# Segurança da informação arquivística: o controle de acesso em arquivos públicos estaduais[1]

***Josiane Ayres Sfreddo***

***Especialista em Gestão em Arquivos da Universidade Federal de Santa Maria/ Universidade Aberta do Brasil***

***Daniel Flores***

***Professor Adjunto Doutor do Departamento de Documentação da UFSM, orientador da Monografia de Especialização do Curso de Pós-Graduação à Distância em Gestão em Arquivos da UFSM/UAB***

*Investigação científica a respeito das políticas de controle de acesso, adotadas em Arquivos Públicos Estaduais. Para isso, busca-se identificar as ações adotadas para controlar o acesso documental e garantir a segurança das informações públicas, tendo como referência os requisitos teóricos das Normas ISO 15489-1; e-ARQ; e da ABNT NBR ISO/IEC 27002. Uma pesquisa realizada no sítio do Conselho Nacional de Arquivos (CONARQ), buscando apenas por arquivos que possuíssem um site acessível para contato, possibilitou definir as instituições que participariam da pesquisa. Após isso, foi possível preparar o instrumento de coleta de dados, por meio de questionário enviado por correio eletrônico (e-mail), aplicados aos responsáveis dos Arquivos Públicos Estaduais selecionados para o estudo. Foi possível verificar que, além de proporcionar medidas de segurança para o arquivo, de alguma forma, as instituições preocupam-se com a segurança da informação que será repassada aos usuários.*

***Palavras-chave:*** *Controle de acesso; Segurança da informação arquivística; Arquivos Públicos Estaduais.*

[1]Monografia de Especialização apresentada à Universidade Federal de Santa Maria (UFSM), para obtenção do grau de Especialista em Gestão em Arquivos.

# Security of archival information: the access control in state public files

*Presents a scientific research based in a study concerning the access control policies adopted in the State Public Archives. For this, seeks to identify the actions taken to control access to documentary and ensure the security of public information, with reference to the theoretical requirements of Standars ISO 15489-1; e-ARQ, and ABNT NBR ISO/IEC 27002. A survey on the site of the National Council on Archives (CONARQ), just looking for files that possessed an accessible website for contact, enabled us to define the institutions that would participate in the research. After that, it was possible to prepare the instrument for collecting data through a questionnaire send by electronic mail (e-mail), applied to those responsible of State Public Archives, selected for the study. It was concluded that, besides providing security measures for the file, otherwise the institutions are concerned about the security of information that will be passed on the users.*

***Keywords:*** *Access control; Security of archival information; Public files state.*

Recebido em 31.05.2011 Aceito em 17.05.2012

## 1 Introdução

Somada à descoberta e à introdução de novas tecnologias, a informação assume uma importância crescente dentro das instituições, tornando-se fundamental e geradora de oportunidades de negócios e gestão de processos. Nesse contexto, a informação arquivística pode ser definida de forma que o conteúdo presente nos documentos contextualize ações sistematizadas e organizadas em uma instituição, produzindo, com sua metodologia arquivística, subsídios para a organização documental. Ao adotar um método baseado em procedimentos que garantam a gestão documental, obtém-se como resultado o bom funcionamento institucional, evidenciando a relevância da prática arquivística como um processo que contribui para a transparência das ações institucionais.

Ao desenvolver atividades de gestão documental, a instituição arquivística não se preocupa somente com a guarda e preservação das informações contidas nos documentos. O controle dos processos de gestão, como um todo, previne as ameaças advindas do furto, das falsificações documentais e outros procedimentos que coloquem em risco

a confiabilidade das informações que serão recebidas pelos usuários. Ao criar ações para reforçar a segurança do acervo documental, garantir-se-á, em contra ponto, a própria segurança institucional.

O arquivista, como gestor da informação, assume o papel de proporcionar o acesso aos documentos institucionais. Para que essa função seja cumprida, não basta apenas elaborar meios de difusão das informações, como é o caso dos instrumentos de pesquisa que servem para este fim, há que propor a realização de ações para monitorar as atividades desenvolvidas na instituição no intuito de garantir que ela alcance seus objetivos, assegurando, assim, a qualidade nos serviços prestados. O controle de acesso serve para monitorar quem acede aos documentos e, também, à área reservada ao arquivo, devendo ser uma das medidas prioritárias nas instituições. Pensando nisso, este trabalho traz como tema: Segurança da Informação Arquivística: o Controle de Acesso em Arquivos Públicos Estaduais. A questão segurança da informação por si só é muito abrangente e, desta forma, a pesquisa delimita-se em identificar as ações adotadas para a segurança da informação em Arquivos Públicos Estaduais sob o aspecto do controle de acesso, tendo como referencial os pressupostos teóricos das Normalizações: e-ARQ, ISO 15489 e ABNT NBR ISO/IEC 27002.

# 2 Fundamentação teórica

## 2.1 Os arquivos e a informação arquivística

Os arquivos podem ser definidos tanto como um conjunto de documentos reunidos em decorrência das atividades ou dos fins para os quais foram criados quanto referir-se à instituição que produziu ou acumulou os documentos, sendo, também, responsável pela sua guarda. Pode-se afirmar, então, que "a informação contida no documento de arquivo é resultado da atividade que o produziu. Dessa forma, em um primeiro momento essa informação, por mais abrangente que seja, é vinculada e marcada por essa atividade" (SANTOS, 2007, p. 110).

É a Arquivologia, então, a responsável pela conservação e organização dos documentos de arquivo e, também, da informação arquivística contida neles e preservada nos arquivos. Um dos serviços que devem ser realizados pelos arquivistas, gestores da informação, é garantir o acesso aos usuários. Neste sentido, Brito (2005) salienta que a arquivística faz parte da ciência da informação, sendo considerada como ciência desde que gere conhecimentos que possam ser verificados e, ainda, que a informação arquivística está sendo considerada objeto de estudo da arquivologia em substituição aos documentos de arquivos. Assim, a informação arquivística, como o documento de arquivo, deve ser autêntica e fidedigna, garantindo, dessa maneira, a segurança na transmissão das informações.

## 2.2 Normas relevantes ao estudo

O uso de Normas como e-ARQ, ISO 15489 e ABNT NBR ISO/IEC 27002 podem auxiliar uma instituição na implementação de ações para o controle de acesso. A última norma, mais especificamente, pode contribuir para aplicar e definir uma política de controle de acesso e, também, dar subsídios para a instituição desenvolver uma política completa de segurança da informação.

### 2.2.1 Information and documentation - Records management - ISO 15489-1

A ISO 15489-1, mesmo sendo uma norma estrangeira, é bastante citada e comentada no meio arquivístico, seja em trabalhos ou eventos que abordem a gestão de documentos. O motivo para tamanha referência se dá devido ao fato de ser a primeira Norma ISO elaborada especificamente para a gestão documental. A ISO 15498 é dividida em duas partes, cuja primeira compõe-se pela parte geral, que compreende os requisitos necessários para dar suporte a um sistema de gestão de documentos, e a segunda parte, que abrange as diretrizes necessárias para a aplicação dos princípios citados na primeira.

Na implementação de um programa de gestão documental, segundo a ISO 15489, os documentos de arquivo apresentam as seguintes características: autenticidade, confiabilidade, integridade e disponibilidade. Segundo a Norma, para a implantação de uma política de gestão de documentos que permita gerar documentos autênticos, é fundamental que a instituição esteja consciente de seus recursos, das atividades que desenvolve e de sua responsabilidade perante a sociedade e o usuário do arquivo, seja ele servidor interno ou externo. A respeito da Norma ISO 15489, Barbedo (2004, p. 108) salienta que seu uso é relevante no contexto arquivístico, já que:

> Trata-se de uma ferramenta indispensável para qualquer arquivista que pretenda intervir activamente na gestão documental e logicamente contribuir significativamente para o aumento da eficiência da sua organização, visto dotá-lo com princípios orientadores, fornecendo respostas ao 'ques', ao mesmo tempo que fornece os métodos e ferramentas dando resposta aos 'comos'.

### 2.2.2 Modelo de requisitos para sistemas informatizados de gestão arquivística de documentos - e-ARQ

A primeira parte da norma corresponde aos aspectos teóricos, iniciando com a compreensão do que é gestão de documentos, relatando os procedimentos a serem usados para sua aplicação e os instrumentos que resultam do processo de gestão documental. Segundo o Conselho Nacional de Arquivos (2007, p.1), essa primeira parte "contém cinco

capítulos que tratam da política arquivística, do planejamento e da implantação do programa de gestão arquivística de documentos" e, ainda, dá diretivas que contribuem para controlar o SIGAD. O e-ARQ apresenta um modelo de requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos, objetivando a confiabilidade e o acesso às informações, dando diretivas que auxiliem a realização das funções arquivísticas. Os Sistemas Informatizados de Gestão Arquivística de Documentos (SIGAD) devem ser capazes de gerenciar tanto documentos convencionais quanto digitais. É importante ressaltar que para aplicar o e-ARQ a instituição deve ter implementado um sistema de gestão de documentos, pois ele serve apenas para auxiliar e facilitar a gestão já existente. A especificação e-ARQ apresenta, ainda, um referencial teórico que auxilia para compreensão de termos específicos referentes à gestão de documentos.

Espera-se, como resultado da aplicação da norma, uma gestão eficaz, segura, com documentos confiáveis, acesso rápido e facilitado aos usuários. No Brasil, a gestão eletrônica é menos comum do que nos países mais desenvolvidos, devido aos custos com equipamentos informáticos ou até mesmo pela falta de interesse por parte do governo de investir em tecnologia. A Arquivística, reconhecida atualmente como parte da ciência da informação, lida com a metodologia e as teorias para o tratamento, não somente dos documentos, mas, sim, com a informação contida neles. Além de orientar tecnicamente na prática de ações para gestão de documentos, o e-ARQ orienta teoricamente os seus usuários nos processos arquivísticos que poderão ser realizados.

## 2.2.3Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação – ABNT NBR ISO/IEC 27002

Esta norma é a versão atual da Norma NBR ISO/IEC 17799, elaborada em 2005, que foi atualizada, em julho de 2007, para a numeração NBR ISO/IEC 27002. Baldissera (2007, p. 40) define que a origem da NBR ISO/IEC 17799:

> Remonta de 1987, quando o departamento de comércio e Indústria do Reino Unido (*UK Depertament of Trade and Industry – DTI)*, com a necessidade de criar um plano para proteção das informações do Reino Unido, criou o Centro de Segurança de Computação Comercial *(Commercial Computer Secury Center – CCSC)*. Este centro tinha como uma de suas finalidades, a criação de uma norma de segurança das informações para empresas britânicas. Em 1989 o CCSC criou um guia de segurança para usuários, o PD0003 - um Código de Práticas para Gerenciamento de Segurança da Informação *(a Code of Practice for Information Security Management)*. Após ter sido disponibilizado para consulta pública, foi

> desenvolvido pelo Padrão Britânico *(British Standard)* em 1995, uma versão final deste documento, a BS 7799:1995.

A Norma Britânica sofreu algumas modificações pela Organização Internacional para Normalizações, conhecida como ISO, tornando-se, assim, um padrão internacional. No Brasil, a mesma norma passou a ser denominada ISO/IEC[2] 17799:200. A Associação Brasileira de Normas Técnicas (ABNT) aceitou a norma como sendo padrão nacional. No ano de 2005, surge o Código de Práticas para Gestão da Segurança da Informação, conhecido como: NBR ISO/IEC 17799:2005. Seu objetivo não é criar um modelo para a segurança da informação, mas apenas orientar as ações empregadas para garantir a segurança institucional e documental, disponibilizando diretrizes que ajudem na elaboração de uma política de segurança da informação.

A norma é estruturada em onze seções e cada uma delas contém um número de categorias principais da segurança da informação. Essas categorias contêm um objetivo de controle para definir o que deve ser alcançado e, ainda, um ou mais controles que podem ser aliados a ele para alcançar os objetivos propostos. O uso dessa norma é mais comum em instituições que prezam pela segurança da informação e foi elaborada para aplicação na área de sistemas da informação. Na arquivologia, sua aplicabilidade poderá ser útil ao sistema de gestão documental, já que ela nada mais é do que um código de prática que auxilia na segurança da informação. O objetivo da arquivística é realizar o tratamento documental e informacional, priorizando pela segurança e confiabilidade que será passada aos usuários.

## 2.2 Segurança da informação

Antes de elaborar medidas que garantam a segurança da informação, é necessário que a insituição elabore uma política ou um programa de gestão de documentos. Este programa deve ter como um de seus objetivos dar acesso, ou melhor, tornar acessível os documentos aos usuários. Mas, para isso, é necessário que a instituição esteja atenta aos problemas de segurança que podem ocorrer. Tais problemas acontecem quando há quebra, denominada incidente de segurança da informação, nos princípios que norteiam as ações realizadas nas organizações.

Um sistema de segurança da informação eficiente se baseia em princípios ou características que norteiam seus processos. Segundo a Norma ABNT NBR ISO/IEC 27002, os princípios seriam: confidencialidade, integridade e disponibilidade. A confidencialidade garante que as informações sejam acessíveis somente a pessoas que possuam permissão para acesso na instituição; a integridade proporciona a proteção das

[2] *International Engineering Consortium*.

informações contra modificações, adulterações ou fraudes; e a disponibilidade assegura que os usuários autorizados tenham acesso às informações, quando requisitadas, e elas se mantenham protegidas e não se tornem indisponíveis.

Aliada a esses princípios, pode estar, ainda, a autenticidade, a responsabilidade, o não repúdio e a confiabilidade. As instituições devem ter a responsabilidade e o interesse pelo tratamento das informações, conscientes de que esses princípios que norteiam suas ações para a segurança ajudam a proteger as informações institucionais.

Quando o assunto é segurança, esteja ela referenciada em fontes como revistas, livros ou artigos que abordem o assunto, sempre se relaciona ao termo ativo. Para Campos (2007), o ativo pode ser definido como um bem patrimonial em função do seu valor e, da mesma forma, a informação e tudo aquilo que a suporta e/ou a utiliza são considerados ativos de informação.

A fim de garantir o gerenciamento eficaz e seguro das informações (ativos), faz-se necessário o planejamento de medidas de segurança adotadas como forma de proteger o acesso e garantir a confiabilidade das informações que circulam no meio institucional. Para isso, a adoção de uma política de segurança da informação faz-se necessária nas instituições e depende só do comprometimento, tanto de funcionários quanto de usuários da organização. A implantação dessa política deve surgir "da necessidade de declaração de regras para: o acesso à informação; o uso da tecnologia da organização; e o tratamento, manuseio e proteção de dados e sistemas informacionais" (BALDISSERA, 2007, p. 56).

É necessário ressaltar, ainda, que a política de segurança da informação varia de instituição para instituição, de acordo com os objetivos e as metas de cada organização. Assim sendo, para que se obtenha um resultado efetivo com essa política, é necessária a aplicação de algumas questões técnicas que, muitas vezes, são comuns entre as instituições. Dentre as questões mais aplicadas estão: ver a informação como um bem institucional; possuir um controle de acesso às informações; manter responsabilidades aos usuários, à administração e ao gestor da informação[3]; estar preparados para situações de contingência e garantir a privacidade do usuário; e, por fim, definir medidas disciplinares, caso as regras sejam descumpridas (MEDEIROS, 2001).

## 2.2.1 Controle de acesso

Dentro dos fatores que contribuem para a segurança da informação em uma instituição encontra-se o controle de acesso. As normas de gestão mais recentes já fazem referência a esse requisito, pois, quando adotado de forma eficaz e cuidadosa, pode evitar vários danos à massa documental e à própria instituição. Conforme o Instituto dos Arquivos

[3] Refere-se ao diretor da área responsável pelo uso dos sistemas e serviços de informação.

Nacionais/Torre do Tombo (2002, p.40), o controle de acesso são regras das quais "as organizações têm de poder controlar quem está autorizado a aceder aos documentos de arquivo e em que circunstâncias o acesso é permitido, dado que os documentos podem conter informação pessoal, comercial ou operacionalmente sensível".

Para que o controle de acesso se consolide em uma instituição, é aconselhável que ela elabore, de acordo com suas necessidades, uma política para o controle de acesso, verificando o melhor modo de prevenir acidentes advindos de problemas com as novas tecnologias ou falta de cuidados básicos com a vigilância adotada no arquivo. Para isso, "convém que as regras de controle de acesso e direitos para cada usuário ou grupos de usuários sejam expressas claramente na política de controle de acesso" (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005, p. 56).

A política de controle de acesso é um dos pontos dentro da política da segurança da informação que pode ser elaborada nas instituições para contribuir na proteção das informações. De nada seria válido criar regras se estas não forem devidamente registradas e conhecidas pelas pessoas que trabalham com o tratamento da informação e, também, por aqueles que possuem o direito de acesso a elas. Assim, o controle de acesso tem como finalidade controlar o acesso, de modo a proteger a informação, os sistemas, o equipamento e o ambiente institucional do acesso não autorizado de usuários e/ou funcionários. Aliado a este fim, está a tecnologia da informação, que, conforme Silva e Saldanha (2006, p. 16), tem como objetivo "garantir que as informações estejam disponíveis para usuários e aplicações de maneira eficiente, além de segura".

Com o propósito de preservar a segurança das informações contidas nos documentos, as instituições adotam medidas para monitorar seu acervo. O controle do acesso pode ser feito por meio do cadastro dos usuários (identificador de usuário), crachá de identificação (credenciais de autenticação) ou até mesmo pela restrição do espaço do acervo a uso exclusivo dos funcionários autorizados (autorização de acesso) (CÂMARA TÊCNICA DE DOCUMENTOS ELETRÔNICOS, 2006).

Um assunto relevante que se refere ao controle de acesso é a classificação da informação quanto ao seu grau de sigilo e, também, a restrição de acesso à informação sensível. As instituições devem atentar ao grau de sigilo das informações e redobrar os cuidados quanto ao acesso. Para isso esses documentos devem estar devidamente contemplados na política de controle de acesso da instituição. A respeito disso, a Norma ISO 15489-1, em resumo, relata que as instituições devem criar normas ou regras formalizadas que direcionem as restrições, permissões e condições de acesso às informações. As restrições de acesso devem ser aplicadas tanto aos funcionários quanto a usuários externos e necessitam ser revisadas periodicamente, pois podem variar ao longo do tempo.

Outra medida que deve ser adotada e cuidadosamente planejada nas instituições é o uso e manutenção de senhas para acesso a sistemas. No caso de sistemas que não possuem senhas individuais ou que tenham

senhas de forma conjunta não é possível identificar quem teve acesso às informações. Para que haja a proteção das informações decorrentes do uso de senhas, depende do comprometimento do funcionário e/ou do usuário do sistema. Assim, Campos (2007, p. 186) ressalta que não "adiantará uma senha muito bem elaborada se o colaborador, após fazer o *logon* (digitar o nome de usuário e senha para ter acesso a um sistema) em um determinado sistema, ausentar-se e deixar o computador logado".

Outra situação é a desconexão do terminal por inatividade, um recurso que deve ser utilizado para evitar os riscos à segurança, no caso de informações ou aplicações que estão sendo utilizadas por funcionários e/ou usuários que se ausentem do local, deixando, assim, o computador desprotegido. Este controle é citado na Norma ABNT NBR ISO/IEC 27002, como sendo importante para locais de alto risco, os quais incluem áreas públicas ou externas, fora dos limites do gerenciamento de segurança da organização. Essa norma ainda referencia o controle de acesso não autorizado aos serviços de rede, relatando basicamente sobre os cuidados com o trabalho remoto, observando que o desligamento das seções previne o acesso por pessoas não autorizadas e ataques de negação de serviço.

Concomitantemente com o controle de acesso, uma instituição pode e deve adotar medidas como as cópias de segurança, criptografia e assinatura digital para preservar a autenticidade das informações que serão controladas e protegidas. As cópias de segurança têm por objetivo prevenir a perda e garantir a disponibilidade da informação. A criptografia para a Câmara Técnica de Documentos Eletrônicos (2006, p. 81) "é um método de codificação de objetos digitais segundo um código secreto (chave), de modo que estes não possam ser apresentados por uma aplicação de forma legível ou inteligível e somente usuários autorizados podem restabelecer sua forma original". Já a assinatura digital, em termos técnicos, pode ser conceituada como sendo "o criptograma resultante da cifração de um determinado bloco de dados (*documento*) pela utilização da chave-privada de quem assina em um algoritmo assimétrico" (GUILHERME, 2003, p. 3).

Para a completa proteção de uma organização é, então, relevante a instalação de um sistema de segurança patrimonial, contemplando o uso de câmeras de segurança e sistemas de alarmes, para evitar roubos e controlar a movimentação no arquivo. Nesse sentido, Cassares (2000, p. 23) recomenda que para proteção do acervo "durante o período de fechamento das instituições, a melhor proteção é feita com alarmes e detectores internos". Essa medida, se adotada pelas instituições, evitará possíveis problemas, controlando, assim, a movimentação da instituição, principalmente à noite.

Por fim, o interesse em evitar problemas com a segurança das informações deve partir da própria instituição, seguindo as medidas que melhor atendam às necessidades de segurança, em consonância com a legislação vigente, regulamentos e normas internas estabelecidas pela própria instituição. Para isso, de imediato é necessário a aplicação de

ações simples de controle de acesso e segurança, para posteriormente, e em conjunto com a administração, criar e aplicar uma política que contemple todas estas medidas, garantindo a segurança dos ativos de informação, evitando incidentes.

# 3 Metodologia

O interesse na temática abordada, deu-se devido à importância em proteger a informação para garantir o acesso seguro e contínuo aos documentos. O universo da presente pesquisa é composto por sete (7) Arquivos Públicos Estaduais, tendo como critério uma pesquisa realizada no *site* do CONARQ (Conselho Nacional de Arquivos), procurando por, apenas, Arquivos Públicos Estaduais que tivessem seu *site* acessível e este possuísse um endereço de *e-mail* ou um campo específico para enviar mensagem direta ao arquivo.

Os passos metodológicos aplicados na realização de uma pesquisa definem a sua classificação. Esta pesquisa, especificamente, procura gerar conhecimentos que posteriormente possam ser implantados para melhorar a segurança da informação em arquivos públicos estaduais; portanto, é classificada como uma pesquisa aplicada. Ao abordar conhecimentos arquivísticos, buscando as respostas das indagações propostas e aplicar instrumentos de coleta de dados que poderão ser quantificados e expressos em números, pode-se definir a pesquisa com abordagem qualitativa e quantitativa. A pesquisa assume, ainda, a forma de multicaso, que, segundo Yin (2001), é um método que engloba o estudo de mais de um caso, pois apresenta o estudo em mais de uma instituição pública estadual.

O contato inicial com as instituições deu-se a partir dos *sites* disponíveis para acesso, nos quais foi possível identificar um *e-mail* para contato ou contato direto ao arquivo, através do preenchimento de alguns dados e envio de uma mensagem, na seção Fale Conosco. Só foram considerados válidos para participação na pesquisa os arquivos públicos estaduais que tivessem os endereços eletrônicos (*site*) acessíveis. Após o acesso ao site de cada arquivo, solicitou-se um endereço de *e-mail* da pessoa responsável, sendo ele (a) diretor (a) ou membro da equipe técnica, e, dessa forma, manteve-se contato até obter uma resposta das instituições, totalizando, no mínimo, duas vezes para tentativas de envio de mensagens.

O instrumento selecionado para a coleta de dados foi um questionário baseado em questões sobre o controle de acesso presente nas Normas ISO 15489, e-ARQ e ABNT NBR ISO/IEC 27002. Depois de enviados os questionários, o prazo para respondê-los foi de 18 dias. Para preservar a identidade dos respondentes, adotou-se um código especificado com as iniciais "APE" (fazendo referência a Arquivo Público Estadual), iniciando no número 01 até o número 07 (APE 01 ao APE 07), aleatoriamente, independente da instituição, considerados válidos todos

os questionários reenviados por *e-mail* respondidos e junto o termo de consentimento livre e esclarecido, devidamente aceito pelo responsável.

# 4 Segurança da informação arquivística

Os Arquivos Públicos Estaduais que constituíram esta pesquisa foram: Arquivo Público do Distrito Federal, Arquivo Público do Paraná, Arquivo Público do Estado do Espírito Santo, Arquivo Público Mineiro, Arquivo Público do Estado do Rio Grande do Sul, Arquivo Público do Estado de Santa Catarina e Arquivo Público do Estado de São Paulo.

## 4.1 A Gestão Eletrônica de Documentos (GED) nos arquivos estudados

A segurança de sistemas eletrônicos deve ser redobrada em instituições que utilizam equipamentos informáticos e trocam informações por meio eletrônico. Para isso, antes de elaborar medidas que garantam a segurança da informação é necessário que a instituição elabore uma política ou um programa de gestão de documentos e, dentro desse, um dos objetivos deve ser dar acesso ou tornar acessíveis os documentos aos usuários. Com relação à política de gestão de documentos, Valentim (2008, f. 8) argumenta que ela deve ter como finalidade "o gerenciamento da produção, manutenção e preservação de documentos confiáveis, autênticos e acessíveis, de maneira que possam apoiar as funções, atividades e tarefas organizacionais".

Em primeiro momento será abordada a aplicação de políticas de GED pelas instituições pesquisadas. Essa questão foi levantada pelo fato de que de nada adiantaria estudar o controle de acesso, objetivando proteger as informações, os sistemas, os equipamentos e o ambiente institucional, se as informações não estivessem gerenciadas, seguindo metodologias apropriadas e possibilitando aos usuários o acesso de forma eficiente e segura.

Dessa forma, buscou-se identificar se as instituições possuíam políticas de gestão de documentos implementadas. Desse questionamento, foi possível obter o dado de que apenas uma (1) das instituições não tem políticas de gestão de documentos implementadas, enquanto seis (6) afirmaram que a instituição aplicava essas políticas. Assim, pode-se verificar que seis (6), das sete (7) instituições estudadas, possuem políticas de gestão de documentos, demonstrando, assim, a relevância dos processos de gestão e ações desenvolvidas pelas instituições desde a produção até a destinação final dos documentos, contribuindo para a racionalização e o acesso às informações.

Com a finalidade de averiguar o uso de GED nos arquivos públicos estaduais, foi questionado aos respondentes se a gestão de documentos aplicada nos arquivos abrangia políticas de GED. Foi possível constatar que apenas uma instituição afirmou adotar políticas de GED, sendo que as outras seis não adotam essa técnica, até o presente momento. Sobre este fato, Silva *et al.* (2004) argumenta que para usar a GED não é necessário

que as informações estejam em meio eletrônico, ou seja, um documento em papel pode cumprir seu fim e, posteriormente, se for de interesse da instituição, pode ser arquivado em meio eletrônico. Nesta mesma linha de pensamento, Filipakis (2009) afirma que o uso de sistemas de GED possibilita, além do gerenciamento da informação, o seu controle e armazenamento de forma eficaz, agilizando o fluxo de trabalho e contribuindo para o desempenho institucional. Assim, Flores (2006, p. 89) complementa que a "principal vantagem da GED é a de compartilhar informações em tempo real".

É possível verificar, conforme as colocações dos autores referenciados, os benefícios do uso de GED. Desse modo, procurou-se, então, analisar na concepção das instituições porque não havia a implantação de políticas de GED, solicitando a elas que explicassem o motivo. As respostas mostram o interesse das instituições pela gestão eletrônica ao relatarem as causa pelas quais ainda não foi implantado o sistema. O que é possível verificar no respondente APE 03 quando diz que "está em andamento um estudo sobre a Política de Gestão Eletrônica de Documentos", e no respondente APE 04 que da mesma forma relata que estão trabalhando em um projeto sobre o assunto. Já pela resposta do respondente APE 02, pode-se notar que está em uma fase mais a frente dos outros arquivos, pois relatou que participa de um grupo de estudos que está organizando um projeto para a implantação do documento eletrônico. Para ele, "a base do projeto são os instrumentos arquivísticos produzidos, ou seja, o Plano de Classificação e a Tabela de Temporalidade de Documentos". A resposta do respondente vai ao encontro de Flores (2006, p. 89), ao relatar que "a GED está caracterizada pela categorização documental, tabelas de temporalidade documental, ações de disposição e níveis de segurança".

A dificuldade para a aplicação de políticas de GED para o APE 05 seria relacionada à falta de recursos financeiros, impossibilitando a compra de equipamentos e aplicação de técnicas de GED. Já o (sujeito) APE 07 relata que a maior dificuldade se dá devido à falta de capacitação dos funcionários para esse tipo de atividade, mas destacou: "Estamos em vias de implantação de um novo sistema de Gestão de Protocolo Eletrônico, com o qual entraremos na área de GED". Frente a esses posicionamentos, Rondinelli (2005) afirma que a gestão de documentos eletrônicos representa um desafio para a comunidade arquivística, sendo que, só na década de 90, buscou-se o conhecimento do bom gerenciamento de documentos criados pela tecnologia da informação.

Nessa perspectiva, a segurança da informação no século XXI é algo que as instituições buscam alcançar para preservar a integridade do que será repassado aos usuários. Enfim, pode-se verificar que as instituições pesquisadas mesmo não tendo recursos ou disponibilidade para a aplicação de técnicas de GED, até o momento, se propõem a estudar métodos para sua aplicação futura. Ainda ficou evidente a consciência das instituições quanto à importância dessa técnica para os serviços de gestão arquivística e para o desenvolvimento institucional.

## 4.2 As políticas de controle de acesso nos Arquivos Públicos Estaduais

A informação e tudo aquilo que a suporta e a utiliza são considerados ativos. Para Campos (2007), o ativo pode ser definido como um bem patrimonial em função do seu valor. A proteção dos ativos de informação torna-se fundamental à medida que contribui para evitar um incidente de segurança da informação, que, de acordo com Campos (2007, p. 25), são acontecimentos que podem "causar interrupções ou prejuízos aos processos do negócio, em consequência da violação de um dos princípios de segurança da informação".

Dentre os fatores que contribuem para a segurança da informação em uma instituição encontra-se o controle de acesso. Sua finalidade é basicamente proteger a informação, os sistemas, os equipamentos e o ambiente institucional do acesso não autorizado de usuários e/ou funcionários. Na visão do Instituto dos Arquivos Nacionais/Torre do Tombo (2002, p. 40), o controle de acesso pode ser definido pelo conjunto de regras as quais "as organizações têm de poder controlar quem está autorizado a aceder aos documentos de arquivo e em que circunstâncias o acesso é permitido [...]".

O segundo conjunto de perguntas abordou questões relativas ao controle de acesso, com o intuito de verificar como as instituições realizam as ações para monitorar o acesso às informações e a proteger sua segurança e integridade. Para isso, objetivou averiguar se os respondentes consideravam a existência de uma política de controle de acesso na instituição. Verificou-se que seis (6) dos respondentes afirmaram que a instituição possui uma política de controle de acesso e apenas um (1) respondeu que não existe essa política.

A respeito do controle de acesso, a Associação Brasileira de Normas Técnicas (2005, p. 56) ressalta que "convém que as regras de controle de acesso e direitos para cada usuário ou grupos de usuários sejam expressas claramente na política de controle de acesso". A política de controle de acesso é um dos pontos, dentro da política da segurança da informação, que pode ser elaborada nas instituições para contribuir na proteção das informações. No entanto, a ABNT NBR ISO/IEC 27002 define que essa política deve ser estabelecida, documentada e analisada criticamente, tomando-se como base os requisitos de acesso dos negócios e segurança da informação. Assim, é relevante destacar que não basta às instituições elaborarem uma política de controle de acesso, se esta não for devidamente registrada e, sobretudo, conhecida pelas pessoas que trabalham com o tratamento da informação e, também, por aqueles que possuem o direito de acesso a ela.

Nesse sentido, foi solicitado aos respondentes, que afirmaram que a instituição possuía uma política de controle de acesso, que descrevessem como era o funcionamento, para assim compreender a política adotada em cada arquivo. As respostas variaram de acordo com a política seguida em cada instituição em estudo, sendo as respostas bem diversificadas.

O respondente APE 01 apenas relata os procedimentos de acesso à pesquisa do acervo documental. Na descrição do APE 02, são apresentados os procedimentos para restrição de acesso, já que afirma que alguns documentos possuem restrição de acesso, conforme legislação. O respondente APE 03 descreveu que o usuário inicialmente é cadastrado em um sistema informatizado e orientado a respeito das normas internas de acesso, mas não citou quais seriam essas normas. Já o respondente APE 04 afirma que o arquivo disponibiliza, em meio eletrônico, o guia de fundos de um dos acervos. O respondente APE 06 foi bem sucinto, deixando a entender que ela funciona baseada na "localização topográfica e guia de acervo utilizando os campos da Norma Brasileira de Descrição Arquivística", não explicando como é realizado o controle de acesso, efetivamente. O último respondente a ser citado, o APE 05, descreveu que a política de controle de acesso aplicada na instituição segue como determinação que os documentos são de acesso livre ao público, "com exceção das que, por questão de sigilo, ainda necessitem ter acesso restrito".

É imprescindível salientar, ainda, que um ponto relevante presente na política de controle de acesso de algumas instituições é referente à classificação da informação quanto ao grau de sigilo e restrição de acesso à informação sensível, que foi citado também pelos respondentes APE 01, APE 02 e o APE 05. As outras instituições também devem estar atentas ao grau de sigilo das informações e redobrar os cuidados quanto ao acesso. Elas devem subordinar-se a esses graus de sigilo e também conhecer e aplicar as determinações legais, visando à disponibilidade das informações para atender as necessidades dos usuários de arquivo. Os documentos de acesso restrito, se ainda não estão presentes, devem estar devidamente contemplados na política de controle de acesso das instituições pesquisadas.

A respeito disso, a Norma ISO 15489-1, em resumo, ressalta que as instituições devem criar normas ou regras formalizadas que direcionem as restrições, permissões e condições de acesso às informações. As restrições de acesso devem ser aplicadas tanto aos funcionários quanto a usuários externos e necessitam ser revisadas periodicamente, pois podem variar ao longo do tempo. Nesse sentido, é relevante fazer menção ao Decreto Nº. 4.553, de 27 de dezembro de 2002, que determina a preservação de dados, informações, documentos e materiais sigilosos, sendo que os últimos possuem acesso restrito. Essa lei define que os documentos podem ser classificados em "ultra-secretos, secretos, confidenciais e reservados" (BRASIL, 2002, art. 5º).

Conforme pode ser observado, alguns respondentes fizeram referência também ao uso de regras e normas internas para acesso aos documentos, sendo essas de conhecimento do usuário, para que este esteja ciente de suas responsabilidades. A política de controle de acesso deve ser embasada em normas que a definam e deem um direcionamento às ações implementadas na instituição.

## 4.3 As ações de controle de acesso comuns entre as instituições pesquisadas

Neste subcapítulo, serão abordadas as medidas de controle de acesso que são realizadas nas instituições em estudo, tendo como base teórica e metodológica as normas ISO 15489, e-ARQ e ABNT NBR ISO/IEC 27002. Após compreender as medidas adotadas nos arquivos, seguindo as questões pesquisadas e relatadas pelos respondentes, foi possível definir entre as ações aplicadas para o controle de acesso quais são comuns nos arquivos públicos estaduais estudados.

A fim de se conhecer as ações realizadas para o controle de acesso nos arquivos pesquisados, o último questionamento trouxe como opções aos respondentes algumas medidas referenciadas nas normas em estudo, principalmente na ABNT NBR ISO/IEC 27002 e na e-ARQ, para que eles pudessem selecionar as que eram aplicadas de acordo com a realidade de cada instituição. Como algumas medidas para controle de acesso podem ser realizadas tanto para usuários de arquivo quanto para funcionários das instituições, foram dadas as duas opções de respostas aos respondentes, dependendo da medida que estava sendo referenciada na questão.

As opções de resposta para esta questão foram: cadastro de usuários de arquivo; uso de identificador (ID único), circuito interno de vídeo; sistema de alarmes; criptografia; cópias de segurança; assinaturas digitais; senha individual de acesso ao sistema operacional: por usuários e/ou por funcionários; uso de credenciais de identificação: por usuários e/ou por funcionários; bloqueio de *sites* não autorizados: por usuários e/ou por funcionários; desconexão do terminal por inatividade: por usuários e/ou por funcionários; autorização para uso de rede sem fio: por usuários e/ou por funcionários; e outras.

Para melhor expor os resultados, foram somados os números de citações dos respondentes totalizando 34, já que na questão poderia marcar mais de uma opção. A medida mais referenciada pelos respondentes foi o cadastro de usuários de arquivo, com seis citações; logo após foi a medida uso de credenciais de identificação, por funcionários, com cinco citações; a seguir, as cópias de segurança e o bloqueio de *site* não autorizados, por funcionários, com quatro citações, e com três citações apareceu o bloqueio de *sites* não autorizados, por usuários.

As opções que tiveram duas citações foram: senha individual de acesso ao sistema operacional, por funcionário; uso de credenciais de identificação, por usuário; autorização para uso de rede sem fio, por funcionário; e a opção Outros. As opções que foram referenciadas por apenas um (1) respondente foram: circuito interno de vídeo; sistema de alarmes; desconexão do terminal por inatividade, por usuário; e autorização para uso de rede sem fio, por usuário. As medidas de controle

de acesso que não são adotadas nos arquivos estudados são: não há controle; uso de identificador de usuário; criptografia; assinaturas digitais; senha individual de acesso ao sistema operacional, por usuário; Desconexão do terminal por inatividade, por funcionário.

No que se trata a opção "Outras", foram encontradas respostas dos seguintes respondentes: APE 02 e APE 03. Para esses sujeitos pesquisados, a instituição realizava outra medida além das citadas no instrumento de coleta de dados. O APE 02 afirmou que o arquivo possui um livro de registro na portaria para usuários quem vão ao arquivo para reuniões e eventos. Esse livro é o controle que o arquivo utiliza como forma de identificar quem visita a instituição, sendo mais uma das ações realizadas para controle de acesso dentro política institucional.

Para o informante APE 03, o "acesso ao acervo digital está condicionado mediante apresentação de documento de identidade", após isso é criado um *login* de acesso para o usuário e emitido um termo de responsabilidade. Esse arquivo realiza o controle da documentação digital com a elaboração desse *login,* que deve ter para o acesso uma senha individual, pela qual o usuário é responsável por suas ações frente ao sistema, podendo ser identificado caso realize alguma ação indevida.

Mostra-se relevante ressaltar que as ações de controle de acesso comuns para fins de análise desta pesquisa foram consideradas aquelas que, por meio da questão anterior, são realizadas por mais de uma instituição. A finalidade do controle de acesso é basicamente proteger a informação, os sistemas, os equipamentos e o ambiente institucional do acesso não autorizado de usuários e/ou funcionários. Dentre as ações comuns entre os respondentes, foi citado o cadastro dos usuários do arquivo e o uso de credenciais de identificação por usuários e por funcionários, que são os controles principais em arquivos para estabelecer o registro dos usuários e também como forma de identificá-los, proporcionando uma medida de segurança para o arquivo.

O controle do acesso, de acordo com a Norma e-ARQ, pode ser realizado por meio do cadastro dos usuários (um identificador de usuário), crachá de identificação (uso de credenciais de autenticação) ou por autorizações para acesso. As instituições pesquisadas, em questões anteriores, não citaram o uso da e-ARQ como referência para a política de controle de acesso implementada na instituição, no caso das instituições que possuem uma política de controle de acesso. Ainda assim, estabelecem os requisitos presentes na norma referente ao cadastro de usuários e o uso de credenciais de identificação.

As cópias de segurança podem ser consideradas medidas complementares ao controle de acesso, já que proporcionam a preservação e a autenticidade das informações que serão controladas, tendo por objetivo prevenir a perda, e garantir a disponibilidade da informação. A Norma ABNT NBR ISO/IEC 27002, no capítulo dez, faz referência às cópias de segurança, cujo objetivo é manter a integridade e disponibilidade à informação. Essas cópias de segurança aparecem entre as ações comuns para o controle de acesso nos arquivos pesquisados devido à conscientização de que as informações devem estar sempre

disponíveis para acesso dos usuários, cumprindo seu fim dentro da instituição.

Os arquivos públicos estaduais pesquisados demonstraram a preocupação com a segurança institucional por meio da aplicação de ações de controle de acesso. Esse fato foi evidenciado, pois várias medidas realizadas para o controle de acesso se repetiram conforme foi possível verificar. Dessa forma, o resultado da pesquisa vai ao encontro de Fontes (2008, p. 206), quando salienta que "identificação individual, controle de senhas, acesso à informação confidencial e cópias de segurança são as primeiras preocupações da organização e, consequentemente, são os primeiros controles a serem desenvolvidos".

As duas últimas medidas consideradas comuns entre as instituições são o bloqueio de *sites* não autorizados, por usuário e por funcionários; e a autorização para uso de rede sem fio, por funcionário. Sendo relevante destacar que essas duas ações são complementares, pois, dentro do controle de acesso a serviços de rede, é relevante que sejam adotadas medidas para controlar tanto o acesso à rede sem fio, como também definir se há necessidade de bloquear *site* que a instituição não autorize o acesso, por considerar indevido. A instituição deve autorizar acesso às redes sem fio apenas a pessoas que, de acordo com a política de segurança institucional, não representem risco para a segurança e proteção das informações.

Para finalizar, é relevante destacar, ainda, que as ações de controle de acesso consideradas comuns entre os arquivos estudados só serão eficazes para proteger as informações, os equipamentos e o ambi institucional se aliadas ao comprometimento das instituições co aplicação e avaliação permanente de regras e normas de segurança e frente, também, ao comprometimento dos usuários em cumpri-las.

# 5 Conclusões

As conclusões apresentadas neste capítulo buscam sintetizar as respostas que basicamente foram propostas nos questionamentos desta pesquisa. Cabe registrar que, para este trabalho, buscou-se analisar a teoria arquivística a respeito do tema de pesquisa e usar, também, como referencial teórico as Normas ISO 15489, e-ARQ e a ABNT NBR ISO/IEC 27002. Dessa forma, foi possível conhecer os procedimentos existentes para aplicação do controle de acesso e, assim, verificar e identificar quais ações eram realizadas pelos Arquivos Púbicos Estaduais pesquisados.

Primeiramente, foi investigada a aplicação de políticas de Gestão Eletrônica de Documentos (GED) nos arquivos estudados, pois de nada adiantaria estudar o controle de acesso, objetivando proteger as informações, os sistemas, o equipamento e o ambiente institucional, se as informações não estivessem gerenciadas de forma eficiente, além de segura. As instituições, em sua maioria, adotam políticas de Gestão de Documentos, no entanto, essas políticas não abrangem a GED. Segundo os próprios respondentes, isso ocorre devido a fatores como falta de

recursos financeiros e falta de capacitação dos funcionários para exercer esse tipo de atividade.

Apesar dessas dificuldades, foi possível verificar que há um interesse por parte das instituições em implementar políticas de GED. Esse fato ficou visível, já que a maioria dos respondentes relatou que está realizando um estudo sobre o assunto para possível aplicação. Esse fato denota a consciência que os Arquivos Públicos Estaduais possuem quanto à relevância dessa técnica para os serviços de gestão arquivística.

Com base no estudo realizado, ficou evidenciado que há uma política de controle de acesso presente nos arquivos públicos estudados. Vale aqui ressaltar que apenas um respondente afirmou que o arquivo não possuía uma política para controle de acesso e, mesmo assim, essa instituição realiza ações para controle de acesso e preocupa-se com a proteção das informações que serão repassadas aos usuários, baseando-se no que foi possível verificar. A política de controle de acesso é um dos pontos dentro da política da segurança da informação que deve ser planejada e implementada nas instituições para contribuir para a proteção das informações.

Além dessa política de controle de acesso, as instituições realizam outras ações no intuito de garantir a segurança das informações. As ações referem-se ao controle de acesso às informações, aos equipamentos e ao ambiente institucional. A finalidade principal de verificar as medidas adotadas era comparar aquelas que se repetiam em mais de uma instituição, a fim de observar quais ações eram primordiais nos arquivos para, assim, proteger a segurança das informações por meio do controle de acesso.

A pesquisa indicou que as ações realizadas para o controle de acesso comum nos arquivos públicos estaduais são: cadastro dos usuários de arquivo; uso de credenciais de identificação, por usuário e por funcionário; cópias de segurança; senha individual de acesso ao sistema operacional, por funcionário; bloqueio de *sites* não autorizados, por usuário e por funcionário; e autorização para uso de rede sem fio, por funcionário.

Em relação às medidas de controle de acesso, pode-se concluir que os arquivos preocupam-se com a segurança das informações, visto que aplicam medidas no intuito de proteger as informações. As ações que podem ser consideradas simples, como o cadastro de usuários e o uso de credenciais para identificação, são relevantes para identificar o usuário de arquivo e, também, diferenciá-lo do funcionário da instituição. Os arquivos, mesmo que a maioria não possua políticas de GED, evidenciam a preocupação com sistemas informatizados. A realização da prática de cópias de segurança para garantir a continuidade da informação, o monitoramento do acesso a *site*, ou seja, o bloqueio de *sites* não autorizados e o procedimento de autorizar uso de redes sem fio à somente funcionários da instituição são medidas que confirmam esse cuidado.

É relevante destacar que não adianta as instituições apenas elaborarem regras se estas não forem devidamente registradas e

conhecidas pelas pessoas que trabalham com o tratamento da informação e, também, por aqueles que possuem o direito de acesso a elas. Os resultados obtidos salientam a importância da definição dessa política de controle de acesso nos arquivos públicos estaduais, embasada em regulamentos, normas e legislação que abordem as ações de controle de acesso que já são realizadas nas instituições e que seja complementada por outras ações, objetivando reforçar e proteger, ainda mais, a segurança das informações públicas.

Dessa forma, recomenda-se que as instituições busquem o embasamento teórico e metodológico de normas como a ISO 15489 e a e-ARQ, que dão subsídios para implantação de um sistema de gestão de documentos e, ainda, abordam diretivas sobre o controle de acesso para elaborar e melhorar sua política de controle de acesso. Também, as instituições podem usar os requisitos e as definições da Norma ABNT NBR ISO/IEC 27002, que é mais ampla, abordando uma completa política de segurança da informação, incluindo o controle de acesso.

## Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO/IEC27002:* tecnologia da informação - técnicas de segurança - código de prática para a gestão da segurança da informação, 2005. Conteúdo técnico idêntico ao da ABNT NBR ISO/IEC 17799.

BALDISSERA, T. A. Gestão da segurança da informação em colégio: uma análise da utilização da Norma NBR/IEC 17799. 119 f. Dissertação (Mestre em Engenharia da Produção) - Universidade Federal de Santa Maria, UFSM, 2007.

BARBEDO, F. Leituras: Norma 15489:2001, information and documentation – records management. *Cadernos BAD,* n. 2, 2004. Disponível em: <http://www.apbad.pt/ CadernosBAD/Caderno22004/LeiturasBAD204.pdf>. Acesso em: 18 nov. 2009.

BRASIL. Conselho Nacional de Arquivos. Decreto nº 4.553, de 27 de dezembro de 2002. Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências. *Diário Oficial*, 30 dez. 2002. p. 6.

BRITO, D. M. de. A informação arquivística na arquivologia pós-custodial. *Arquivística.net*, Rio de Janeiro, v. 1, n. 1, p. 31-50, jan./jun. 2005. Disponível em: <www.arquivistica.net>. Acesso em: 15 maio 2008.

CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS. *Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos:* e-ARQ. Rio de Janeiro: Conarq, 2006. Disponível em: <http://www.conarq.arquivonacional.gov.br/Media/publicacoes/ earqbrasilv1. pdf>. Acesso em: 9 out. 2007.

CAMPOS, A. Sistema de segurança da informação: controlando os riscos. 2. ed. Florianópolis: Visual Books, 2007.

CASSARES, N. C.; MOI, C. *Como fazer conservação preventiva em arquivos e bibliotecas*. São Paulo: Arquivo do Estado; Imprensa Oficial, 2000.

FILIPAKIS, C. Gestão eletrônica de documentos científicos. Tocantins: Centro Universitário Luterano de Palmas, 2009. Disponível em: <http://www.ulbra-to.br/Noticias/Gestao-Eletronica-de-Documentos-Cientificos.aspx>. Acesso em: 2 jun. 2010.

FLORES, D. *A gestão eletrônica de documentos (GED) e o impacto das políticas de software livre:* uma perspectiva "transdisciplinar", comparada nos arquivos do Brasil e Espanha. 538 f. Tese (Doutorado em Documentação) - Universidad de Salamanca, 2006.

fontes, E. L. G. *Praticando a segurança da informação*. Rio de Janeiro: Brasport, 2008.

GUILHERME, J. *Criptografia, chaves públicas e assinatura digital para leigos.* [S.l: s.n.], 2003. Disponível em: <*www.sbis.org.br/Criptografia.doc*>. *Acesso em: 19 maio 2010.*

INSTITUTO DOS ARQUIVOS NACIONAIS/TORRE DO TOMBO. *Caderno de Recomendações para gestão de documentos de arquivo electrónicos:* modelo de requisitos para gestão de arquivos electrónicos (MoReq). Lisboa: [s.n.], 2002. Disponível em: <http://www.iantt.pt>. Acesso em: 21 nov. 2007.

MEDEIROS, C. D. R. *Segurança da informação:* implantação de medidas e ferramentas de segurança da informação. Joinville: Universidade da Região de Joinville – INIVI; Departamento de Informática, 2001. Disponível em: <http://www.linuxsecurity.com.br/info/general/TCE_Seguranca_da_Informacao.pdf>. Acesso em: 24 maio 2010.

RODRIGUES, A. C. *Diplomática contemporânea como fundamento metodológico da identificação de tipologia documental em arquivos. 258 f.* Tese (Doutorado em História Social) - Universidade de São Paulo, São Paulo, 2008. Disponível em: <http://www.asocarchi.cl/DOCS/134.PDF>. Acesso em: 7 nov. 2009.

RONDINELLI, R. C. *Gerenciamento arquivístico de documentos eletrônicos:* uma abordagem teórica da diplomática arquivística contemporânea. Rio de Janeiro: Editora FGV, 2005.

SANTOS, V. B. dos. *Gestão de documentos eletrônicos:* uma visão arquivística. Brasília: ABARQ, 2005.

SILVA, A. T. S. da; SALDANHA, H. V. *Controle de acesso baseado em papéis na informatização de processos judiciais.* 66 f. Monografia (Bacharelado em Ciência da Computação) - Universidade de Brasília (UnB), Brasília, 2006.

SILVA, D. P. da *et al. GED – gerenciamento eletrônico de documentos:* a tecnologia que está mudando o mundo. Faculdade de Administração e Informática, 2004. Disponível em: <http://www.curitiba.arquivar.com.br/espaco_profissional/sala_leitura/artigos/GED_Gerenciamento_Eletronico_de_Documentos.pdf>. Acesso em: 7 jun. 2010.

YIN, R. K. *Estudo de caso:* planejamento e métodos. Porto Alegre: Bookman, 2001.