UNIVERSIDADE FEDERAL DE SANTA MARIA
UNIVERSIDADE ABERTA DO BRASIL
CENTRO DE CIENCIAS SOCIAIS E HUMANAS
CURSO DE PÓS-GRADUAÇÃO A DISTÂNCIA
ESPECIALIZAÇÃO *LATO-SENSU* GESTÃO EM ARQUIVOS

A CONTEXTUALIZAÇÃO DA GESTÃO ARQUIV. DE DOCUMENTOS COM ÊNFASE NA AUTENTICIDADE E CONFIABILIDADE DOS DOCUMENTOS DIGITAIS

MONOGRAFIA DE ESPECIALIZAÇÃO

Adriana Herkert Netto

Restinga Sêca, RS, Brasil
2012

A CONTEXTUALIZAÇÃO DA GESTÃO ARQUIVÍSTICA DE DOCUMENTOS COM ÊNFASE NA AUTENTICIDADE E CONFIABILIDADE DOS DOCUMENTOS DIGITAIS

por

Adriana Herkert Netto

Monografia apresentada ao Curso de Pós-Graduação a Distância Especialização *Lato-Sensu* Gestão em Arquivos, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do título de
Especialista em Gestão em Arquivos

Orientador: André Zanki Cordenonzi

Restinga Sêca, RS, Brasil

2012

Universidade Federal de Santa Maria
Centro de Educação
Curso de Pós-Graduação a Distância
Especialização *Lato-Sensu* Gestão em Arquivos

A Comissão Examinadora, abaixo assinada,
aprova a Monografia de Especialização

A CONTEXTUALIZAÇÃO DA GESTÃO ARQUIVÍSTICA DE DOCUMENTOS COM ÊNFASE NA AUTENTICIDADE E CONFIABILIDADE DOS DOCUMENTOS DIGITAIS

elaborada por
Adriana Herkert Netto

como requisito parcial para obtenção do título de
Especialista em Gestão em Arquivos

COMISSÃO EXAMINADORA:

André Zanki Cordenonzi, Dr. (UFSM)
(Presidente/Orientador)

Luiz Patric Kayser, Ms. (UFSM)

Carlos Blaya Perez, Dr. (UFSM)

Restinga Sêca, 22 de dezembro de 2012.

Não há fatos eternos, como não há verdades absolutas.

(Friedrich Wilhelm Nietzsche)

O que sabemos é uma gota, o que ignoramos é um oceano.

(Isaac Newton)

RESUMO

Monografia de Especialização
Curso de Pós-Graduação a Distância
Especialização *Lato-Sensu* Gestão em Arquivos

Universidade Federal de Santa Maria

A CONTEXTUALIZAÇÃO DA GESTÃO ARQUIVÍSTICA DE DOCUMENTOS COM ÊNFASE NA AUTENTICIDADE E CONFIABILIDADE DOS DOCUMENTOS DIGITAIS

AUTORA: ADRIANA HERKERT NETTO
ORIENTADOR: ANDRÉ ZANKI CORDENONZI
Restinga Sêca/RS, 22 de dezembro de 2012.

Atualmente, muitas organizações estão implementando sistemas informatizados, visando tornar seus processos administrativos mais ágeis, sendo na maioria dos casos, levado em conta somente os aspectos tecnológicos. O que pode ocasionar inúmeros prejuízos, dentre eles: informações não confiáveis, não autênticas, descarte ou invalidação de registros documentais únicos, lacunas na história organizacional e prejuízos financeiros. Diante disso, esta pesquisa buscou reunir conhecimentos e apresenta-los de forma a contextualizar como a gestão arquivística em sistemas informatizados pode colaborar para manter a autenticidade e a confiabilidade dos documentos digitais, para que a administração tenha a sua disposição sempre que necessário acesso a informações íntegras. Para tanto, foram analisados os pontos de vista de diferentes autores, as Normas Brasileiras (NBR) ISO/ IEC 17799: 2005 e ISO/ IEC 27001: 2006, e as recomendações do CONARQ relacionadas a esse tema. Assim, o estudo foi conduzido sob a forma de Pesquisa Bibliográfica. Com base nos diferentes pontos de vista reunidos e analisados, concluiu-se que a atuação do arquivista em conjunto com os profissionais de tecnologia possibilita o desenvolvimento/adequação do sistema de informação, tendo como base as necessidades da empresa, e em observância aos fatores legais envolvidos. Por fim, que nenhum sistema informatizado será completamente livre de fragilidades. Entretanto, com o estabelecimento de políticas de segurança da informação alinhadas à realidade organizacional, e em sinergia com um SIGAD, adequadamente estruturado, pode-se diminuir substancialmente as possibilidades da organização ter comprometida a autenticidade e/ou confiabilidade de seus documentos arquivísticos.

Palavras-chave: documento arquivístico digital; autenticidade; confiabilidade.

ABSTRACT

Monografia de Especialização
Curso de Pós-Graduação a Distância
Especialização *Lato-Sensu* Gestão em Arquivos

Universidade Federal de Santa Maria

A CONTEXTUALIZAÇÃO DA GESTÃO ARQUIVÍSTICA DE DOCUMENTOS COM ÊNFASE NA AUTENTICIDADE E CONFIABILIDADE DOS DOCUMENTOS DIGITAIS

AUTOR: ADRIANA HERKERT NETTO
ADVISER: ANDRÉ ZANKI CORDENONZI
Restinga Sêca/RS, 22 de dezembro de 2012.

Currently, many organizations are implementing computerized systems in order to make its administrative processes more agile, being in most cases, taken into account only the technological aspects. What can cause many losses, including: unreliable information, inauthentic, disposal or invalidation only documentary records, gaps in organizational history and financial losses. Thus, this research sought to gather knowledge and presents them as a way to contextualize the archival management in computer systems can collaborate to maintain the authenticity and reliability of digital documents, that the administration has at his disposal whenever necessary access information integrity. Therefore, we analyzed the views of different authors, the Brazilian Standards (NBR) ISO/ IEC 17799: 2005 and ISO/ IEC 27001: 2006, and the recommendations of CONARQ related to this issue. Thus, the study was conducted in the form of Bibliographic Search. Based on the different viewpoints gathered and analyzed, it was concluded that the actions of the Archivist in conjunction with the professional technology enables the development/adaptation of information system, based on business needs, and in compliance with the legal factors involved. Finally, that no computer system is completely free from frailties. However, with the establishment of information security policies aligned with organizational reality, and in synergy with a SIGAD, properly structured, can substantially reduce the chances of the organization has compromised the authenticity and/or trustworthiness of their records.

Key-words: digital archivistic document; authenticity; reliability.

LISTA DE FIGURAS

LISTA DE SIGLAS

ABNT - Associação Brasileira de Normas Técnicas

AC - Autoridade Certificadora

AR - Autoridade de Registro

CG - Comitê Gestor

CONARQ - Conselho Nacional de Arquivos

CTDE - Câmara Técnica de Documentos Eletrônicos

DBTA - Dicionário Brasileiro de Terminologia Arquivística

e-Arq Brasil - Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos

GADE - Gerenciamento Arquivístico de Documentos Eletrônicos

GED - Gerenciamento Eletrônico de Documentos

ICP-Brasil - Infra-Estrutura de Chaves Públicas Brasileira

IEC - International Electrotechnical Commission

INTERPARES - The International Research on Permanent Authentic Records in Electronic Systems

ISO - International Organization for Standardization

NBR - Norma Brasileira

PDCA - Plan-Do-Check-Act (Planejar-Executar-Verificar-Agir)

SGSI - Sistema de Gestão de Segurança da Informação

SIGAD - Sistemas Informatizados de Gestão Arquivística de Documentos

TI - Tecnologia de Informação

UFSM - Universidade Federal de Santa Maria

UNIFRA - Centro Universitário Franciscano

SUMÁRIO

1 INTRODUÇÃO

As informações contidas nos documentos, independente do suporte, comunicam atividades do fazer humano com organicidade, demonstrando a evolução ocorrida na vida de pessoas físicas e na existência das pessoas jurídicas. Sendo assim, a evolução da sociedade está registrada em conjuntos documentais (fundos) por todo o mundo, o que possibilita o estudo de vários aspectos religiosos, sociais, econômicos, jurídicos, administrativos, históricos, etc.

No âmbito administrativo, o conhecimento da arquivologia pode propiciar inúmeros benefícios no que tange ao sistema de informação. O arquivista ao iniciar seu trabalho em uma organização realiza um levantamento de dados para conhecer sua estrutura, seu funcionamento, os tipos documentais produzidos, seus usos e os prazos que necessitam estar disponíveis. Com base nesse exame da situação atual, diagnóstico, propõem as alterações consideradas necessárias, a fim de assegurar um melhor desempenho na gestão das informações, e por consequência, contribuindo para a eficiência e eficácia administrativa.

Atualmente, muitas organizações estão implementando sistemas informatizados, visando tornar seus processos administrativos mais ágeis, produzindo seus documentos somente em formato digital. Esses sistemas informatizados estão sendo, em muitos casos, projetados por profissionais unicamente provenientes da área da tecnologia da informação, sem a visão arquivística de fluxo de documentos e ciclo vital. O que pode ocasionar inúmeros prejuízos, dentre eles: informações não confiáveis, não autênticas, descarte ou invalidação (caso de prova documental) de registros documentais únicos, lacunas na história organizacional e prejuízos financeiros.

Para serem incorporados ao sistema de informação eletrônico os documentos produzidos/recebidos anteriormente, em suporte papel, estão sendo digitalizados, ocorrendo o descarte dos originais sem o adequado esclarecimento sobre as implicações legais desse processo, incorrendo em um erro. A atuação do arquivista

em conjunto com os profissionais de tecnologia possibilita o desenvolvimento/adequação do sistema de informação, tendo como base as necessidades da empresa, e em observância aos fatores legais envolvidos.

A gestão arquivística de documentos nas organizações proporciona o aumento de sua capacidade competitiva, pois agiliza o acesso às informações necessárias ao seu processo decisório.

1.1 Objetivos

1.1.1 Objetivo Geral

Essa pesquisa buscou reunir conhecimento e apresenta-los de forma a contextualizar como a gestão arquivística em sistemas informatizados pode colaborar para manter a autenticidade e a confiabilidade dos documentos digitais, para que a administração tenha a sua disposição sempre que necessário acesso a informações íntegras.

1.1.2 Objetivos Específicos

Como objetivos específicos tiveram-se:

- examinar as recomendações do Conselho Nacional de Arquivos (CONARQ) sobre o gerenciamento arquivístico de documentos digitais;
- analisar publicações das áreas de administração e tecnologia da informação que tratem da gestão de riscos de tecnologia da informação;
- analisar a abordagem que as Normas Brasileiras (NBR) ISO/ IEC 17799: 2005 e a ISO/ IEC 27001: 2006 fazem com relação a gestão de documentos digitais e com a segurança da informação.

1.2 Justificativa

Em um cenário onde a competitividade entre as organizações, em qualquer área de negócio, exige rapidez na troca de informações o gerenciamento dos documentos e das informações nele contidas tornaram-se necessários para o bom desempenho das atividades organizacionais, pois podem contribuir efetivamente para o sucesso e para a sobrevivência destas organizações. Nesse contexto, muitas organizações estão informatizando seus sistemas de informação e, na maioria dos casos, isto está ocorrendo levando em conta somente os aspectos tecnológicos.

A gestão arquivística em um sistema informatizado pode, por meio dos princípios e técnicas arquivísticas, contribuir para a manutenção da autenticidade e da confiabilidade dos documentos digitais. Pois, como se sabe, eles são mais vulneráveis que os documentos tradicionais a alterações por se encontrarem em código binário e necessitarem do uso de máquinas para produção e leitura. As especificidades dos documentos digitais têm de ser levadas em conta na gestão, caso contrário às informações necessárias para alicerçar o processo decisório podem não estarem integras quando necessárias à administração.

Para a sistematização deste estudo, este relatório está organizado da seguinte forma: o capítulo 2 apresenta a metodologia utilizada para seu desenvolvimento, enquanto o capítulo 3 aborda a arquivística e o documento digital. O capítulo 4 discorre sobre o gerenciamento arquivístico de documentos digitais. No capítulo 5 faz-se uma breve contextualização sobre segurança da informação e gestão de risco. Já no capítulo 6 são apresentados os principais aspectos das normas NBR ISO/ IEC 17799: 2005 e NBR ISO/ IEC 27001: 2006. O capítulo 7 trata do e-Arq Brasil. O capitulo 8 reuni e apresenta as principais ponderações sobre a manutenção da autenticidade e confiabilidade de documentos arquivísticos digitais. Por fim, o capítulo 9 apresenta as conclusões a respeito da temática dessa pesquisa.

2 METODOLOGIA

"Pesquisa é a atividade científica pela qual descobrimos a realidade" (Demo, 1987, p. 23). Este trabalho foi conduzido sob forma de pesquisa exploratória, pois seu objetivo principal buscou “o aprimoramento de ideias ou a descoberta de intuições” (Gil, 1991, p. 45), e, como este tipo de pesquisa é bastante flexível, o estudo foi conduzido sob a forma de Pesquisa Bibliográfica.

Os autores, Gil (2006), Marconi e Lakatos (2006) definem a pesquisa bibliográfica como sendo a que se realiza sob materiais já elaborados, constituído principalmente de livros e artigos científicos. Esse tipo de pesquisa “é um apanhado geral sobre os principais trabalhos já realizados, revestidos de importância, por serem capazes de fornecer dados atuais e relevantes relacionados com o tema”. (Marconi e Lakatos, 2006, p.158)

Ferrari Trujillo (1982, p. 209) afirma que “a pesquisa bibliográfica tem por finalidade conhecer as contribuições científicas que se efetuaram sobre determinado assunto”.

O tipo de revisão de literatura, de acordo com o apresentado por Silva (2001), utilizado para alcançar os objetivos delineados nessa pesquisa foi a determinação “do estado da arte”. Pois, a revisão buscou relacionar questões acerca do tema, analisando o ponto de vista de diferentes autores, e as questões metodológicas envolvidas.

Essa pesquisa do ponto de vista da sua natureza, considerando o exposto por Silva (2001), classifica-se como pesquisa básica, pois seu objetivo consistiu em gerar conhecimentos novos úteis para o avanço da ciência sem aplicação prática prevista. Quanto à abordagem do problema classificou-se como pesquisa qualitativa, uma vez que:

> [...] considera que há uma relação dinâmica entre o mundo real e o sujeito, isto é, um vínculo indissociável entre o mundo objetivo e a subjetividade do

> sujeito que não pode ser traduzido em números. [...] Não requer o uso de métodos e técnicas estatísticas. O ambiente natural é a fonte direta para coleta de dados e o pesquisador é o instrumento-chave. É descritiva. Os pesquisadores tendem a analisar seus dados indutivamente. O processo e seu significado são os focos principais de abordagem. (Silva, 2001, p. 20)

A abordagem descrita justificou-se pela existência de publicações a respeito do assunto investigado. As fontes bibliográficas foram buscadas principalmente nas bibliotecas da Universidade Federal de Santa Maria (UFSM) e do Centro Universitário Franciscano (UNIFRA), ainda, em sites da internet. As fontes foram selecionadas de acordo com os seguintes critérios:

- deveriam tratar do assunto autenticidade e/ou confiabilidade dos documentos em sistemas informatizados;
- deveriam tratar do tema segurança da informação tendo relação com Arquivologia, Tecnologia da Informação, e/ou Administração.

Ao mesmo tempo, foi realizado um levantamento das recomendações do Conselho Nacional de Arquivos (CONARQ) sobre o tema em estudo.

Por fim, foram analisados os pontos de vista de diferentes autores, as Normas Brasileiras (NBR) ISO/ IEC 17799: 2005 e ISO/ IEC 27001: 2006, e as recomendações do CONARQ relacionadas ao tema dessa pesquisa, a fim de reunir conhecimento e esclarecer como a gestão arquivística em sistemas de informatizados pode contribuir para manter a autenticidade e confiabilidade dos documentos digitais, e, por consequência, das informações por ele comunicadas.

3 ARQUIVÍSTICA E DOCUMENTO DIGITAL

Conforme Bellotto e Camargo (1996, p. 5), Arquivologia é também conhecida como Arquivística, “disciplina que tem por objeto o conhecimento da natureza dos arquivos e das teorias, métodos e técnicas a serem observados na sua constituição, organização, desenvolvimento e utilização”.

Na arquivística encontram-se correntes de pensamento distintas, que podem ser assim resumidas: Arquivística Tradicional (ocupa-se com os arquivos permanentes/valor secundário); *Records Management* (trata dos arquivos correntes/valor primário); Arquivística Integrada (preocupa-se com o tratamento simultâneo das três idades dos arquivos).

Os profissionais brasileiros atualmente utilizam-se da visão sistêmica, denominada Arquivística Integrada. Esta procura intervir desde a produção do documento até a sua destinação final (eliminação ou preservação permanente).

Os arquivos são os conjuntos documentais, ou seja, os documentos produzidos e acumulados por pessoas físicas ou jurídicas no desempenho de suas atividades ao longo de suas existências. Documento, por sua vez, é uma unidade constituída pela informação e seu suporte, já documento arquivístico é o “documento produzido (elaborado ou recebido) no curso de uma atividade prática, como instrumento ou resultado dessa atividade e retido para ação ou referência.” (e-Arq, 2011, p. 128)

A lei 8.159, de 08 de janeiro de 1991, no artigo 2º considera arquivo ”os conjuntos de documentos produzidos e recebidos por órgãos Públicos, instituições de caráter Público e entidades Privadas, bem como Pessoa Física, qualquer que seja o suporte da informação”. (CONARQ)

Gonçalves (1998) afirma que os arquivos são formados por diversos registros (nascimento/criação, crescimentos/desenvolvimento e morte/desativação), nos mais variados suportes.

A autora Duranti (1994, p. 50) ressalta o papel dos arquivos no seguinte fragmento: “através dos milênios os arquivos têm representado, alternada e cumulativamente, os arsenais da administração, do direito, da história, da cultura e da informação”.

É atribuído ao documento arquivístico um maior grau de confiabilidade quanto à veracidade das informações nele contidas, devido ao seu caráter único, das rotinas de trabalho pelas quais passa e da relação dele com um ou mais documentos dentro do fundo documental denominada organicidade[1]. Para Duranti (1996) as características dos documentos arquivísticos são:

- imparcialidade: os documentos arquivísticos são gerados sem a prévia intenção de comunicar os fatos e atos a posteriori, ou seja, teoricamente sem a preocupação de comprometimento das partes, tanto emissor como receptor;
- autenticidade: é a qualidade que o documento tem de prestar testemunho escrito das atividades exercidas no passado por seu autor, uma vez que é produzido em decorrência da necessidade de se agir por intermédio dele, e mantido como garantia para futuras ações ou para informações;
- naturalidade: corresponde ao acúmulo progressivo dos documentos no curso das atividades do organismo produtor. O que os dota de coesão;
- inter-relacionamento: um documento relaciona-se com outros dentro de um conjunto documental em função da produção de diferentes documentos para o cumprimento de uma mesma atividade; e
- unicidade: diz respeito ao caráter único que um documento assume na estrutura documental, logo, sendo insubstituível.

Na concepção de Rondinelli (2002 a), o documento arquivístico possui os seguintes elementos:

[1] “Relação natural entre documentos de um arquivo em decorrência das atividades da entidade produtora”. (DBTA, 2005, p. 127)

- suporte: o meio físico onde a informação é fixada;
- forma documentária: refere-se aos elementos intrínsecos e extrínsecos do documento que comunicam seu conteúdo, contexto e autoridade;
- anotações: acréscimos feitos ao documento após sua criação; e
- contexto: refere-se a estrutura jurídico-administrativa (normas, regimentos, regulamentos, estrutura organizacional) e documentária (envolve regras de Workflow e anotações).

Os documentos arquivísticos convencionais e os eletrônicos são constituídos por elementos que podem ser identificados e avaliados por meio da Análise Diplomática. Para proceder à *análise diplomática*, é adequado utilizar o *método diplomático*. Este consiste em isolar os elementos formais do documento, a fim de analisá-los separadamente, independentemente do contexto social e temporal em que foram criados.

A arquivologia e a diplomática[2] tem uma estreita relação, pois a primeira estuda os conjuntos documentais e a segunda preocupa-se com a autenticidade do documento arquivístico em questões que envolvem reclamação de bens e direitos por intermédio de provas documentais.

Para Duranti e Macneil (1996), a diplomática pode analisar todos os documentos. De acordo com Rondinelli (2002 c), atualmente os documentos tradicionais e eletrônicos são constituídos pela mesma forma documentária (elementos externos e internos) estudada nos primórdios da diplomática, porém, um pouco mais elaborada.

Duranti (1994, p. 61) salientando a importância da análise diplomática para os arquivistas, afirma que:

> [...] Nos dias atuais os conceitos diplomáticos constituem a chave intelectual dos arquivistas para o mundo eletrônico. [...] A diplomática explicita os laços entre os componentes intelectuais de um documento, os elementos de uma

[2] Diplomática é a disciplina que tem por objeto a estrutura formal e a autenticidade dos documentos. (Bellotto e Camargo, 1996)

> ação específica, enfatiza as relações entre os tipos de documentos, os tipos de ações e de etapas de procedimentos, mostra todos os tipos de interação entre pessoas e documentos.

Para facilitar a compreensão das particularidades existentes na forma documentária do documento convencional e do documento eletrônico apresento a seguir o quadro comparativo elaborado por Rondinelli (2002 b, p. 158):

Peculiaridades quanto a	Documento Convencional	Documento Eletrônico
Registro e uso de símbolos	Suporte: papel Símbolos: alfabeto, desenhos. Leitura direta.	Suporte: magnético ou óptico. Símbolos: dígitos binários Leitura indireta (hardware/software).
Conexão entre conteúdo e suporte	Conteúdo e suporte não se separam; visualização simultânea de ambos.	Conteúdo e suporte perfeitamente separáveis; visualização não simultânea de ambos.
Forma física	Tipo e tamanho da letra; idioma; cor; símbolos (logomarca).	Tipo e tamanho da letra (fonte); idioma; cor; símbolos (logomarca, indicação de "atachados", assinatura digital).
Forma intelectual	Configuração da informação (textual, gráfica e imagnética). Articulação do conteúdo (saudação, data assinatura manual). Anotações (autenticação, observações, número de protocolo, código de classificação, temporalidade).	Idem. Articulação do conteúdo (saudação, data, nome do autor, nome do destinatário, nome do originador). Idem.
Metadados Obs.: integram a forma física e intelectual do documento	Atributos concomitantes ou posteriores à criação do documento: anotações instrumentos de pesquisa (inventários, catálogos, índices).	Atributos concomitantes ou posteriores à criação do documento: ▪ inerentes ao aplicativo - data e hora da elaboração do documento; ▪ especiais - código de classificação, temporalidade, status de transmissão (minuta[3], original ou cópia), o próprio sistema de gerenciamento arquivístico de documentos, anotações, instrumentos de pesquisa (inventários, catálogos, índices).
Identificação	Entidade física.	Entidade lógica.
Preservação	Acondicionamento correto + ambiente climatizado.	Fragilidade do suporte + obsolescência tecnológica.

Apesar das semelhanças entre os elementos formais dos suportes em questão, a autora Macneil (2000, p. 103) faz a seguinte observação:

> [...] Qualquer documento transmitido através de fronteiras eletrônicas é recebido do outro lado como original, mas é salvo no espaço do originador como uma minuta final porque não é capaz de alcançar seu propósito e assim falta-lhe efetividade.

[3] A minuta é uma subclassificação de rascunho.

Duranti (1996), abordando a mesma questão, afirma que é mais apropriado dizer que os documentos eletrônicos são gerados como rascunho e recebidos pelo destinatário como um original, porque um documento recebido contém elementos automaticamente atribuídos pelo sistema de transmissão, que não se encontram incluídos no documento que fora enviado. Assim, o documento recebido, ao contrário do enviado, é completo e efetivo.

Deste modo, é adequado mencionar a questão crucial que envolve três pontos críticos de discussão sobre os documentos eletrônicos, que de acordo com Dollar (1994) são quanto a:

- unicidade: garantir a manutenção da proveniência do documento;
- autenticidade: impedir distorções ou falsificações sem deixar vestígios; e
- preservação: enfrentar a obsolescência tecnológica.

Documento eletrônico arquivístico “é um documento arquivístico sujeito à manipulação, transmissão ou processamento por um computador digital” (Committee On Electronic Record, apud. Rondinelli, 2002 b, p. 50), e, de acordo com Santos (2002), os documentos eletrônicos podem estar armazenados em: mídia magnética (fita magnética de computador, discos rígidos de computador e disquetes), discos ópticos (CD-ROMs, WORM, DVDs, discos ópticos regraváveis) e em bases de dados.

O e-Arq Brasil (2011, p. 9) define documento digital como sendo “a informação registrada, codificada em dígitos binários e acessível por meio de sistema computacional”. De acordo com a autora Rondinelli (2002?), “os documentos digitais são suscetíveis a intervenções não autorizadas (perda, adulteração, destruição) degradação física e obsolescência tecnológica (hardware, software e formatos), o que compromete sua qualidade e integridade.”

Documento arquivístico digital “é um documento digital que é tratado e gerenciado como um documento arquivístico, ou seja, incorporado ao sistema de arquivos”. (e-Arq Brasil, 2011, p. 9)

Para um documento digital ser arquivístico ele deve cumprir os seguintes requisitos: ter conteúdo estável, forma fixa, contexto identificável, relação orgânica com os demais e, por fim, ser mantido como evidência das atividades.

O autor Innarelli (2007, p. 26) identifica que o documento digital tem como base três elementos: o hardware, o software e a informação armazenada em um suporte conforme a representação:

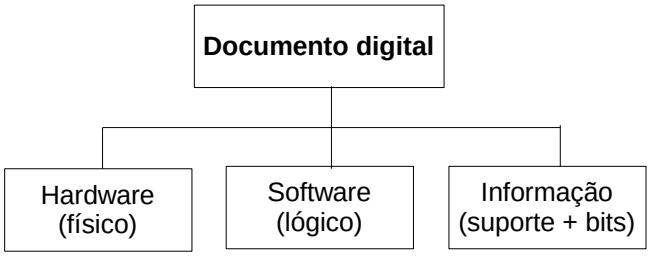

Figura 1 - Estrutura do documento digital

As grandes especificidades apresentadas pelos documentos digitais, conforme Rondinelli (2002 a) são a visualização não simultânea do suporte e da informação, leitura indireta (necessidade de hardware e software) e, a mais preocupante, a facilidade de alteração lícita e ilícita, sem deixar vestígios, uma vez que, para modificar o conteúdo informativo do documento utiliza-se o mesmo processo de edição utilizado na sua produção.

A facilidade de adulteração do conteúdo informativo dos documentos arquivísticos digitais trouxe a tona à preocupação com a manutenção de sua integridade e deste modo, sua autenticidade, confiabilidade e acessibilidade. Para facilitar a compreensão é adequado relacionar os respectivos conceitos:

Manter a *integridade* de um documento, conforme o autor Gonçalves L. (2002?), implica que toda vez que uma informação seja manipulada ela permaneça consistente, ou seja, que não sofra alteração ou adulteração por um acesso legal ou ilegal.

Autenticidade para Macneil (apud. Rondinelli, 2002 b, p. 69) é:

> [...] a capacidade de se provar que um documento arquivístico é o que diz ser. A autenticidade refere-se ao modo, a forma e ao status de transmissão do documento, às condições de sua preservação e custódia (método de verificação).

A *confiabilidade*[4] é conceituada no e-Arq Brasil (2011, p. 126) como:

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

Conforme o e-Arq (2011, p. 22) "um documento arquivístico *acessível* é aquele que pode ser localizado, recuperado, apresentado e interpretado".

O acesso a documentos depende da natureza das informações nele contidas, podendo ser ostensiva ou sigilosa. Em âmbito público os documentos produzidos na esfera governamental são classificados de acordo com graus de sigilo, regulamentados por meio do Decreto n° 4.553, de 27 de dezembro de 2002, constantes no seguinte artigo:

> Art. 5º Os dados ou informações sigilosos serão classificados em ultra-secretos, secretos, confidenciais e reservados, em razão do seu teor ou dos seus elementos intrínsecos.
> § 1º São passíveis de classificação como ultra-secretos, dentre outros, dados ou informações referentes à soberania e à integridade territorial nacionais, a planos e operações militares, às relações internacionais do País, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo conhecimento não-autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade e do Estado.
> § 2º São passíveis de classificação como secretos, dentre outros, dados ou informações referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, a assuntos diplomáticos e de inteligência e a planos ou detalhes, programas ou instalações estratégicos, cujo conhecimento não-autorizado possa acarretar dano grave à segurança da sociedade e do Estado.
> § 3º São passíveis de classificação como confidenciais dados ou informações que, no interesse do Poder Executivo e das partes, devam ser de conhecimento restrito e cuja revelação não-autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado.
> § 4º São passíveis de classificação como reservados dados ou informações cuja revelação não-autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos. (CONARQ)

[4] O termo confiabilidade neste trabalho é considerado como sinônimo do termo fidedignidade.

As categorias de sigilo foram estabelecidas para que informações confidenciais de setores estratégicos da Administração Pública não fossem divulgadas de forma inadequada, pois poderiam comprometer as ações ou decisões da mesma. Entretanto, com a utilização de meios eletrônicos para a transmissão das informações restritas, tornou-se necessário prevenir ações indevidas que visem manipular ou até mesmo destruir informações públicas.

O autor Innarelli (2007, p. 68) sugere o estabelecimento de alguns critérios e ferramentas, visando garantir a autenticidade dos documentos digitais, dentre eles ações relacionadas ao controle de acesso, conforme o esquema a seguir:

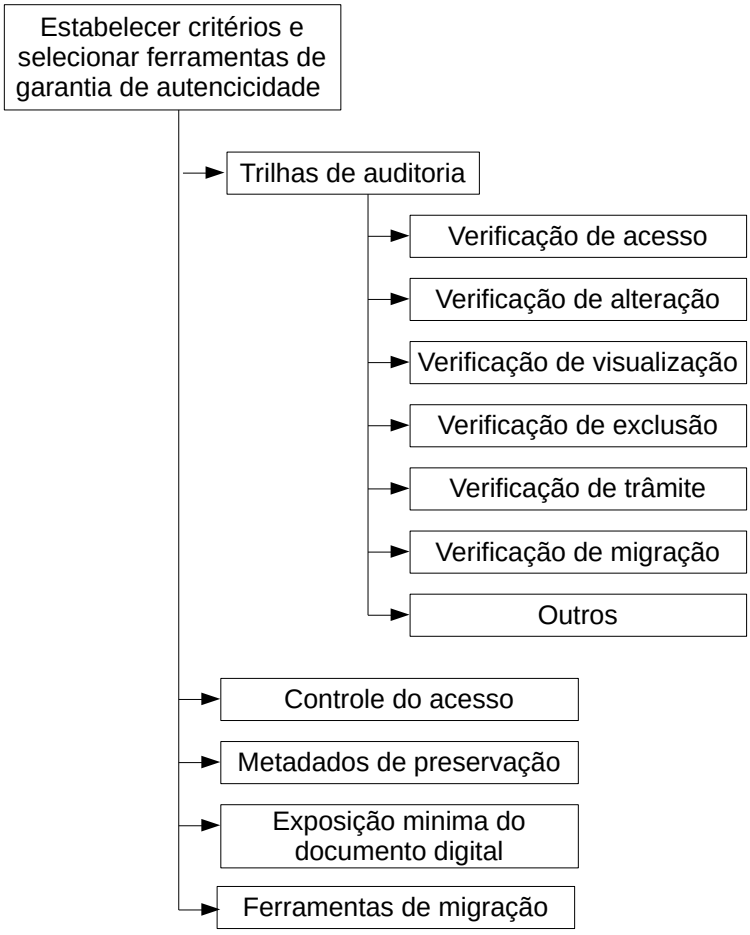

Figura 2 - Critérios e ferramentas para garantia da autenticidade

O acesso indevido a um documento digital pode ocasionar prejuízo financeiro e intelectual, pois, a divulgação do teor de um documento, por meio do qual se está realizando alguma negociação (compra, venda, lançamento de produto, programa,

projeto) pode prejudicar uma pessoa física ou jurídica. Além disso, há outro tipo de prejuízo, o histórico, pois é correto afirmar que, caso não consigamos preservar os documentos digitais de adulterações ilícitas, teremos no futuro a construção de uma história equivocada, pois as provas das atividades e das transações terão sido "falsificadas"; ainda, podem ocorrer lacunas históricas pela destruição dos registros. "A preservação de documentos com conteúdos informacionais significativos é a garantia *sine qua non* para a escrita da história" (Lopes, 1996, p. 22).

Santos (2002, p. 36) afirma que não é adequada a generalização quanto à vulnerabilidade[5] dos documentos em meio digital, pois não se deve partir do princípio de que "qualquer documento eletrônico é um convite explícito a sua adulteração e que isto não ocorre com os documentos em suportes tradicionais".

3.1 Certificação Eletrônica de Documentos

Por intermédio da Câmara Técnica de Documentos Eletrônicos (CTDE), grupo de trabalho de formação multidisciplinar que tem por objetivo definir e apresentar normas, diretrizes, procedimentos técnicos e instrumentos legais sobre gestão arquivística e preservação dos documentos digitais, a validade jurídica dos documentos digitais está sendo discutida pelo Conselho Nacional de Arquivos (CONARQ). No entanto, através da certificação eletrônica, é possível garantir a autenticidade e a integridade de um documento digital e, por consequência, atribuir valor jurídico ao mesmo.

A certificação eletrônica é um mecanismo de proteção a documentos digitais, regulamentado da seguinte forma:

> [...] Em 28 de Junho de 2001, foi editada a Medida Provisória nº 2.200, que institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, disciplinando a questão da presunção de integridade, autenticidade e validade dos documentos eletrônicos. Dentre as principais disposições,

[5] "Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças." (ABNT NBR ISO/IEC 17799: 2005)

> destacamos a figura da Autoridade Certificadora Raiz (AC Raiz), representada pelo Instituto Nacional de Tecnologia da Informação, o qual, de acordo com o Decreto 4036 de 28/11/2001, passa a ser órgão vinculado diretamente à Presidência da República. (BLUM, [2002])

A certificação eletrônica pode ser obtida por meio da solicitação a Autoridade de Registro - AR que encaminha o pedido para a Autoridade Certificadora – AC, responsável pela emissão de certificados digitais, que vinculará determinado código criptográfico ao respectivo titular. A figura a seguir esquematiza esse processo:

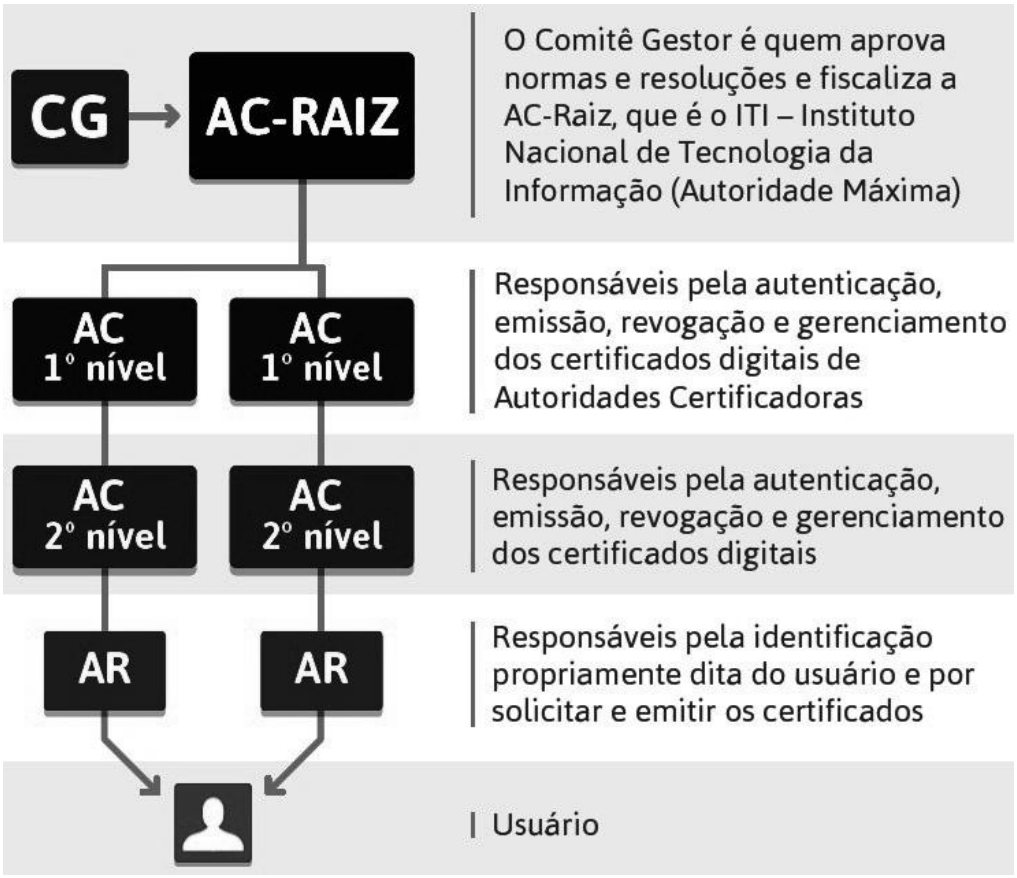

Figura 3 - Esquema certificação digital (Fonte: http://www.beneficioscd.com.br/pdf)

A certificação eletrônica é uma codificação garantida e atribuída por uma terceira pessoa (certificador), representada por um certificado que identifica a origem e protege o documento de qualquer alteração sem vestígios. Basicamente a certificação eletrônica funciona da seguinte forma, quem transmite o documento usa uma chave privada para codificar a mensagem, que só poderá ser decodificada por quem possuir a chave pública, uma vez que o par de chaves é matematicamente vinculado entre si. Ela baseia-se em criptografia de dados. Por meio da encriptação

de dados, a certificação torna textos inteligíveis a quem não conheça o padrão de conversão necessário para a leitura do documento.

Recomenda-se a utilização da certificação eletrônica a quem costuma realizar transmissão de documentos de conhecimento reservado e transações comerciais em redes eletrônicas.

A assinatura digital[6] atribuída pelo processo de certificação eletrônica ao documento digital assegura sua autenticidade e confiabilidade, pois é acrescentada ao mesmo pelo sistema de transmissão de dados. Ela possibilita ao destinatário identificar se o documento sofreu alguma adulteração até ser recebido.

Ainda assim, “o uso de assinaturas digitais, garantem que os documentos arquivísticos são autênticos apenas quando recebidos e não podem ser repudiados, porém, tais medidas não asseguram que eles permanecerão autênticos depois disso”. (INTERPARES) Isso ocorre porque “os avanços tecnológicos (incluindo avanços criptográficos, revogação e expiração/caducidade da assinatura digital) não garantem a sua preservação a longo prazo, o que levanta inúmeros problemas/desafios.” (Freitas, p. 2, 2012)

[6] Apenas as assinaturas e certificados digitais emitidos por entidades certificadoras (AC) reconhecidas oficialmente como tais, e aplicados de forma correta, possuem valor jurídico.

4 GERENCIAMENTO ARQUIVÍSTICO DE DOCUMENTOS DIGITAIS

Frente às possibilidades tecnológicas “há quem pense, sem conseguir provar cientificamente, que o uso das tecnologias da informação, em especial os computadores, a microfilmagem e a digitalização, dispensaria o esforço arquivístico” (Lopes, 1997, p. 289). Pelo contrário, “como se aplicaram métodos tecnológicos modernos à produção de documentos, seu crescimento nas últimas décadas tem sido em progressão antes geométrica do que aritmética” (Schellenberg, 2002, p. 179).

O tratamento arquivístico dos documentos denomina-se gestão de documentos. Ela consiste em um conjunto de procedimentos que abrange todo o ciclo de vida do documento, ou seja, as “sucessivas fases por que passam os documentos de um arquivo da sua produção à guarda permanente ou eliminação.” (DBTA, p. 47, 2005).

A teoria das três idades é a sistematização do ciclo vital dos documentos de arquivo. Ela é definida pelo Dicionário de Terminologia Arquivísitico (p. 159, 2005) como: “teoria segundo a qual os arquivos são considerados arquivos correntes, intermediários ou permanentes de acordo com a freqüência de uso por suas entidades produtoras e a identificação de seus valores primário e secundário.”

A lei 8.159, de 08 de janeiro de 1991, no capítulo I, artigo 3º, define a gestão de documentos como o “conjunto de procedimentos e operações técnicas referentes à sua produção, tramitação, uso, avaliação e arquivamento em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente”. (CONARQ)

As funções arquivística, segundo Rousseau e Couture (1998), dividem-se em sete, sendo elas: a criação/produção, a avaliação, a aquisição, a classificação, a descrição, a difusão/acesso e a conservação/preservação.

A produção pode significar tanto a elaboração do documento pelo próprio organismo, como a recepção e a guarda. Para compreender o contexto da produção de um documento de arquivo, é preciso o conhecimento da história, funções, atividades por ele desenvolvidas, da estrutura e do funcionamento.

A compreensão do contexto da produção de documentos é primordial para o arquivista, pois, ela permite ao profissional detectar com clareza as principais funções assumidas pelo organismo produtor. O conjunto de funções encontradas envolverá atividades-meio (referente à administração interna) e atividades-fim (referente ao trabalho técnico-profissional). Em consonância com Gonçalves (1998) isso significa reunir elementos para a classificação dos documentos que permitirá a elaboração do plano de classificação, e esse instrumento deverá esboçar com fidedignidade o fazer da organização proporcionando a maior proximidade com a realidade.

Para Rousseau e Couture (1998), Arquivística Integrada possibilita uma política integrada de organização de arquivos, permitindo acesso rápido às informações, através da integração dos procedimentos de classificação, avaliação e descrição, onde a classificação é a base para os demais procedimentos.

De acordo com Lopes (2000), os procedimentos de classificar, avaliar e descrever são funções arquivísticas inseparáveis e complementares, pois a classificação produz a possibilidade de uma avaliação que mantenha as informações necessárias e descarte o dispensável. Para Garcia e Junior (2002, p. 47) “ao se classificar já se está estabelecendo juízo de valor”, e para Lopes (1997), a elaboração de uma tabela de temporalidade é, ao mesmo tempo, um procedimento classificatório, avaliativo e descritivo, preso à questão do valor das informações. Portanto, a descrição inicia na classificação, segue na avaliação e se aprofunda no desenvolvimento dos instrumentos de busca.

Conforme Lopes (1997), a classificação é o fornecimento dos meios para a compreensão do valor das informações arquivísticas. Ela tem como objetivo auxiliar na recuperação das informações possibilitando a administração o controle (interno e externo) e o acesso às mesmas, processo que só é possível se os documentos

estiverem corretamente classificados e ordenados. A descrição arquivística identifica e explica o contexto e o conteúdo dos documentos de arquivo a partir de elementos formais, a fim de desenvolver instrumentos de busca, promovendo o acesso aos mesmos, uma vez que, “um arquivo sem os instrumentos de pesquisa adequados corre o risco de se tornar um verdadeiro mistério para os usuários” (Lopez, 2002, p. 13).

De modo que o arquivista deve realizar os processos de classificação, avaliação e descrição simultaneamente, a fim de manter uma visão sistêmica para o desenvolvimento e aplicação de políticas e atividades arquivísticas, visto que, a classificação proporciona uma primeira análise dos valores dos documentos e é também a primeira fase do processo de descrição.

A avaliação “consiste fundamentalmente em identificar valores e definir prazos de guarda para os documentos de arquivo” (Bernardes, 1998, p. 14). Os valores dos documentos são divididos em primário e secundário. Os fatores significativos para atribuir prazos de guarda para os documentos são a frequência de uso e os valores dos documentos.

O valor primário compreende o arquivo corrente, documentos frequentemente consultados de caráter administrativo, vigentes, e intermediário, documentos menos consultados, não mais vigentes, mas que cumprem o prazo precaucional. A vigência do documento é o período em que ele serve a administração que o produziu como prova documental, permitindo a ela assegurar seus direitos. O prazo precaucional de guarda de um documento deve ser atribuído após o término de sua vigência, é um prazo em que se preserva o documento por precaução. O valor secundário abrange o arquivo permanente constituído de documentos que perderam seu valor primário, porém, são providos de valor secundário, probatório e histórico-cultural.

Resultam do processo avaliativo os seguintes instrumentos de destinação: plano de destinação; relação de recolhimento e de transferência; calendário de recolhimento e de transferência; termo de eliminação e tabela de temporalidade de documentos.

A tabela de temporalidade de documentos consiste no “instrumento de destinação, aprovado pela autoridade competente, que determina prazos para transferência, recolhimento, eliminação e reprodução de documentos” (Bellotto e Camargo, 1996, p. 72). Ela define quando poderão ser eliminados, transferidos ou recolhidos, os documentos, ou seja, determina o ciclo vital do documento. A aplicação da tabela permite a eliminação dos documentos destituídos de valor secundário, liberando espaço de armazenamento, recursos financeiros e humanos, para serem empregados na melhoria das condições de armazenamento e conservação dos documentos que devem ser preservados e assim para que as informações necessárias à administração estejam acessíveis quando solicitadas.

Santos (2007, p. 176, 177) identifica que:

> A informação de interesse específico do administrador ou do acumulador/produtor do documento encontra-se, predominantemente, na primeira fase documental, ou seja, nos arquivos correntes – preservando-se uma parcela na fase intermediária, porém com utilização reduzida.
> [...] Com a valorização da informação como recurso para a tomada decisão e como ativo das instituições, o papel da unidade de arquivo pode passar de ser o de fontes de informações administrativas e técnicas e, em consequência, o arquivista que atua na gestão de arquivos deve tornar-se um provedor para a tomada de decisões.

Discorrendo sobre informação Lopes (1996, p. 15) afirma:

> [...] a informação nasce no cérebro, a partir da captação exterior dos sentidos e é expressa ou registrada pelas faculdades mentais e motoras dos homens, com ou sem a ajuda de ferramentas, objetos ou máquinas. Relaciona-se com a cultura, seja ela oral ou escrita. Pode ser pesquisada, hierarquizada e dissecada pelas mais diferentes profissões.

Rousseau e Couture (1998, p. 63) salientam que “a informação constitui uma mercadoria tão vital para a empresa como os recursos humanos, materiais ou financeiros, sem os quais ela não conseguiria viver”. As informações registradas nos documentos são essenciais para análise das ações empreendidas pela própria administração que as produziu, servindo como subsídio ao planejamento das ações futuras. Os documentos decorrentes das atividades administrativas são o testemunho de suas ações, e prova legal dos atos administrativos.

A gestão arquivística de documentos é fundamental para a eficiência e eficácia da gestão administrativa, uma vez que, apoia a gestão da informação, indispensável para a gestão da qualidade total que consiste em uma visão integrada dos processos, sistemas e recursos disponíveis na organização. O arquivo pode ser considerado um subsistema do sistema informação, e este do sistema organização.

Sistema de informação, e-Arq Brasil (2011, p. 10), é o:

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

Na conjuntura atual, as organizações estão investindo em recursos tecnológicos, visando melhorar a comunicação e o desempenho de seus processos. Dentre eles destaca-se o Gerenciamento de Documentos Eletrônicos (GED) ou (GDE), conforme Baldam et al. (2004), é a tecnologia que permite armazenar, localizar e recuperar informações existentes em documentos e dados eletrônicos.

Rondinelli (2002 a) ressalta que o GED diferencia-se do Gerenciamento Arquivístico de Documentos Eletrônicos (GADE), pois o primeiro trata do documento de forma compartimentada e o segundo o faz por meio de uma concepção orgânica, ou seja, os documentos possuem uma inter-relação (organicidade - princípio elementar arquivístico) refletindo as atividades da organização que os produziu. Isso se deve ao fato de que o GADE respeita os seguintes princípios arquivísticos: *respeito aos fundos* (princípio de proveniência sob o ponto de vista externo) e *respeito à ordem original* (princípio de proveniência sob o ponto de vista interno), uma vez que, “tanto o contexto quanto o conteúdo dos documentos dão testemunho da fidedignidade e da autenticidade” (Dollar, 1994, p. 75).

De acordo com Duchein (1977, apud Rousseau e Couture, 1998) respeito aos fundos consiste em agrupar os arquivos ou fundos de arquivo de determinada procedência sem os misturar com outros.

Campillo (1996 apud Guimarães e Yado [ ], p. 11), afirma que o respeito à ordem original consiste em manter os documentos dentro de cada arquivo ou fundo com a classificação e a ordem que o próprio produtor/acumulador os deu em sua origem, refletindo sua organização interna.

Rousseau e Couture (1998, p. 79) entendem que “o princípio da proveniência é a base teórica, a lei que rege todas as intervenções arquivísticas”. Ele tem como desdobramento o princípio de respeito à ordem original dos fundos. Sua aplicação pode dar-se em qualquer das idades dos arquivos. Ainda, a observância a esses princípios garantem a autenticidade e a fidedignidade dos documentos dentro do arquivo, pois, mantém sua relação orgânica, permitido que sirvam como prova jurídica e como testemunho dos atos e fatos que contem.

Para Schellemberg (2002) o Princípio da Proveniência protege a integridade dos documentos, pois, reflete no seu arranjo as origens e os processos pelos quais os documentos passaram, ajuda na compreensão de seu significado, dá ao arquivista um guia que auxilia no arranjo, descrição e utilização dos documentos.

A fim de ratificar o exposto, anteriormente, pela autora Rondinelli sobre a importância do controle arquivístico dos documentos digitais em um sistema de gerenciamento eletrônico apresento a definição de Sistema de Gestão Arquivística de Documentos:

> [...] um conjunto de procedimentos e operações técnicas cuja interação permite a eficiência e a eficácia na produção, tramitação, uso, avaliação e destinação (eliminação ou guarda permanente) de documentos arquivísticos correntes e intermediários de uma organização. Inclui código de classificação de assuntos, controle sobre a modificação dos documentos de arquivo, controle sobre os prazos de guarda e eliminação e fornece um repositório protegido para os documentos de arquivo que sejam significativos para a organização. (Rondinelli, 2002?)

De acordo com Rondinelli (2002 c), a Comunidade Arquivística Internacional reconhece o GADE como meio capaz de garantir a criação e manutenção de documentos eletrônicos confiáveis (fidedignos e autênticos). Convém salientar que a integridade dos documentos eletrônicos está intimamente relacionada com a

eficiência do GADE, e, de acordo com Rondinelli (2002 c), pode ser alcançada, com a definição de estratégias que visem à proteção desses documentos, tais como:

- prevenção: limitação do acesso ao sistema pela utilização de senhas ou identificação de usuários por meio de características físicas individuais (digitais, voz ou íris); e
- verificação: estabelecimento de um mecanismo que registra todas as intervenções feitas no documento, como: visualizar, modificar, transmitir, copiar ou apagar.

Ressalta-se que o gerenciamento dos documentos convencionais difere do gerenciamento dos documentos eletrônicos. Isso ocorre porque nos documentos eletrônicos os seus elementos constitutivos não se encontram reunidos de forma inseparável, implicando no armazenamento e gerenciamento desses elementos separadamente como metadados.

Metadados são “dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e/ou preservar documentos arquivísticos ao longo do tempo” (CTDE, 2010, p. 17), são atributos concomitantes ou posteriores a criação do documento[7]. Deste modo, os primeiros metadados passam a integrar o documento eletrônico no momento da transmissão, e esta diz respeito:

- ao modo: a maneira como o documento entrará e circulará no GADE;
- a forma: física e intelectual que o documento tem no momento em que é recebido pelo destinatário; e
- ao status: grau de completude e efetividade do documento, podendo enumerar-se três estados distintos: original - primeiro documento completo e efetivo; rascunho - versão temporária, passível de alteração; e cópia - reprodução do documento em qualquer dos estados identificados.

O metadado é considerado uma anotação e, portanto, integra a forma física e intelectual do documento, além de constituir-se em componente do documento

[7] Ver metadados no quadro comparativo página 16.

digital arquivístico e em instrumento para a análise diplomática. É através dessa análise que será possível estabelecer meios que visam garantir a confiabilidade e autenticidade de documentos arquivísticos em ambiente eletrônico.

Portanto, é por meio dos metadados incorporados ao documento eletrônico no momento da transmissão ou posteriormente atribuído em função do seu trâmite pelo sistema gerenciador que o GADE reconstituí o caminho percorrido pelo documento eletrônico. Ele faz esta verificação com a finalidade de identificar se o documento sofreu alguma adulteração.

Atualmente o GADE apresenta-se como meio capaz de controlar as intervenções realizadas nos documentos. Isso pode ser assegurado com a definição de políticas de segurança de informação (critérios para acesso e *firewall*). Com base no gerenciamento dos metadados ele pode revelar todo o trâmite do documento, as fases pelas quais ele passa até atingir o objetivo pelo qual foi gerado. Assim, permite verificar se o documento foi adulterado e quando isto ocorreu. No entanto, a autora Rondinelli afirma que:

> [...] o gerenciamento arquivístico de documentos eletrônicos se constitui hoje no maior desafio da comunidade arquivística em todo o mundo. As peculiaridades dos documentos em suporte magnético ou óptico têm suscitado uma série de questionamentos sobre as práticas arquivísticas adotadas até o advento desse tipo de documento, bem como sobre os fundamentos teóricos que as permeiam. (Rondinelli, 2002 c, p. 77)

A preservação de documentos digitais ainda é um obstáculo a ser transposto pelo GADE, visto que, os documentos arquivísticos digitais gerenciados devem ser cercados por cuidados especiais, pois diferem dos documentos tradicionais tanto na necessidade de migração de suporte quando da preservação e custódia. Isto se deve principalmente pelo fato de que os metadados podem ser alterados por qualquer um dos processos descritos a seguir, como alerta a autora Rondinelli (2002 c, p. 70):

> [...] É importante ressaltar que **cópia**[5] e **migração**[5] têm consequências diferentes para a autenticação dos documentos. A primeira consiste em uma reprodução completa dos elementos de forma e conteúdo de um documento [...] os documentos copiados se constituem em reproduções fiéis dos

[5] Grifo meu.

> documentos originais. Entretanto, há que se ressaltar que, apesar de menos invasiva, a cópia de documentos eletrônicos também se constitui em uma intervenção, logo interfere na autenticidade desses documentos. No tocante à migração, esta implica mudanças na configuração que afetam o documento por inteiro. Na verdade, ao serem migrados os documentos podem parecer os mesmos, mas não o são. Sua forma física é profundamente alterada, com perda de alguns dados e acréscimo de outros.

Nesse contexto, Levy (2002) alerta para o fato de ser difícil preservar as características necessárias à presunção da autenticidade dos documentos digitais nas cópias subsequentes.

5 SEGURANÇA DA INFORMAÇÃO E GESTÃO DE RISCOS

"Podemos definir Segurança da Informação como uma área do conhecimento dedicada à proteção de ativos[8] da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade". Sêmola (2003, p. 43)

Os princípios da segurança da informação são:

- confidencialidade: garantia de que a informação seja acessível somente a pessoas autorizadas a terem acesso;
- integridade: a informação é alterada somente por pessoas autorizadas;
- disponibilidade: garantia de que as pessoas autorizadas obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

De modo que, investir em segurança da informação, é investir para que as informações permaneçam confidenciais, integras e disponíveis para a pessoa certa na hora certa.

A segurança da informação evoluiu ao longo dos anos saindo do nível puramente técnico e restrito à área da TI, onde a preocupação consistia em ter antivírus, firewall e um conjunto de backup, para um nível de gestão, onde além dos aspectos tecnológicos, atenta a necessidade de investir e desenvolver os processos e as pessoas, sendo "composta de políticas, padrões, programas de conscientização, estratégias de segurança, etc." Gabbay (2003, p. 14)

Atualmente, a segurança da informação é compreendida como um conjunto de software, hardware, procedimentos e padrões implementados para proteger as informações das ameaças que possam explorar as vulnerabilidades do ambiente e impactar no seu negócio da organização.

Sêmola (2003, p. 47) conceitua ameaça como sendo:

[8] "Qualquer coisa que tenha valor para a organização." (ABNT NBR ISO/IEC 17799:2005)

> Agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio de exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, consequentemente, causando impactos aos negócios de uma organização.

As ameaças de segurança podem ser divididas em ameaças humanas e ameaças naturais, conforme ilustrado na figura a seguir.

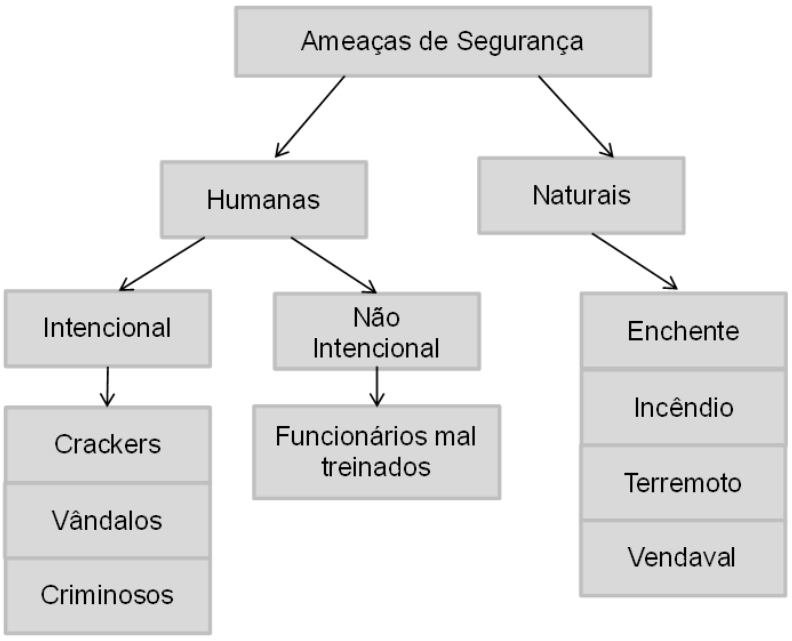

Figura 4 - Quadro de ameaças

As vulnerabilidades são pontos em que o sistema é susceptível a ataques. Assim, as ameaças exploram as vulnerabilidades resultando no risco, o que se pode fazer é reduzir as vulnerabilidades, ou seja, as fragilidades.

Risco é “probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, causando, possivelmente, impactos nos negócios”. Sêmola (2003, p. 50)

O risco de tecnologia da informação (TI) é a probabilidade de algum serviço de TI, seus componentes, processos e/ou pessoas, gerar algum impacto negativo na capacidade de negócio da organização.

Para proteger seus ativos a organização deve estabelecer de acordo com sua realidade, cultura e processos de negócio uma política de segurança da informação,

a fim de formalizar todos os aspectos considerados relevantes para a proteção (lógica e física), abrangendo o controle e monitoramento de seus recursos computacionais e, consequentemente, das informações manipuladas.

Para o efetivo sucesso uma política de segurança da informação deve integrar a gestão de risco com os componentes de gestão e tecnologia.

A gestão de riscos consiste em um conjunto de fatores que se articulam para o aperfeiçoamento da gestão e controle do negócio, tratando as fontes de incertezas que podem produzir eventos negativos, controlando-as de forma eficiente, para gerar oportunidades, essas como consequência da prática bem realizada.

A figura a seguir faz uma analogia com um iceberg (apenas cerca de 10% da sua massa emerge a superfície) para demonstrar como é a visão gerencial de uma organização que desconhece seu risco de negócio e de outra que os considera e os trata.

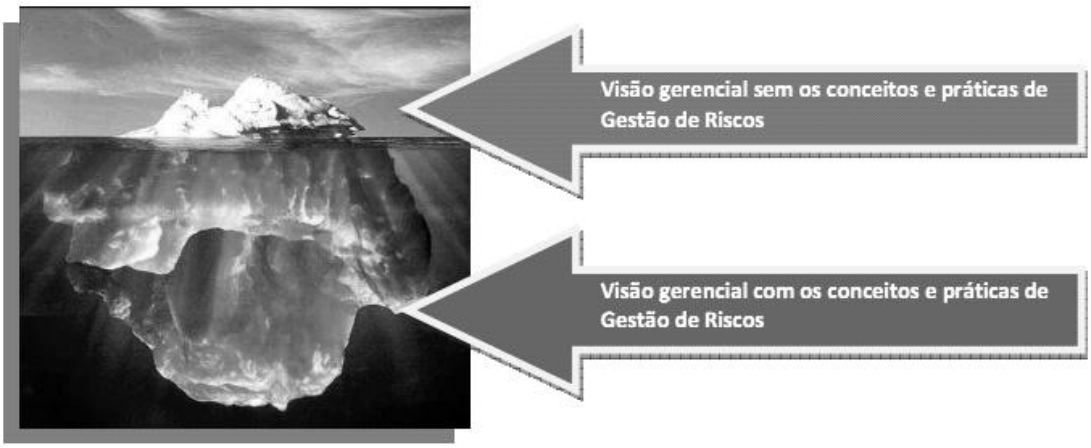

Figura 5 - Visão gerencial com e sem conceitos de gestão de risco
(Fonte: http://www.valcann.com/publicacoes/riscos_conceitosaplicacoes.pdf)

As atividades concernentes à prevenção de risco denominam-se mitigação de riscos. As atividades de reação quando o risco aconteceu são chamadas de contingência do risco.

Convém ressaltar que a norma NBR ISO/ IEC 17799 é o principal padrão relacionado à gestão de segurança da informação, portanto o entendimento das práticas nela contidas pelos gestores de TI e segurança da informação auxiliam a organização no desenvolvimento de uma política de segurança forte. É preciso esclarecer que a partir de 2007 a nova edição da NBR ISO/IEC 17799 foi incorporada ao novo esquema de numeração como NBR ISO/IEC 27002. Ainda, essa norma é indispensável para a aplicação da norma NBR ISO/IEC 27001. O próximo capítulo trata em mais detalhes sobre essas normas.

6 NORMAS BRASILEIRAS (NBR) ISO/ IEC 17799: 2005 E ISO/ IEC 27001: 2006

Este capítulo busca contextualizar as Normas Brasileiras, ISO/ IEC 17799: 2005 e ISO/ IEC 27001: 2006, que discorrem sobre a segurança da informação e relacioná-las ao objeto de estudo dessa pesquisa, a autenticidade e a confiabilidade dos documentos arquivísticos digitais.

6.1 NBR ISO/ IEC 17799: 2005

A NBR ISO/ IEC 17799 Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação estabelece requisitos e procedimentos para garantir a segurança das informações em sistemas informatizados que podem ser usados pelas organizações tanto para aplicação interna quanto para certificação, considerando que:

> A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectvidade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades
> A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.
> Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.
> A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software e hardware.* Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio. (ABNT NBR ISO/ IEC 17799: 2005, p. ix)

Essa norma define segurança da informação como:

> [...] preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas. (ABNT NBR ISO/ IEC 17799: 2005, p. 1)

A preocupação com a segurança da informação justifica-se porque, atualmente, os sistemas de informação e redes de computadores das organizações estão

> [...] expostos a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação. Danos causados por código malicioso, hackers e ataques de denial of service estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados. (ABNT NBR ISO/ IEC 17799: 2005, p. ix)

Nesses sistemas informatizados encontram-se os documentos digitais arquivísticos expostos a todas as ameaças anteriormente citadas. Caso a segurança do sistema informatizado não seja adequadamente estruturada e garantida não haverá como manter a integridade dos documentos aquivísticos digitais.

A informação contida no documento arquivístico digital é um importante ativo para a organização, ela subsidia o planejamento administrativo e assim a tomada de decisão. Para tanto, deve ser idônea. O que só é possível de ser alcançado com a definição e melhoria contínua das estratégias e processos para a segurança da informação, pois disso depende a sobrevivência e competitividade da organização.

A NBR ISO/ IEC 17799: 2005 tem por objetivo proporcionar a análise dos sistemas informatizados que não foram projetados levando em consideração as necessidades de segurança das informações, com vistas à revisão e adequação, e orientar o desenvolvimento e implementação de novos sistemas informatizados que incluam controles para a proteção da informação.

A parte principal da norma se encontra distribuída em 11 seções, que correspondem a controles de segurança da informação, conforme resumidamente apresentado a seguir.

1. Política de segurança da informação: relaciona os principais assuntos que devem ser abordados numa política de segurança. Deve ser criado um documento definindo a política de segurança da informação da organização. A política deve ser do conhecimento de todos, devendo ser analisada e revisada criticamente em intervalos regulares ou quando mudanças se fizerem necessárias.

2. Organizando a segurança da informação: aborda a estrutura de uma gerência para a segurança de informação, as responsabilidades incluindo terceiros e fornecedores de serviços. Tem como objetivo gerenciar a segurança da informação dentro da organização.

3. Gestão de ativos: tem como objetivo alcançar e manter a proteção adequada dos ativos da organização. Trabalha a classificação, o registro e o controle dos ativos da organização.

4. Segurança em recursos humanos: abordada a inclusão de responsabilidades relativas à segurança na descrição dos cargos, a forma de contratação e o treinamento em assuntos relacionados à segurança.

5. Segurança física e do ambiente: corresponde à manutenção das condições operacionais e da integridade dos recursos materiais componentes dos ambientes e plataformas computacionais. Visa prevenir o acesso físico não autorizado, danos e interferência em instalações e em informações da organização.

6. Gerenciamento das operações e comunicações: objetiva garantir a operação segura e correta dos recursos de processamento da informação.

7. Controle de acessos: o acesso à informação, recursos de processamento das informações e processos de negócio tem de ser controlados com base nos requisitos de negócio e segurança da informação. Portanto, deve ser assegurado o

acesso ao usuário autorizado e prevenido o acesso não autorizado a sistemas de informação.

8. Aquisição, desenvolvimento e manutenção de sistemas de informação: busca garantir que a segurança seja parte integrante do sistema de informação. Recomenda que os requisitos de segurança devam ser identificados e acordados antes do desenvolvimento e/ou implantação do sistema de informação.

9. Gestão de incidentes de segurança da Informação: seu objetivo é assegurar que todos os eventos e fragilidades da segurança da informação sejam comunicados, permitindo assim a tomada de uma ação corretiva em tempo hábil.

10. Gestão de continuidade do negócio: consiste em amenizar o impacto que a perda de algum ativo pode causar na organização. Deve impedir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar que a sua retomada ocorra em tempo hábil, se for o caso. Para isso, planos de continuidade do negócio, incluindo controles para identificar e reduzir riscos, devem ser desenvolvidos e implementados, para assegurar que as operações essenciais sejam rapidamente recuperadas.

11. Conformidade: visa garantir e evitar a violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação, respeitando os requisitos legais de cada localidade.

Analisados os controles acima nota-se que a norma prima pelas atividades de prevenção, uma vez que evita a adoção de medidas de caráter reativo, pois o plano de continuidade de negócios que se configura como uma medida reativa deve ser previamente planejado, para que, se necessário, seja devidamente implementado.

6.2 NBR ISO/ IEC 27001: 2006

A norma ISO/ IEC 27001: 2006 institui “um modelo para estabelecer,

implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI)" (ABNT NBR ISO/ IEC 27001: 2006, p. v). Essa norma, como a norma NBR ISO/ IEC 17799: 2005, apresentada anteriormente, também pode ser usada pelas organizações tanto para aplicação interna quanto para a certificação.

> O SGSI é projetado para assegurar a seleção de controles de segurança adequados e proporcionados para proteger os ativos de informação e propiciar confiança às partes interessadas. (ABNT NBR ISO/ IEC 27001: 2006, p. 1)

Nessa norma é salientado que a adoção de um SGSI trata-se de uma decisão estratégica para a organização e deve ter como base suas necessidades e objetivos, requisitos de segurança, processos e estrutura organizacional, ou seja, o SGSI deve ser dimensionado de acordo com o objeto. Portanto, uma situação simples requer uma solução de um SGSI simples.

A norma requer a abordagem por processo para estabelecer e implementar, operar, monitorar, analisar criticamente, manter e melhorar o SGSI de uma organização.

Marsh (p. 81, 2000) define processo como "*una de las herramientas esenciales más importantes para la mejora continua. Se utiliza para entender procesos existentes y para diseñar procesos nuevos o perfeccionados*".

A norma adota o modelo conhecido como "Plan-Do-Check-Act" (PDCA) para estruturar todos os processos do SGSI.

O Ciclo PDCA, ciclo de Shewhart ou ciclo de Deming, foi introduzido no Japão após a guerra, idealizado por Shewhart e divulgado por Deming, quem efetivamente o aplicou. "O PDCA é um método de gerenciamento de processos ou de sistemas. É o caminho para se atingirem as metas atribuídas aos produtos dos sistemas empresariais" (Campos, 1996, p. 262). Moura descreve o ciclo PDCA como "uma ferramenta que orienta a sequência de atividades para se gerenciar uma tarefa, processo, empresa, etc." (Moura, 1997, p. 90) O PDCA tem por princípio tornar mais

claros e ágeis os processos envolvidos na execução da gestão, como por exemplo, na gestão da segurança da informação, dividindo-a em quatro principais passos:

- *Plan* (planejar): estabelecer uma meta ou identificar o problema; analisar o processo e elaborar um plano de ação.
- *Do* (executar): realizar, executar as atividades conforme o plano de ação.
- *Check* (verificar): monitorar e avaliar periodicamente os resultados, avaliar processos e resultados, confrontando-os com o planejado.
- *Act* (agir): determinar e confeccionar novos planos de ação, de forma a melhorar a qualidade, eficiência e eficácia, aprimorando a execução e corrigindo eventuais falhas.

A imagem a seguir esquematiza o ciclo PDCA:

Figura 6 - Ciclo PDCA
Fonte: http://necs.preservaambiental.com/ciclo-pdca-abordagem-de-processo-e-escopo-do-sistema-de-gestao-ambiental/

O ciclo PDCA é utilizado para gerenciar processos. Ele permite verificar como eles estão ocorrendo, se podem ser simplificados e ou melhorados. A norma ISO/ IEC 27001: 2006 apresenta o modelo a seguir para ilustrar como isso deve ocorrer:

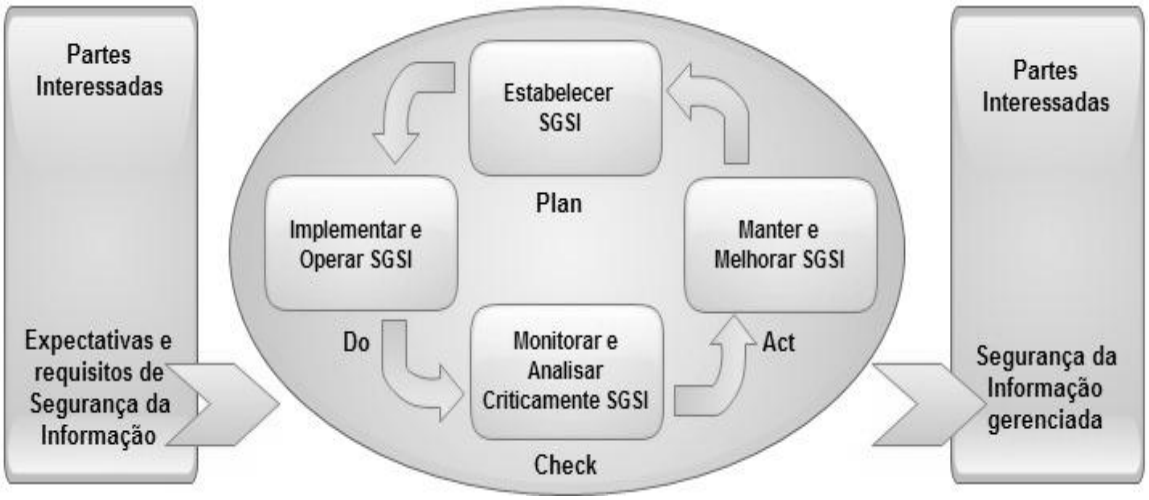

Figura 7 - Modelo PDCA aplicado aos processos do SGSI

***Plan* (planejar) (estabelecer o SGSI)**	Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.
***Do* (fazer) (implementar e operar o SGSI)**	Implementar e operar a política, controles, processos e procedimentos do SGSI.
***Check* (checar) (monitorar e analisar criticamente o SGSI)**	Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.
***Act* (agir) (manter e melhorar o SGSI)**	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

A norma possibilita, com a aplicação do PDCA, a análise/avaliação de riscos, especificação e implementação de segurança, gerenciamento de segurança e reavaliação. Foi desenvolvida em conformidade com a ABNT NBR ISO 9001: 2000 e ABNT NBR ISO 14001: 2004 para apoiar a implementação e a operação de forma consistente e integrada com normas de gestão relacionadas.

Na norma ISO/ IEC 27001: 2006 é ressaltado que os requisitos nela definidos são genéricos e, portanto, podem ser aplicados em todas as organizações, independentemente de tipo, tamanho e natureza. Ainda que, a exclusão de quaisquer dos requisitos especificados não é aceitável quando uma organização reivindica conformidade com a norma. A seguir resumem-se os requisitos estabelecidos na norma.

1. Sistema de gestão de segurança da informação (SGSI): “A organização deve estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto das atividades de negócio globais da organização e os riscos que ela enfrenta.” (ABNT NBR ISO/ IEC 27001: 2006, p. 4)

2. Responsabilidade da direção: a direção deve fornecer evidência do seu comprometimento com o estabelecimento, implementação, operação, monitoramento, análise crítica, manutenção e melhoria do SGSI.

3. Auditorias internas do SGSI: tem por objetivo verificar se os controles do seu SGSI estão sendo cumpridos.

4. Análise crítica do SGSI pela direção: a direção deve analisar criticamente o SGSI da organização a intervalos planejados (pelo menos uma vez por ano) para assegurar a sua contínua pertinência, adequação e eficácia. Esta análise crítica deve incluir a avaliação de oportunidades para melhoria e a necessidade de mudanças do SGSI, incluindo a política de segurança da informação e objetivos de segurança da informação. Os resultados dessas análises críticas devem ser claramente documentados e os registros devem ser mantidos.

5. Melhoria do SGSI: a organização deve continuar fazendo uso das políticas de segurança da informação, para garantir sempre os resultados da segurança. Deve executar ações corretivas, assim eliminando as causas da não conformidade para evitar a repetição dos eventos e ações preventivas para evitar futuras ocorrências de não conformidade.

Concluindo, embora essas normas sejam um importante padrão para nortear a gestão da segurança da informação, pois a aplicação de ambas visa garantir a segurança desse ativo, independente das informações estarem registradas em documentos convencionais, eletrônicos ou digitais, em se tratando de documentos arquivísticos digitais é necessário ainda mais.

Para que um documento arquivístico digital se caracterize como fonte de informação confiável para a administração e como prova em juízo, tem de ser mantida sua autenticidade, assim, é necessário preservá-lo de acessos indevidos e registrar todas as alterações por ele sofridas (autorizadas ou não) nas diferentes fases do ciclo vital. No próximo capítulo é abordado o e-Arq Brasil, cuja observância muito tem a contribuir para o alcance de tal objetivo.

7 E-ARQ BRASIL

O e-Arq Brasil Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos é fruto do desafio imposto pelos avanços tecnológicos à gestão arquivística de produzir, manter e preservar documentos autênticos, confiáveis e acessíveis.

O e-Arq Brasil, desenvolvido pela Câmara Técnica de Documentos Eletrônicos (CTDE), do Conselho Nacional de Arquivos (CONARQ), órgão colegiado vinculado ao Arquivo Nacional, consiste na especificação de um conjunto de requisitos a serem cumpridos pelo sistema de gestão arquivística e pelos próprios documentos produzidos/recebidos no decurso das atividades de uma organização, com vistas à manutenção da autenticidade, confiabilidade e acessibilidade dos documentos arquivísticos digitais. Nesse contexto, tem como objetivo orientar a identificação de documentos arquivísticos digitais dentre as informações e os documentos produzidos/recebidos ou armazenados em meio digital; orientar a implantação da gestão arquivística de documentos; fornecer especificações técnicas e funcionais, e os metadados para orientar a aquisição e/ou o desenvolvimento de sistemas informatizados de gestão arquivística de documentos. Ainda, podendo ser utilizado para desenvolver um sistema novo ou para avaliação de um sistema já existente.

O e-Arq Brasil está dividido em duas partes. A primeira trata da gestão arquivística de documentos e relaciona as seguintes questões: definição da política arquivística; designação de responsabilidades; o planejamento e o programa de gestão arquivística de documentos; procedimentos e operações técnicas dos sistema de gestão arquivística de documentos digitais e convencionais, nesta seção: da captura, avaliação temporalidade e destinação, pesquisa localização e apresentação dos documentos, segurança controle de acesso, trilhas de auditoria e cópias de segurança, armazenamento e preservação; e instrumentos utilizados na gestão arquivística de documentos, nesta seção: plano de classificação e código de classificação, tabela de temporalidade e destinação, manual de gestão arquivística

de documentos, esquema de classificação de acesso e segurança, glossário, vocabulário controlado e tesauro.

A segunda parte do e-Arq apresenta as especificações de requisitos para sistemas informatizados de gestão arquivística de documentos (SIGAD) seus aspectos e funcionalidades, ficando estruturada do seguinte forma: 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; conformidade com a legislação e regulamentações; usabilidade; interoperabilidade; disponibilidade; desempenho; e escalabilidade. O documento ainda traz o esquema de metadados e um glossário.

O e-Arq institui requisitos mínimos para um Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD), independentemente da plataforma tecnológica em que for desenvolvido e/ou implantado. Ele deve ser capaz de gerenciar, simultaneamente, os documentos digitais e os documentos convencionais, ou seja, ser aplicável também em sistemas híbridos. Seu sucesso dependerá essencialmente da implementação a priori de um programa de gestão arquivística de documentos.

Salienta-se que a base da gestão arquivísitica de documentos é o plano de classificação de documentos, sendo a tabela de temporalidade de documentos seu cerne. Os referidos instrumentos tem especial importância no SIGAD, visto que para ser incorporado ao sistema o documento tem de ser classificado e com base nessa classificação a tabela de temporalidade define todo o seu ciclo vital. Por tanto, o SIGAD abrange as fases correntes e intermediárias da gestão de documentos e apoia os procedimentos de preservação.

O e-Arq define o SIGAD como:

> [...] um conjunto de procedimentos e operações técnicas, característico do sistema de gestão arquivística de documentos, processado por computador. Pode compreender um software particular, um determinado número de softwares integrados, adquiridos ou desenvolvidos por encomenda, ou uma combinação destes. (e-Arq Brasil, 2011, p. 10)

Complementando, o e-Arq enumera os requisitos arquivísticos que caracterizam um SIGAD:

> - captura, armazenamento, indexação e recuperação de todos os tipos de documentos arquivísticos;
> - captura, armazenamento, indexação e recuperação de todos os componentes digitais do documento arquivístico como uma unidade complexa;
> - 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. (e-Arq Brasil, 2011, p. 11)

Quanto ao programa de gestão arquivística de documentos, o e-Arq salienta que ele terá de atender a exigências referentes ao documento arquivístico e ao seu próprio funcionamento, deste modo:

> **O documento arquivístico deve:**
> - refletir corretamente o que foi comunicado, decidido ou a ação implementada;
> - conter os metadados necessários para documentar a ação;
> - ser capaz de apoiar as atividades;
> - prestar contas das atividades realizadas.
>
> **O programa de gestão arquivística de documentos deve:**
> - contemplar o ciclo de vida dos documentos;
> - garantir a acessibilidade dos documentos;
> - manter os documentos em ambiente seguro;
> - reter os documentos somente pelo período estabelecido na tabela de temporalidade e destinação;
> - implementar estratégias de preservação dos documentos desde sua produção e pelo tempo que for necessário;
> - garantir as seguintes qualidades do documento arquivístico: organicidade, unicidade, confiabilidade, autenticidade e acessibilidade. (e-Arq Brasil, 2011, p. 21)

A fim de manter a confiabilidade do documento arquivístico é necessário que:

> [...] o programa de gestão arquivística dos órgãos e entidades deve assegurar que os documentos arquivísticos sejam produzidos no momento em que ocorre a ação, ou imediatamente após, por pessoas diretamente envolvidas na condução das atividades e devidamente autorizadas; e com o

> grau de completeza[9] requerido tanto pelo próprio órgão ou entidade como pelo sistema jurídico. (e-Arq Brasil, 2011, p. 21)

Em se tratando de assegurar a autenticidade do documentos arquivístico:

> [...] o programa de gestão arquivística tem que garantir sua identidade[10] e integridade[11]. Para tanto, deve implementar e documentar políticas e procedimentos que controlem a transmissão, manutenção, avaliação, destinação e preservação dos documentos, garantindo que eles estejam protegidos contra acréscimo, supressão, alteração, uso e ocultação indevidos. (e-Arq Brasil, 2011, p. 21)

Com vistas a garantir a integridade dos documentos o SIGAD deve prever os procedimentos de segurança elencados a seguir pelo e-Arq.

- Controle de acesso: “O sistema de gestão arquivística precisa limitar ou autorizar o acesso a documentos por usuário e/ou grupos de usuários.” (e-Arq Brasil, 2011, p. 21)

- Uso e rastreamento: “O uso dos documentos pelos usuários deve ser registrado pelo sistema nos seus respectivos metadados.” (e-Arq Brasil, 2011, p. 21)

- Trilha de auditoria: “é o conjunto de informações registradas que permite o rastreamento de intervenções ou tentativas de intervenção no documento arquivístico digital ou no SIGAD.” (e-Arq Brasil, 2011, p. 21) Nesse sentido, é também um metadado sobre os documentos arquivísticos digitais e informa sobre sua autenticidade. (e-Arq Brasil, 2011, p. 71) Ela deve:

> [...] registrar o movimento e o uso dos documentos arquivísticos dentro de um SIGAD (captura, registro, classificação, indexação, arquivamento, armazenamento, recuperação da informação, acesso e uso, preservação e destinação), informando quem operou, a data e a hora, e as ações realizadas. (e-Arq Brasil, 2011, p. 21)

---

[9] *Completeza* se refere à presença, no documento arquivístico, de todos os elementos intrínsecos e extrínsecos exigidos pela organização produtora e pelo sistema jurídico-administrativo ao qual pertence, de maneira que esse mesmo documento possa ser capaz de gerar consequências. (e-Arq, 2011, p. 126)

[10] *Identidade* refere-se a atributos que caracterizam o documento arquivístico e o distinguem dos demais. Esses atributos se constituem nos elementos intrínsecos da forma documental e nas anotações. (e-Arq, 2011, p. 22)

[11] *Integridade* refere-se ao estado dos documentos que se encontram completos e não sofreram nenhum tipo de corrupção ou alteração não autorizada nem documentada. (e-Arq, 2011, p. 22)

- Cópias de segurança: “O SIGAD deve prever controles para proporcionar a salvaguarda regular dos documentos arquivísticos e dos seus metadados.” (e-Arq Brasil, 2011, p. 22)

- Segurança da infraestrutura: controle de acesso às instalações, instalação e monitoramento de equipamentos contra incêndio, dentre outras medidas.

A aplicação dos requisitos funcionais de segurança especificados no e-Arq Brasil, da página 66 a página 77, melhoram substancialmente a qualidade dos documentos arquivísticos. Eles confluem para a manutenção da integridade do documento, colaborando para assegurar a autenticidade, influenciando na inferência da sua confiabilidade.

Deste modo, pode-se afirmar que o desenvolvimento e implementação de sistemas informatizados em conformidade com os requisitos de gestão arquivística estabelecidos no e-Arq Brasil conferem credibilidade à produção e à manutenção de documentos arquivísticos, pois, como mencionado a priori, ele abrange todas as funções arquivísticas, da produção, tramitação, utilização e arquivamento, a destinação final do documento. Portanto, o SIGAD contribui para que os documentos arquivísticos digitais permaneçam autênticos, confiáveis e acessíveis à administração que os produziu e, caso possuam valor para a guarda permanente, para que possam ser preservados com essas características.

8 AUTENTICIDADE E CONFIABILIDADE DOS DOCUMENTOS ARQUIVÍSTICOS DIGITAIS

No contexto digital, a questão da presunção da autenticidade:

> [...] está agora muito mais fragilizada implicando o envolvimento e um trabalho estreito entre o produtor e o "gestor da informação", dado que a segurança da informação, o garantir da sua autenticidade, integridade, fidedignidade e inteligibilidade devem ser pensadas mesmo antes da mesma ser produzida, isto é, quando os próprios sistemas tecnológico-organizacionais que sustentarão a criação da informação estão a ser planeados e concebidos". (Pinto, p. 7, 2007)

Nas organizações a política de segurança da informação resulta da necessidade de gerenciar os riscos de negócio, mais precisamente, os riscos de tecnologia da informação, para viabilizar um ambiente seguro para os ativos da organização e a continuidade do negócio.

Na análise dos profissionais de tecnologia a autenticidade deve ser garantida através da adoção de métodos que assegurem que a informação não sofra alteração/adulteração após sua criação, durante a transmissão, manipulação e armazenamento. Dessa maneira, os controles que tratam do acesso priorizam a manutenção da confidencialidade, integridade e disponibilidade da informação, tentando impedir que pessoas não autorizadas tenham acesso a informações restritas, assegurando a confidencialidade da informação e a sua não manipulação sem autorização.

Como ponderado nos capítulos: gestão da segurança da informação e gestão de riscos; normas brasileiras ISO/ IEC 17799: 2005 e ISO/ IEC 27001: 2006, a abordagem acima relatada está correta sob a ótica da manutenção da integridade da informação. No entanto, estando estas informações contidas em documentos arquivísticos digitais manter a integridade é um requisito fundamental, mas não resolve totalmente a questão sob o prisma da autenticidade. Isso posto, um documento arquivístico digital pode estar íntegro, mas pode não ter sua autenticidade aferida como verdadeira, em decorrência de sua gestão ter sido

realizada por um sistema informatizado não preparado adequadamente para mantê-la, comprometendo deste modo a confiabilidade dos fatos que atesta, muito embora, a informação permaneça íntegra.

Na perspectiva arquivística a autenticidade relaciona-se profundamente à capacidade probatória dos documentos, não apenas no sentido jurídico, mas também como testemunho autêntico dos atos, ações e atividades que representam.

O e-Arq Brasil, aprofundando-se no tema autenticidade e confiabilidade de documentos, explica como essas características se relacionam, e, a dificuldade de presumir-se a confiabilidade.

> [...] Enquanto a confiabilidade está relacionada ao momento da produção, a autenticidade está ligada à transmissão do documento e à sua preservação e custódia. Um documento autêntico é aquele que se mantém da mesma forma como foi produzido e, portanto, apresenta o mesmo grau de confiabilidade que tinha no momento de sua produção. Assim, um documento não completamente confiável, mas transmitido e preservado sem adulteração ou qualquer outro tipo de corrupção, é autêntico.
> [...] Dificilmente pode-se assegurar a veracidade do conteúdo de um documento; ela é inferida da completeza e dos procedimentos de produção. A confiabilidade é uma questão de grau, ou seja, um documento pode ser mais ou menos confiável.

Manter a autenticidade do documento digital durante as etapas de gestão é tão importante como será na preservação em longo prazo, sendo isso vital para que o documento ingresse, caso tenha valor para tal, a preservação permanente, mantendo suas características.

Como exposto na subunidade 3.1 de fato a certificação eletrônica assegura a autenticidade e confiabilidade ao documento arquivístico digital e, por consequência, atribui valor jurídico ao mesmo, mas, somente até ser recebido pelo seu destinatário, pois, a partir do momento em que ingressa em um sistema informatizado de documentos, eles têm de serem adequadamente gerenciados, para assim permanecer, sendo esse o desafio que se impõe. O estabelecimento de um Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD), cumprindo os requisitos definidos pelo e-Arq Brasil, analisado no capítulo anterior, tem como um dos principais objetivos primar pela manutenção da autenticidade desse documento.

Uma questão que gera confusão entre os profissionais de tecnologia da informação é a compreensão da diferença entre o SIGAD e o Gerenciamento Eletrônico de Documentos (GED). Por sua vez, o GED é uma ferramenta que visa apoiar e facilitar a condução de uma ou mais atividades da rotina administrativa da organização, enquanto o SIGAD tem como foco o controle completo do ciclo de vida do documento (independente do suporte ou formato). Como especificado no fragmento a seguir:

> Um GED trata os documentos de maneira compartimentada, enquanto o SIGAD parte de uma concepção orgânica, qual seja, a de que os documentos possuem uma inter-relação que reflete as atividades da instituição que os criou. Além disso, diferentemente do SIGAD, o GED nem sempre incorpora o conceito arquivístico de ciclo de vida dos documentos; (e-Arq, 2011, p. 11)

Portanto, as organizações que desenvolverem e/ou utilizarem sistemas informatizados estabelecidos conforme as recomendações arquivísticas de gestão de documentos terão como benefício o controle total dos documentos arquivísticos e a manutenção de sua qualidade, logo assegurando seu o caráter testemunhal e probatório.

Por fim, nenhum sistema informatizado será completamente livre de fragilidades. Entretanto, com o estabelecimento de políticas de segurança da informação alinhadas à realidade organizacional, e em sinergia com um SIGAD, adequadamente estruturado, pode-se diminuir substancialmente as possibilidades da organização ter comprometida a autenticidade e/ou confiabilidade de seus documentos arquivísticos. Desta forma, garantindo que a organização tenha disponíveis informações integras para alicerçar seu processo de gestão administrativa.

9 CONCLUSÃO

A informação, como muitos outros recursos das organizações, apresenta o conhecido fenômeno dos rendimentos decrescentes, ou seja, quanto maior é a massa documental acumulada desordenadamente, menor é a relevância das informações contidas nos documentos, por isso a importância da gestão arquivística de documentos. Ela viabiliza o adequado tratamento aos documentos, mantendo as informações acessíveis à administração que os produziu de forma eficiente, e descartando o que não mais é necessário, proporcionando a realocação de espaço físico, recurso financeiro e humano.

Na conjuntura atual, o arquivista deve ter em mente que é necessário agregar a sua formação o conhecimento de outras áreas, como a de tecnologia da informação, para que possa ser mais efetivo no desempenho de suas atividades e para que assegure seu papel de gestor da informação, no âmbito administrativo. Isso não significa dominar por completo o fazer dessas outras áreas, mas sim conhecer o seu contexto de atuação e seu vocabulário.

Em se tratando da gestão de documentos arquivísticos digitais considera-se essencial que sejam correlacionadas as teorias e práticas arquivísticas as teorias e práticas de áreas como a administração e tecnologia da informação. Elas muito têm a agregar para que o sistema informatizado contemple os requisitos necessários para manter a integridade das informações. Por exemplo, conhecer as normas brasileiras de segurança de informação pode auxiliar o arquivista a melhor dialogar com os desenvolvedores do sistema informatizado que a organização esteja pretendendo adquirir ou aperfeiçoar, isso lhe permitirá associar ao projeto os conhecimentos arquivísticos para que, além de íntegra, a informação contida em um documento arquivístico digital tenha a manutenção de sua autenticidade, e por consequência, a confiabilidade assegurada.

Sempre que necessário deve-se esclarecer aos profissionais de tecnologia e aos administradores a diferença existente entre o documento digital e o documento arquivístico digital, principalmente referente ao seu caráter testemunhal e probatório.

O CONARQ, o órgão máximo de arquivos no Brasil, tem por finalidade definir a política nacional de arquivos públicos e privados, bem como exercer orientação normativa visando à gestão documental e à proteção especial aos documentos de arquivo. Nos últimos anos por meio da Câmara Técnica de Documentos Eletrônicos (CTDE) tem buscado fornecer bases e diretrizes para que a gestão dos documentos arquivísticos eletrônicos seja desenvolvida, cada vez mais, de forma eficiente e segura, um dos resultados desse trabalho é o e-Arq Brasil, analisado no capítulo 8, que figura como um dos instrumentos mais importantes no que se refere à gestão de documentos arquivísticos eletrônicos, pois consiste um Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (SIGAD).

Esta pesquisa buscou contextualizar como a gestão arquivística em sistemas informatizados pode colaborar para manter a autenticidade e a confiabilidade dos documentos digitais. Para tanto, analisou-se os pontos de vista de diferentes autores das áreas da arquivologia, administração e tecnologia da informação, as Normas Brasileiras (NBR) ISO/ IEC 17799: 2005 e ISO/ IEC 27001: 2006, e as recomendações do CONARQ relacionados ao tema em estudo, concluindo-se que o SIGAD por si só não garante a autenticidade e a confiabilidade do documento digital, mas ele colabora para isso. Por tanto, o sistema deve ser alinhado aos controles de segurança da informação no sistema informatizado. As normas NBR ISO/ IEC 17799: 2005 e ISO/ IEC 27001: 2006 tem papel preponderante nesse sentido, visto que norteiam as ações nesse âmbito. Por fim, que a questão da segurança da informação em um ambiente digital está intrinsecamente relacionada com manutenção da autenticidade e da confiabilidade dos documentos digitais.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação**. Rio de Janeiro, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos**. Rio de Janeiro, 2005.

BALDAM, Roquemar de Lima; VALLE, Rogerio; CAVALCANTI, Marcos. **GED:** gerenciamento eletrônico de documentos. São Paulo: Érica, 2004.

BELLOTTO, Heloísa Liberalli; CAMARGO, Ana Maria de Almeida. **Dicionário de Terminologia Arquivística.** São Paulo: Secretaria da Cultura, 1996.

BELLOTTO, Heloísa Liberalli. **Como fazer análise diplomática e análise tipológica de documento de arquivo.** São Paulo: Arquivo do Estado e Imprensa Oficial do Estado, 2002.

BRASIL. Arquivo Nacional. **Dicionário brasileiro de terminologia arquivística.** Rio de Janeiro: Arquivo Nacional. 2005.

BERNARDES, Ieda Pimenta. **Como avaliar documentos de arquivo**. São Paulo: Arquivo do Estado, 1998.

CAMPOS, Vicente Falconi. **Gerenciamento pelas diretrizes (Hoshin Kanri)**. Belo Horizonte: Fundação Chistiano Ottoni, Escola de Engenharia da UFMG, 1996.

CONARQ. Câmara Técnica de Documentos Eletrônicos – CTDE; **Glossário**: versão 5.1 / março de 2010. Disponível em: <http://www.documentoseletronicos.arquivonacional.gov.br/media/publicacoes/glossario/2010glossario_v5.1.pdf>. Acesso em: 5 de nov. 2012.

_____. **Legislação arquivística.** Disponível em: <http://www.arquivonacional.gov.br>. Acesso em: 03 de mai. 2012.

DEMO, Pedro. **Introdução à metodologia da ciência.** 2. ed. São Paulo: Atlas, 1987.

DOLLAR, Charles. Tecnologia da informação digital e pesquisa acadêmica na ciências sociais e humanas: o papel crucial da arquivologia. **Estudos Históricos**, Rio de Janeiro, v. 7, n.13, 1994.

DURANTI, Luciana; MACNEIL, Heather. **The protection of the integrity of electronic records an overview of the UBC- MAS research project.** Archivaria. Ottawa, 1996.

DURANTI, Luciana.Registros documentais contemporâneos como prova de ação. **Estudos Históricos**, Rio de Janeiro, v. 7, n.13, 1994.

_____. **Diplomática usos nuevos para una antigua ciencia.** 1. ed. Carmona: S e C ediciones, 1996.

E-ARQ Brasil. **Modelo de requisitos para sistemas informatizados de gestão arquivística de documentos.** Disponível em: <http://www.conarq.arquivonacional.gov.br/Media/publicacoes/earqbrasilv1.pdf>. Acesso em 30 de mai. 2012.

FREITAS, Cristina Vieira de. **Garantir a autenticidade e o acesso continuado à informação digital:** os desafios da preservação digital em arquivos. Disponível em:< http://www.bad.pt/publicacoes/index.php/congressosbad/article/view/272>. Acesso em: 29 de out. 2012.

GABBAY, Max Simon. **Fatores influenciadores na implementação de ações de gestão de segurança da informação: um estudo com executivos e gerentes de tecnologia da informação em empresas do Rio Grande do Norte.** Tese (mestrado) – Universidade Federal do Rio Grande do Norte, 2003.

GARCIA, Olga Maria Correa; JUNIOR, Vitor Francisco S. **A aplicação da Arquivística Integrada, considerando os desdobramentos do processo a partir da Classificação.** Inf. Inf., Londrina, v. 7, n. 1, p. 41-56, jan./jun. 2002.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 5.ed. São Paulo: Atlas, 2006.

GUIMARÃES, José Augusto Chaves; YADO, Aline Midori Manfré. **O Princípio da Proveniência: uma abordagem conceitual no âmbito da literatura arquivística.** Disponível em: <http://cead.ufsm.br/moodle/file.php/3801/5e_artigo_principio_proveniencia_11.04.2009.pdf > . Acesso em 9 de abr. 2012.

GONÇALVES, Janice. **Como classificar e ordenar documentos de arquivo.** São Paulo: Divisão de Arquivo de São Paulo, 1998.

GONÇALVES, Luís Rodrigo de Oliveira. **O surgimento da norma nacional de segurança de informação [NBR ISO/IEC-1779:2001].** Disponível em: <http://www.lockabit.coppe.ufrj.br/print.php?id=85>. Acesso em: 3 de jun. 2005.

INTERPARES. **Diretrizes do preservador: a preservação de documentos arquivísticos digitais: diretrizes para organização.** Disponível em: <http://www.interpares.org/display_file.cfm?doc=ip2_preserver_guidelines_booklet--portuguese.pdf>. Acesso em: 29 de out. 2012.

LEVY, David M. Where´s Waldo? Reflections on copies and authenticity in a digital environment. **Páginas a&b**. n. 9, p. 81 – 90, 2002.

INNARELLI, Humberto Celeste. Preservação digital e seus dez mandamentos. In: SANTOS, Vanderlei Batista dos. (Org). In:. **Arquivística temas contemporâneos: classificação, preservação digital, gestão do conhecimento.** Distrito Federal: SENAC, 2007.

LOPES, Luís Carlos. **A informação e os arquivos teorias e práticas.** Rio de Janeiro: Arquivo do Estado do Rio de Janeiro, 1996.

_____. **A gestão da informação:** as organizações, os arquivos e a informática aplicada. Rio de Janeiro: Arquivo do Estado do Rio de Janeiro, 1997.

_____. **A nova arquivística na modernização administrativa**. Rio de Janeiro: Sérgio Milagres, 2000.

LOPEZ, André Porto Ancona. **Como descrever documentos de arquivo:** elaboração de instrumentos de pesquisa. São Paulo: Arquivo do Estado, Imprensa Oficial do Estado, 2002.

MARCONI, Marina de Andrade e LAKATOS, Eva Maria. **Técnicas de pesquisa:** planejamento e execução de pesquisas, amostragens e técnicas de pesquisa, elaboração, análise e interpretação de dados. 6.ed. São Paulo: Atlas, 2006.
MARSH, John. **Herramientas para la mejora continua.** Madrid, ES: AENOR, 2000.

MOURA, Luciano Raizer. **Qualidade uma abordagem simplesmente total:** simples e prática da gestão de qualidade. Rio de Janeiro: Qualitymark Ed., 1997.

PINTO, Maria Manuela Gomes de Azevedo. Da acção à informação: o desafio digital. In CONGRESSO NACIONAL DE BIBLIOTECÁRIOS ARQUIVISTAS E DOCUMENTALISTAS, 9, Ponta Delgada, 2007 – **Bibliotecas e Arquivos: Informação para a cidadania, o desenvolvimento e a inovação: actas** [em linha]. Lisboa: BAD. Disponível em: <http://repositorio-aberto.up.pt/bitstream/10216/25384/2/manuelapintodaaccao000100393.pdf>. Acesso em: 30 de out. 2012.

RONDINELLI**,** Rosely Curi. **Gestão de documentos arquivísticos eletrônicos:** iniciativas brasileiras. 2002 a. Disponível em: <http://www.arquivonacional.gov.br/not_eve/seminario/sessao%202/rcr_w.htm>. Acesso em: 14 de abr. 2004.

_____. **O gerenciamento do documento eletrônico:** uma abordagem teórica da diplomática arquivística contemporânea. 2002 b. 172f.: il. Dissertação (Mestrado em Ciência da Informação) – Escola de Comunicação, Universidade Federal do Rio de Janeiro, Rio de Janeiro. Orientadores: Nélida González de Gomés e José Maria Jardim.

_____.**Gerenciamento arquivístico de documentos eletrônicos.** 1. ed. Rio de Janeiro: FGV, 2002 c.

RONDINELLI, Rosely Cury; et al. **Gestão arquivística de documentos eletrônicos**. Câmara Técnica de Documentos Eletrônicos. Disponível em: <http://www.arquivonacional.gov.br/conarq/cam_tec_doc_ele/download/GT%20gestao%20arquivistica.pdf>. Acesso em: 30 mai. 2005.

ROUSSEAU, Jean-Yves; COUTURE, Carol. **Os fundamentos da disciplina arquivística**. Rio de Janeiro: Nova Enciclopédia, 1998.

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

SANTOS, Vanderlei Batista dos. (Org.). A prática arquivística em tempos de gestão do conhecimento. In:. **Arquivística temas contemporâneos: classificação, preservação digital, gestão do conhecimento.** Distrito Federal: SENAC, 2007.

SÊMOLA, Marcos. **Gestão da Segurança da Informação***.* 1. Ed. Rio de Janeiro: Campus, 2003.

SCHELLENBERG, Theodore R. **Arquivos modernos:** princípios e técnicas. (Trad. Nilza Teixeira). 2ª ed. Rio de Janeiro: FGV, 2002.

SILVA, Edna Lúcia. **Metodologia da pesquisa e elaboração de dissertação**. 3 ed. UFSC: Florianópolis, 2001.

TRUJILLO FERRARI, Alfonso. **Metodologia da pesquisa científica**. São Paulo: MacGraw-Hill do Brasil, 1982.