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

Adriana Herkert Netto*

RESUMO

Este estudo buscou reunir conhecimentos e apresentá-los de forma a contextualizar como a gestão arquivística em sistemas informatizados pode colaborar para manter a autenticidade e a confiabilidade dos documentos digitais, com vistas assegurar que a administração tenha à sua disposição acesso a informações íntegras sempre que necessário. O estudo foi conduzido sob a forma de pesquisa bibliográfica. 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. Nessa conjuntura, concluiu-se que a atuação do arquivista em conjunto com os profissionais de tecnologia possibilita o desenvolvimento/ a adequação de sistemas de informação que diminuem, substancialmente, as possibilidades de a organização ter comprometida a autenticidade e/ou confiabilidade de seus documentos arquivísticos ao estabelecer políticas de segurança da informação alinhadas à realidade organizacional, em observância aos fatores legais envolvidos e em sinergia com um SIGAD estruturado adequadamente.

Palavras-chave: Documento arquivístico digital. Autenticidade. Confiabilidade.

* Bacharel em Arquivologia e Especialista em Gestão de Arquivos pela Universidade Federal de Santa Maria (UFSM). *E-mail*: adriana.netto@gmail.com

1 INTRODUÇÃO

Atualmente, muitas organizações investem na implementação de sistemas informatizados com vistas a tornar seus processos administrativos mais ágeis com a produção de seus documentos somente em formato digital. Esses sistemas informatizados são projetados, em muitos casos, 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 (em 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 são digitalizados; a posteriori, ocorre 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 com base nas necessidades da empresa e em observância aos fatores legais envolvidos.

Em um cenário onde a competitividade entre as organizações, em qualquer área de negócio, exige rapidez na troca de informações, a gestão dos documentos e das informações nele contidas tornaram-se necessárias para o bom desempenho das atividades organizacionais, pois podem contribuir efetivamente para o sucesso e para a sobrevivência destas organizações.

Nesse contexto, 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. Logo, a gestão arquivística em um sistema informatizado pode, por meio dos princípios e das técnicas arquivísticas, contribuir para a manutenção da autenticidade e da confiabilidade dos documentos digitais. Pois, como se sabe, eles são mais vulneráveis do 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, as informações necessárias para alicerçar o

processo decisório podem não estar íntegras quando necessárias à administração.

Esse estudo buscou reunir conhecimento e apresentá-lo 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 à sua disposição, sempre que necessário, o acesso a informações íntegras.

Este trabalho foi conduzido sob forma de pesquisa bibliográfica. Os autores, Gil (2006) e Marconi e Lakatos (2006) definem a pesquisa bibliográfica como a que se realiza sob materiais já elaborados, constituídos 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). A abordagem descrita justificou-se pela existência de publicações a respeito do assunto investigado.

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, a fim de reunir conhecimento e esclarecer como a gestão arquivística em sistemas informatizados pode contribuir para manter a autenticidade e a confiabilidade dos documentos digitais, e, por conseqüência, das informações por ele comunicadas.

2 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).

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" (BRASIL, 2013, p. 16).

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, autenticidade, naturalidade, inter-relacionamento e unicidade.

Na concepção de Rondinelli (2002 a), o documento arquivístico possui os seguintes elementos: suporte, forma documentária, anotações e contexto.

Os documentos arquivísticos convencionais e os eletrônicos são constituídos por elementos que podem ser identificados e avaliados por meio da Análise Diplomática. Para Duranti e Macneil (1996), a diplomática pode analisar todos os documentos, visto que, atualmente, os documentos tradicionais e os eletrônicos são constituídos pela mesma forma documentária (elementos externos e internos) estudada nos primórdios da diplomática, porém, um pouco mais elaborada. Para facilitar a compreensão, pode-se analisar o Quadro 1, que apresenta o comparativo elaborado por Rondinelli (2002 a, p. 158).

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.

Duranti (1996), sobre 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

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

enviado. Assim, o documento recebido, ao contrário do enviado, é completo e efetivo.

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[2], 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.

Quadro 1 - Documento convencional x Documento eletrônico

[2] A minuta é uma subclassificação de rascunho.

De acordo com Dollar (1994), a discussão sobre documentos eletrônicos envolve três pontos críticos: unicidade: garantir a manutenção da proveniência do documento; autenticidade: impedir distorções ou falsificações sem deixar vestígios; e preservação: enfrentar a obsolescência tecnológica.

O e-Arq (BRASIL,2011, p. 9) define documento digital como "a informação registrada, codificada em dígitos binários e acessível por meio de sistema computacional". Documento arquivístico digital "é um documento digital que é tratado e gerenciado como um documento arquivístico, ou seja, incorporado ao sistema de arquivos". (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:

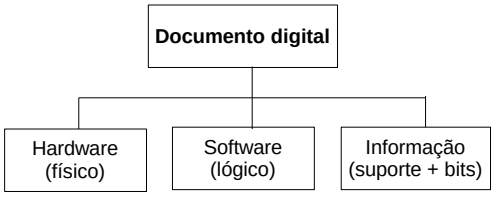

Figura 1 -Estrutura do documento digital

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 à tona a 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 (2004), 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, à forma e ao status de transmissão do documento, às condições de sua preservação e custódia (método de verificação).

A *confiabilidade*[3]é conceituada em 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(BRASIL, 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 nº 7.845, de 14 de novembro de 2012.

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 que se estabeleçam alguns critérios e ferramentas para garantir a autenticidade dos documentos digitais, dentre eles, ações relacionadas ao controle de acesso, conforme o esquema a seguir:

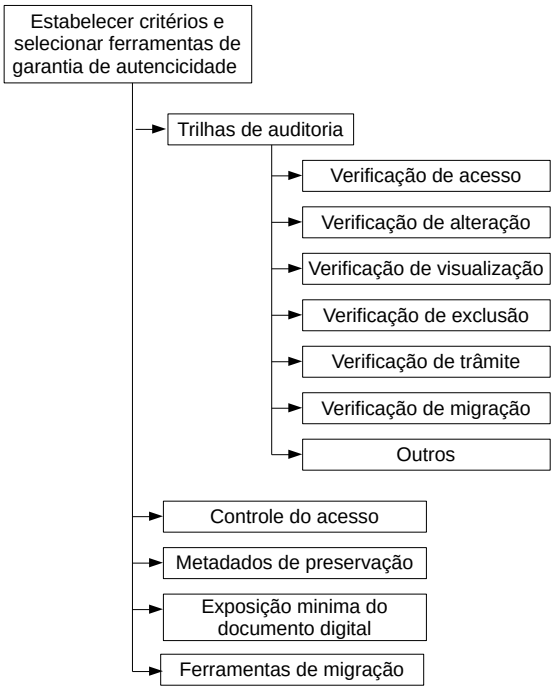

Figura 2 -Critérios e ferramentas para garantia da autenticidade

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 realiza alguma negociação (compra, venda, lançamento de produto, programa, projeto), pode prejudicar uma

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

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[4]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".

2.1 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 em discussão no Conselho Nacional de Arquivos (CONARQ). No entanto, por meio 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, regulamentada pela Medida Provisória nº 2.200, que institui a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil – que disciplina a questão da presunção de integridade, autenticidade e validade dos documentos eletrônicos.

A certificação eletrônica pode ser obtida por meio da solicitação à 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 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

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

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[5] atribuída pelo processo de certificação eletrônica ao documento digital assegura sua autenticidade e confiabilidade, pois é acrescentada a ele 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 garante 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 (tais como: 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).

3 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." (BRASIL, p. 47, 2005).

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

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" (BRASIL, 2013, p. 16).

As funções arquivísticas, 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.

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, servem de subsídio para o planejamento das ações futuras. Os documentos decorrentes das atividades administrativas são o testemunho de suas ações, e prova legal dos atos administrativos. Assim, a gestão arquivística de documentos é fundamental para a eficiência e eficácia da gestão administrativa.

Na conjuntura atual, as organizações têm investido em recursos tecnológicos, a fim de 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).

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 (BRASIL, 2004, p. 8).

De acordo com Rondinelli (2002 b), 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 b), 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: estabelecer um mecanismo que registre 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, portanto, o armazenamento e gerenciamento desses elementos ocorre separadamente como metadados.

Metadados são "dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e/ou preservar documentos arquivísticos ao longo do tempo" (BRASIL, 2010, p. 17), são atributos concomitantes ou posteriores a criação do documento[6]. 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;
- à 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, enumeram-se três estados distintos: original – primeiro documento completo e efetivo; rascunho – versão temporária,

[6] Ver metadados no Quadro 1.

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 digital arquivístico e em instrumento para a análise diplomática. É por meio 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 reconstitui 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 b, 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 quanto na 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:

> [...] É importante ressaltar que **cópia**[7]e **migração**[7] 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 documentos originais. Entretanto, há que se ressaltar que, apesar de menos in-

[7]Grifo meu.

> vasiva, 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 (RONDINELLI, 2002 b, p. 70).

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.

4 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, íntegras e disponíveis para a pessoa certa na hora certa.

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) conceitua ameaça como:

> 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 (SÊMOLA, 2003, p. 47).

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,

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

possivelmente, impactos nos negócios"(SÊMOLA, 2003, p.50).

O risco de tecnologia da informação (TI) é a probabilidade de algum serviço, 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);deve abranger o controle e monitoramento de seus recursos computacionais e, consequentemente, das informações manipuladas.

A norma NBR ISO/IEC 17799[9] é o principal padrão relacionado à gestão de segurança da informação, portanto, a assimilação das práticas nela contidas pelos gestores de TI e segurança da informação auxiliam a organização no desenvolvimento de uma política de segurança forte. Essa norma é indispensável para a aplicação da norma NBR ISO/IEC 27001.

[9] A partir de 2007, a nova edição da NBR ISO/IEC 17799 foi incorporada ao novo esquema de numeração como NBR ISO/IEC 27002.

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

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.

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).

Nos sistemas informatizados encontram-se os documentos digitais arquivísticos expostos a ameaças. Portanto, caso a segurança do sistema informatizado não seja adequadamente estruturada e garantida, não haverá como manter a integridade dos documentos arquivísticos digitais, importante ativo para a organização, 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 a 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 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.

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 assegurara seleção de controles de segurança adequados 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.

O Ciclo PDCA, idealizado por Shewhart e divulgado por Deming, 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), *do* (executar), *check* (verificar) e *act* (agir).

A norma possibilita, com a aplicação do PDCA, a análise/avaliação de riscos, especificação e implementação de segurança, gerenciamento de segurança e reavaliação.

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 seja aceitável quando uma organização reivindica conformidade com a norma.

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.

6 E-ARQ BRASIL

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, pode ser utilizado para desenvolver um sistema novo ou para avaliação de um sistema já existente.

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.

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 (BRASIL, 2011, p. 10).

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[10] requerido tanto pelo próprio órgão ou entidade como pelo sistema jurídico (BRASIL, 2011, p. 21).

Em se tratando de assegurar a autenticidade do documento arquivístico:

> [...] o programa de gestão arquivística tem que garantir sua identidade[11]e integridade[12].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 (BRASIL, 2011, p. 21).

Com vistas a garantir a integridade dos documentos, o SIGAD deve prever os seguintes procedimentos de segurança elencados pelo e-Arq: controle de acesso, uso e rastreamento, trilha de auditoria[13], cópias de segurança e segurança da infraestrutura.

Deste modo, pode-se afirmar que o desenvolvimento e a 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,à destinação final do documento.Portanto, o SIGAD contribui para que os documentos arquivísticos digitais permaneçam autênticos, confiáveis e acessíveis à administração que os

[10]*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 (BRASIL, 2011, p. 126).

[11]*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 (BRASIL, 2011, p. 22).

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

[13][...] 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 (BRASIL, 2011, p. 21).

produziu e, caso possuam valor para a guarda permanente, para que possam ser preservados com essas características.

7 AUTENTICIDADE E CONFIABILIDADE DOS DOCUMENTOS ARQUIVÍSTICOS DIGITAIS

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.

No tema autenticidade e confiabilidade de documentos, o e-Arq Brasil 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 (BRASIL, 2011, p. 21).
> [...] 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 (BRASIL, 2011, p. 22).

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

Como exposto na subseção 2.1, 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, é esse o desafio que se impõe. Assim, estabelecer um Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD) que cumpre os requisitos definidos pelo e-Arq Brasil tem como um dos principais objetivos primar pela manutenção da autenticidade desse documento.

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 o seu caráter testemunhal e probatório.

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

8 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 descarta o que não mais é necessário, proporcionando a realocação de espaço físico, recurso financeiro e humano.

Ao que se refere à gestão de documentos arquivísticos digitais, considera-se essencial que sejam correlacionadas às 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.

Conclui-se que, o SIGAD por si só não garante a autenticidade e a confiabilidade do documento digital, mas colabora para isso. Portanto, o sistema informatizado da organização deve ser alinhado aos controles de segurança da informação. As normas NBR ISO/IEC 17799:2005 e ISO/IEC 27001:2006têm papel preponderante nesse sentido, visto que norteiam as ações nesse âmbito. Por fim, a questão da segurança da informação em um ambiente digital está intrinsecamente relacionada com manutenção da autenticidade e da confiabilidade dos documentos digitais.

THE CONTEXTUALISATION OF RECORDS MANAGEMENTWITH EMPHASIS ON RELIABILITY AND AUTHENTICITY OF DIGITAL DOCUMENTS

ABSTRACT

This study sought to gather knowledge and introduces them to provide context as the archival management in computer systems can collaborate to maintain the authenticity and reliability of digital documents, in order to ensure that management has at its disposal access to straightforward information whenever necessary. This study was conducted in the form of literature where the views of different authors were analyzed, the Brazilian Standards (NBR) ISO/ IEC 17799: 2005 and ISO/ IEC 27001: 2006, and the recommendations of CONARQ related to the theme. At this juncture, it was concluded that the role of the archivist in conjunction with professional technology enables the development/adaptation of information systems that reduce substantially the possibilities of the organization have compromised the authenticity and/or reliability of its records to establish information security policies in compliance with the legal factors involved, aligned to organizational reality, and in synergy with a properly structured SIGAD.

Keywords: Digital archivistic document. Authenticity. Reliability.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 17799: Tecnologia da informação - técnicas de segurança - código de prática para a gestão da segurança da informação**.Rio de Janeiro, 2005.

_____. **NBR ISO/IEC 27001: Tecnologia da informação - técnicas de segurança - sistemas de gestão de segurança da informação - Requisitos**.Rio de Janeiro, 2006.

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.

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

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

CONSELHO NACIONAL DE ARQUIVOS (BRASIL). **e-ARQ Brasil**: modelo de requisitos para sistemas informatizados de gestão arquivística de documentos. Câmara Técnica de Documentos Eletrônicos. Rio de Janeiro: Arquivo Nacional, 2011. Disponível em: <http://www.conarq.arquivonacional.gov

.br/Media/publicacoes/earqbrasilv1.pdf>. Acesso em: 30 mai. 2012.

CONSELHO NACIONAL DE ARQUIVOS (BRASIL). **Gestão arquivística de documentos eletrônicos**.Câmara Técnica de Documentos Eletrônicos. 2004.Disponível em: <http://www.documentoseletronicos.arquivonacional.gov.br/Media/publicacoes/gt_gestao_arquivistica__pagina_web_corrigido3.pdf>. Acesso em: 13 ago 2013.

_____. **Glossário**. Câmara Técnica de Documentos Eletrônicos. Rio de Janeiro: Arquivo Nacional, 2010. Disponível em: <http://www.documentoseletronicos.arquivonacional.gov.br/media/publicacoes/glossario/2010glossario_v5.1.pdf>. Acesso em: 5 de nov 2012.

_____. **Legislação arquivística. 2013.** Disponível em: <http://www.arquivonacional.gov.br>. Acesso em: 03 de mar 2013.

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

DURANTI, Luciana. **Diplomática ususnuevos para una antiguaciencia.** 1. ed. Carmona: S e C ediciones, 1996.

_____. Registros documentais contemporâneos como prova de ação. **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.

FREITAS, Cristina Vieira de. **Garantir a autenticidade e o acesso continuado à informação digital:** os desafios da preservação digital em arquivos. n. 11, 2012. Disponível em:<http://www.bad.pt/publicacoes/index.php/congressosbad/article/view/272>. Acesso em: 29 de out 2012.

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

GONÇALVES, Luís Rodrigo de Oliveira. **O surgimento da norma nacional de segurança de informação [NBR ISO/IEC-1779:2001].** 2004. Disponível em: <http://www.batori.com.br/pag__con.asp?id_pagina=436>. Acesso em: 3 de jun 2013.

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.

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>. Acessoem: 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.

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

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

MACNEIL, Heather. **Trusting records:** legal, historical, and diplomatic perspectives.The Netherlands: KluwerAcademicPublishers, 2000.

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.

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

RONDINELLI**,** Rosely Curi. **Gerenciamento arquivístico de documentos eletrônicos.** 1. ed.Rio de Janeiro: FGV, 2002 b.

_____. **O gerenciamento do documento eletrônico:** uma abordagem teórica da diplomática arquivística contemporânea.2002 a, 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.

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.

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

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

Trabalho recebido em: 16 ago. 2013 **Trabalho aceito em: 02 abr. 2014**