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

SEGURANÇA DA INFORMAÇÃO ARQUIVÍSTICA: O CONTROLE DE ACESSO EM ARQUIVOS PÚBLICOS ESTADUAIS

MONOGRAFIA DE ESPECIALIZAÇÃO

Josiane Ayres Sfreddo

São João do Polêsine, RS, Brasil

2010

SEGURANÇA DA INFORMAÇÃO ARQUIVÍSTICA: O CONTROLE DE ACESSO EM ARQUIVOS PÚBLICOS ESTADUAIS

por

Josiane Ayres Sfreddo

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

Orientador: Profº. Dr. Daniel Flores

São João do Polêsine, RS, Brasil
2010

Universidade Federal de Santa Maria
Universidade Aberta do Brasil
Centro de Ciências Sociais e Humanas
Curso de Pós-Graduação a Distância
Especialização *Lato-Sensu* em Gestão em Arquivos

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

SEGURANÇA DA INFORMAÇÃO ARQUIVÍSTICA: O CONTROLE DE ACESSO EM ARQUIVOS PÚBLICOS ESTADUAIS

elaborada por
Josiane Ayres Sfreddo

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

COMISSÃO EXAMINADORA:

Daniel Flores, Dr.
(Presidente/Orientador)

Rosani Beatriz Pivetta da Silva, Ms. (UFSM)

Sônia Elisabete Constante, Ms. (UFSM)

São João do Polêsine, 10 de julho de 2010.

Aos meus pais, Hermes Sfreddo e Rosane Ayres Sfreddo pela dedicação e amor constantes, e por me fazerem acreditar que apesar das dificuldades que enfrentamos nessa vida devemos lutar pela realização de nossos sonhos, pois sempre vale à pena.

AGRADECIMENTOS

Agradeço primeiramente os meus familiares pelo incentivo e por todos os momentos em que não pude dar atenção e carinho de que são merecedores.

Ao Prof. Dr. Daniel Flores, orientador desta monografia, por todo empenho, sabedoria, compreensão e exigência.

À coordenadora do Curso de Pós-Graduação a Distância em Gestão em Arquivos, Profª. Denise Molon Castanho, por sempre me incentivar na busca do crescimento, sendo exemplo de competência e determinação.

Agradeço também respectivamente aos Arquivos Públicos: Mineiro, do Distrito Federal, do Paraná, do Estado do Rio Grande do Sul, do Estado de São Paulo, do Estado de Santa Catarina, e do Estado do Espírito Santo, pela colaboração, disponibilidade e compreensão da relevância da pesquisa realizada.

Por fim, a todas as pessoas que, direta ou indiretamente, contribuíram para a execução desta pesquisa.

RESUMO

Monografia de Especialização
Curso de Pós-Graduação a Distância
Especialização *Lato-Sensu* em Gestão em Arquivos
Universidade Aberta do Brasil
Universidade Federal de Santa Maria

SEGURANÇA DA INFORMAÇÃO ARQUIVÍSTICA: O CONTROLE DE ACESSO EM ARQUIVOS PÚBLICOS ESTADUAIS

AUTORA: JOSIANE AYRES SFREDDO
ORIENTADOR: PROF. DR. DANIEL FLORES
Data e Local da Defesa: São João do Polêsine/RS, 10 de julho de 2010.

Este trabalho apresenta uma investigação científica baseada no estudo a respeito das políticas de controle de acesso adotadas em Arquivos Públicos Estaduais. Para isso, busca 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 os arquivos preocupam-se com a segurança da informação que será repassada aos usuários. Os resultados obtidos salientam a importância da definição da 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 e ainda fundamentadas em outras ações que poderão ser implementadas objetivando reforçar e proteger, ainda mais, a segurança das informações públicas.

Palavras-chave: Controle de acesso. Segurança da informação arquivística. Arquivos públicos estaduais.

ABSTRACT

Monografia de Especialização
Curso de Pós-Graduação a Distância
Especialização *Lato-Sensu* em Gestão em Arquivos
Universidade Aberta do Brasil
Universidade Federal de Santa Maria

SEGURANÇA DA INFORMAÇÃO ARQUIVÍSTICA: O CONTROLE DE ACESSO EM ARQUIVOS PÚBLICOS ESTADUAIS

SECURITY OF ARCHIVAL INFORMATION: THE ACCESS CONTROL IN STATE PUBLIC FILES

AUTHOR: JOSIANE AYRES SFREDDO
ADVISER: PROF. DR. DANIEL FLORES
Data e Local da Defesa: São João do Polêsine/RS, 10 de julho de 2010.

This paper 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 files are concerned about the security of information that will be passed on the users. The results underline the importance of defining of access control policy in the state public archives, based on regulations, standards and legislation that address the access control actions already undertaken and still reasoned on the other actions that could be implemented aiming at reinforce and protect, even more, the security of public information.

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

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE GRÁFICOS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT - Associação Brasileira de Normas Técnicas

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

APERS - Arquivo Público do Estado do Rio Grande do Sul

APM - Arquivo Público Mineiro

ArPDF – Arquivo Público do Distrito Federal

CONARQ - Conselho Nacional de Arquivos

e-ARQ, - Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos

GED - Gestão Eletrônica de Documentos

ISAD (G) - G*eneral International Standard Archival Description*

ISO 15489-1 - *Information and documentation - Records management* -

NOBRADE - Norma Brasileira de Descrição Arquivística

SIARQ/RS - Sistema de Arquivo do Estado do Rio Grande do Sul

SIGAD - Sistemas Informatizados de Gestão Arquivística de Documentos

SINAR - Sistema Nacional de Arquivos

TI - Tecnologia da Informação

LISTA DE APÊNDICES

SUMÁRIO

1 INTRODUÇÃO

Nos dias atuais a informação assume uma importância crescente dentro das instituições, tornando-se fundamental somada à descoberta e a introdução de novas tecnologias, oportunidades de negócios e a 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. A metodologia arquivística dá subsídios para a organização documental. Ao adotar uma metodologia baseada em procedimentos que garantam a gestão documental resultando no bom funcionamento institucional, evidencia 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, a instituição, em contraponto, garantirá a segurança da instituição arquivo.

O predomínio do uso de computadores e a troca de informações através das mensagens eletrônicas aliadas a rapidez de comunicação *on-line*, assume relevância no contexto institucional. Os documentos resultantes destes processos podem ser considerados documentos arquivísticos à medida que sejam produzidos no contexto institucional, comprovando atividades administrativas, ou legais realizadas nas instituições.

A tecnologia aliada à metodologia arquivística trouxe benefícios para a gestão de documentos arquivísticos, agilizando os processos e proporcionando rápida recuperação das informações. A criação, uso e tramitação de informações públicas onde as atividades são realizadas em computadores públicos, carecem de tratamento mais cuidadoso para assegurar a confiabilidade e a disseminação das informações de forma segura aos diversos tipos de usuários.

O arquivista como gestor da informação, assume o papel de proporcionar o acesso aos documentos institucionais. Para que esta 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. Além disso, ele deve propor a realização de ações para monitorar as atividades desenvolvidas na instituição no intuito de garantir que a instituição alcance seus objetivos assegurando a qualidade nos serviços prestados. Dessa forma, a adoção de ações para a segurança em instituições arquivísticas é fundamental para preservar e garantir a integridade do patrimônio documental e material.

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 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.

Este estudo está estruturado em seis capítulos, sendo o primeiro capítulo correspondente a introdução e suas subdivisões apresentando os objetivos, justificativas e pergunta de pesquisa. O segundo capítulo aborda os conceitos relacionados aos arquivos e a informação arquivística, gestão de documentos, análise de normas relevantes ao estudo, segurança da informação e controle de acesso. No terceiro capítulo é apresentada a metodologia adotada para a realização da pesquisa. Algumas colocações sobre o histórico e atividades desenvolvidas pelas instituições pesquisadas, são apresentadas no quarto capítulo. O quinto capítulo, por sua vez, apresenta a análise e discussão dos resultados, relacionando os objetivos propostos na pesquisa com os resultados obtidos da coleta de dados. No sexto capítulo, são relatadas as considerações finais de pesquisa. E por fim, são apresentadas as referências utilizadas para a construção desta investigação.

1.1 Justificativa

O avanço tecnológico pode proporcionar modificações na vida das pessoas, em decorrência da evolução da tecnologia e do uso de novos equipamentos. Nesse contexto de evolução tecnológica, é imprescindível que as instituições preocupem-se também, de alguma forma, com a segurança das informações que circulam em diversos meios como a internet,

cujo acesso é fácil a qualquer hora e em qualquer lugar. Assim, torna-se fundamental o domínio da informática, o uso de programas informatizados para auxiliar nos processos gestão da informação, e ainda, empregar medidas que reforcem a segurança das informações que serão repassadas no meio institucional.

O controle de acesso é um dos fatores empregados no intuito de garantir a segurança da informação, seu estudo determinará medidas a serem implementadas proporcionando a segurança das instituições contra possíveis furtos materiais e documentais. A presente pesquisa dará continuidade a uma investigação sobre o controle de acesso, de mesma autoria deste, para obtenção do título de Bacharel em Arquivologia, no ano de 2008, que teve como tema: “O Controle de acesso na percepção dos profissionais de arquivo: uma questão de segurança das informações institucionais”. O tema de pesquisa tornou-se relevante à medida que a falsificação documental, os furtos e a violência preocupam os profissionais arquivistas, já que os assaltos a patrimônios documentais apresentam-se cada vez mais frequentes nos dias atuais.

Esta pesquisa justifica-se ainda pela sua relevância prática e teórica. A primeira possibilitará o contato com diferentes instituições arquivística do Brasil, compartilhando experiências que contribuirão para que outras instituições aprimorem os métodos usados no controle de acesso, garantindo a segurança da informação. Já a relevância teórica justifica-se por proporcionar uma reflexão a respeito do controle de acesso como ação empregada para a segurança da informação. O tema de estudo possui pouca bibliografia que a subsidie, por isso Normas ISO 15489-1, e-ARQ e a ABNT NBR ISO/IEC 27002, resultam de estudos da base teórica presente que servem para implantar sistemas mais seguros de informação arquivística assegurando a confiabilidade no acesso aos documentos.

1.2 Objetivos

1.2.1 Objetivo Geral

Identificar quais as ações adotadas para o controle do acesso documental em Arquivo Públicos Estaduais, no intuito de garantir a segurança das informações.

1.2.2 Objetivos Específicos

- identificar se há aplicação da gestão eletrônica de documentos (GED) nos arquivos estudados;

- realizar o levantamento das políticas de controle de acesso utilizadas nos arquivos públicos estaduais;

- conhecer as ações de controle de acesso comuns entre as instituições pesquisadas.

1.3 Problema de Pesquisa

Quais as ações adotadas para controlar o acesso documental em sete (7) Arquivos Públicos Estaduais, no intuito de garantir a segurança das informações públicas?

A revisão da bibliografia, apresentada no segundo capítulo, serve como forma de explicitar o tema proposto através da compilação de teorias, estudos e autores relevantes para a compreensão e desenvolvimento da pesquisa.

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 fim que foram criados quanto, referir-se à instituição que produziu ou acumulou os documentos sendo, também, responsável pela sua guarda. Neste sentido "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).

A importância dos arquivos pode ser verificada por Richter (2004, p. 41) quando remonta a criação dos arquivos de estado afirmando que "os arquivos significavam direitos para os soberanos, para os feudistas e para os juristas. Todos os estados desejavam controlar os arquivos e nas conquistas territoriais eram valorizados como um bem precioso".

A Arquivologia é responsável pela conservação e organização dos documentos como, 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. Brito (2005) salienta que a arquivística faz parte da ciência da informação, sendo considerada como ciência desde que gere conhecimentos que possam ser verificados. O autor ainda relata, por meio do resultado de uma pesquisa, que a informação arquivística está sendo considerada objeto de estudo da arquivologia em substituição aos documentos de arquivos.

A informação arquivística, como o documento de arquivo, deve ser autêntica e fidedigna garantindo, assim a segurança na transmissão das informações. A diplomática é a ciência que estuda a estrutura formal dos documentos e "estuda as partes que compõem os documentos produzidos por entidades públicas e privadas no desempenho de suas funções, com fins de crítica sobre a autenticidade." (RICHTER, 2004, p. 87).

A diplomática assume uma nova visão em relação aos seus estudos, direcionando-os a contextualização das atividades e funções desenvolvidas em uma instituição, ou seja, estando mais ligada a gestão de documentos. Esse desenvolvimento da diplomática, denominada, "diplomática contemporânea é uma área nova, produto de uma revisão do desenvolvimento e

da atualização dos princípios formulados pela diplomática clássica.” (RODRIGUES, 2008, p. 152).

2.1.1 Políticas públicas arquivísticas

As políticas públicas arquivísticas constituem uma das dimensões das políticas públicas informacionais. No Brasil a política nacional de arquivos sugere diversas questões à pesquisa em Ciência da Informação. O Conselho Nacional de Arquivos – CONARQ (órgão colegiado e vinculado ao Arquivo Nacional da Casa Civil da Presidência da República) foi criado em 1991, incumbido de definir uma política nacional de arquivos e atuar como órgão central de um Sistema Nacional de Arquivos - SINAR.

No entanto, uma declaração por si só não garante uma boa gestão arquivística de documentos. Para que a implantação de uma política arquivística contribua para atingir os objetivos de uma instituição é fundamental o comprometimento da administração com investimento de recursos que possibilitem as atividades de gestão. Para a adoção de políticas arquivísticas, uma instituição deve ter um embasamento teórico amplo, reconhecer suas atividades, os documentos que produz e o contexto que eles são criados. (SFREDDO, 2008).

Para dar início à construção desta política, a instituição deve declarar oficialmente suas intenções quanto à adoção de métodos e estratégias para a gestão de documentos. Segundo a Câmara Técnica de Documentos Eletrônicos (2006, p. 15) “a declaração pode incluir as linhas gerais do programa de gestão, bem como os procedimentos necessários para que essas intenções sejam alcançadas. Deve também ser comunicada e implementada em todos os níveis dos órgãos e entidades.”

Uma política arquivística eficaz é aquela que atende as necessidades institucionais referentes ao acesso, recuperação, conservação e todos os outros processos realizados desde a produção até a destinação final dos documentos. Além disso, é necessário que os funcionários estejam conscientes das suas responsabilidades para que o tratamento documental seja fluído de acordo com a designação de cada membro da equipe.

Desde sua criação, o CONARQ desenvolve diversas ações referentes à gestão documental. No entanto, não existe legalmente uma política nacional de arquivos. A sua

ausência em nível nacional acarreta, também, dificuldades no desenvolvimento de atividades realizadas pelo Estado. Com a criação de uma política pública arquivística, legalmente registrada, seria possível padronizar os processos de gestão documental utilizados em instituições participantes do CONARQ, ampliando os direitos e obrigações dos cidadãos no que tange a gestão arquivística.

A Lei brasileira de nº 8.159, de 08 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados, considera a gestão de documentos como dever do Poder Público, assim como a proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação. Nesta Lei "considera-se gestão de documentos o conjunto de procedimentos e operações técnicas referentes à sua produção, tramitação, uso, avaliação e arquivamento em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente" (BRASIL, 1991, Art. 3). Na forma desta lei, a gestão de documentos compreende todas as ações empregadas durante qualquer fase do ciclo de vida dos documentos, seja qual for o suporte em que esteja registrada a informação.

2.2 Gestão de documentos

A aplicação e uso do termo, gestão de documentos, surgiu gradativamente da evolução dos conceitos e técnicas arquivísticas. Com a distinção das fases documentais, através do ciclo de vida documental, que inicia com o processo de elaboração do documento e termina definindo o seu destino final. Esse processo resultou na criação da teoria das três idades. Ela surge para distinguir as fases pelas quais passam os documentos, sistematizando o ciclo de vida documental, separando os documentos em correntes, intermediários e permanentes. Nessa linha, Rousseau e Couture (1998) afirmam que o ciclo de vida foi o ponto crucial para proporcionar o entendimento e a divisão dos documentos em conjunto que apresentam características comuns.

Com essa teoria surge o processo de gestão de documentos que de acordo com Lopes (2000) teve início nos Estados Unidos sob a denominação de *Records Management*, originando a corrente de pensamento arquivístico, focada na administração e tratamento de arquivos ativos, melhor definido como arquivo corrente. Lopes (2000) define, ainda, que são

correntes de pensamento arquivístico a denominada “arquivística tradicional”, que tem como pressuposto o tratamento de arquivos permanentes ou históricos e a corrente chamada de “arquivística integrada”, mais utilizada atualmente, destinada ao tratamento da documentação como um todo e respeitando todas as fases do ciclo documental, ou seja, os documentos correntes, intermediários e permanentes.

Para implantar um sistema de gestão documental, é necessário ter o apoio e o conhecimento da instituição, pois a gestão contribuirá no desempenho de suas atividades. Sendo que um sistema de gestão facilita o processo documental, pois por meio da avaliação, evitará o acúmulo de documentos ou eliminação não criteriosa que acarretaria na perda de informações importantes para o desenvolvimento institucional. O processo de gestão envolve todas as ações desde a produção até a destinação final dos documentos, buscando a racionalização e acesso facilitado às informações.

A gestão de documentos é expressa através de programas de gestão de documentos e, se materializa, por meio do planejamento e execução de um sistema de gestão de documentos, que pode ser convencional ou eletrônica/digital. (CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS, 2006). Uma política de gestão arquivística de documentos deve ser formulada com base na análise das necessidades institucionais, de acordo com a estrutura e as funções desempenhadas pela instituição no cumprimento de seus objetivos. A Gestão de documentos em instituições arquivísticas pode ser realizada da forma convencional, que é mais comum ou feita em meio eletrônico que é denominada Gestão Eletrônica de Documentos (GED).

A GED visa à gestão de documentos de forma eletrônica, não somente documentos produzidos no meio eletrônico. Inicialmente era um instrumento que se preocupava com a digitalização dos documentos, passando o documento em papel para o meio digital, através do uso de scanner. Segundo Santos (2005) apud Koch (1998) assim, GEDs buscam cada vez mais unir conceitos arquivísticos com a informática, para criar subsídios que apóiem um sistema de gestão de documentos, sejam eles eletrônicos ou não. Atualmente a TI (Tecnologia da Informação) preocupa-se com a automação de atividades oriundas dos processos de produção, tramitação e uso das informações.

A GED visa o gerenciamento completo dos documentos desde sua criação até seu destino final, não importando se os documentos permanecem em suporte papel ou estão em meio eletrônico. Para Rondinelli (2005) 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 das informações que serão repassadas aos usuários.

Para facilitar o acesso, os profissionais arquivistas elaboram instrumentos de pesquisa para cooperar na gestão documental. Nessa perspectiva, Cardoso (2005) afirma que ao se produzir e difundir as informações, sejam eletrônicas ou digitais, compete aos profissionais estar constantemente atualizados para empregar ações inovadoras no tratamento dos documentos. A descrição é materializada através dos instrumentos de pesquisa, pois são estes que orientam as possíveis consultas à documentação, facilitando deste modo, a busca da informação pelo usuário.

Pode-se afirmar, também, que a descrição arquivística proporciona o conhecimento mais amplo do conteúdo documental de um acervo, pois através dos instrumentos de busca é possível facilitar a localização dos documentos. Os instrumentos de pesquisa são resultados da utilização de normas de descrição e contribuem para racionalizar a massa documental acumulada, permitindo assim, a rápida recuperação da informação para consulta por meio da descrição, com o emprego de instrumentos de pesquisa. Sousa (2006) os instrumentos de pesquisa podem ser: Guia, Inventário, Catálogo, Repertório ou Catálogo Seletivo, Índices, Tabela de Equivalência ou Concordância.

Os autores Lopes (2000) e Lopez (2002) citam a ISAD (G) (Norma Internacional de Descrição Arquivística), como padrão utilizado nos processos descritivos no Brasil. É relevante destacar que no final do ano de 2007 foi editada a versão final da NOBRADE (Norma Brasileira de Descrição Arquivística) elaborada com base na ISAD (G), tendendo ser usada como padrão de descrição no Brasil ao invés da ISAD (G). Além das normalizações para descrição de documentos tradicionais existem normas específicas para descrição de documentos eletrônicos, como é o caso do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-ARQ).

2.3 Normas de Descrição Arquivística: ISAD (G) e Nobrade

A ISAD (G) (*General International Standard Archival Description)* foi a primeira normalização para descrição Arquivística, aprovada no Brasil, que abrangia documentos independente de seu suporte. A Norma ISAD (G), apesar de fazer referência à documentação eletrônica, não cita em suas especificações campos específicos para tal tratamento. Essa norma é muito bem aceita no Brasil, pois até o ano de 2006 não existia Normalização Brasileira.

É utilizada principalmente na descrição de documentos tradicionais, mas pode ser empregada para documentação eletrônica, devido a sua facilidade de descrição já que não utiliza mecanismos computacionais para ser aplicada. Com relação a esse aspecto, Lopes (2000), Lopez (2002) comentam em seus trabalhos a relevância desta norma para a descrição arquivística brasileira.

Essa norma estabelece orientações gerais para a descrição arquivística, devendo ser conjugada com normas nacionais existentes, ou então servir de base para o desenvolvimento delas. Ainda que as regras que constituem a presente norma se centrem na descrição de documentação de arquivo permanente, também podem ser aplicadas às fases anteriores. Essa norma contém regras gerais para a descrição arquivística que podem ser aplicadas independentemente da forma ou do suporte dos documentos.

O conteúdo da ISAD (G) determina a divisão de sete (7) áreas de informação descritiva, e é constituído por vinte seis (26) elementos para descrição. As áreas dividem-se em: 1.Identificação; 2.Contexto; 3.Conteúdo e estrutura; 4.Condições de acesso e utilização; 5.Documentação associada; 6.Notas e 7.Controle de descrição. O acesso documental é abordado, na zona de condições de acesso, da ISAD (G), cujo objetivo é proporcionar informação consoante a legislação, oferecendo acesso à unidade de descrição. Para Leão (2006), com a Normalização ISAD (G) o acesso ao conteúdo dos documentos foi definido prioritário e fundamental para a descrição arquivística.

A Nobrade “estabelece diretivas para a descrição no Brasil de documentos arquivísticos, compatíveis com as normas internacionais em vigor ISAD(G) e ISAAR (CPF), e tem em vista facilitar o acesso e o intercâmbio de informações em âmbito nacional e internacional”. (BRASIL, 2006, p. 10).

Sua versão final foi recentemente publicada, sendo elaborada para ser utilizada no Brasil e pode estar em conformidade com a ISAD (G). A Norma Brasileira de Descrição deve ser difundida tornando-se conhecida não somente pelos profissionais arquivistas, mas também pelos profissionais das áreas afins, possibilitando, assim, o seu aperfeiçoamento.

A Nobrade prevê a existência de 28 elementos de descrição, distribuídos em oito áreas, que são as seguintes: 1. Identificação; 2. Contextualização; 3. Conteúdo e estrutura; 4. Condições de acesso e uso; 5. Fontes relacionadas; 6. Notas; 7. Controle da descrição e 8. Pontos de acesso e descrição de assuntos. Sua descrição sobre o acesso assemelha-se muito a ISAD (G), porém apresenta os tipos mais comuns de restrição de acesso e traz de uma forma mais simplificada os procedimentos técnicos de descrição arquivística.

2.4 Análise de Normas relevantes ao estudo: ISO 15489, e-ARQ e ABNT NBR ISO/IEC 27002

2.4.1 *Information and documentation - Records management* - ISO 15489-1

Essa norma 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. As Normas ISO são conhecidas pela sua excelência e competência na padronização de processos, sendo elaboradas pela Associação Brasileira de Normas Técnicas (ABNT).

A ISO 15498 é dividida em duas partes, sendo a primeira composta 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.

No que tange o gerenciamento de documentos a parte I serve como subsídio para regulamentar um sistema de gestão documental de instituições públicas e privadas no intuito de facilitar o acesso aos documentos para os usuários. Neste sentido Henriques (2002) afirma

que essa norma pode ser aplicada para todos os tipos documentais independentemente do seu suporte.

A ISO 15489-1 está dividida em onze capítulos, sendo que o primeiro explicita o seu campo de aplicação expondo o conteúdo da mesma e definindo quem pode utilizá-la. O capítulo dois faz alusão às normalizações que originaram a ISO 15489-1, de forma bastante sucinta. Essa norma, como pode ser utilizada por diversas áreas e pessoas diversificadas envolvidas na gestão documental em uma instituição, traz no seu terceiro capítulo termos e definições no intuito de esclarecer dúvidas a respeito de terminologia própria.

O conteúdo da ISO 15489-1, mesmo sendo escrito em outro idioma, apresenta-se de forma clara e precisa. Caso o leitor não conheça os benefícios da gestão de documentos, ela traz no seu quarto capítulo as vantagens que a aplicação de um sistema de gestão trará para a instituição. É relevante que a instituição ao adotar uma política e procedimentos de gestão, elabore normalizações e atos legais que reflitam suas atividades e objetivos. O quinto capítulo refere-se a esse tipo de procedimento apresentando o meio legal, que são nada mais que as leis e regulamentos relacionados diretamente com os documentos de arquivo e que são primordiais para o funcionamento de um sistema eficaz de gestão documental.

A Norma ISO 15489-1 apenas faz referência a ações que podem ser aplicados para o bom funcionamento de um sistema de gestão. O capítulo seis da norma complementa o capítulo anterior descrevendo a relevância do registro das políticas, procedimentos e das atividades praticadas para a gestão de documentos dentro da instituição. 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.

Os requisitos que compõe os princípios de gestão de documentos e sua representação são apresentados no sétimo e oitavo capítulo da norma, respectivamente. Segundo a ISO 15489-1 para a aplicação de um programa de gestão devem ser seguidos onze itens, são eles:

> a) Determinar o arquivamento de documentos que devem ser criados em cada processo de negócio e as informações a serem incluídas nesses documentos;
> b) decidir a forma e estrutura, que deve criar e capturar os documentos de arquivo, e tecnologias a serem utilizadas;

> c) determinar que metadados se deva estabelecer junto com os documentos de arquivo e ao longo dos processos referentes a ele, e relacioná-los de maneira consistente;
> d) determinar os requisitos para a recuperação, uso e tramitação de documentos de arquivo entre os diferentes processos e usuários, e quanto tempo os documentos devem ser conservados no arquivo, a fim de atender a esses requisitos;
> e) decidir como organizar os documentos de arquivo, de modo a cumprir requisitos necessários para seu uso;
> f) avaliar os riscos resultantes da falta de documentos que sejam um reflexo fidedigno das atividades realizadas pela instituição;
> g) preservar os documentos de arquivo e permitir o acesso a eles ao longo do tempo, a fim de satisfazer as necessidades da instituição e as expectativas da sociedade;
> h) cumprimento dos requisitos legais e regulamentadas, normas e políticas da organização;
> i) garantir que os documentos de arquivo sejam mantidos em ambiente seguro;
> j) garantir que os registros arquivísticos são mantidos somente para o período de tempo necessário ou exigido;
> k) identificar e avaliar formas de melhorar a eficácia, a eficiência ou a qualidade dos processos, decisões e ações que podem resultar para melhor gerir os documentos de arquivo. (ISO 15489-1, 2001, P. 6, TRADUÇÃO NOSSA).

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. Além de seu conteúdo, o documento de arquivo deve incluir metadados necessários para justificar uma determinada operação. A estrutura do documento e seu formato precisam permanecer inalterados, já que o documento tem a função de refletir seu contexto de produção.

As estratégias usadas para a aplicação de um sistema de gestão de documentos podem incluir um esboço de um sistema de gestão, os documentos, as pessoas envolvidas na gestão, novos sistemas de arquivamento e o uso de normas para o controle desse sistema. Esse sistema deve ser confiável, íntegro, estar em conformidade com os regulamentos institucionais e adotar um caráter sistemático. O capítulo nove da norma dá seguimento às estratégias relatadas no capítulo oito, explicitando os processos e controles usados na gestão de documentos.

Os capítulos dez e onze da ISO 15489 finalizam as diretrizes para aplicação de um sistema de gestão. O primeiro, monitoramento e auditoria, serve para regular e garantir os procedimento adotados na instituição para que sejam aplicados em conformidade com as políticas institucionais alcançando os resultados esperados. O segundo, formação, sugere a adoção de programas que sirvam para treinar as pessoas responsáveis pelo sistema de gestão de documentos auxiliando-os no desenvolvimento de suas atividades institucionais. 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".

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

O e-ARQ apresenta um modelo de requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos objetivando a confiabilidade e acesso às informações. O SIGAD (Sistemas Informatizados de Gestão Arquivística de Documentos) deve ser capaz de gerenciar tanto documentos convencionais quanto digitais. Esta norma dá diretivas que auxiliam a realização das funções arquivísticas. 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 a gestão de documentos.

O resultado esperado da aplicação da norma é 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 teorias para o tratamento não somente dos documentos, mas sim, com a informação contida neles.

A elaboração de normas brasileiras como é o caso da e-ARQ, demonstra a preocupação com a gestão de documentos digitais, tanto para instituições públicas como privadas. O CONARQ é uma organização, vinculada ao Arquivo Nacional e tem como finalidade determinar a política nacional de arquivos elaborando normas, leis e outras

orientações que contribuam na gestão documental em instituições públicas e privadas de todo o território nacional.

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. A Parte I 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) esta 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.

A Parte II da norma descreve os requisitos necessários para desenvolver o SIGAD, iniciando sua descrição pelas funcionalidades do sistema. A primeira seção trata da Administração do Plano de Classificação, da Classificação de metadados dos processos e seus gerenciamentos, dos volumes e, ainda, faz alusão à manutenção de documentos arquivísticos convencionais e híbridos. O SIGAD, neste contexto, deve ser capaz de permitir a gestão de documentos de forma semelhante ao realizado com documentos convencionais, só que em meio eletrônico, proporcionando, assim, a manutenção do plano de classificação com suas devidas divisões. Já que o SIGAD pode compreender um ou mais softwares integrados, a inclusão dos requisitos adicionais varia de acordo com as necessidades institucionais. Os softwares são responsáveis pela execução de funções determinadas pelas instituições, podendo ser capaz de manipular dados, e manter programas. (VERGÍLIO, 2009).

A segunda seção da norma, como na gestão de documentos tradicional, retrata a tramitação documental e o fluxo de trabalho, ou seja, se refere ao caminho que o documento percorre durante o cumprimento de sua função na instituição. Um sistema de fluxo de trabalho, também denominado workflow, objetiva a automação dos processos de gestão. Para Araújo e Borges (2001, p. 3) "um processo pode ser considerado como um conjunto de atividades que, ao serem realizadas, atingem um determinado objetivo de trabalho". Nessa seção ainda é possível através dos requisitos da e-ARQ, identificar por meio do seu recurso de fluxo de trabalho, se o documento é minuta, original ou cópia.

Na terceira seção é abordada a captura documental, ou seja, a captura de documentos arquivísticos que posteriormente serão agrupados no sistema através das ações de: registro,

classificação, indexação, atribuição de metadados e arquivamento. O SIGAD deve ser capaz de proporcionar a captura de documentos originários de outros sistemas. Nessa seção é relatado o uso do correio eletrônico para receber, enviar ou trocar mensagens e documentos digitais entre os computadores na instituição. Um SIGAD deve proporcionar, ainda, a captura de documentos digitais convencionais e híbridos, sendo uma das subdivisões desta seção enumerar os requisitos necessários para a realização deste processo.

> A gestão arquivística de documentos digitais prevê o estabelecimento de três domínios dentro do ambiente eletrônico, a saber: espaço individual, espaço do grupo e espaço geral. O espaço individual corresponde ao espaço designado a cada funcionário. O espaço do grupo corresponde ao espaço designado a cada grupo de trabalho, equipe, comitê etc. O espaço geral corresponde ao serviço de protocolo e arquivo corrente do órgão ou entidade. Sua principal característica é que uma vez ali, o documento não poderá mais ser alterado. (CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS, 2006, p. 60).

Para Santos (2007, p. 178) as funções arquivísticas são divididas em sete, seguindo a proposta de Rosseau e Couture (1998, p. 265), se fazendo presente entre elas a função de avaliação documental que “demanda conhecimento do funcionamento da instituição, sua estrutura, sua missão, objetivos e atividades geradoras de documentos”, resultando na destinação final de acordo com o valor documental evitando, assim, a eliminação equivocada de documentos relevantes para o funcionamento institucional.

Devido a importância do processo avaliativo para a racionalização documental, a seção quatro da e-ARQ apresenta os requisitos referentes à elaboração e manutenção da tabela de temporalidade dentro de um SIGAD. Estes requisitos referem-se à aplicação da tabela de temporalidade, ou seja, definem os processos de controle e verificação dos prazos de guarda e define anteriormente a provável destinação antes de ser executada. O sistema adotado na instituição tem que ser capaz de exportar documentos contribuindo nas atividades de transferência e recolhimento documental, podendo ainda realizar a migração ou envio de cópias para outro local na instituição ou no sistema. A eliminação de documentos arquivísticos da mesma forma que a tradicional deve ser realizada de acordo com o que foi estipulado na tabela de temporalidade seguindo as determinações legais.

A seção cinco oferece funcionalidades para a pesquisa e localização dos documentos arquivísticos objetivando promover o acesso mais facilitado aos usuários. Já a seção seis contextualiza a segurança da informação, trazendo requisitos para proceder nas ações de: cópias de segurança, controle de acesso, classificação da informação quanto ao grau de sigilo,

trilhas de auditoria, assinaturas digitais, criptografia, marcas d'água digitais, acompanhamento de transferência, autoproteção e ainda define condições para alterar, apagar e truncar documentos arquivísticos digitais.

O armazenamento é assunto presente na seção sete, que aborda a durabilidade, a capacidade e a efetividade de armazenamento. A gestão informatizada de documentos, da mesma forma que a gestão tradicional, para a preservação dos documentos a longo prazo, é imprescindível adotar medidas que contribuam na conservação das informações independente do seu suporte. A e-Arq apresenta requisitos dos aspectos físicos, lógicos e digitais para a preservação de documentos em um SIGAD, detalhado na seção oito da norma.

As seções nove, dez, onze, doze, treze e quatorze, trazem respectivamente: Funções Administrativas, Conformidade com a legislação e regulamentações, Usabilidade, Interoperabilidade, Disponibilidade, Desempenho e escalabilidade. Quanto às numerações das seções e o sumário presente na norma é possível identificar um erro, que só pode ser verificado no decorrer da análise de todo o documento.

O sumário apresenta as seções como foi citado anteriormente até a seção quatorze, mas no decorrer do texto a seção onze ganha continuidade nos requisitos apresentados, porém, é tratada da interoperabilidade e não mais da usabilidade como referenciado no sumário, sendo contado a sessão doze a partir da disponibilidade. Este erro não altera a compreensão da norma, entretanto pode confundir o leitor no primeiro momento parecendo que as seções referem-se ao mesmo assunto. Os metadados, por sua vez, não são apresentados na primeira versão da e-ARQ, sua conclusão estava em processo avaliativo. O Esquema de Metadados do Modelo e-ARQ Brasil foi publicado na versão da e-ARQ de dezembro de 2009 e encontra-se disponível no site[1] do CONARQ.

2.4.3 Tecnologia 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 numeração NBR ISO/IEC 27002. Conforme Baldissera (2007, p. 40) define que a origem da NBR ISO/IEC 17799:

[1] [http://www.conarq.arquivonacional.gov.br]

> 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 conhecida como: NBR ISO/IEC 17799:2005.

O objetivo da norma não é criar um modelo para a segurança da informação, mas apenas orientar as ações empregadas para garantir a segurança institucional e documental. Ela disponibiliza diretrizes que ajudam na elaboração de uma política de segurança da informação. 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 é nada mais que um código de prática que auxilia na segurança da informação e, o objetivo da arquivística é realizar o tratamento documental e informacional, priorizando pela segurança e confiabilidade que será passada aos usuários.

É uma norma bastante extensa e trata de questões sobre a segurança da informação em todos os níveis em uma instituição, apresenta requisitos que abordam desde a parte física do acervo até a segurança das pessoas que trabalham nele. Nas primeiras páginas da norma são apresentados conceitos a respeito da segurança da informação. Na primeira parte da norma, que pode ser definida por abranger conceitos e regras iniciais, apresentam, ainda, a avaliação dos riscos (advindos das falhas de pessoas ou sistêmicas), a seleção dos controles de segurança da informação, fatores críticos e, finalizando, ressalta a necessidade das instituições criarem suas próprias diretrizes para a segurança da informação.

---

[2] *International Engineering Consortium*

È relevante destacar que essa norma é estrutura, contendo os seus capítulos subdivididos em subcapítulos, onde apresenta informações como: controle, diretrizes para implementação e informações adicionais. Ao analisar a ABNT NBR ISO/IEC 27002, ela não se deterá em explicitar seus controles e seguir fielmente sua estrutura, apenas será exposto um relato sintético de seus capítulos para passar um conhecimento geral de suas especificações e ações permitindo assim conhecer para posteriormente desenvolvê-la e aplicá-la dentro de uma instituição.

Mesmo não sendo uma norma arquivística, a ABNT NBR ISO/IEC 27002, traz inicialmente o objetivo de sua aplicação, termos e definições que auxiliam os usuários na compreensão de seu conteúdo, como nas normas arquivísticas. 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 esse para alcançar os objetivos propostos.

Antes de apresentar as seções da segurança da informação propriamente ditas, a norma aborda no capítulo quatro a análise/ avaliação e tratamento de riscos, salientando a importância de a instituição realizar periodicamente a avaliação dos riscos que as ações de segurança da informação podem gerar de ameaças a segurança institucional. Para tratar os riscos advindos de falhas na segurança é necessário que as instituições: apliquem controles para reduzir os riscos, conheçam e aceitem estes riscos verificando se eles atendem a política da organização e aos critérios para a aceitação de risco, evitar os riscos não permitindo ações que possam provocá-los e ainda, transferir a ocorrência deste risco a outras partes como uma seguradora, por exemplo.

A primeira seção, sobre a segurança da informação, e consecutivamente o capítulo cinco da norma apresenta a Política de Segurança da Informação. Para Spanceski (2004) é fundamental que as instituições elaborem uma política de segurança da informação, pois, só através de uma metodologia específica, de normas e responsabilidades definidas será possível garantir o controle e a segurança das informações institucionais. O objetivo da política de segurança da informação é dar uma orientação a administração da instituição, baseada em regulamentos e de acordo com os propósitos institucionais. Esse capítulo aborda ainda, o Documento da política de segurança da informação que nada mais é que a elaboração de um documento aprovado pela instituição comprometendo-se e relatando seu enfoque para

gerenciar a segurança das informações. O capítulo cinco traz, ainda, a análise crítica da política de segurança da informação, que tem como controle o dever da instituição de analisar periodicamente as mudanças que ocorrerem na política implantada para, só assim, assegurar sua eficácia.

Para compreender melhor, deve ser estabelecida a política de segurança da informação dentro da instituição, o capítulo seis da ABNT NBR ISO/IEC 27002 é denominado: Organizando a segurança da informação. A primeira subdivisão desse capítulo fala sobre a Infra-estrutura da segurança da informação, relatando que a direção deve aprovar a política de segurança da informação e atribuir às funções da segurança. A próxima subdivisão comenta sobre o Comprometimento da direção com a segurança da informação, relatando que esta deve apoiar a segurança da informação dentro da organização, demonstrando o seu comprometimento, definindo atribuições de forma clara e conhecendo as responsabilidades pela segurança da informação. A implementação dessa política deve ser coordenada por representantes de diferentes partes da instituição e com funções e papéis relevantes, pois a participação deve envolver desde administradores até usuários. Esse assunto é abordado no subcapítulo Coordenação da segurança da informação

As diretrizes sobre as responsabilidades pela segurança da informação são comentadas no subcapítulo: Atribuição de responsabilidades para a segurança da informação, após a norma ainda traz outra subdivisão que compreende o Processo de autorização para os recursos de processamento da informação. Além disso, a norma apresenta através das diretrizes denominadas, Acordos de confidencialidade dando requisitos para a confidencialidade ou acordos de não divulgação para proteger as informações institucionais.

É no capítulo seis que são apresentados requisitos para o contato com autoridade e o contato com grupos especiais. O primeiro refere-se aos incidentes em segurança da informação que podem ocorrer e que tipo de autoridade pode ser contatada para cada tipo de serviço. O segundo faz referência a contatos mantidos com grupos de interesses especiais ou outros fóruns especializados de segurança da informação e associações profissionais.

A Análise crítica independente de segurança da informação é o requisito que propõe que seja realizada uma avaliação dos riscos para identificar quaisquer requisitos de controles específicos, onde existir uma necessidade que permita o acesso de uma parte externa aos recursos de processamento da informação ou às informações na instituição.

Muitas vezes a instituição arquivística além de prestar serviços externos necessita da prestação de serviços terceirizados em suas dependências. Os riscos decorrentes das manutenções de mais trabalhos realizados por partes externas a instituição, podem causar incidentes de segurança da informação. Pensando nisso ao tratar às políticas de segurança da informação, as instituições devem prever e atribuir requisitos para possíveis implicações e danos a segurança quando se trabalha com partes externas. As partes externas como preocupação de quem trabalha na segurança da informação também está presente nos requisitos do capítulo da norma abordando a Identificação dos riscos relacionados com partes externas; Identificando a segurança da informação, quando tratando com os clientes; e Identificando segurança da informação nos acordos com terceiros.

O Capítulo sete, Gestão de ativos, trata da responsabilidade pelos ativos, ou seja, que dentro da instituição existam responsáveis pela proteção desses ativos. Para isso convém que todos os ativos sejam identificados e documentados em um inventário dos ativos, permitindo recuperar em caso de desastre, incluindo o tipo de ativo, forma, localização, informação sobre cópias de segurança, informações sobre licenças e a importância dele para a instituição. Nesse sentido, Fontes (2008, p. 225) afirma que "para possibilitar a proteção adequada da informação é necessário que se tenha a identificação dos ativos (recursos) de informação, seus responsáveis, sua forma de sua classificação em termos de sigilo".

Dentro desse processo torna-se fundamental que todas as informações e ativos aliados aos recursos de processamento de informação possuam um proprietário[3]. Outro requisito tratado dentro da gestão dos ativos é a Classificação da informação, que tem como objetivo assegurar que a informação receba um nível adequado de proteção indicando, assim, a necessidade e a prioridade para seu tratamento. As recomendações para classificação estão de acordo com o seu valor, requisitos legais e sensibilidade levando em consideração as necessidades de compartilhamento ou restrição.

Em geral, a classificação dada à informação é uma forma de determinar seu tratamento e proteção dentro da instituição. A última subdivisão desse capítulo relata sobre os rótulos e o tratamento da informação dando diretivas a fim de proporcionar que as informações recebam rótulos apropriados de acordo com sua classificação. A rotulação e o tratamento seguro da

[3] Pessoa ou organismo responsável e autorizado para controlar a produção, o desenvolvimento, a manutenção, o uso e a segurança dos ativos.

classificação da informação é um requisito fundamental para os procedimentos de compartilhamento da informação.

No capítulo oito, Segurança em recursos humanos, “são abordados a inclusão de responsabilidades relativas à segurança na descrição dos cargos, a forma de contratação e o treinamento em assuntos relacionados à segurança. (BALDISSERA, 2007, p. 43). Esses requisitos proporcionam aos funcionários contratados (sejam temporários ou por longa duração) o conhecimento de suas responsabilidades dentro da instituição, reduzindo assim, o risco de roubos, fraudes e mau uso de recursos. Em caso de término ou mudança da contratação, convém a devolução dos ativos da organização e a retirada de todos os direitos de acesso que estejam em posse dos funcionários, fornecedores e terceiros, após o encerramento de suas atividades na instituição.

O capítulo nove aborda a Segurança física e do ambiente para proporcionar áreas seguras prevenindo o acesso físico não autorizado, danos e interferências com as instalações e informações da instituição. Para isso é relevante o uso de perímetros de segurança, que podem ser as paredes, portões de entrada controlados por cartão ou balcões de recepção com recepcionistas para proteger e evitar o acesso livre as áreas que contenham as informações e instalações de processamento da informação. Nessas áreas só podem ter acesso as pessoas que possuírem autorização. As áreas devem ser projetadas e aplicadas com proteção física contra incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem. A proteção dos equipamentos é necessária para reduzir o risco de acesso não autorizado às informações e para proteger contra perdas ou danos. Os equipamentos têm que ser protegidos contra falta de energia elétrica e a manutenção deve ser apropriada para assegurar a disponibilidade e integridade dos equipamentos.

O capítulo dez, gerenciamento das operações e comunicações certamente é o mais extenso da ABNT NBR ISO/IEC 27002 e para compreender melhor sua abordagem segue-se Baldissera (2007, p. 43) ao relatar que essa seção:

> Aborda as principais áreas que devem ser objeto de especial atenção e segurança. Dentre estas áreas destacam-se as questões relativas a procedimentos operacionais e respectivas responsabilidades, homologação e implantação de sistemas, gerência de redes, controle e prevenção de vírus, controle de mudanças, execução e guarda de backup, controle de documentação, segurança de correio eletrônico, entre outras.

Esse capítulo faz referência às cópias de segurança, cujo objetivo é manter a integridade e disponibilidade à informação e são recursos de processamento de informação. As cópias de segurança das informações e dos softwares tem que ser testados regularmente seguindo definições estabelecidas pela instituição. Outro ponto importante nesse capítulo é o gerenciamento e controle em redes para evitar ameaças e manter seguro os sistemas. Além desses, outro ponto comentado na norma e muito relevante para a segurança das informações institucionais é o manuseio das mídias. Esse, se realizado de forma correta evita a divulgação não autorizada, modificação, emoção ou destruição aos ativos e interrupção das atividades de gestão.

Os procedimentos de descarte de mídias devem ocorrer de forma segura e protegida evitando riscos. A norma apresenta ainda diretrizes para o gerenciamento das mídias removíveis. E nessa linha, Sudré (2005) alerta que o aumento da capacidade de armazenamento das mídias removíveis resulta, também, no aumento do volume de informações que são gravadas nos CDs, DVDs e Pen-drives. Dessa forma as mídias podem se tornar um risco para a segurança dos dados e informações nelas contidas.

No capítulo onze é apresentado diretrizes para a implementação do Controle de acesso. Esse capítulo abrange basicamente as normas e regras para garantir manter seguras as informações dentro de uma instituição. Expõem também, a relevância do estabelecimento de uma política de controle de acesso com base nos requisitos de acesso e na segurança da informação. Relata o gerenciamento de acesso de usuários e suas responsabilidades. Comenta sobre o controle de acesso à rede e o controle ao sistema operacional. As últimas abordagens desse capítulo referem-se ao controle de acesso às aplicações e à informação, e também faz referência a computação móvel e o trabalho remoto.

A questão da Aquisição, desenvolvimento e manutenção de sistemas de informação, abordando requisitos para garantir a segurança da informação é referenciada no capítulo doze na ABNT NBR ISO/IEC 27002. Esse capítulo, além disso, faz menção aos controles criptográficos objetivando proteger a confidencialidade, a autenticidade ou a integridade das informações. Para isso, é sugerido o desenvolvimento de uma política para o uso de controles criptográficos, resultando na proteção da informação. O capítulo apresenta, também, requisitos para o controle de segurança dos arquivos do sistema, para a segurança em processos de desenvolvimento e de suporte para a gestão de vulnerabilidade técnicas.

No capítulo treze são discutidos assuntos referentes à Gestão de incidentes de segurança. O primeiro ponto abordado são as notificações de fragilidades, cujo propósito é assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam notificados, permitindo a tomada de ação corretiva em tempo hábil. O capítulo trata ainda da gestão de incidentes de segurança da informação e melhorias, expondo o estabelecimento de responsabilidades e procedimentos de gestão para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação.

O penúltimo capítulo da norma, capítulo quatorze, correspondendo à seção dez do conjunto de assuntos sobre a segurança da informação, traz a Gestão da Continuidade do negócio. Relata a relevância em não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres, e assegurar a sua retomada em tempo hábil. Para Fontes (2008, p. 73) as instituições necessitam “elaborar um plano de continuidade que deve ser efetivo e possibilitar que a organização funcione em um nível aceitável para a sua sobrevivência e absorva possíveis impactos financeiros, operacionais e de imagem.”

A conformidade é abordada no capítulo quinze, correspondendo a última seção do conjunto de assuntos sobre segurança da informação presente na norma. Comenta a necessidade de observar os requisitos estatutários, regulamentares e contratuais relevantes, e o enfoque da organização. De acordo com esses requisitos os registros importantes têm que ser protegidos contra perda, destruição e falsificação. A instituição deve estar atenta também aos controles de criptografia para que sejam usados em conformidade com todas as leis, acordos e regulamentações relevantes. Essas ações devem garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação.

2.5 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 e dentro desse um dos objetivos deve se dar acesso, ou melhor, tornar acessível os documentos aos usuários. É necessário salientar que “a segurança da informação evoca a proteção dos ativos da informação, sistemas, recursos e serviços contra desastres, erros, uso indevido, roubos,

manipulação não autorizada, visando minimizar os danos ao negócio e maximar o retorno dos investimentos e das oportunidades de negócio". (CAPEMISA, 2008, p. 2).

Em relação ao acesso às informações arquivísticas, Castanho, Garcia e Silva (2006, p.37) afimam que "o objetivo da arquivística é tornar as informações acessíveis ao usuário, por meio do tratamento das mesmas, buscando valorizar o conteúdo informacional dos documentos, sem desconsiderar sua organicidade.".

Os problemas de segurança da informação acontecem quando há quebra nos princípios que norteiam as ações realizadas nas organizações. Essa quebra é denominada, na área da segurança da informação, como um incidente de segurança da informação. 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.

- Confidencialidade: Garantir que as informações sejam acessíveis somente a pessoas que possuam permissão para acesso na instituição;

- Integridade*:* Proporcionar a proteção das informações contra modificações, adulterações ou fraudes;

- Disponibilidade*:* Assegurar que os usuários autorizados tenham acesso às informações quando requisitadas, e estas, se mantenham protegidas e não se tornem indisponíveis.

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

Quando o assunto é segurança seja pesquisado em fontes como revistas, livros ou artigos que abordem o assunto sempre é relacionado o termo: ativo. Para compreender melhor o que seriam os ativos de segurança é relevante fazer sua relação a um bem material ou imaterial que pertençam à instituição. Nesse sentido, seguindo 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.

Campos (2007) afirma, ainda, que os ativos de uma forma geral podem apresentar quatro grupos distintos conforme a vulnerabilidade, ou seja, as fraquezas, que apresentam em relação aos incidentes de segurança da informação. O primeiro grupo é constituído pelas tecnologias onde aparecem os computadores, arquivos de aço, impressoras, cabos de rede, aparelhos celulares e sistemas de informação. O segundo grupo é constituído pelas pessoas que trabalham em uma determinada instituição, podendo divulgar determinadas informações dentro e fora do ambiente de trabalho. E ainda quando ocorre à demissão ou afastamento de funcionário, este pode levar consigo informações confidenciais sobre o funcionamento institucional ocasionando um incidente de segurança da informação.

O terceiro grupo é composto pelos processos e diz respeito às normas, regras e demais medidas que deveriam ser adotadas nas instituições como forma de orientar os procedimentos como contratações e demissões de funcionários, as relações desses com as informações institucionais gerando, assim, um compromisso por parte do funcionário ao lidar com os ativos da informação. O último grupo é relacionado aos ambientes, já que podem ocorrer desastres como incêndios, alagamentos e outros. A ação dos poluentes pode causar danos em equipamentos. Outro perigo para a segurança nos ambientes, ainda, é o acesso a pessoas que muitas vezes mesmo não sendo permitido ocorre. (CAMPOS, 2007)

Para que o gerenciamento das informações se torne eficaz e seguro, 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. A adoção de uma política de segurança da informação deve envolver tanto funcionários quanto usuários da organização. A sua confiabilidade dependerá do cumprimento das responsabilidades, quanto às ações de controle e segurança das informações, pelos membros da organização. De acordo com Baldissera (2007, p. 56) a implantação de uma Política de Segurança da Informação “surge 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”.

Para que a política de segurança da informação tenha resultado efetivo, é necessária a aplicação de questões que, segundo Medeiros (2001) podem ser comuns entre as organizações. As questões comuns entre as organizações são: que a informação deve ser vista como um bem institucional; devem preocupar-se com o controle do acesso às informações; manter responsabilidades aos usuários e a administração e ao gestor da informação; estar

preparados para situações de contingência; garantir a privacidade do usuário e ainda definir medidas disciplinares, caso as regras sejam descumpridas.

A Política de Segurança da Informação para ser aplicada deve seguir algumas orientações de Spanceski (2004, p. 38) fazendo referência a NBR ISO 17799 afirmando ser:

> · Definição de segurança da informação, resumo das metas e escopo e a importância da segurança como um mecanismo que habilita o compartilhamento da informação.
> · Declaração do comprometimento da alta direção, apoiando as metas e princípios da segurança da informação.
> · Breve explanação das políticas, princípios, padrões e requisitos de conformidade de importância específica para a organização, por exemplo:
> · Definição das responsabilidades gerais e especificas na gestão de segurança da informação, incluindo o registro dos incidentes de segurança.
> · Referência à documentação que possam apoiar a política, por exemplo, políticas, normas e procedimentos de segurança mais detalhados de sistemas, áreas específicas, ou regras de segurança que os usuários devem seguir.

A política de segurança da informação varia de instituição para instituição de acordo com os objetivos e metas de cada organização. 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. As questões mais aplicadas seriam: que a informação deve ser vista como um bem institucional; possuir um controle de acesso às informações, manter responsabilidades aos usuários, à administração e ao gestor da informação[4], 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).

2.5.1 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 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

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

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. A Associação Brasileira de Normas Técnicas (2005, p. 56), relata 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".

Nessa linha, 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 à 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 cujo objetivo "é garantir que as informações estejam disponíveis para usuários e aplicações de maneira eficiente, além de segura". (SILVA e SALDANHA, 2006, p. 16)

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 ponto relevante no que tange o controle de acesso é a classificação da informação quanto ao grau de sigilo e restrição de acesso à informação sensível. As instituições devem atentar ao grau de sigilo das informações e redobrar os cuidados quanto ao acesso. 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.

O uso e manutenção de senhas para acesso a sistemas deve ser uma medida adotada e cuidadosamente planejada nas instituições. 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".

Quanto à colocação do autor é possível verificar que mesmo com a garantia da proteção do uso da senha é necessário redobrar cuidados simples como no caso da ausência do usuário, atentando-se que o computador não permaneça liga, no caso de sua ausência, pois essa atitude pode provocar um incidente em segurança da informação. 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.

O controle é citado na Norma ABNT NBR ISO/IEC 27002, como sendo importante em locais de alto risco, os quais incluem áreas públicas ou externas fora dos limites do gerenciamento de segurança da organização. Essa norma faz referência ao controle de acesso não autorizado aos serviços de rede, relatando basicamente sobre os cuidados com o trabalho remoto. Realizar o desligamento das seções previne o acesso por pessoas não autorizadas e ataques de negação de serviço. Deve existir um controle de acesso das redes de serviços internas e para que o usuário com acesso às redes e aos serviços de rede não comprometa a segurança dos mesmos.

Se tratando do controle de acesso a serviços de rede é relevante que seja adotado medidas para controle de acesso a rede sem fio, e consequentemente o bloqueio de sites que não autorizem o acesso. A instituição deve permitir acesso às redes sem fio apenas a pessoa que, de acordo com a política de segurança institucional não represente risco para a segurança

e proteção das informações. Da mesma forma que o bloqueio de sites é muito comum em instituições públicas e privadas como forma de controlar o acesso a internet não deixando livre o acesso ao usuário e/ou funcionário da instituição. O mais comum é a proibição de sites de relacionamento como: orkut, facebook e twitter.

Uma entrevista realizada por Vicentin (2009) com profissionais de empresas renomadas sobre o bloqueio a sites de relacionamento em ambiente de trabalho demonstrou que em muitas empresas o acesso a esses sites ainda é liberado. O que provoca a restrição e monitoramento da rede é o uso abusivo. Entre as vantagens da proibição de acesso a alguns sites, estão: redução de vírus, melhor aproveitamento com o uso de links, redução de gastos, melhora na qualidade, produtividade e desempenho de cada função dentro da instituição.

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.

Para a Câmara Técnica de Documentos Eletrônicos (2006, p. 81), a “criptografia 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”. Em termos técnicos “uma assinatura digital é 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 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 e controlar a movimentação da instituição principalmente à noite.

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.

É relevante destacar, ainda, que estas normas são orientações para que as instituições tenham conhecimento sobre o assunto. O interesse em evitar problemas com a segurança das informações deve partir da própria instituição, seguindo as medidas que melhor atendam as 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 nesta pesquisa deu- se devido à importância em proteger a informação para garantir o acesso seguro e contínuo aos documentos. Nesse contexto o controle de acesso é um dos meios citados em muitas Normas Arquivísticas e não arquivísticas entre um dos requisitos principais para garantir a segurança institucional e informacional. Por esse motivo a pesquisa terá como referencial teórico as Normas ISO 15489, e-ARQ e ABNT NBR ISO/IEC 27002. As duas primeiras dão determinações sobre a gestão arquivística de documentos e a terceira trata da segurança da informação servindo, assim, como subsídio para a implantação de sistemas de gestão seguros e confiáveis.

O universo da presente pesquisa é composto por Arquivos Públicos Estaduais, para tal, foram escolhidas 13 instituições, tendo como critério uma pesquisa no site do CONARQ realizando uma busca apenas aos arquivos que tivessem um site acessível para contato e que possuíssem endereço de e-mail ou um campo específico para enviar mensagem direta ao arquivo. Caso algum não atendesse a esses critérios, seriam excluídos da pesquisa. Os arquivos públicos estaduais mencionados no site do CONARQ, representadas no Quadro 1, são respectivamente:

- Arquivo Público do Distrito Federal: <http://www.arpdf.df.gov.br>;
- Arquivo Público do Estado da Bahia: <http://www.saeb.ba.gov.br/perfil99/apeb_histori.htm>;
- Arquivo Público do Estado do Ceará: <http://www.secult.ce.gov.br/APEC/Apec.asp>;
- Arquivo Público do Estado do Espírito Santo: <http://www.ape.es.gov.br>;
- Arquivo Público de Mato Grosso: <http://www.apmt.mt.gov.br>;
- Arquivo Público Mineiro: <http://www.cultura.mg.gov.br/?task=home&sec=5>;
- Arquivo Público do Pará: <http://www.arqpep.pa.gov.br>
- Arquivo Público do Estado do Paraná: <http://www.pr.gov.br/arquivopublico>;
- Arquivo Público do Estado do Rio de Janeiro: <http://www.aperj.rj.gov.br>;
- Arquivo Público do Estado do Rio Grande do Norte: <http://www.ape.rn.gov.br/ >;
- Arquivo Público do Estado do Rio Grande do Sul: <http://www.apers.rs.gov.br/portal/index.php>;
- Arquivo Público do Estado de Santa Catarina: <http://www.sea.sc.gov.br/index.php?>;
- Arquivo Público do Estado de São Paulo: <http://www.arquivoestado.sp.gov.br/>.

Quadro 1 – Arquivos Públicos Estaduais

3.1 Classificação da pesquisa

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. Por tanto, 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. Sanchez (2009, slide 7) comenta que a pesquisa qualitativa "considera a existência de uma relação dinâmica entre mundo real e sujeito. É descritiva e utiliza o método indutivo". A pesquisa, neste caso, assume ainda a forma de multicaso, pois apresenta o estudo em mais de uma instituição pública estadual. Segundo Yin (2001) o estudo multicaso é um método que engloba o estudo de mais de um caso.

3.2 Instrumentos e coleta de dados

O contato inicial com as instituições deu-se a partir dos sites disponíveis para acesso onde 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 (sites) 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 (Apêndice A) baseado em questões sobre o controle de acesso presente nas Normas ISO 15489, e-ARQ e ABNT NBR ISO/IEC 27002. Após a produção do questionário, um professor do corpo docente do Curso de Arquivologia da UFSM, validou o mesmo. Elaborou-se também, um questionário *on-line,* elaborado pela ferramenta do Google Docs, (Apêndice B) para facilitar o preenchimento e possibilitar a rapidez nas respostas sendo enviado, também, aos arquivos,

ficando a critério do responsável escolher qual responderia. Os questionários foram enviados a apenas, um responsável em cada instituição, que atendeu aos critérios metodológicos para seleção da pesquisa. É relevante destacar que o primeiro questionário (Vide Apêndice A) foi o mais respondido pelos entrevistados.

Além do questionário enviou-se às instituições, por meio eletrônico, um Termo de Consentimento Livre e Esclarecido (Apêndice C) como forma de registrar a aceitação do sujeito em participar da pesquisa, por livre e espontânea vontade. Solicitou-se ainda, que após assiná-los os digitalizassem (caso a instituição contasse com um scâner) e o reenviassem via e-mail ou mandassem uma declaração de aceitação por e-mail institucional afirmando a sua livre concordância para participação da pesquisa. Para o andamento da pesquisa, estabeleceu-se, além de contato via e-mail institucional, contato através do telefone do arquivo com os responsáveis, como forma de reiterá-los do prazo para entrega dos questionários e agradecer antecipadamente a atenção e colaboração com a pesquisa. O prazo para responder os questionários foi de 18 dias contando a data de envio.

Como forma de preservar a identidade dos entrevistados 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.

3.2.1 Cronograma

O cronograma foi desenvolvido a partir dos primeiros contatos com as instituições selecionadas até o processo de análise dos dados coletados. As atividades realizadas, objetivando a coleta de dados, representadas no Quadro 1, são respectivamente:

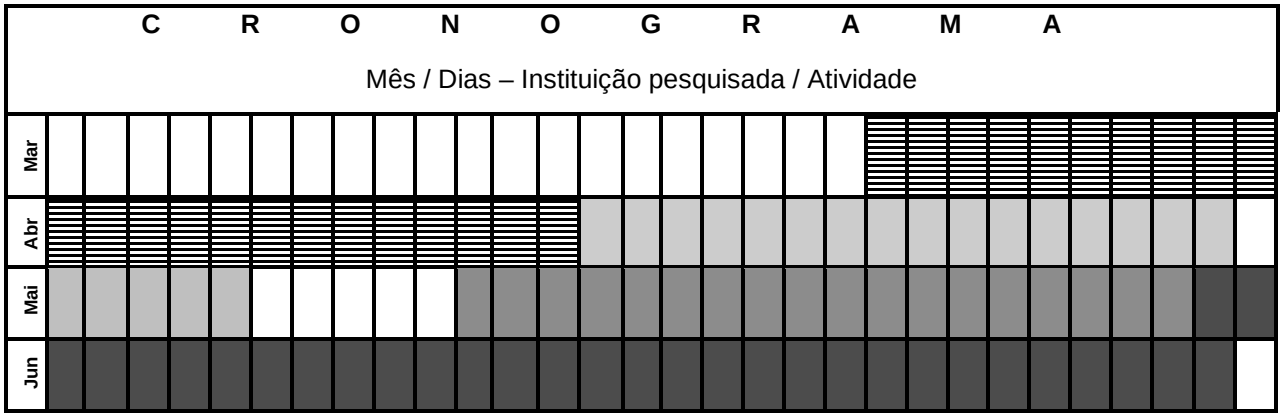
- **Pesquisa no site do CONARQ e definição das instituições:** A pesquisa possibilitou conhecer treze (13) Arquivos Públicos Estaduais, de acordo com os critérios metodológicos, e selecionar as sete (7) instituições que participariam da pesquisa.

Contatos com as instituições: Estabelecido os primeiros contatos com as instituições, troca de e-mail para verificar as possibilidades para posterior envio do instrumento de coleta de dados.

Coleta de Dados: A coleta de dados foi realizada por meio eletrônico com dezoito (18) dias para a devolução dos questionários.

Análise dos dados: Sistematização das informações dos questionários conforme os objetivos definidos na pesquisa.

Para dar menção às datas realizadas na coleta dos dados da presente pesquisa, foi elaborado um cronograma simplificado, objetivando a análise dos passos realizados até a conclusão da pesquisa e o tempo destinado para sua execução.



Legenda:

	1- Pesquisa no site do CONARQ e definição das instituições		2- Estabelecimentos dos contatos com as instituições
	3- Envio e recebimento dos instrumentos de coleta de dados		4 - Análise dos dados

Quadro 2 - Cronograma de pesquisa

3.3 Tabulação dos dados pesquisados

Para a tabulação e análise dos dados, foram elaborados quadros e tabelas confeccionados no *Microsoft Word*, expressando as variáveis da pesquisa. Ainda foi adotado o código, conforme especificado no subcapítulo instrumento e coletas de dados, como forma de identificar cada arquivo e reunir as informações no intuito de organizar os resultados da pesquisa.

O capítulo quatro traz uma breve apresentação sobre os Arquivos Públicos Estaduais que participaram desta pesquisa.

4 ARQUIVOS PÚBLICOS ESTADUAIS

Este capítulo é constituído por uma síntese das atividades, histórico e ações mais relevantes dos Arquivos Públicos Estaduais que participaram da pesquisa. Estes dados foram retirados dos sites dos arquivos para melhor compreender suas trajetórias como instituições arquivísticas, desempenhando suas funções em cada estado que representam.

4.1 Arquivo Público do Distrito Federal

O Arquivo Público do Distrito Federal[5] - ArPDF (Figura 1) reúne, principalmente, a documentação que retrata a história da Capital Federal, desde o período da interiorização, previsto na Constituição de 1892, a construção até os dias atuais. O acervo apresenta documentos em diferentes suportes e formatos podendo ser textuais, audiovisuais, cartográficos, dentre outros. Compõem o acervo sete Fundos Públicos e três Fundos Privados.

Figura 1 – Prédio do Arquivo Público do Distrito Federal
Fonte: Arquivo Publico do Distrito Federal

Além dos documentos de valor permanente acumulados pelos órgãos do Governo do Distrito Federal, o ArPDF pode recolher a documentação de caráter privado, quando o acervo for considerado relevante para a história do Distrito Federal e não houver outra solução viável para sua preservação ou acesso. No Quadro 3 é apresentada a identificação do arquivo.

[5] Informações sobre o arquivo, retiradas do site: <http://www.arpdf.df.gov.br/>

Arquivo Público do Distrito Federal Setor de Áreas Públicas. Lote B. Bloco 41 - NOVACAP Brasília/DF – CEP 71.215-000, Fones: (61) 3361 1454 - 3361 5203 Fax: (61) 3233 2191 Atendimento ao público: de segunda à sexta-feira, de 8h às 17h

Quadro 3 - Identificação do Arquivo Público do Distrito Federal

4.2 Arquivo Público do Paraná

O Arquivo Público do Paraná[6] foi criado pela Lei n.º 33, sancionada pelo 1º Presidente da Província do Paraná, Conselheiro Zacarias de Góes e Vasconcellos, em 7 de abril de 1855. Denominado "Archivo Publico", tinha como finalidade reunir a memória impressa e manuscrita sobre a história e geografia do Paraná , - incluindo coleções de leis provinciais e gerais -,e funcionou por todo o período provincial (1855-1889) junto ao Palácio da Presidência onde foi instalada a Secretaria do Governo Provincial. No âmbito administrativo, desde a sua criação, o Arquivo Público do Paraná recebeu diferentes denominações e pertenceu a diversas secretarias. Sua primeira sede foi na Rua XV de Novembro. A segunda na Rua Mal. Floriano Peixoto. Em terreno da Rua dos Funcionários foram edificadas e adaptadas sedes em 1960, 1978 e 2001. Em 2001 foi inaugurada a nova sede (Figura 2), no mesmo terreno da Rua dos Funcionários.

Figura 2: Sede atual do Arquivo Público do Paraná
Fonte: Arquivo Público do Paraná

[6] Informações sobre o arquivo, retiradas do site: <http://www.arquivopublico.pr.gov.br/>

A nova sede possui 12 áreas de guarda de documentos, que podem abrigar até 13 mil metros lineares de documentos – se aplicada as técnicas de avaliação e gestão de documentos, - ambientes próprios para as atividades de higienização e reparos, de microfilmagem e digitalização (reprografia), sala de consultas, auditório, áreas administrativas e Espaço Cultural que abrange a biblioteca de apoio à pesquisa e aos acervos bibliográficos dos professores Cecília Maria Westphalen e Ruy Wachowicz, e local para exposições, totalizando 5.523 m2. A identificação do arquivo encontra-se no Quadro 4.

Arquivo Público do Paraná Rua dos Funcionários 1796, Cabral - Curitiba - Paraná - Brasil CEP: 80035-050 Telefones: (41) 3352-2299 - Fax: (41) 3252-1728 Horário: segunda-feira a sexta-feira, das 09h00 às 12h00 e das 13h30 às 17h30.

Quadro 4 - Identificação do Arquivo Público do Paraná

4.3 Arquivo Público do Estado do Espírito Santo

O Arquivo Público do Estado do Espírito Santo[7] (Figura 3) é criado com o nome de Archivo Público Espírito-Santense em 18 de Julho de 1908 pelo decreto nº 135 do Presidente do Estado, Dr. Jerônimo de Souza Monteiro.

Figura 3 - Sede do Arquivo Público do Estado do Espírito Santo
Fonte: Arquivo Público do Estado do Espírito Santo

[7] Informações sobre o arquivo, retiradas do site: <http://www.ape.es.gov.br/index2.htm>

Atualmente conta com aproximadamente 11 fundos documentais, de valor permanente, sendo estes preservados em caráter definitivo, em função do seu valor probatório ou informativo. A maior parte da documentação é oriunda do Poder Executivo ou de instituições a ele vinculadas. Além das atribuições legais de recolher, tratar, preservar e divulgar a documentação pública do Executivo, o Arquivo Público do Espírito Santo, recebeu conjuntos de documentos produzidos por diversas pessoas, em decorrência de suas atividades intelectuais, possuindo uma relação orgânica perceptível através de processo de acumulação. Esses recolhimentos são frutos de doações familiares.

O acervo de origem privada é composto por quatro (4) fundos documentais, nas quais constam arquivos pessoais de um ex-governador, um político, uma historiadora e um desembargador. A localização e horários de funcionamento do arquivo podem ser verificados no Quadro 5.

Arquivo Público do Estado do Espírito Santo Rua Sete de Setembro, 414 - Centro - Vitória - Espírito Santo Caixa Postal 85 - CEP: 29.015-905 Tel: (27) 32.23.75.24 - Fax: (27) 32.23.29.52 Atendimento ao público: das 10:00 às 17:30 horas

Quadro 5 - Identificação do Arquivo Público do Estado do Espírito Santo

4.4 Arquivo Público Mineiro

O Arquivo Público Mineiro[8] (APM), superintendência da Secretaria Estadual de Cultura, é responsável por planejar e coordenar o recolhimento de documentos produzidos e acumulados pelo Poder Executivo de Minas Gerais, assim como de documentos privados de interesse público. Uma vez integrados ao acervo, a instituição tem a missão de tratar e preservar esses documentos com o objetivo de colocá-los à disposição da sociedade. Nesse sentido, para facilitar e ampliar o acesso ao acervo do APM, na sua sede ou por meio da Internet, nasceu o SIA/APM, base informatizada que concentra os instrumentos de pesquisa e parte dos documentos do APM. Nela estão disponíveis para consulta: instrumentos de

[8] Informações sobre o arquivo, retiradas do site:: <http://www.siaapm.cultura.mg.gov.br/>

pesquisa, milhares de documentos, fotografias (Figura 4), filmes e a coleção centenária da Revista do Arquivo Público Mineiro.

Figura 4 - Prédio do Arquivo Público Mineiro
Fonte: Acervo do Arquivo Público Mineiro

O acervo do APM é constituído por documentos produzidos e acumulados por órgãos da Administração Pública de Minas Gerais e por arquivos privados, abrangendo desde o século XVIII até o século XX. Além de manuscritos e impressos, reúne mapas, plantas, fotografias, gravuras, filmes, livros, folhetos e periódicos. Além de reunir a documentação referente à memória do poder público, o Arquivo é o órgão responsável pela execução e administração da política relativa ao patrimônio documental do Estado, e por meio da organização, guarda e conservação dos documentos acumulados pelo Poder Executivo do Governo do Paraná, visa possibilitar o acesso rápido e seguro às informações de interesse da administração pública e do cidadão, bem como implementar e acompanhar a política estadual de arquivos (Vide Quadro 5: Identificação do Arquivo Público Mineiro) .

Arquivo Público Mineiro Av. João Pinheiro 372, Funcionários - 30130-180 Belo Horizonte, MG - Brasil Telefax: (31)3269-1060 / (31)3269-1167

Quadro 6 - Identificação do Arquivo Público Mineiro

4.5 Arquivo Público do Estado do Rio Grande do Sul

Em 8 de março de 1906, pelo Decreto 876, o então presidente do Estado, Antônio Augusto Borges de Medeiros, determinou a criação do Arquivo Público do Estado do Rio Grande do Sul[9], compondo a Repartição de Arquivo Público, Estatística e Biblioteca do Estado do Rio Grande do Sul, subordinada à Secretaria do Interior e Exterior. É composto por três prédios, sendo o prédio I foi concluído em 1912. A crescente demanda de documentos fez com que o prédio I fosse esgotando seu espaço físico. Como solução para o problema, em 1918, iniciou-se a construção do prédio II. Já o prédio III (Figura 5) é composto pela parte administrativa e técnica do arquivo, concluído no ano de 1950.

Figura 5 - Prédio do Arquivo Público do Estado do Rio Grande do Sul

O Arquivo Público do Estado do Rio Grande do Sul (APERS), Departamento da Secretaria da Administração e dos Recursos Humanos, é constituído pelas: Divisão de Documentação, Divisão de Pesquisa e Projetos e Seção de Apoio Administrativo. Desenvolve serviços diversos com o objetivo precípuo da guarda, manutenção e disponibilização do acervo, a fim de que a comunidade tenha um acesso rápido e facilitado aos documentos. Realiza atividades como: recuperação e encadernação de documentos; disponibilização de sala de microfilme de segurança; elaboração de instrumentos de pesquisa, entre outros. O APERS é, ainda, responsável pela implantação de políticas arquivísticas no Estado, como órgão de Coordenação do Sistema de Arquivo do Estado do Rio Grande do Sul (SIARQ/RS). A localização e contatos do APERS se apresentam no Quadro 7.

[9] Informações sobre o arquivo, retiradas do site: <http://www.apers.rs.gov.br/portal/index.php?menu=historico>

Arquivo Público do Estado do Rio Grande do Sul Endereço: Rua Riachuelo, 1031 – Porto Alegre Fones: (51) 3288-9100 CEP: 90010-270 Horário: de segunda-feira a sexta-feira das 8h 30 min às 17 h e sábados, das 9 às 14 h

Quadro 7 - Identificação do Arquivo Público do Estado do Rio Grande do Sul

4.6 Arquivo Público do Estado de Santa Catarina

A Lei nº 1.196 de 26 de setembro de 1918, no Governo de Felipe Schmidt, criou o Arquivo Público do Estado de Santa Catarina[10]. Nesta ocasião, o fato de não ter sido designado um Diretor provocou sua extinção natural, pois não há registro de ações no período compreendido entre os anos de 1918 a 1931. Por meio do Decreto nº 186 de 28 de dezembro do ano de 1931, no Governo do Interventor Federal Ptolomeu de Assis Brasil, o Arquivo Público é "re"criado. Mas, dois anos depois, em 1933, já no Governo do Interventor Federal Aristiliano Ramos, o Arquivo Público é extinto por meio do Decreto nº 349 de 10 de maio. Em 1960, no Governo de Heriberto Hulse, o Arquivo Público (Figura 6) é então, mais uma vez, "re"criado, pela Lei nº 2.378 de 28 de junho, e subordinado à Secretaria de Estado dos Negócios do Interior e Justiça.

Figura 6 - Prédio do Arquivo Público do Estado de Santa Catarina
Fonte: Arquivo Público do Estado de Santa Catarina

[10] Informações sobre o arquivo, retiradas do site:
<http://www.sea.sc.gov.br/index.php?option=com_content&task=view&id=90&Itemid=245&lang=>

Hoje, o Arquivo Público do Estado está subordinado à Secretaria de Estado da Administração, como um Órgão Normativo do Sistema de Gestão Documental, com a finalidade de implementar e acompanhar a Política Nacional de Arquivos, e cumpre a sua função de recolher, preservar, organizar e prestar assessoramento técnico, divulgando o patrimônio documental e colaborando com programas culturais e educativos do Estado de Santa Catarina. No Quadro 8 é apresentada a identificação e localização do arquivo.

Arquivo Público do Estado de Santa Catarina Rua Duque de Caxias, 261 – Saco dos Limões – Cx Postal 138 CEP: 88045-250 – Florianópolis, SC. Telefone: (048) 3239-6000 / 3239-6086 Horário de Funcionamento - de segunda a sexta-feira, das 13 às 19 horas Horário de Atendimento - de segunda a sexta-feira, das 13h30min às 18h30min

Quadro 8 - Identificação do Arquivo Público do Estado de Santa Catarina

4.7 Arquivo Público do Estado de São Paulo

As origens do Arquivo Público do Estado[11] remontam a 1721, pouco tempo depois do desmembramento dos territórios de São Paulo e Minas Gerais. A primeira tentativa de formalizar a atividade ocorreu com a Lei nº 20, de 8 de março de 1842, que criava um *Arquivo Provincial*, subordinado à Secretaria do Governo, mas que não chegou a ser executada. Apenas com a Repartição de Estatística e do Archivo do Estado, criada em 1891, subordinada à Secretaria do Interior, é que a atividade foi institucionalizada, com a atribuição formal de guarda de toda a documentação administrativa paulista.

Desde então o Arquivo Público do Estado recebe documentação de origem e natureza bastante diversificadas, proveniente das Secretarias de Estado, do Poder Judiciário, de cartórios e municípios, além de acervos de natureza privada, que compõem um riquíssimo acervo para a pesquisa. A repartição foi desmembrada em 1938, constituindo-se o então Departamento de Arquivo do Estado, diretamente subordinado à Secretaria de Educação e Saúde Pública.

[11] Informações sobre o arquivo, retiradas do site: <http://www.arquivoestado.sp.gov.br/ins_historico.php>

O projeto de reforma e ampliação do Arquivo Público do Estado de São Paulo atende a uma série de demandas técnicas acumuladas ao longo das últimas décadas. Em um primeiro momento, as atuais dependências da instituição, compostas por aproximadamente 7.007m² de área, serão reformadas. O novo edifício (Figura 7) será construído no mesmo terreno, o que garantirá a continuidade espacial das tarefas de gestão documental do acervo permanente. Serão 11 pavimentos, de 1.600m² cada um, e capacidade para abrigar 90 mil metros lineares de documentação sobre a história de São Paulo (Vide Quadro 9: Identificação do Arquivo público do Estado de São Paulo).

Figura 7 - Nova Sede do Arquivo Público do Estado de São Paulo
Fonte: Arquivo Público do Estado de São Paulo

Arquivo Público do Estado de São Paulo Av. Cruzeiro do Sul, 1777 – Santana – São Paulo – SP CEP: 02031-000 Fone: (11) 2089 -8100 Horário de Atendimento - das 9h00 às 17h00, de terça a sábado.

Quadro 9 - Identificação do Arquivo Público do Estado de São Paulo

No capítulo cinco, se apresentará a análise e discussão dos resultados coletados junto aos Arquivo Públicos Estaduais, estabelecendo relações entre os dados obtidos e os problemas propostos nesta investigação.

5 ANÁLISE E DISCUSSÃO DOS RESULTADOS

Neste capítulo será apresentada a análise dos dados coletados na presente pesquisa. Serão discutidos os objetivos desta investigação, com a finalidade de responder às perguntas de pesquisa propostas. A principal finalidade deste capítulo é expor as ações realizadas para o controle de acesso nos arquivos públicos estaduais estudados que contribuem para garantir e proteger a segurança das informações.

Os critérios metodológicos possibilitaram a definição das instituições que participariam da pesquisa, por meio da exclusão daquelas a qual o site obtido, na lista inicial apresentada no capítulo de metodologia deste trabalho, não fosse possível o acesso. É relevante destacar que a lista no site do CONARQ foi atualizada e realizando a busca por arquivos públicos estaduais se encontra uma lista com endereço eletrônico e contato do Arquivo Nacional, Arquivos Públicos Estaduais e do Distrito Federal[12].

O contato com as instituições deu-se por e-mail e também por telefone institucional, o que possibilitou a coleta total de sete (7) questionários válidos (de acordo com os critérios metodológicos). Os Arquivos Públicos Estaduais que participaram desta pesquisa, em busca de responder as indagações propostas, são apresentados juntamente com seu endereço eletrônico no Quadro 10:

- Arquivo Público do Distrito Federal: <http://www.arpdf.df.gov.br>;
- Arquivo Público do Estado do Paraná: <http://www.pr.gov.br/arquivopublico>;
- Arquivo Público do Estado do Espírito Santo: <http://www.ape.es.gov.br>;
- Arquivo Público Mineiro: <http://www.cultura.mg.gov.br/?task=home&sec=5>;
- Arquivo Público do Estado do Rio Grande do Sul: <http://www.apers.rs.gov.br/portal/index.php>;
- Arquivo Público do Estado de Santa Catarina: <http://www.sea.sc.gov.br/index.php?>;
- Arquivo Público do Estado de São Paulo: <http://www.arquivoestado.sp.gov.br/>;

Quadro 10 – Arquivos Públicos Estaduais selecionados para a pesquisa

[12] [http://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm]

No intuito de responder as indagações de pesquisa, este capítulo será dividido em três subcapítulos, correspondendo aos objetivos desta investigação que foram determinados no capítulo introdução deste trabalho. A análise dos dados coletados nas instituições seguirá o embasamento teórico conforme proposto na fundamentação teórica de pesquisa, e em relação ao controle de acesso seu embasamento corresponderá, mais especificamente, aos pressupostos das Normas ISO 15489, e-ARQ e ABNT NBR ISO/IEC 27002.

Visando preservar a identidade dos entrevistados adotou-se um código especificado com as iniciais “APE” (fazendo referencia a: Arquivo Público Estadual) iniciando no número 01 até o número 07 (APE 01 ao APE 07), aleatoriamente, independente da instituição. Esse código será apresentado ao longo dos subcapítulos proporcionando a análise das respostas sem que se faça necessário identificar os arquivos.

5.1 A Gestão Eletrônica de Documentos (GED) nos arquivos estudados

Neste subcapítulo será abordado o uso pelas instituições de políticas de GED. Essa questão foi levantada, pois de nada adiantaria estudar o controle de acesso objetivando proteger as informações, sistemas, equipamentos e o ambiente institucional, se as informações não estiverem gerenciadas seguindo metodologias apropriadas, possibilitando o acesso aos usuários de forma eficiente, além de segura.

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, slide 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”.

Dessa forma, num primeiro momento 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.

Tabela 1 – Gestão de Documentos

A Instituição tem políticas de Gestão de Documentos implementadas?	**Informantes**	**Percentual**
Sim	6	85,71%
Não	1	14,29%
Total	**7**	**100%**

Foi possível verificar que 85,71% das instituições 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 acesso às informações. Apenas a instituição APE 07 não possui políticas de gestão de documentos implementadas, correspondendo a 14,29% das respostas, sendo de melhor compreensão pelo Gráfico 1: Gestão de Documentos.

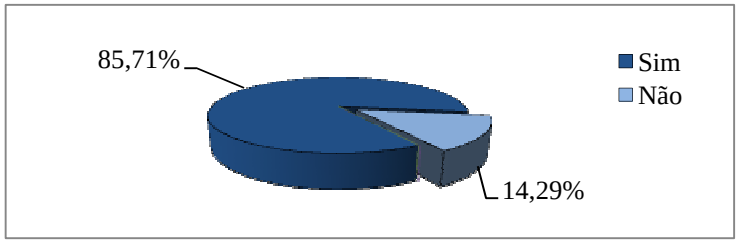


Gráfico 1 – Gestão de Documentos

Conforme a Câmara Técnica de Documentos Eletrônicos (2006), a gestão de documentos pode ser expressa através de programas e, materializada, por meio do planejamento e execução de um sistema de gestão de documentos, podendo ser convencional ou eletrônica. Desse modo facilitando o processo documental, pois por meio da avaliação, evita o acúmulo de documentos ou a eliminação não criteriosa que acarretaria na perda de

informações importantes para o desenvolvimento institucional. A gestão de documentos em instituições arquivísticas pode ser realizada da forma convencional, o que é mais comum, ou feita em meio eletrônico que é denominada Gestão Eletrônica de Documentos (GED).

Com a finalidade de averiguar o uso de GED nos arquivos públicos estaduais foi questionado aos entrevistados 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. Na Tabela 2: Gestão Eletrônica de Documentos denota-se que 85,71% das instituições não aplicam políticas de GED enquanto que 14,29% aplicam.

Tabela 2 – Gestão Eletrônica de Documentos

Essa política abrange a GED?	**Informantes**	**Percentual**
Sim	1	14,29%
Não	6	85,71%
Total	**7**	**100%**

O único entrevistado que afirmou que a instituição aplicava políticas de GED, foi o APE 01, não sendo necessário explicar sobre o assunto. O Gráfico 2: Gestão Eletrônica de Documentos, representa o percentual das respostas.

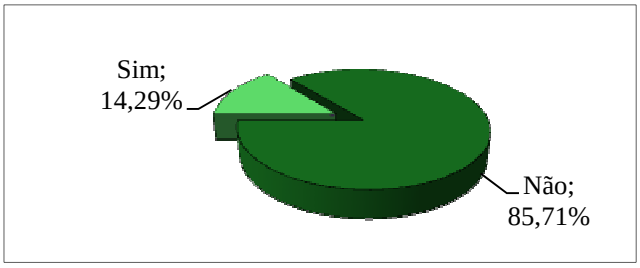


Gráfico 2 - Gestão Eletrônica de Documentos

Conforme Silva (2004), 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. De acordo com Filipakis (2009), 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 contribuindo para o desempenho institucional. Nesse sentido, Flores (2006, p. 89), complementa ainda 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, solicitado 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 entrevistado APE 03 quando diz que "está em andamento um estudo sobre a Política de Gestão Eletrônica de Documentos" e no entrevistado APE 04 que da mesma forma relata que estão trabalhando em um projeto sobre o assunto "junto à companhia de informática do Estado, mas ainda nada está definido".

O entrevistado APE 02 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 entrevistado está em concordância com 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". E ainda, sobre esse assunto, o entrevistado APE 06 não explicou o motivo da instituição não implantar GED apenas afirmou não ter sido aplicado até o momento.

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 das informações que serão repassadas 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.

5.2 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, sistemas, 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 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 [...]”.

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 proteger sua segurança e integridade. Para isso, objetivou averiguar se os entrevistados consideravam a existência de uma política de controle de acesso na instituição. Verificou-se que 85,71% dos entrevistados, afirmou que a instituição possui uma política de controle de acesso e 14,29% respondeu que não existe essa política (Vide Tabela 3: Política de Controle de Acesso).

Tabela 3 – Política de Controle de Acesso

Política de Controle de Acesso	**Informantes**	**Percentual**
Sim	6	85,71%
Não	1	14,29%
Total	**7**	**100%**

Para representar melhor visualmente os dados coletados junto aos informantes, foi elaborado o Gráfico 3: Política de Controle de Acesso.

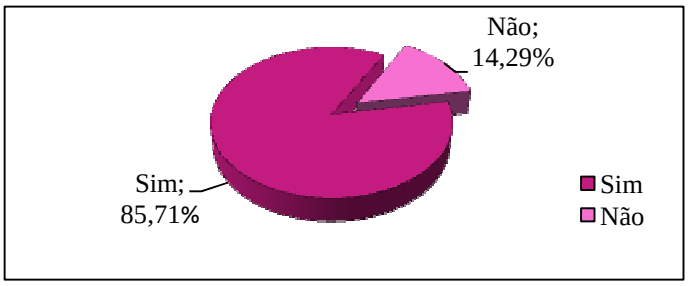


Gráfico 3 – Política de Controle de Acesso

A Associação Brasileira de Normas Técnicas (2005, p. 56) relata 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 a política de controle de acesso 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, ainda dentro da questão anterior foi solicitado aos entrevistados que afirmaram que a instituição possuía uma política de controle de acesso, 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 entrevistado APE 01 relata que os procedimentos de acesso à pesquisa do acervo documental perpassam pelo seguinte fluxo:

1- O usuário comparece a sala de pesquisa para consultar os instrumentos de busca.

2 - Após o contato com os catálogos, o usuário envia um e-mail de solicitação para agendamento de consulta aos documentos de seu interesse.

3 - O setor responsável pelo atendimento encaminha ao setor de documentação o pedido, que se encarrega de preparar, juntamente com o setor de preservação, a documentação a ser consultada.

4 - Em um prazo mínimo de 48 horas o usuário recebe a informação quanto ao agendamento de sua pesquisa.

Ainda é relatado que os documentos de caráter sigiloso possuem restrição de acesso, esclarecidas em um “Termo de Responsabilidade pelo uso da informação emitido pela instituição”.

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. Para o entrevistado essa restrição compreende três fundos documentais (não serão citados para não identificar a instituição e assim garantir o sigilo das informações). O acesso a esses documentos também é possível, mas de acordo com o entrevistado, “a parte” interessada, teria livre acesso a eles, e da mesma forma o acesso seria permitido a um terceiro, mas somente “mediante procuração”. Já para a realização de pesquisa só “será permitido o acesso a partir da apresentação de projeto de pesquisa e assinatura de termo de compromisso”. Os outros tipos documentais são de acesso livre.

O entrevistado 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 qual seriam essas normas. Já o entrevistado APE 04 afirma que o arquivo disponibiliza em

meio eletrônico o guia de fundos de um dos acervos (que não será citado para não identificar o arquivo). Trabalham por demanda, digitalizando acervos que são solicitados. Esses acervos não são apenas documentos textuais, mas também documentos sonoros que são migrados para o meio digital correspondendo as demandas de pesquisadores. “Trabalhamos na descrição arquivística de acervos com grande potencial informativo, pois entendemos que mais do que acessar o documento, o usuário precisa conhecer nossos fundos documentais”.

A respeito da política de controle acesso, o entrevistado 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 entrevistado 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”. Os documentos considerados de caráter ostensivo, ou seja, aqueles que não necessitam de restrição para acesso, “o pesquisador vem ao Arquivo, faz pesquisa em inventário e é atendido por técnico que o auxilia na pesquisa, o material que for do interesse do pesquisador, caso seja possível tecnicamente, é reproduzido ao pesquisador, que assina um termo de responsabilidade quanto ao seu uso”.

Nota-se assim, que as instituições seguem os princípios da segurança da informação que segundo a Norma ABNT NBR ISO/IEC 27002 são: confidencialidade, integridade e disponibilidade. A confidencialidade define que somente pessoas autorizadas podem acessar as informações. O uso de restrições de acesso pelos arquivos estudados pode ser um exemplo da aplicação desse princípio, já que demonstram sua atenção quanto à aplicação da legislação, ficando claro quem pode ter o acesso aos documentos e em quais condições isto é permitido.

Ainda tratando-se do uso dos princípios de segurança da informação, o APE 03 fez referência ao uso de senha para sistema informatizado, o que possibilita identificar que a pessoa está acessando ao sistema e por isso evita que aconteça adulterações nas informações, sendo um procedimento muito importante para controlar o acesso aos documentos informatizados. Pode-se perceber que essa instituição aplica o primeiro princípio de segurança da informação, a confidencialidade, e também o segundo princípio, a integridade que “é

garantido quando a informação está completa, sem alteração e, portanto, confiável". (CAMPOS, 2007, p. 18).

O último princípio, podendo ser relacionado ao comentário do APE 04, é a disponibilidade, tendo como base que a informação deve estar acessível sempre que necessário. O entrevistado citou o uso de guia do acervo que fica disponível para acesso no site do arquivo, nesse caso, a instituição realiza também a difusão do acervo sem comprometimento da segurança da informação. Para facilitar o acesso, os profissionais arquivistas elaboram instrumentos de pesquisa para cooperar na gestão documental. Desse modo, Cardoso (2005) considera que ao se produzir e difundir as informações, sejam eletrônicas ou digitais, compete aos profissionais estar constantemente atualizados para empregar ações inovadoras no tratamento dos documentos.

A preocupação com o acesso às informações pode ser verificada por meio do APE 06, quando afirma que a política de controle de acesso adota o uso de normas de descrição do acervo. Complementando o exposto Castanho, Garcia e Silva (2006, p.37), referindo-se ao acesso às informações arquivísticas salientam que "o objetivo da arquivística é tornar as informações acessíveis ao usuário, por meio do tratamento das mesmas, buscando valorizar o conteúdo informacional dos documentos, sem desconsiderar sua organicidade."

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 entrevistados 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. As instituições 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 entrevistados fizeram referência também ao uso de regras e normas internas para acesso aos documentos sendo 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 as ações implementadas na instituição. Assim sendo, o seguinte questionamento objetivou constatar se a aplicação dessa política de controle de acesso, nas instituições, seguia alguma normalização. Na Tabela 4: Uso de normalizações, apresentam-se as respostas conforme a realidade institucional dos entrevistados.

Tabela 4 – Uso de Normalizações

Essa Política é baseada em alguma normalização?	**Informantes**	**Percentual**
Sim	6	85,71%
Não	1	14,29%
Total	**7**	**100%**

No Gráfico 4: Uso de Normalizações, é possível verificar que 85,71% dos entrevistados responderam SIM, e 14,29% responderam que NÃO, ao uso de normas que baseassem as políticas de controle de acesso adotadas na instituições.

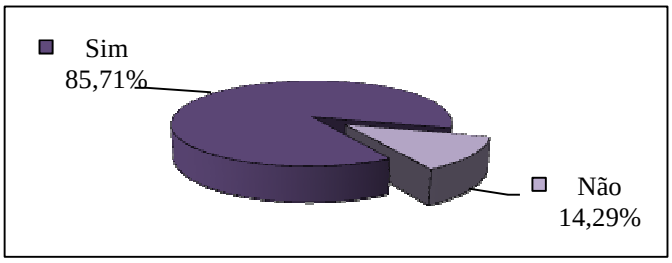


Gráfico 4 - Uso de Normalizações

No que se refere ao uso de normalizações, duas instituições citaram apenas o uso de normas de descrição arquivística. Os instrumentos de pesquisa são resultados da utilização de normas de descrição e contribuem para racionalizar a massa documental acumulada, permitindo assim, a rápida recuperação da informação para consulta, por meio da descrição. Os instrumentos de pesquisa podem ser definidos como "as ferramentas utilizadas para descrever um arquivo, ou parte dele, tendo a função de orientar a consulta e de determinar com exatidão quais são e onde estão os documentos". (LOPEZ, 2002, p. 10).

Os entrevistados APE 04 e APE 06 citaram o uso da Nobrade para a descrição do acervo. A Nobrade "estabelece diretivas para a descrição no Brasil de documentos arquivísticos, compatíveis com as normas internacionais em vigor ISAD(G) e ISAAR (CPF), e tem em vista facilitar o acesso e o intercâmbio de informações em âmbito nacional e internacional". (BRASIL, 2006, p. 10)

O pesquisado APE 03, ao invés de citar normalização, citou normas internas que se referem ao acesso do usuário na instituição, deixando subentendido que a política é baseada praticamente em normas internas estabelecidas pela própria instituição. Da mesma forma o sujeito APE 05 citou as normas como sendo o uso de "princípios e rotinas arquivísticas de preservação e atendimento ao pesquisador, bem como atenção quanto à legislação federal e estadual, e também quanto ao tratamento à documentação pública histórica".

Os dois últimos entrevistados citaram praticamente as mesmas normas que são seguidas para a elaboração da política de controle de acesso institucional. O APE 02 fez referência à Constituição Federal e, também, à Lei 8.159 e suas alterações, e ainda afirmou estar subordinado às regras de acesso definidas por uma secretaria do estado. Da mesma forma, o APE01 referenciou a Constituição Federal e a Lei de Arquivos, Lei 8.159 e ainda a

Lei 11.111 como sendo as normas seguidas para a elaboração da política de controle de acesso na instituição.

A relevância do uso dessas normalizações citadas pelas últimas instituições é o que fará a diferença para a proteção efetiva da segurança da informação e também para o bom desenvolvimento das ações de gestão, acesso e controle de acesso. A Lei do Arquivo, ou seja, a Lei de nº 8.159, em especial, dispõe sobre a política nacional de arquivos públicos e privados, considerando a gestão de documentos como dever do Poder Público, assim como, a proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação. A outra Lei referenciada foi a Lei nº 11.111/2005 e tratando-se dela, Santos (2005, p. 86), relata que "dispõe sobre a instituição, no âmbito da Casa Civil, de "Comissão de Averiguação e análise de Informações Sigilosas, com a finalidade de decidir sobre a aplicação e ressalva ao acesso dos documentos" (Art. 4º) e ratifica os prazos estabelecidos pela lei 8.159/91".

Cabe ressaltar que o uso das Normalizações assegura a qualidade dos processos de gestão, buscando que os documentos cumpram seu fim, permanecendo acessíveis o maior tempo possível. As instituições estudadas demonstram a preocupação com o uso de normalizações, mesmo não referenciando o controle de acesso, sendo que sua aplicação contribui para a organização institucional ao definir ações que objetivam o acesso e proteção das informações. Dessa forma, destaca-se a definição de Beyea, (2007, p. 34) para motivar as instituições na aplicação de normalizações, ao definir que os "arquivistas devem ser instruídos sobre o objetivo e os detalhes de uma norma. Eles devem ser encorajados a apoiar e a implementar normas. Normas devem ser mantidas e revisadas".

5.3 As ações de controle de acesso comuns entre as instituições pesquisadas.

Nesse 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 entrevistados, foi possível definir entre as ações aplicadas para o controle de acesso quais são comuns nos arquivos públicos estaduais estudados.

Alguns entrevistados afirmaram, anteriormente, que dentro da política de controle de acesso, alguns documentos são de acesso restrito, de acordo com a legislação. Desse modo, torna-se relevante salientar que o acesso aos documentos dentro da própria instituição deve seguir regras e/ou normas com o intuito de fiscalizar a movimentação de pessoas em áreas não permitidas. O capítulo nove da ABNT NBR ISO/IEC 27002, aborda essa questão (Segurança física e do ambiente), apresenta diretivas para proporcionar áreas seguras prevenindo o acesso físico não autorizado, danos e interferências com as instalações e informações da instituição.

Para garantir a segurança nos arquivos, segundo essa mesma norma, é relevante o uso de perímetros de segurança, que podem ser as paredes, portões de entrada controlados por cartão ou balcões de recepção com recepcionistas para proteger e evitar o acesso livre as áreas que contenham as informações e instalações de processamento da informação. Nessas áreas só podem ter acesso as pessoas que possuírem autorização. Para isso, é fundamental reforçar o controle nos locais onde é guardada a documentação, pois essa área pode ser considerada de risco, baseado no propósito que a informação como um ativo institucional, deve ser protegida e permanecer segura.

O questionamento seguinte teve base o interesse de saber sobre os cuidados com o acesso não permitido aos locais de guarda da documentação. Foi perguntado aos entrevistados quem possuía livre acesso aos locais de guarda da documentação para verificar como as instituições realizavam esse controle. Dessa forma foram ofertadas as seguintes opções de resposta em relação a quem teria acesso aos locais de guarda (Vide Tabela 5: Acesso Livre aos locais de guarda da documentação):

- Todos os funcionários;

- Somente funcionários responsáveis pela gestão documental;

- Visitantes, com acompanhamento de responsáveis;

- Pesquisadores;

- Usuários;

- Outros.

Tabela 5 – Acesso livre aos locais de guarda da documentação

Acesso aos locais de guarda da documentação	**Número de Citações**	**Percentual**
Todos os funcionários	2	20%
Somente funcionários responsáveis pela gestão documental	4	40%
Visitantes, com acompanhamento de responsáveis	3	30%
Pesquisadores	0	0
Usuários	0	0
Outros: Funcionários do setor de conservação e do setor de atendimento e pesquisa, e um representante do órgão produtor que tem cadastro para acessar a documentação de caráter intermediária.	1	10%
Total	**10**	**100%**

De acordo com o Gráfico 5: Acesso Livre aos locais de guarda da documentação, pode-se observar visualmente que os usuários de arquivos não foram citados nenhuma vez pelos entrevistados. Torna-se relevante deixar claro que nesse sentido, usuários de arquivos são considerados todas as pessoas físicas ou jurídicas que realizam pesquisas em arquivos, sendo denominadas também de “consulentes, leitor ou pesquisador”. (D.B.T.A, 2005, p. 169). No entanto, a opção “Todos os funcionários” recebeu duas (2) citações correspondendo a 20%. A opção “Somente funcionários responsáveis pela gestão documental” foi a que recebeu o maior número de citações, quatro (4) correspondendo a 40%, no caso da opção “Visitantes, com acompanhamento de responsáveis” recebeu 3 citações correspondendo a 30% das citações e, ainda, na opção “Outros” foi citado por um entrevistado, representando 10% das respostas.

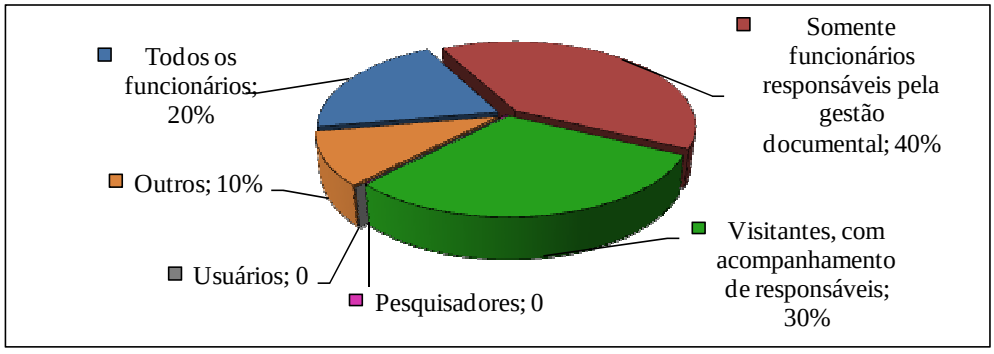


Gráfico 5 - Acesso livre aos locais de guarda da documentação

Em muitos arquivos o usuário só tem acesso à sala de consulta, onde pode realizar a pesquisa documental, e dentro dela seguem normas elaboradas com o intuito de manter a ordem no local e proporcionar o acesso com segurança, evitando possíveis danos às informações. A existência de uma sala de consulta demanda a criação de regras para acesso a esses usuários. Regras estas, que existem nos arquivos públicos estaduais e foram citados no subcapítulo anterior, (As políticas de controle de acesso nos Arquivos Públicos Estaduais) incluídas dentro da política de controle de acesso das instituições. Com a finalidade de examinar a existência de salas de consultas nos arquivos públicos estaduais, foi questionado aos entrevistados se a instituição possuía sala de consulta. A partir desse questionamento, foi possível obter o dado de que para a totalidade dos informantes, as instituições possuem sala de consulta para usuários, conforme Tabela 6: Sala de consulta.

Tabela 6 – Sala de Consulta

A instituição possui sala de consulta?	**Informantes**	**Percentual**
Sim	7	100%
Não	0	0
Total	**7**	**100%**

Como forma de verificar o acesso de usuários a computadores nos arquivos e complementando o questionamento anterior, foi perguntado aos entrevistados se a sala de consulta possuía computadores para acesso de usuários. A Tabela 7: Uso de computadores por usuários na sala de consulta, demonstra claramente uma divisão nas respostas dos entrevistados.

Tabela 7 – Uso de computadores por usuários na sala de consulta

A sala de consulta possui computadores acessíveis aos usuários?	**Informantes**	**Percentual**
Sim	4	57,14%
Não	3	42,86%
Total	**7**	**100%**

Visando esboçar melhor as respostas dos entrevistados foi elaborado o Gráfico 6: Uso de computadores por usuários na sala de consulta, que demonstra claramente que 57,14% das respostas são afirmativas, e 42,86% representam as respostas negativas, resultando que a maioria dos arquivos dispõe de computadores para acesso a usuários.

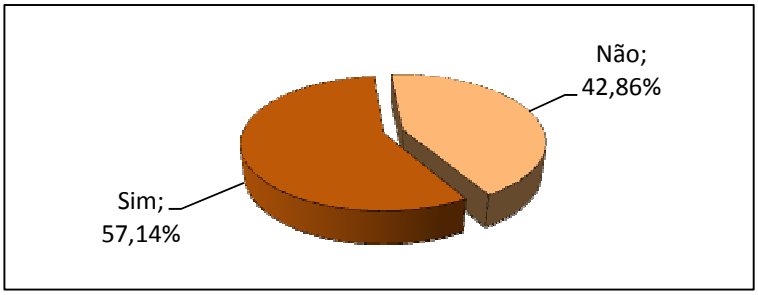


Gráfico 6 - Uso de computadores por usuários na sala de consulta

Cabe salientar que as instituições que possuem sala de consulta com acesso a computadores para usuários foram o APE 01, APE 03, APE 04 e o APE 06. Essas instituições devem ter cuidados redobrados quanto à segurança da informação, elaborando regras para condicionar esse acesso, também, como forma de manter o desempenho institucional sem comprometer a segurança de sistemas, das informações e dos equipamentos. Por outro lado, as instituições que não possuem computadores para acesso a usuário são APE 02, APE 05 e APE 07. Pode-se dizer que essa instituição possui um risco menor quanto à segurança das informações se baseado no fato do que não possibilitam o uso de sistemas computacionais a usuários.

As regras de acesso existentes nos arquivos devem servir de auxilio para a elaboração de regras e normas específicas para acesso e uso de computadores, necessitando ser também conhecidas pelos usuários. Os computadores utilizados na sala de consulta podem ser compartilhados por várias pessoas, representando um risco tanto para a segurança da instituição quanto do próprio usuário, sendo “o elemento que faz a diferença para que o processo de segurança exista de forma eficaz. Para tanto, ele precisa ser treinado e conscientizado. Isso acontecendo, o usuário sairá do estágio de envolvimento com a segurança para o estágio de comprometimento”. (FONTES, 2008, p 186).

A fim de se conhecer as ações realizadas para o controle de acesso nos arquivos pesquisados, o último questionamento trouxe como opções aos entrevistados, 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, foi dada as duas opções de respostas aos entrevistados dependendo da medida que estava sendo referenciada na questão. (Vide Tabela 8: Medidas adotadas para o controle de acesso).

Tabela 8 – Medidas adotadas para o controle de acesso

Medidas adotadas para o controle de acesso	**Número de Citações**	**Percentual**
Não há controle	0	0
Uso de identificador de usuário	0	0
Criptografia	0	0
Assinaturas digitais	0	0
Senha individual de acesso ao sistema operacional, por usuário	0	0
Desconexão do terminal por inatividade, por funcionário	0	0
Autorização para uso de rede sem fio, por usuário	1	2,85%
Desconexão do terminal por inatividade, por usuário	1	2,85%
Sistema de alarmes	1	2,85%
Circuito interno de vídeo	1	2,85%
Outro	2	5,72%
Autorização para uso de rede sem fio, por funcionário	2	5,72%
Uso de credenciais de identificação, por usuário	2	5,72%
Senha individual de acesso ao sistema operacional, por funcionário	3	8,58%
Bloqueio de sites não autorizados, por usuário	3	8,58%
Bloqueio de sites não autorizados, por funcionário	4	11,43%
Cópias de segurança	4	11,43%
Uso de credenciais de identificação, por funcionário	5	14,28%
Cadastro dos usuários do arquivo	6	17,14%
Total	**35**	**100%**

Para melhor expor os resultados foram somados os números de citações dos entrevistados totalizando 34, já que na questão poderia marcar mais de uma opção. A medida mais referenciada pelos entrevistados foi o “Cadastro de usuários de arquivo” com 6, citações,

logo após foi a medida “Uso de credenciais de identificação”, por funcionários” com 5 citações, depois, as “Cópias de segurança” e o “Bloqueio de sites não autorizados, por funcionários” com 4 citações, e com 3 citações apareceu o “Bloqueio de sites não autorizados, por usuários”.

As opções que tiveram 2 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 entrevistado 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 Gráfico 7: Medidas adotadas para o controle de acesso, apresenta somente as opções citadas pelos entrevistados como ações de controle de acesso aplicada nos arquivos.

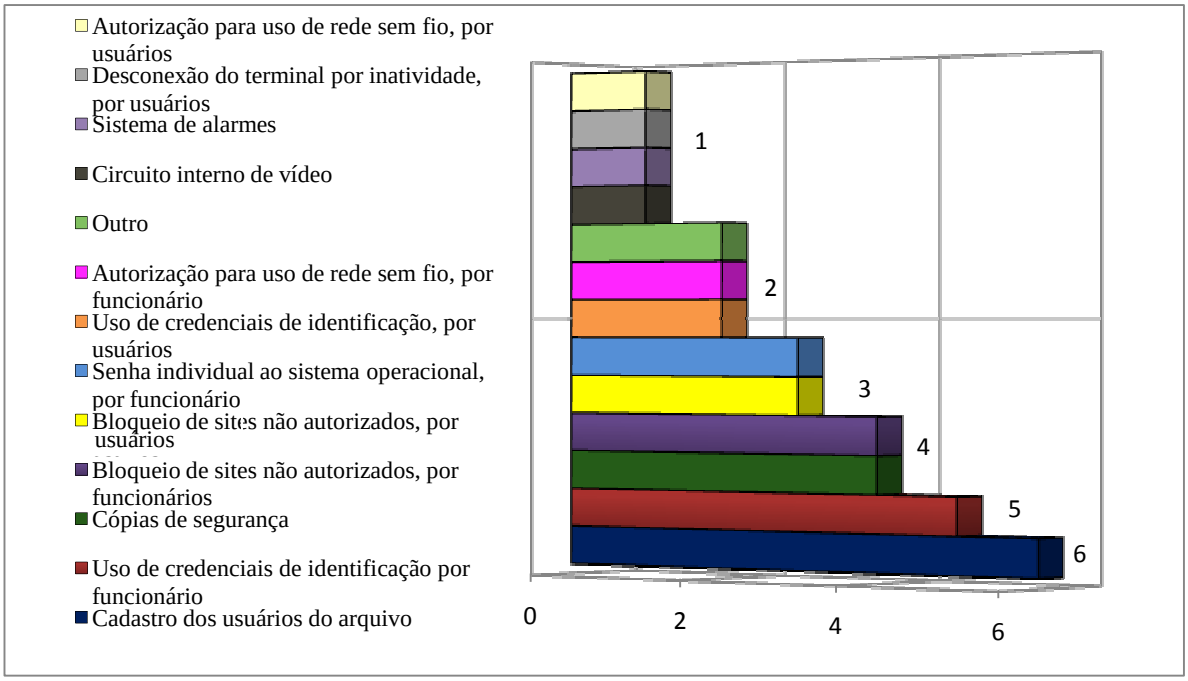


Gráfico 7 – Medidas adotadas para o controle de acesso

No que se trata a opção “Outros”, foram encontradas respostas dos seguintes entrevistados: APE 02 e APE 03. Para esses sujeitos pesquisados a instituição realizava outra medida além das citadas no instrumento de coleta de dados (Vide Apêndice A). 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 onde 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. No Quadro 11 é possível visualizar a relação de respostas entre as instituições pesquisadas, a respeito das ações de controle de acesso consideradas comuns nesta pesquisa.

AÇÕES DE CONTROLE DE ACESSO	ENTREVISTADOS					
1. Autorização para uso de rede sem fio, por funcionário;	APE 01	APE 02				
2. Uso de credenciais de identificação, por usuário;	APE 03	APE 06				
3. Senha individual de acesso ao sistema operacional, por funcionário;	APE 01	APE 02	APE 07			
4. Bloqueio de sites não autorizados, por usuário;	APE 01	APE 03	APE 06			
5. Bloqueio de sites não autorizados, por funcionário;	APE 01	APE 02	APE 03	APE 06		
6. Cópias de segurança;	APE 01	APE 03	APE 04	APE 06		
7. Uso de credenciais de identificação, por funcionário;	APE 01	APE 03	APE 04	APE 06	APE 07	
8. Cadastro dos usuários do arquivo;	APE 01	APE 02	APE 03	APE 05	APE 06	APE 07

Quadro 11 – Ações de controle de acesso comuns entre as instituições pesquisadas

Deste modo, as ações realizadas para controle de acesso que são comuns 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; Bloqueio de sites não autorizados, por funcionário e Autorização para uso de rede sem fio, por funcionário.

A finalidade do controle de acesso é basicamente proteger a informação, sistemas, equipamentos e o ambiente institucional do acesso não autorizado de usuários e/ou funcionários. Dentre as ações comuns entre os entrevistados 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 com 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. Aquelas têm 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: Bloqueio de sites não autorizados, por usuário e por funcionários e Autorização para uso de rede sem fio, por funcionário. Sendo relevante destacar que estas duas ações são complementares, pois dentro do controle de acesso a serviços de rede é relevante que seja adotado medidas para controlar tanto o acesso a rede sem fio, como também, definir se há necessidade de bloquear sites que a instituição não autorize o acesso, achando indevido. A instituição deve autorizar acesso às redes sem fio a apenas pessoas que, de acordo com a política de segurança institucional não representem risco para a segurança e proteção das informações.

Conforme entrevista realizada por Vicentin (2009) com profissionais de empresas renomadas sobre o bloqueio a sites de relacionamento em ambiente de trabalho demonstrou que em muitas empresas o acesso a esses sites ainda é liberado, mas que conforme os profissionais o uso abusivo é o que obriga as empresas a adotar a uma política de restrição e monitoramento da rede. O bloqueio de sites não autorizados, adotado como uma medida de controle de acesso comum entre os arquivos públicos estaduais estudados demonstra além da preocupação com o rendimento do trabalho um cuidado maior com a segurança das informações que serão recebidas e enviadas por meio da instituição.

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, equipamentos e ambiente institucional, se aliadas ao comprometimento das instituições com a aplicação e avaliação permanente de regras e normas de segurança, e frente também ao comprometimento dos usuários em cumpri-las.

O capitulo seis, apresentará um fechamento das inferências comentadas até aqui, expondo de forma clara e concisa as considerações finais acerca dos objetivos desta pesquisa.

6 CONSIDERAÇÕES FINAIS

As conclusões apresentadas nesse capítulo buscam sintetizar as respostas que basicamente foram propostas nos questionamentos desta pesquisa. Assim, esse capítulo retoma os objetivos de pesquisa definidos na introdução deste trabalho, como forma de demonstrar os resultados obtidos por meio das respostas dos entrevistados podendo- se chegar à apresentação de conclusões resultantes da presente investigação.

O foco desse estudo, no caso, o controle de acesso, encontra-se dentre os fatores que contribuem para a segurança da informação em uma instituição. Para que o gerenciamento das informações se torne eficaz e seguro, 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.

Inicialmente cabe registra 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 às informações, sistemas, equipamento e o ambiente institucional, se as informações não estiverem 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 entrevistados, 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 entrevistados relatou que estão 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 entrevistado afirmou que o arquivo não possuía uma política para controle de acesso, 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.

A pesquisa possibilitou encontrar seis políticas de controle de acesso, de acordo com as explanações apresentadas pelos entrevistados dos arquivos públicos estaduais, conforme resultado da pesquisa são essas:

1ª – Baseada em procedimentos de acesso à pesquisa do acervo documental. Nessa política o usuário comparece à sala de pesquisa para consultar os instrumentos de busca. Após consultá-los pode enviar um e-mail de solicitação para agendamento de consulta aos documentos de seu interesse, assim, o setor responsável pelo atendimento encaminha o respectivo pedido ao setor de documentação, que se encarrega de preparar, juntamente com o setor de preservação, a documentação a ser consultada. Em um prazo mínimo de 48 horas o usuário recebe a informação quanto ao agendamento de sua pesquisa. Ainda dentro dessa política estão os documentos de caráter sigiloso que, possuem restrição de acesso esclarecido de acordo com o termo de responsabilidade pelo uso da informação, emitido pela instituição;

2ª – Embasada em procedimentos de restrição de acesso, conforme legislação. O acesso a esses documentos é possível, mas conforme essa política somente mediante procuração e para fins de pesquisa mediante apresentação de projeto de pesquisa e assinatura de termo de compromisso;

3ª – O acesso a sistemas informatizados só é permitido mediante cadastro dos usuários Os usuários de arquivos para consulta e acesso a documentos devem seguir regras internas de controle de acesso determinadas pela instituição;

4ª – Os usuários têm acesso livre ao guia de fundo em ambiente *on-line*, como forma de conhecer o acervo da instituição. Trabalham por demanda, digitalizando acervos que são solicitados, no caso por pesquisadores. A política dessa instituição é baseada no princípio de

que o usuário necessita conhecer o acervo presente no arquivo além de apenas acessar os documentos;

5ª – Se baseia na localização topográfica e guia de acervo, ou seja, as ações realizadas têm como prioridade facilitar a localização e acesso aos documentos. Essa política não define claramente as ações de controle de acesso, sendo a menos específica, entre todas as políticas citadas;

6ª – De acordo com as regras estabelecidas por essa política, os documentos são considerados de caráter ostensivo, ou seja, de livre acesso ao público, com exceção aos documentos sigilosos, que necessitem ter acesso restrito. O usuário realiza a pesquisa no arquivo e caso tenha interesse em algum material, se for possível tecnicamente, este é reproduzido, no entanto o mesmo, por medidas de controle, assina um termo de responsabilidade quanto ao seu uso.

De um modo geral, a políticas de controle de acesso expostas pelas instituições estudadas comprovam a preocupação com o acesso às informações, podendo ser notada, por meio da aplicação de questões legais quando se referem aos documentos de acesso restrito e uso de normalizações. Portanto, as políticas apresentadas como resultado desta pesquisa, contribuem no desenvolvimento institucional ao definir ações que objetivam o acesso e 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, 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 sites, 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.

Contudo, podem-se atingir certamente os objetivos propostos na pesquisa. 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. Ainda, 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.

Deve-se salientar ainda que, embora nenhum modelo de controle de acesso seja totalmente perfeito, as instituições devem sempre procurar elaborar aquele que melhor se encaixe as necessidades institucional de modo que se consiga minimizar, cada vez mais, os riscos de incidentes em segurança da informação.

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 (Conteúdo técnico idêntico ao da ABNT NBR ISO/IEC 17799), 2005.

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

BEYEA, Marion et. al. A Favor de Normas para a Prática Arquivística**. Acervo:** revista do Arquivo Nacional. Rio de Janeiro: Arquivo Nacional, v. 20 n. 1-2, p. 31-38, jan/dez 2007.

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 de 30 de dezembro de 2002, p. 6.

___. Conselho Nacional de Arquivos. **Lei n. 8.159, de 8 de janeiro de 1991.** Dispõe sobre a política nacional de arquivo público e privados e dá outras providências. Diário Oficial. Brasília, n. 6, p 455, 9 de janeiro de 1999, seção 1.

___. Conselho Nacional de Arquivos. **NOBRADE:** Norma Brasileira de Descrição Arquivística. Rio de Janeiro: Arquivo Nacional, 2006. Disponível em <http://www.conarq.arquivonacional.gov.br/Media/publicacoes/nobrade.pdf>. Acesso em 15 mai. 2008.

BRITO, Djalma Mandu de. **A informação arquivística na arquivologia pós-custodial.** Arquivística.net - www.arquivistica.net, Rio de Janeiro, v.1, n.1, p. 31- 50 jan/jun.2005.

CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS. **Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos:** e-ARQ**.** Conarq, 2006. Disponível em: <http://www.conarq.arquivonacional.gov.br/Media/publicacoes/earqbrasilv1. pdf>. Acesso em 09 out. 2007.

CAMPOS, André. **Sistema de Segurança da Informação:** controlando os riscos. 2. ed. Florianópolis: Visual Books, 2007.

CAPEMISA. **Diretrizes e Políticas de Segurança da Informação.** Conselho de Administração, 2008. Disponível em: <http://www.capemisa.com.br/SegurancadaInformacao.pdf>. Acesso em: 14 mai. 2010.

CARDOSO, Julio Cesar; LUZ, André Ricardo. Os arquivos e os sistemas de gestão da Qualidade. **Arquivística**.net, Rio de Janeiro, v.1, n.1, p.51-64, jan./jun. 2005. Disponível em <www.arquivistica.net/ojs/include/getdoc.php?id=51&article=6&mode=pdf> Acesso em 18 nov. 2006.

CASTANHO, Denise Molon; GARCIA, Olga Maria Correa; SILVA; Rosani Beatriz Pivetta. **Arranjo e descrição de documentos arquivísticos.** Santa Maria: Universidade Federal de Santa Maria, 2006.

DICIONÁRIO BRASILEIRO DE TERMINOLOGIA ARQUIVÍSTICA. Rio de Janeiro:Arquivo Nacional, 2005.

FILIPAKIS, Cristina. **Gestão Eletrônica de Documentos Científicos.** Centro Universitário Luterano de Palmas. Tocantins, 2009. Disponível em: <http://www.ulbra-to.br/Noticias/Gestao-Eletronica-de-Documentos-Cientificos.aspx>. Acesso em: 02 jun. 2010.

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

FONTES, Edson Luiz Gonçalves. **Praticando a segurança da informação.** Rio de Janeiro: Brasport, 2008.

GUILHERME, Joel. **Criptografia, Chaves Públicas e Assinatura Digital para Leigos.** [S.l], 2003. Disponível em: <www.sbis.org.br/Criptografia.doc>. Acesso em: 19 mai. 2010.

HENRIQUES, Cecília. **ISO 15489-1 e ISO/TR 15489-2**: uma Norma para gestão de arquivos. Instituto dos Arquivos Nacionais/Torre do Tombo, 2002. Disponível em: <www.dotecome.com/infoimagem/infoimagem/info38/38art3.htm - 15k> Acesso em 21 abr. 2008.

ISO 15489-1: 2001 - Information and documentation – Records management - Part 1: General.

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, 2002. Disponível em: <http://www.iantt.pt>. Acesso em 21 nov. 2007.

LOPES, Luis Carlos. **A nova arquivística na Modernização Administrativa.** Rio de Janeiro: Papéis e Sistemas Assessoria Ltda, 2000.

LOPEZ, André Porto Ancona. **Como descrever documentos de arquivo:** elaboração de instrumentos de pesquisa. São Paulo: Arquivo do Estado, Imprensa Oficial do Estado, 2002. (Projeto como fazer; v.6).

MEDEIROS, Carlos Diego Russo. **Segurança da Informação:** Implantação de Medidas e Ferramentas de Segurança da Informação. Universidade da Região de Joinville – INIVI. Departamento de Informática. Joinville, 2001. Disponível em: <http://www.linuxsecurity. com.br/info/general/TCE_Seguranca_da_Informacao.pdf>. Acesso em: 24 mai. 2010.

RICHTER, Eneida Izabel Schirmer. **Introdução à Arquivologia.** 2. ed – Santa Maria: FACOS-UFSM, 2004.

RODRIGUES, Ana Célia. **Diplomática contemporânea como fundamento metodológico da identificação de tipologia documental em arquivos.** Tese (Doutora em História Social) Universidade de São Paulo. São Paulo, 2008. Disponível em: <http://www.asocarchi. cl/DOCS/134.PDF>. Acesso em: 07 nov. 2009.

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

SANCHEZ, Sandra. **Instrumentos da Pesquisa Qualitativa.** Disponível em: <http://www.ia.ufrrj.br/ppgea/conteudo/T2-5SF/Sandra/Instrumentos%20da%20Pesquisa%20Qualitativa.ppt#260,7,Slide 7> Acesso em: 16 jun. 2009.

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

SFREDDO, Josiane Ayres. **O controle de acesso na percepção dos profissionais de arquivo:** uma questão de segurança das informações institucionais. Trabalho de Conclusão de Curso (Bacharel em Arquivologia). Universidade Federal de Santa Maria, 2008.

SILVA, André Thiago Souza da; SALDANHA, Hugo Vasconcelos. **Controle de Acesso Baseado em Papéis na Informatização de Processos Judiciais.** Monografia (Bacharelado em Ciência da Computação). Universidade de Brasília - UnB. Brasília, 2006.

SILVA, Danielle Pereira 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: 07 jun. 2010.

SOUSA, Ana Paula de Moura. et al. **Princípios da descrição arquivística do suporte convencional ao eletrônico.** Arquivística.net (www.arquivística.net), Rio de Janeiro, v.2, n.2, p. 38-51. ago./dez., 2006.

SPANCESKI, Francini Reitz. **Política de Segurança da Informação -** Desenvolvimento de um modelo de segurança da informação voltado para instituições de ensino. Trabalho de Conclusão de Curso (Bacharel em Sistemas de Informação). Instituto Superior Tupy. Joinville, 2004. Disponível em: <http://www.mlaureano.org/aulas_material/orientacoes2/ist_2004_francini_politicas.pdf>. Acesso em: 20 abr. 2010.

SUDRÉ, Gilberto. **Mídias removíveis:** risco a segurança das suas informações. Setembro de 2005. Disponível em: < http://imasters.uol.com.br/artigo/3591/seguranca/midias_removiveis_risco_a_seguranca_das_suas_informacoes/>. Acesso em: 18 mai. 2010.

VALENTIM, Marta. **Gestão Documental.** Universidade Estadual Paulista. Marília, 2008. Disponível em: <www.valentim.pro.br/Slides/Arquivos/**Gestao**_Documental. ppt>. Acesso em: 29 mai. 2010.

VICENTIN, Tissiane. **Sites de relacionamento no ambiente de trabalho.** Vila Sucesso, 2009. Disponível em: <http://vilamulher.terra.com.br/sites-de-relacionamento-no-ambiente-de-trabalho-5-1-37-374.html>. Acesso em 30 mai. 2010.

VERGÍLIO, Sílvia Regina. **Software e engenharia de software.** Universidade Federal do Paraná, 2009. Disponível em: <http://www.inf.ufpr.br/silvia/ES/SweES/SweESalunos.pdf> Acesso em: 11 out. 2009.

YIN, Robert K. **Estudo de Caso:** planejamento e métodos. Porto Alegre: Bookma

APÊNDICES

APÊNDICE A – Questionário de Pesquisa

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

QUESTIONÁRIO DE PESQUISA

Apresentamos este questionário como instrumento de coleta de dados para a pesquisa científica denominada "*SEGURANÇA DA INFORMAÇÃO ARQUIVÍSTICA: O CONTROLE DE ACESSO EM ARQUIVOS PÚBLICOS ESTADUAIS*". Sendo requisito para a obtenção do grau de especialista em Gestão em Arquivos. Elaborado e executado pela Bacharel em Arquivologia Josiane Ayres Sfreddo, sob orientação do Profº. Dr. Daniel Flores da Universidade Federal de Santa Maria.

josisfreddo@mail.ufsm.br
flores@smail.ufsm.br

Instituição: _____

Nome do Entrevistado: _____(Em sigilo)

Cargo/função que exerce: _____

GESTÃO DE DOCUMENTOS

1. A Instituição tem políticas de Gestão de Documentos implementadas?

( ) Sim	( ) Não

1.1 Se afirmativo, essa política abrange a Gestão Eletrônica de Documentos (GED)?

( ) Sim	( ) Não

1.1.1 Se negativo (a questão 1.1), explique por quê:

SEGURANÇA DA INFORMAÇÃO: O CONTROLE DE ACESSO

2. A instituição possui uma política de controle de acesso?

( ) Sim	( ) Não

2.1 Descreva como ela funciona:

2.2 Essa política é baseada em alguma normalização?

( ) Sim	( ) Não

2.2.1 Se afirmativo, qual ou quais?

3. Quem possui acesso livre aos locais de guarda da documentação? (pode ser marcada mais de uma opção)

( ) Todos os funcionários	( ) Somente funcionários responsáveis pela gestão documental;
( ) Visitantes, com o acompanhamento de responsáveis	( ) Pesquisadores;
( ) Usuários	( ) Outros. Quais? _____

4. A instituição possui sala de consulta?

( ) Sim	( ) Não

4.1 Se afirmativo, a sala possui computadores acessíveis aos usuários?

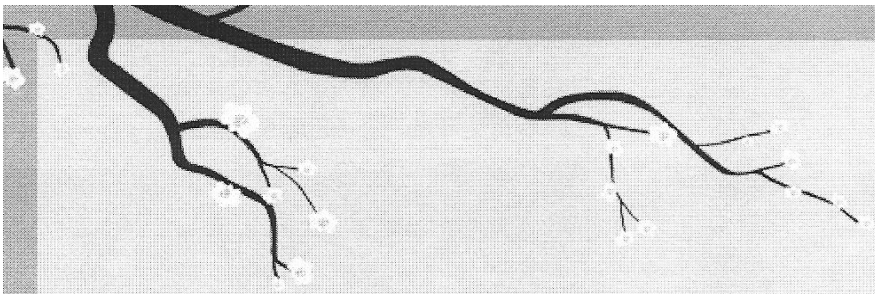
( ) Sim	( ) Não

5. Marque a (as) medida (as) adotada (as) para o controle de acesso às informações, ambientes e equipamentos na instituição:

( ) Cadastro dos usuários do arquivo	( ) Uso de identificador de usuário (ID único)
( ) Circuito interno de vídeo;	( ) Sistema de alarmes;
( ) Criptografia;	( ) Cópias de segurança
( ) Assinaturas digitais	Senha individual de acesso ao sistema operacional: ( ) Por usuários ( ) Por funcionários
Uso de credenciais de identificação: ( ) Por usuários ( ) Por funcionários	Bloqueio de sites não autorizados: ( ) Por usuários ( ) Por funcionários
Desconexão do terminal por inatividade: ( ) Por usuários ( ) Por funcionários	Autorização para uso de rede sem fio ( ) Por usuários ( ) Por funcionários
( ) Não há controle	( ) Outras. Quais?_____

Obrigada!

APÊNDICE B – Questionário *on-line*



QUESTIONÁRIO DE PESQUISA

Apresentamos este questionário como instrumento de coleta de dados para a pesquisa científica denominada "SEGURANÇA DA INFORMAÇÃO ARQUIVÍSTICA: O CONTROLE DE ACESSO EM ARQUIVOS PÚBLICOS ESTADUAIS". Sendo requisito para a obtenção do grau de especialista em Gestão em Arquivos da Universidade Federal de Santa Maria/Univerdsidade Aberta do Brasil. Elaborado e executado pela Bacharel em Arquivologia Josiane Ayres Sfreddo, sob orientação do Profº. Dr. Daniel Flores da Universidade Federal de Santa Maria.

josisfreddo@mail.ufsm.br
flores@smail.ufsm.br

GESTÃO DE DOCUMENTOS

1. A Instituição tem políticas de Gestão de Documentos implementadas?

- ◯ Sim
- ◯ Não

1.1.1 Se negativo (a questão 1.1), explique por quê:

1.1 Se afirmativo, essa política abrange a Gestão Eletrônica de Documentos (GED)?

- ◯ Sim
- ◯ Não

SEGURANÇA DA INFORMAÇÃO: O CONTROLE DE ACESSO

2. A instituição possui uma política de controle de acesso as informações?

- ◯ Sim
- ◯ Não

2.1 Descreva como ela funciona:

2.2 Essa política é baseada em alguma normalização?

- ◯ Sim
- ◯ Não

2.2.1 Se afirmativo, qual ou quais?

3. Quem possui acesso livre aos locais de guarda da documentação? (pode ser marcada mais de uma opção)

- ☐ Todos os funcionários
- ☐ Somente funcionários responsáveis pela gestão documental;
- ☐ Visitantes, com o acompanhamento de responsáveis
- ☐ Pesquisadores;
- ☐ Usuários
- ☐ Outro:

4. A instituição possui sala de consulta?

- ◯ Sim
- ◯ Não

4.1 Se afirmativo, a sala possui computadores acessíveis aos usuários?

- ◯ Sim
- ◯ Não

5. Marque a (as) medida (as) adotada (as) para o controle de acesso às informações, ambientes e equipamentos na instituição:

- ☐ Cadastro dos usuários do arquivo
- ☐ Uso de identificador de usuário (ID único)
- ☐ Circuito interno de vídeo;
- ☐ Sistema de alarmes;
- ☐ Criptografia;
- ☐ Cópias de segurança
- ☐ Uso de credenciais de identificação, por usuários;
- ☐ Uso de credenciais de identificação, por funcionários;
- ☐ Bloqueio de sites não autorizados, por usuários;

- [ ] Desconexão do terminal por inatividade, por usuários;
- [ ] Desconexão do terminal por inatividade, por funcionsários;
- [ ] Autorização para uso de rede sem fio, por usuários;
- [ ] Autorização para uso de rede sem fio, por funcionários;
- [ ] Não há controle
- [ ] Outro:

Instituição:

Nome do Entrevistado:

Cargo/função que exerce:

Obrigada!

Enviar

APÊNDICE C – Termo de Consentimento Livre e Esclarecido

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

Acadêmica: *Josiane Ayres Sfreddo*
Orientador: *Daniel Flores*

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Você está sendo convidado (a) a participar, da pesquisa intitulada "SEGURANÇA DA INFORMAÇÃO ARQUIVÍSTICA: O CONTROLE DE ACESSO EM ARQUIVOS PÚBLICOS ESTADUAIS.".

O objetivo que norteia esta pesquisa é identificar as ações adotadas para controlar o acesso documental em Arquivos Públicos Estaduais. A sua participação é fundamental para que se possa dar continuidade aos estudos, dessa forma, solicitamos sua colaboração na realização desta pesquisa.

Sua participação não é obrigatória, mas caso você concorde em participar, esta pesquisa será composta por um questionário com perguntas a respeito da gestão de documentos e do controle de acesso, para a segurança das informações arquivísticas.

As informações fornecidas por você serão confidenciais. Os sujeitos da pesquisa não serão identificados em nenhum momento, mesmo quando os resultados forem divulgados em qualquer forma. É assegurada a assistência durante toda pesquisa, bem como é garantido o livre acesso a todas as informações e esclarecimentos adicionais sobre o estudo.

Diante dos esclarecimentos prestados, concordo em participar da pesquisa.

_____

Responsável

Santa Maria, maio de 2010.