objeto digital, o SIGAD tem que: <ul style="list-style-type: none"> • tratar o documento como uma unidade indivisível, assegurando a relação entre os objetos digitais; • preservar a integridade do documento, mantendo a relação entre os objetos digitais; • garantir a integridade do documento quando de sua recuperação, visualização e gestão posteriores; • gerenciar a destinação de todos os objetos digitais que compõem o documento como uma unidade indivisível. 	EC
3.1.22 Um SIGAD tem que emitir um aviso caso o usuário tente registrar um documento que já tenha sido registrado no mesmo dossiê/processo.	NC
3.2 Captura em lote	
3.2.1 Um SIGAD tem que proporcionar a captura em lote de documentos gerados por outros sistemas. Esse procedimento tem que: <ul style="list-style-type: none"> • permitir a importação de transações predefinidas de arquivos em lote; • registrar, automaticamente, cada um dos documentos importados contidos no lote; • permitir e controlar a edição do registro dos documentos importados; • validar a integridade dos metadados. Exemplos de lotes de documento: mensagens de correio eletrônico, correspondência digitalizada por meio de escâner, documentos provenientes de um departamento, grupo ou indivíduo, transações de aplicações de um computador ou, ainda, documentos oriundos de um sistema de gestão de documentos. 	NC

3.3 Captura de mensagens de correio eletrônico	
3.3.1 Um SIGAD tem que permitir que, na fase de configuração, seja escolhida uma das seguintes operações: <ul style="list-style-type: none"> • capturar mensagens de correio eletrônico após selecionar quais serão objeto de registro; ou • capturar, automaticamente, todas as mensagens de correio eletrônico. 	NC
3.4 Captura de documentos convencionais ou híbridos	
3.4.1 O SIGAD tem que poder capturar também os documentos convencionais e/ou híbridos.	EC
3.4.2 O SIGAD tem que acrescentar aos metadados dos documentos convencionais informações sobre sua localização. Essa informação só será acessada por usuários autorizados.	EC
3.5 Formato de arquivo e estrutura dos documentos a serem capturados	
3.5.1 Um SIGAD tem que possuir a capacidade de capturar documentos com diferentes formatos de arquivo e estruturas.	EC
3.5.3 Um SIGAD tem que capturar documentos que se apresentam com as seguintes estruturas: <ul style="list-style-type: none"> • simples: texto, imagens, mensagens de correio eletrônico, slides digitais, som. • composta: mensagens de correio eletrônico com anexos, páginas web, publicações eletrônicas, bases de dados. 	PC
3.5.4 Um SIGAD tem que ser capaz de incluir novos formatos de arquivos à medida que forem sendo adotados pelo órgão ou entidade.	EC
3.6 Estrutura dos procedimentos de gestão	
3.6.1 Um SIGAD tem que ser capaz de reconhecer três domínios para o controle dos procedimentos de gestão: espaço individual, espaço do grupo e espaço geral.	EC
3.6.2 Um SIGAD tem que ser capaz de operacionalizar as regras estabelecidas pelo sistema de gestão arquivística de documentos nos três espaços.	EC
3.6.3 Um SIGAD tem que impedir que o conteúdo de um documento seja alterado por usuários e administradores, exceto se a alteração fizer parte do processo documental.	EC
4. Avaliação e destino	
4.1 Configuração da tabela de temporalidade e destinação de documentos	
4.1.1 Um SIGAD tem que prover funcionalidades para definição e manutenção de tabela de temporalidade e destinação de documentos, associada ao plano de classificação do órgão ou entidade.	NC
4.1.2 Um SIGAD tem que associar, automaticamente, ao dossiê/processo o prazo e a destinação previstos na classe em que o documento foi inserido.	NC
4.1.3 Um SIGAD tem que manter tabela de temporalidade e destinação de documentos com as seguintes informações: <ul style="list-style-type: none"> • identificador do órgão ou entidade; • identificador da classe; • prazo de guarda na fase corrente; • prazo de guarda na fase intermediária; 	NC

<ul style="list-style-type: none"> • destinação final; • observações; • evento que determina o início da contagem do prazo de retenção na fase corrente e na fase intermediária. <p>A tabela de temporalidade e destinação de documentos dos integrantes do SINAR deve estar de acordo com a legislação e ser aprovada pela instituição arquivística na específica esfera de competência.</p>	
<p>4.1.4 Um SIGAD tem que prever, pelo menos, as seguintes situações para destinação:</p> <ul style="list-style-type: none"> • apresentação dos documentos para reavaliação em data futura; • eliminação; • exportação para transferência; • exportação para recolhimento (guarda permanente). 	NC
<p>4.1.5 Um SIGAD tem que prever a iniciação automática da contagem dos prazos de guarda referenciados na tabela de temporalidade e destinação de documentos, pelo menos, a partir dos seguintes eventos:</p> <ul style="list-style-type: none"> • abertura de dossiê; • arquivamento de dossiê/processo; • desarquivamento de dossiê/processo; • inclusão de documento em um dossiê/processo. <p>Acontecimentos específicos, descritos na tabela de temporalidade e destinação, como, por exemplo, “cinco anos a contar da data de aprovação das contas”, quando não puderem ser detectados automaticamente pelo sistema, deverão ser informados ao SIGAD por usuário autorizado.</p>	NC
<p>4.1.6 Um SIGAD tem que prever que a definição dos prazos de guarda seja expressa por:</p> <ul style="list-style-type: none"> • um número inteiro de dias ou • um número inteiro de meses ou • um número inteiro de anos ou • uma combinação de um número inteiro de anos, meses e dias. 	NC
<p>4.1.7 Um SIGAD tem que limitar a definição e a manutenção (alteração, inclusão e exclusão) da tabela de temporalidade e destinação de documentos a usuários autorizados.</p>	NC
<p>4.1.8 Um SIGAD tem que permitir que um usuário autorizado altere o prazo ou destinação prevista em um item da tabela de temporalidade e destinação de documentos e garantir que a alteração tenha efeito em todos os documentos ou dossiês/processos associados àquele item. As alterações na tabela de temporalidade e destinação só poderão ser feitas como resultado de um processo de reavaliação realizado pela comissão de avaliação do órgão ou entidade em virtude de mudança do contexto administrativo, jurídico ou cultural. Os integrantes do SINAR deverão ainda ter suas tabelas aprovadas pela instituição arquivística na específica esfera de competência.</p>	NC
<p>4.1.11 Um SIGAD tem que prover funcionalidades para elaboração de relatórios que apoiem a gestão da tabela de temporalidade e destinação, incluindo a capacidade de:</p> <ul style="list-style-type: none"> • gerar relatório completo da tabela de temporalidade e destinação de documentos; • gerar relatório parcial da tabela de temporalidade e destinação de documentos a partir de um ponto determinado na hierarquia do plano de 	NC

classificação; • gerar relatório dos documentos ou dossiês/processos aos quais foi atribuído um determinado prazo de guarda; • identificar as inconsistências existentes entre a tabela de temporalidade e destinação de documentos e o plano de classificação.	
4.2 Aplicação da tabela de temporalidade e destinação de documentos	
4.2.1 Um SIGAD tem que fornecer recursos integrados à tabela de temporalidade e destinação de documentos para implementar as ações de destinação.	NC
4.2.2 Para cada dossiê/processo, um SIGAD tem que acompanhar automaticamente os prazos de guarda determinados para a classe à qual pertence.	NC
4.2.3 Um SIGAD tem que prover funcionalidades para informar ao usuário autorizado sobre os documentos ou dossiês/processos que já cumpriram ou estão para cumprir o prazo de guarda previsto.	NC
4.2.4 Um SIGAD tem de prover funcionalidades para gerenciar o processo de destinação, que tem de ser iniciado por usuário autorizado e cumprir os seguintes passos: • identificar automaticamente os documentos ou dossiês/processos que atingiram os prazos de guarda previstos; • informar o usuário autorizado sobre todos os documentos ou dossiês/ processos que foram identificados no passo anterior; • possibilitar a alteração do prazo ou destinação previstos para aqueles documentos ou dossiês/processos, caso necessário; • proceder à ação de destinação quando confirmada pelo usuário autorizado.	NC
4.2.6 Um SIGAD deve prever, em determinados casos, dispositivo de aviso antes do início de uma ação de destinação.	NC
4.2.7 Um SIGAD tem que restringir as funções de destinação a usuários autorizados.	NC
4.2.8 Quando um administrador transfere documentos ou dossiês/processos de uma classe para outra, em virtude de uma reclassificação, o SIGAD tem que adotar automaticamente a temporalidade e a destinação vigentes na nova classe	NC
4.2.9 Quando um documento digital (objeto digital) estiver associado a mais de um dossiê ou processo, e tiver prazos de guarda diferentes associados a ele, o SIGAD tem que automaticamente verificar todos os prazos de guarda e as destinações previstas para esse documento e garantir que ele seja mantido em cada dossiê/processo pelo tempo definido na tabela de temporalidade e destinação de documentos, de forma que: • a remoção de um documento de um dossiê/processo não prejudique a manutenção desse mesmo documento em outro dossiê/processo, até que todas as referências desse documento tenham atingido o prazo de guarda previsto; • a manutenção de um documento em um dossiê/processo por prazo mais longo não obrigue a permanência desse mesmo documento em outro dossiê/processo de prazo mais curto. Nesse caso o registro do documento com prazo mais curto tem que ser removido, mas o documento é mantido no SIGAD.	NC
4.3 Exportação de documentos	
4.3.1 Um SIGAD tem que ser capaz de exportar documentos e dossiês/ processos digitais e seus metadados para outro sistema dentro ou fora do órgão ou entidade	NC
4.3.2 Quando um SIGAD exportar os documentos e dossiês/processos de uma classe para executar uma ação de transferência ou recolhimento, tem que ser capaz de exportar todos os documentos e dossiês/processos da classe incluídos na ação de destinação, com seus respectivos volumes, documentos e metadados associados.	NC

4.3.3 Um SIGAD tem que ser capaz de exportar um documento e dossiê/ processo ou grupo de documentos e dossiês/processos numa sequência de operações, de modo que: <ul style="list-style-type: none"> • o conteúdo, o contexto e a estrutura dos documentos não se degradem; • todos os componentes de um documento digital sejam exportados como uma unidade. Por exemplo, uma mensagem de correio eletrônico e seus respectivos anexos; • todos os metadados do documento sejam relacionados a ele de forma que as ligações possam ser mantidas no novo sistema; • todas as ligações entre documentos, volumes e dossiês/processos sejam mantidas 	NC
4.3.6 Um SIGAD tem que ser capaz de exportar todos os tipos de documentos que está apto a capturar.	NC
4.3.7 Um SIGAD tem que produzir um relatório detalhado sobre qualquer falha que ocorra durante uma exportação. O relatório tem que identificar os documentos e dossiês/processos que originaram erros de processamento ou cuja exportação não tenha sido bem sucedida.	NC
4.3.8 Um SIGAD tem que conservar todos os documentos e dossiês/processos digitais que foram exportados, pelo menos até que tenham sido importados no sistema destinatário com êxito.	NC
4.3.9 Um SIGAD tem que manter metadados relativos a documentos e dossiês/ processos que foram exportados. O administrador deve indicar o subconjunto de metadados que deverá ser mantido	NC
4.3.10 Um SIGAD tem que gerar listagem em meio digital e em papel para descrever documentos e dossiês/processos digitais que estão sendo exportados. Este requisito se aplica principalmente nos casos em que é feita exportação para transferência ou recolhimento a uma instituição arquivística pública. Nesse caso, a listagem deverá ser produzida no formato estabelecido pela instituição arquivística recebedora.	NC
4.4 Eliminação	
4.4.1 Um SIGAD tem que restringir a função de eliminação de documentos ou dossiês/processos somente a usuários autorizados.	NC
4.4.2 Um SIGAD tem que pedir confirmação da eliminação a um usuário autorizado antes que qualquer ação seja tomada com relação ao documento e dossiê/ processo e cancelar o processo de eliminação se a confirmação não for dada.	NC
4.4.3 Um SIGAD tem que avisar o usuário autorizado quando um documento ou dossiê/processo que estiver sendo eliminado se encontrar relacionado a outro; os sistemas também têm de suspender o processo até que seja tomada uma das medidas abaixo: <ul style="list-style-type: none"> • confirmação pelo usuário autorizado para prosseguir ou cancelar o processo; • produção de um relatório especificando os documentos ou dossiês/ processos envolvidos e todas as ligações com outros documentos ou dossiês/processos 	NC
4.4.5 Quando um documento tem várias referências armazenadas no sistema, um SIGAD tem que garantir que todas essas referências sejam verificadas antes de eliminar o objeto digital.	NC
4.4.6 Um SIGAD tem que produzir um relatório detalhando qualquer falha que ocorra durante uma eliminação. O relatório tem que identificar os documentos cuja eliminação não tenha sido bem sucedida.	NC

4.4.8 Um SIGAD tem que gerar relatório com os documentos e dossiês/ processos que serão eliminados. Essa listagem deve seguir o formato da listagem de eliminação conforme o estabelecido na norma vigente.	NC
4.4.9 Um SIGAD tem que manter metadados relativos a documentos e dossiês/ processos eliminados. O administrador deve indicar o subconjunto de metadados que deverá ser mantido.	NC
4.5 Avaliação e destinação de documentos arquivísticos convencionais e híbridos	
4.5.1 Um SIGAD tem que aplicar a mesma tabela de temporalidade e destinação de documentos para os documentos convencionais, digitais ou híbridos.	NC
4.5.2 Um SIGAD tem que acompanhar os prazos de guarda dos documentos convencionais e deve dar início aos procedimentos de eliminação ou transferência desses documentos, tomando em consideração suas especificidades.	NC
4.5.3 Um SIGAD tem que alertar o administrador sobre a existência e a localização de uma parte convencional associada a um documento híbrido que esteja destinado a ser exportado, transferido ou eliminado.	NC
5. Pesquisa, localização e apresentação dos documentos	
5.1 Aspectos gerais	
5.1.1 Um SIGAD tem que fornecer facilidades para pesquisa, localização e apresentação dos documentos.	EC
5.2 Pesquisa e localização	
5.2.1 Um SIGAD tem que fornecer uma série flexível de funções que atuem sobre os metadados relacionados com os diversos níveis de agregação (documento, unidade de arquivamento e classe) e sobre os conteúdos dos documentos arquivísticos por meio de parâmetros definidos pelo usuário, com o objetivo de localizar e acessar os documentos e/ou metadados, seja individualmente ou reunidos em grupo.	EC
5.2.2 Um SIGAD tem que executar pesquisa de forma integrada, isto é, apresentar todos os documentos e dossiês/processos, sejam eles digitais, híbridos ou convencionais, que satisfaçam aos parâmetros da pesquisa.	NC
5.2.3 Um SIGAD tem que permitir que todos os metadados de gestão de um documento ou dossiê/processo possam ser pesquisados.	EC
5.2.5 Um SIGAD tem que permitir que um documento ou dossiê/processo possa ser recuperado por meio de um número identificador.	EC
5.2.6 Um SIGAD tem que permitir que um documento ou dossiê/processo possa ser recuperado por meio de todas as formas de identificação implementadas, incluindo, no mínimo: <ul style="list-style-type: none"> • identificador; • título; • assunto; • datas; • procedência/interessado; • autor/redator/originador; • classificação de acordo com plano ou código de classificação. 	EC

5.2.17 Um SIGAD tem que permitir a pesquisa e recuperação de uma unidade de arquivamento completa e exibir a lista de todos os documentos que a compõem, como uma unidade e num único processo de recuperação.	EC
5.2.18 Um SIGAD tem que limitar o acesso a qualquer informação (metadado ou conteúdo de um documento arquivístico) se restrições de acesso e questões de segurança assim determinarem.	EC
5.3 Apresentação: visualização, impressão, emissão de som	
5.3.1 Um SIGAD tem que apresentar o resultado da pesquisa como uma lista de documentos e dossiês/processos digitais, convencionais ou híbridos que cumpram os parâmetros da consulta e deve notificar o usuário se o resultado for nulo.	NC
5.3.3 Após apresentar o resultado da pesquisa, um SIGAD tem que oferecer ao usuário as opções: • visualizar os documentos e dossiês/processos resultantes da pesquisa; • redefinir os parâmetros de pesquisa e fazer nova consulta.	EC
5.3.7 Um SIGAD tem que ser capaz de apresentar o conteúdo de todos os tipos de documentos arquivísticos digitais capturados, de forma que: • preserve as características de exibição visual e de formato apresentadas pela aplicação geradora; • exiba todos os componentes do documento digital em conjunto, como uma unidade.	EC
5.3.8 Um SIGAD tem que ser capaz de exibir em tela todos os tipos de documentos capturados.	EC
5.3.9 Um SIGAD tem que ser capaz de imprimir os documentos capturados, preservando o formato produzido pelas aplicações geradoras.	EC
5.3.10 Um SIGAD tem que ser capaz de exibir/reproduzir o conteúdo de documentos que incluam imagem fixa, imagem em movimento e som.	PC
5.3.11 Um SIGAD tem que proporcionar ao usuário formas flexíveis de impressão de documentos com seus metadados e possibilitar a definição dos metadados a serem impressos.	NC
5.3.12 Um SIGAD tem que ser capaz de exibir em tela e imprimir todos os metadados associados aos documentos e dossiês/processos resultantes de uma pesquisa.	NC
5.3.13 Um SIGAD tem que permitir a impressão de uma lista dos documentos e dossiês/processos resultantes de uma pesquisa.	NC
5.3.14 Um SIGAD tem que permitir a impressão de uma lista dos documentos que compõem um dossiê/processo.	NC
5.3.16 Um SIGAD tem que permitir que todos os documentos de um dossiê/ processo sejam impressos em uma única operação, na sequência determinada pelo usuário.	NC
5.3.17 Um SIGAD tem que incluir recursos destinados a transferir para suportes adequados documentos que não possam ser impressos, tais como documentos sonoros, vídeos e páginas web.	NC
5.3.19 Um SIGAD tem que ser capaz de realizar pesquisa e exibição de documentos e dossiês/processos, simultaneamente, para diversos usuários.	EC
6.Segurança	
6.1 Cópias de segurança	

6.1.1 Um SIGAD tem que permitir que, sob controle do seu administrador, mecanismos de backup criem cópias de todas as informações nele contidas (documentos arquivísticos, metadados e parâmetros do sistema).	NC
6.1.2 O administrador do SIGAD tem que manter o controle das cópias de segurança, prevendo testes de restauração.	NC
6.1.7 Um SIGAD tem que incluir funções para restituir os documentos de arquivo e metadados a um estado conhecido, utilizando uma combinação de cópias restauradas e rotinas de auditoria.	NC
6.2 Controle de acesso	
6.2.1 Para implementar o controle de acesso, um SIGAD tem que manter pelo menos os seguintes atributos dos usuários, de acordo com a política de segurança: <ul style="list-style-type: none"> • identificador do usuário; • autorizações de acesso; • credenciais de autenticação. Senha, crachá, chave criptográfica, token USB, smartcard, biometria (de impressão digital, de retina etc.) são exemplos de credenciais de autenticação. 	NC
6.2.2 Um SIGAD tem que exigir que o usuário esteja devidamente identificado e autenticado antes de iniciar qualquer operação no sistema.	NC
6.2.3 Um SIGAD tem que garantir que os valores dos atributos de segurança e controle de acesso, associados ao usuário, estejam dentro de conjuntos de valores válidos.	NC
6.2.5 Um SIGAD tem que permitir acesso a funções do sistema somente a usuários autorizados e sob controle rigoroso da administração do sistema, a fim de proteger a autenticidade dos documentos arquivísticos digitais.	NC
6.2.7 Somente administradores autorizados têm que ser capazes de criar, alterar, remover ou revogar permissões associadas a papéis de usuários, grupos de usuários ou usuários individuais.	NC
6.2.11 Um SIGAD tem que implementar a política de controle de acesso a documentos por grupos de usuários considerando: <ul style="list-style-type: none"> • a identidade do usuário e sua participação em grupos; • os atributos de segurança, associados ao documento arquivístico digital, às classes e/ou aos dossiês/processos. 	NC
6.2.12 O acesso a documentos, a dossiês/processos ou classes tem que ser concedido se a permissão requerida para a operação estiver associada a pelo menos um dos grupos aos quais pertença o usuário.	NC
6.2.13 Um SIGAD tem que permitir que um usuário pertença a mais de um grupo.	NC
6.2.15 Um SIGAD tem que usar os seguintes atributos do usuário ao implementar a política de controle de acesso aos documentos digitais por papéis de usuários: <ul style="list-style-type: none"> • identificação do usuário; • papéis associados ao usuário. 	NC

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"> • identificação do documento digital; • operações permitidas aos vários papéis de usuários, sobre as classes ou unidades de arquivamento a que o documento pertence. 	EC
6.2.17 O acesso a documentos, dossiês/processos ou classes tem que ser concedido somente se a permissão requerida para a operação estiver presente em pelo menos um dos papéis associados ao usuário.	NC
6.2.18 Um SIGAD tem que impedir que um usuário assuma papéis com direitos conflitantes.	NC
6.3 Classificação da informação quanto ao grau de sigilo e restrição de acesso à informação sensível	
6.3.1 Um SIGAD tem que implementar a classificação de grau de sigilo de documentos, dossiês/processos e classes do plano de classificação, e de todas as operações de usuários nos documentos.	EC
6.3.2 Um SIGAD tem que implementar a classificação de grau de sigilo baseando-se nos seguintes atributos de segurança: <ul style="list-style-type: none"> • grau de sigilo do documento; • credencial de segurança do usuário. O grau de sigilo tem que estar associado à credencial de segurança. 	EC
6.3.3 Um SIGAD tem que recusar o acesso de usuários a documentos que possuam grau de sigilo superior à sua credencial de segurança.	EC
6.3.4 Um SIGAD tem que garantir que documentos sem atribuição de grau de sigilo, importados a partir de fontes externas ao SIGAD, estejam sujeitos às políticas de controle de acesso e de sigilo.	NC
6.3.5 Um SIGAD tem que ser capaz de manter a marcação de sigilo original durante a importação de documentos a partir de fontes externas ao SIGAD.	NC
6.3.7 Um SIGAD tem que permitir que um dos itens abaixo seja selecionado durante a configuração: <ul style="list-style-type: none"> • graus de sigilo a serem atribuídos a classes e dossiês/processos; • classes e dossiês/processos sem grau de sigilo. 	EC
6.3.8 Em caso de erro ou reavaliação, o administrador tem que ser capaz de alterar o grau de sigilo de todos os documentos arquivísticos de um dossiê/processo ou de uma classe, numa única operação.	NC
6.3.9 Um SIGAD tem que garantir que o grau de sigilo de um documento importado esteja associado a um usuário autorizado com a credencial de segurança pertinente para receber o documento.	NC
6.3.10 Um SIGAD tem que permitir somente aos administradores autorizados a possibilidade de alterar a configuração dos valores predefinidos (default) para os atributos de segurança e marcação de graus de sigilo, quando necessário e apropriado.	NC
6.3.11 Somente administradores autorizados têm que ser capazes de realizar as seguintes ações: <ul style="list-style-type: none"> • remover ou revogar os atributos de segurança dos documentos; • criar, alterar, remover ou revogar as credenciais de segurança dos usuários. 	EC

6.3.12 Um SIGAD tem que permitir somente ao usuário autorizado, mediante confirmação, a desclassificação ou redução do grau de sigilo de um documento.	EC
6.3.14 Um SIGAD tem que impedir que um documento sigiloso seja eliminado. Os documentos sigilosos têm que se tornar ostensivos para serem submetidos ao processo de avaliação e receberem a destinação prevista.	NC
6.3.15 Um SIGAD tem que implementar metadados nos níveis de dossiê, documento ou extrato de documento para controlar o acesso à informação sensível.	EC
6.4 Trilhas de auditoria	
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"> • data e hora da captura de todos os documentos; • responsável pela captura; • reclassificação, desclassificação ou redução do grau de sigilo de um documento ou dossiê/processo, com a classificação inicial e final. • qualquer alteração na tabela de temporalidade e destinação de documentos; • qualquer ação de reavaliação de documentos; • qualquer alteração nos metadados associados a classes, dossiês/ processos ou documentos; • data e hora de produção, aditamento e eliminação de metadados; • alterações efetuadas nas permissões de acesso que afetem um dossiê/processo, documento ou usuário; • ações de exportação e importação envolvendo os documentos; • tentativas de exportação (inclusive para backup) e importação (inclusive restore); • usuário, data e hora de acesso ou tentativa de acesso a documentos e ao SIGAD; • tentativas de acesso negado a qualquer documento; • ações de eliminação de qualquer documento e seus metadados; • infrações cometidas contra mecanismos de controle de acesso; • mudanças no relógio gerador de carimbos de tempo; • todas as ações administrativas sobre os atributos de segurança (papéis, grupos, permissões etc.); • todas as ações administrativas sobre dados de usuários (cadastro, ativação, bloqueio, atualização de dados e permissões, troca de senha etc.); • todos os eventos de administração e manutenção das trilhas de auditoria (alarmes, cópias, configuração de parâmetros etc.) 	PC
6.4.2 Um SIGAD tem que registrar, em cada evento auditado, informações sobre a identidade do usuário, desde que essa identificação esteja de acordo com a política de privacidade da organização e a legislação vigente.	NC
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.	NC
6.4.6 Um SIGAD tem que ser capaz de impedir qualquer modificação na trilha de auditoria.	NC
6.4.7 Somente administradores autorizados têm que ser capazes de exportar as trilhas de auditoria sem afetar a trilha armazenada, ou transferir as trilhas de auditoria de um suporte de armazenamento para outro. A trilha de auditoria não pode ser excluída antes da data indicada na tabela de temporalidade. Porém, a transferência implica a cópia da trilha para outro espaço de armazenamento, com a subsequente liberação do espaço original.	NC

A exportação é a cópia sem liberação do espaço.	
6.4.12 Um SIGAD tem que fornecer relatórios sobre as ações que afetam classes, unidades de arquivamento e documentos, em ordem cronológica e organizados por: <ul style="list-style-type: none"> • documento arquivístico, unidade de arquivamento ou classe; • usuário; • tipo de ação ou operação. 	NC
6.4.14 Somente administradores autorizados têm que ser capazes de configurar o conjunto de eventos auditáveis e seus atributos.	NC
6.4.15 Somente administradores autorizados, acompanhados do auditor, têm que ser capazes de configurar o conjunto de eventos auditáveis e seus atributos.	NC
6.5 Assinaturas digitais	
6.5.2 Somente administradores autorizados têm que ser capazes de incluir, remover ou atualizar no SIGAD os certificados digitais de computadores ou de usuários.	EC
6.5.3 Um SIGAD tem que ser capaz de verificar a validade da assinatura digital no momento da captura do documento.	NC
6.5.4 Um SIGAD, no processo de verificação da assinatura digital, tem que ser capaz de registrar, nos metadados do documento, o seguinte: <ul style="list-style-type: none"> • validade da assinatura verificada; • registro da verificação da assinatura; • data e hora em que ocorreu a verificação. 	NC
6.6 Criptografia	
6.6.1 Um SIGAD tem que usar criptografia no armazenamento, na transmissão e na apresentação de documentos arquivísticos digitais ao implementar a política de sigilo.	EC
6.6.2 Um SIGAD tem que limitar o acesso aos documentos cifrados somente àqueles usuários portadores da chave de decifração.	EC
6.6.3 Um SIGAD tem que registrar os seguintes metadados sobre um documento cifrado: <ul style="list-style-type: none"> • indicação sobre se está cifrado ou não; • algoritmos usados na cifração; • identificação do remetente; • identificação do destinatário 	NC
6.6.5 Somente usuários autorizados têm que ser capazes de realizar as operações a seguir: <ul style="list-style-type: none"> • incluir, remover ou alterar parâmetros dos algoritmos criptográficos instalados no SIGAD; • incluir, remover ou substituir chaves criptográficas de programas ou usuários do SIGAD; 	NC

6.6.6 Em caso de remoção da cifração do documento, os seguintes metadados adicionais têm que ser registrados na trilha de auditoria: <ul style="list-style-type: none"> • data e hora da remoção da cifração; • identificação do executor da operação; • motivo da remoção da cifração. 	NC
6.7 Marcas d'água digitais	
6.7.1 Um SIGAD tem que ser capaz de recuperar informação contida em marcas d'água digitais.	NC
6.7.2 Um SIGAD tem que ser capaz de armazenar documentos arquivísticos digitais que contenham marcas d'água digitais, assim como informação de apoio relacionada à marca d'água.	NC
6.8 Acompanhamento de transferência	
6.8.2 Um SIGAD tem que fornecer um recurso de acompanhamento para monitorar e registrar informações acerca do local atual e da transferência de dossiês/processos digitais e convencionais.	NC
6.8.3 A função de acompanhamento de transferência tem que registrar metadados que incluam: <ul style="list-style-type: none"> • número identificador dos documentos atribuído pelo sistema; • localização atual e localizações anteriores, definidas pelo usuário; • data e hora de envio/transferência; • data e hora da recepção no novo local; • destinatário; • usuário responsável pela transferência (sempre que for adequado); • método de transferência. 	NC
6.9 Autoproteção	
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. Na restauração ao estado seguro, um SIGAD deve ser capaz de garantir a recuperação de perdas ocorridas, inclusive dos documentos de transações mais recentes.	NC
6.9.5 Um SIGAD tem que garantir que as funções de controle de acesso sejam invocadas antes de qualquer operação de acesso e retornem sem erros antes do prosseguimento da operação.	NC
6.9.6 Um SIGAD tem que preservar um estado seguro de funcionamento, interrompendo completamente a interação com usuários comuns, quando ocorrer um dos erros a seguir: <ul style="list-style-type: none"> • falha de comunicação entre cliente e servidor; • perda de integridade das informações de controle de acesso; • falta de espaço para registro nas trilhas de auditoria. 	NC
6.10 Alterar, apagar e truncar documentos arquivísticos digitais	

6.10.1 Um SIGAD tem que permitir, a um administrador autorizado, anular a operação em caso de erro do usuário ou do sistema. Anular uma operação não significa apagar um documento arquivístico capturado pelo SIGAD. A anulação da eliminação definitiva de documentos, por ser irreversível, não é possível.	NC
6.10.3 Em situações excepcionais, o administrador tem que ser autorizado a apagar ou corrigir dossiês/processos, volumes e documentos. Nesse caso, um SIGAD tem que: <ul style="list-style-type: none"> • registrar integralmente a ação de apagar ou corrigir na trilha de auditoria; • produzir um relatório de anomalias para o administrador; • eliminar todo o conteúdo de um dossiê/processo ou volume, quando forem eliminados; • garantir que nenhum documento seja eliminado se tal ação resultar na alteração de outro documento arquivístico; • informar o administrador sobre a existência de ligação entre um dossiê/processo ou documento prestes a ser apagado e qualquer outro dossiê/processo ou documento, solicitando confirmação antes de concluir a operação; • manter a integridade total do metadado, a qualquer momento. 	NC
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.	NC
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.	NC
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.	NC
6.10.10 Um SIGAD tem que armazenar, na trilha de auditoria, qualquer alteração efetuada para satisfazer os requisitos desta seção.	NC
7. Armazenamento	
7.1 Durabilidade	
7.1.2 A escolha de dispositivos tem que ser revista sempre que a evolução tecnológica indicar mudanças importantes.	EC
7.1.3 Atividades de migração têm que ser efetivadas, preventivamente, sempre que se torne patente ou previsível a obsolescência do padrão corrente.	EC
7.1.4 Para as memórias secundárias, um SIGAD tem que manter registro de MTBF (mean time between failure), bem como suas datas de aquisição.	NC
7.1.5 Para as memórias secundárias e terciárias, um SIGAD tem que fazer o gerenciamento das mídias por meio do registro de durabilidade prevista, data de aquisição e histórico de utilização. As informações técnicas sobre previsibilidade de duração de mídias referidas no item/elemento 7.1.3 devem ser obtidas, preferencialmente, a partir de órgãos independentes. Quando isso não for possível, podem ser utilizadas informações de fornecedores. Em ambos os casos deve ficar registrada a origem da informação.	NC
7.1.9 Quando se proceder à eliminação de documentos, as memórias de suporte têm que ser, devidamente, “sanitizadas”, isto é, ter suas informações, efetivamente, indisponibilizadas. Este requisito aplica-se, principalmente, às memórias secundária e terciária, por sua característica não volátil. As informações devem ser eliminadas de forma irreversível, incluindo, no caso de memória terciária, a possibilidade de destruição física das mídias.	NC
7.2 Capacidade	

7.2.1 Um SIGAD tem que possuir capacidade de armazenamento suficiente para acomodação de todos os documentos e suas cópias de segurança. Para grandes volumes de dados, é conveniente o uso de dispositivos com maior capacidade unitária de armazenamento, a fim de reduzir a sobrecarga operacional.	NC
7.2.2 Em um SIGAD, tem que ser prevista a possibilidade de expansão da estrutura de armazenamento. A quantidade de memória primária deve ser superestimada no momento da aquisição, a fim de minimizar as indisponibilidades do SIGAD nas situações de expansão desse tipo de memória. Quando da aquisição de disk arrays, as possibilidades de expansão dos equipamentos de controle devem ser consideradas. Para backups em fita magnética, em sistemas com grande volume de informação, devem ser utilizados sistemas automáticos de seleção, troca e controle de fitas (robots).	NC
7.3 Efetividade de armazenamento	
7.3.2 Um SIGAD tem que utilizar técnicas de restauração de dados em caso de falhas.	NC
7.3.3 Um SIGAD tem que utilizar mecanismos de proteção contra escrita, que previnam alterações indevidas e mantenham a integridade dos dados armazenados.	NC
7.3.5 A integridade dos dispositivos de armazenamento tem que ser, periodicamente, verificada.	NC
8. Preservação	
8.1 Aspectos físicos	
8.1.1 Os suportes de armazenamento de um SIGAD têm que ser acondicionados, manipulados e utilizados em condições ambientais compatíveis com sua vida útil prevista e/ou pretendida, de acordo com as especificações técnicas do fabricante e de entidades isentas, e com base em estatísticas de uso. A vida útil pretendida de um suporte pode ser menor que sua vida útil prevista, o que permite condições ambientais mais flexíveis.	NC
8.1.3 Um SIGAD tem que permitir o controle da vida útil dos suportes para auxiliar no processo de atualização.	NC
8.2 Aspectos lógicos	
8.2.1 Um SIGAD tem que manter cópias de segurança. As cópias de segurança devem ser guardadas em ambientes seguros, em locais diferentes de onde se encontra a informação original.	NC
8.2.2 Um SIGAD tem que possuir funcionalidades para verificação periódica dos dados armazenados, visando à detecção de possíveis erros. Nesse caso, recomenda-se o uso de um checksum robusto, ou seja, que permita a constatação da integridade dos dados e seja seguro quanto a fraudes.	NC
8.2.3 Um SIGAD tem que permitir a substituição dos dados armazenados que apresentarem erros.	NC
8.2.7 Ações de preservação têm que ser efetivadas sempre que se torne patente ou previsível a obsolescência da tecnologia utilizada pelo SIGAD.	NC
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.	NC
8.3 Aspectos gerais	
8.3.1 Um SIGAD tem que registrar, em trilhas de auditoria, as operações de preservação realizadas.	NC
8.3.3 As modificações em um SIGAD e em sua base tecnológica têm que ser verificadas num ambiente exclusivo para essa finalidade, de modo a garantir que, após a implantação das alterações, os dados continuem sendo acessados sem alteração de conteúdo.	NC

8.3.6 Um SIGAD tem que gerir metadados relativos à preservação dos documentos e seus respectivos componentes.	NC
9. Funções administrativas	
9.1.1 Um SIGAD tem que permitir que os administradores, de maneira controlada e sem esforço excessivo, recuperem, visualizem e reconfigurem os parâmetros do sistema e os atributos dos usuários.	EC
9.1.2 Um SIGAD tem que fornecer relatórios flexíveis para que o administrador possa gerenciar os documentos e seu uso. Esses relatórios devem apresentar, no mínimo: <ul style="list-style-type: none"> • quantidade de dossiês/processos, volumes e itens a partir de parâmetros ou atributos definidos (tempo, classe, unidade administrativa etc.); • estatísticas de transações relativas a dossiês/processos, volumes e itens; • atividades por usuário. 	EC
9.1.3 Um SIGAD tem que dispor de documentação referente a aspectos de administração do sistema. A documentação deve incluir todas as informações necessárias para o correto gerenciamento do sistema.	EC
10. Conformidade com a legislação e regulamentações	
10.1.1 Um SIGAD tem que estar de acordo com a legislação e as normas pertinentes, tendo em vista a admissibilidade legal e o valor probatório dos documentos arquivísticos.	NC
10.1.2 Um SIGAD tem que estar de acordo com a legislação e as normas específicas para gestão e acesso de documentos arquivísticos.	NC
10.1.3 Um SIGAD tem que estar em conformidade com requisitos regulamentares específicos e códigos de boa prática necessários para a execução de determinadas atividades. Este requisito pode ser personalizado para cada contexto, como, por exemplo, saúde, justiça, educação, previdência.	NC
11. Usabilidade	
11.1.24 Um SIGAD tem que restringir o acesso às funcionalidades administrativas e impossibilitar sua visualização pelo usuário final. Exemplos: As operações não disponíveis aparecem com fonte atenuada nos menus e possuem efeito nulo quando acionadas. O acesso às operações indisponíveis é restringido pela configuração dos menus, que não apresentam essas operações ao usuário sem permissão para executá-las.	NC
12. Interoperabilidade	
12.1.3 Um SIGAD tem que aplicar os requisitos de segurança descritos neste documento para executar operações de interoperabilidade. Isso é fundamental para que as operações, feitas em ambiente com interoperabilidade, não afetem a integridade dos documentos e impossibilitem acessos não autorizados.	NC
13. Disponibilidade	
13.1.1 Um SIGAD tem que se adequar ao grau de disponibilidade estabelecido pela organização.	NC

14. Desempenho e escalabilidade	
<p>14.1.3 Um SIGAD tem que incluir rotina de manutenção de:</p> <ul style="list-style-type: none"> • dados de usuários e de grupos; • perfis de acesso; • plano de classificação; • bases de dados; • tabelas de temporalidade. Essas tarefas devem atender às mudanças planejadas da organização, sem causar grande sobrecarga de administração. 	NC

Fonte: e-Arq Brasil

Legenda	
EC	Em conformidade
PC	Parcialmente em conformidade
NC	Não conformidade