UNIVERSIDADE ESTADUAL DA PARAÍBA – UEPB
CENTRO DE CIÊNCIAS BIOLÓGICAS E SÓCIAS APLICADAS-CCBSA
ARQUIVOLOGIA

BRUNO TALES MARQUES FERNANDES

A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO DIGITAL PARA A ARQUIVOLOGIA

JOÃO PESSOA – PB

2015

BRUNO TALES MARQUES FERNANDES

A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO DIGITAL PARA A ARQUIVOLOGIA

Monografia apresentada ao Curso de Bacharel em Arquivologia, do Centro de Ciências Biológicas e Sociais Aplicadas-CCBSA, da Universidade Estadual da Paraíba, como requisito parcial para obtenção do título de Graduado em Arquivologia.

Orientador: Dr. Josemar Henrique de Melo

João Pessoa-PB
2015

F363i Fernandes, Bruno Tales Marques
A importância da segurança da informação digital para a Arquivologia [manuscrito] / Bruno Tales Marques Fernandes. - 2015.
61 p.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Arquivologia) - Universidade Estadual da Paraíba, Centro de Ciências Biológicas e Sociais Aplicadas, 2015.
"Orientação: Prof. Dr. Josemar Henrique de Melo, Departamento de Arquivologia".

1. Arquivologia. 2. Segurança da informação. 3. Documento digital. I. Título.

21. ed. CDD 025.82

BRUNO TALES MARQUES FERNANDES

A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO DIGITAL PARA A ARQUIVOLOGIA

Monografia apresentada ao Curso de Bacharelado em Arquivologia, do Centro de Ciências Biológicas e Sociais Aplicadas-CCBSA, da Universidade Estadual da Paraíba, como requisito parcial para obtenção do título de Graduado em Arquivologia, sob orientação do Profº. Dr. Josemar Henrique de Melo.

Trabalho de Conclusão de Curso aprovado em 20/02/206 para obtenção do título de Bacharel em Arquivologia.

BANCA EXAMINADORA

Prof. Dr. JOSEMAR HENRIQUE DE MELO– UEPB
Orientador

Profº Ms HENRIQUE ELIAS CABRAL FRANÇA
Presidente da Banca

Profº Ms DANILO DE SOUSA FERREIRA
Membro

Profº Esp. KROL JANIO REMIGIO PALITO
Membro

Dedico esta monografia a minha família, a qual esteve comigo em todos os momentos.

AGRADECIMENTOS

Ao meu Deus, por mais uma etapa vencida em minha vida. Sei que não conseguiria se não fosse a presença Dele em minha vida, me dando forças para prosseguir, mostrando o caminho certo a seguir, colocando pessoas fundamentais em minha vida, cujas contribuições foram fundamentais para a conquista de mais um degrau de minha vida profissional. Mesmo sem merecer, Deus tem me presenteado todos os dias, sendo esta graduação um presente imensurável!

Ao professor Dr. Josemar Henrique de Melo, responsável pelo apoio deste trabalho.

Aos meus pais, meus maiores exemplos.

A minha esposa, pela força e estímulo.

Aos meus amigos, Francisca e Sérgio, por todos os momentos vivenciados juntos na vida acadêmica.

Obrigado a todos que, mesmo não estando citados aqui, contribuíram para a conclusão desta etapa.

“Talvez não tenha conseguido fazer o melhor, mas lutei para que o melhor fosse feito. Não sou o que deveria ser, mas Graças a Deus, não sou o que era antes”.
(Marthin Luther King).

RESUMO

Com o avanço das tecnologias da informação, o crescimento das diferentes instituições e a complexificação do Estado, a produção de documentos aumentou, tanto no suporte analógico como no digital. A informação, como ativo importante para os negócios, traz consigo, a necessidade de mantê-la segura, para que sejam garantidas as características de documento arquivístico e assim seu valor probatório. Assim, com foco nos documentos digitais, tendo como principal objetivo compreender as formas e mecanismos de segurança da informação arquivística, buscou-se analisar a importância da segurança da informação digital para a Arquivologia, descrevendo os conceitos de documento analógico, digital, arquivístico e arquivístico digital; buscando, pois distinguir os conceitos de segurança da informação digital, bem como os mecanismos de segurança da informação digital, para só então apresentar aos arquivistas, assim como, aos analistas de sistemas, cientistas da computação e informação, quais as formas para assegurar a segurança dos documentos arquivísticos digitais. No estudo, partimos da hipótese de que existem formas para conferir aos documentos arquivísticos digitais às qualidades de autenticidade, segurança e fidedignidade. Para a contextualização do tema, sendo uma pesquisa básica, descritiva, qualitativa e bibliográfica, remetemo-nos a revisão na literatura da área da Arquivologia, como RONDINELLI (2005,2013), DURANTI (1998), BELLOTO (2006), EARQ-Brasil (2011), Ciência da Informação com normas de segurança como NBR ISO/17799, NBR ISO/27002, NBR ISO/27005 e Ciência da Computação, como STALLINGS (2008), MARAKAS, O'BRIEN(2007). Abordamos sobre a segurança da informação e suas formas, apresentando também mecanismos de controle da segurança da informação digital. Como conclusão, evidencio a possibilidade de manter nos documentos arquivísticos digitais suas características, quando estabelecidas formas e mecanismos de controle que podem ser gerais com políticas de segurança, estabelecendo-se nos sistemas de informação mecanismos de segurança, como também específicas utilizando-se de mecanismos de segurança no documento considerando-o como único.

Palavras-chave: Arquivologia. Segurança da informação. Documento digital.

ABSTRACT

With the advance of information tecnologies, the development of the different institutions and the complexification of the state, the production of documents increased in both, analogue and digital support. The information as an important asset for the business, brings the need to keep her safe in order to garantee the characteristics of the Archival document as well as its probative value. Thus, as a focus in the digital documents, having as a primary objective to understand the forms of security of the archivistic information, an attempt was made to expose the importance of the security of digital information for the Archival Education. In the study, we started from the hypothesis that there are ways to give to the digital archival documents the qualities of authenticity, security and reliability. To contextualize the theme, being this a basic, descriptive, qualitative and bibliographical research, please refer to the revew of literature in the field of Archival Education, as Rodinelle(2005.2013), Duranti(1998), Belloto(2006), Brazil-EARQ(2011), Information Science with safety regulations as NBR ISO/17799, NBR ISO/27002, NBRISO/27005 and Computer Science, as STALLINGS(2008), Maracas, O'Brien(2007). In this way I present firstly concepts of analogue and digital archival documents, describing them diplomatically and exposing its characteristics. We approached to the security of information and its forms, also presenting mechanisms that control the security of digital information. In conclusion, I emphasize the possibility to give to the digital archival documents their characteristics when established forms and mechanisms of safety as well as specifics, using the mechanisms of safety in the document regarding it as unique. Therefore, was carried out a multidisciplinary work, as a tool to assist in the area of information of the digital Archivist.

Keywords: Archival Education. Security of information. Digital document.

LISTA DE ABREVIAÇÕES

ACCIS	Advisory Committe for the co-ordination of Information System
CTDE	Câmara Técnica de Documentos Eletrônicos
CONARQ	Conselho Nacional de Arquivos
NBR ISO/IEC	Norma Brasileira de Segurança da Informação
PDF	Portable Document Format
DOC-X	Formato de Documento Word
JPG	Joint Photographics Experts Group
GIFF	Graphics Interchange Format
RFC	Request for Coments
SIGAD	Sistema Informatizado de Gestão de Documentos
MAC	Código de Autenticação de Mensagens
IDS	Sistema de Detecção de Intruso

LISTA DE QUADROS E TABELAS

QUADRO 1	Definições Ameaça X Ataque
QUADRO 2	Elementos de Metadados
QUADRO 3	Exemplos de Vulnerabilidades e Ameaças
QUADRO 4	Tipos de IDS
QUADRO 5	Requisitos de Sistema para Trilhas de Auditoria

LISTA DE FIGURAS

FIGURA 1	Tendências na sofisticação do ataque e conhecimento do intruso
FIGURA 2	Formas de interceptação da informação
FIGURA 3	Criptografia Simétrica

SUMÁRIO

1. CONSIDERAÇÕES INICIAIS 10

2. METODOLOGIA 13

3. DOCUMENTO 15

3.1 DOCUMENTO ARQUIVÍSTICO 16

3.1.1 Composição Física e Intelectual do Documento Arquivístico – Diplomática 18

3.2 DOCUMENTO DIGITAL 20

3.2.1 Documento arquivístico digital 21

3.2.2 Características dos Documentos Arquivísticos 21

3.2.2.1 Autenticidade **22**

3.2.2.2 Fidedignidade **23**

3.2.2.3 Integridade **23**

3.2.2.4 Confidencialidade **24**

3.2.2.5 Organicidade ..... Erro! Indicador não definido.**6**

4. SEGURANÇA DA INFORMAÇÃO: Uma visão centrada nos documentos arquivísticos digitais 27

4.1 METADADOS 30

5. SEGURANÇA NO DESENVOLVIMENTO DE SISTEMAS DE GESTAO DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS 33

6. MECANISMOS PARA CONTROLE DE SEGURANÇA 41

6.1 CRIPTOGRAFIA 41

6.1.1 Criptografia simétrica 42

6.1.2 Criptografia Assimétrica 43

6.2 ASSINATURA DIGITAL 44

6.3 BIOMETRIA 47

6.4 FIREWALL 49

6.5 DETECTOR DE INTRUSOS 50

6.6 TRILHAS DE AUDITORIA 52

6.7 RECURSOS HUMANOS 55

7. CONSIDERAÇÕES FINAIS 57

REFERÊNCIAS 59

1. CONSIDERAÇÕES INICIAIS

Com o avanço das tecnologias da informação, o crescimento das diferentes instituições e a complexificação do Estado, ocorridos após a Segunda Grande Guerra Mundial (1939-1945), a produção documental aumentou exponencialmente, não só no suporte analógico como também no digital.

Importante para os negócios, tanto para instituições públicas como privadas, tais informações devem possuir características tais como: autenticidade, fidedignidade, integridade, sendo essenciais para preservar a competitividade, o faturamento, a lucratividade e principalmente a memória institucional.

A partir de todos estes pré-requisitos, surge a necessidade de manter a segurança da informação, e quando se tratando dos documentos digitais, os quais podem ser denominados, segundo o EARQ-Brasil (2011, p.9), como sendo "Informação registradas, codificada em dígitos binários acessíveis por meio de sistemas computacionais", temos um desafio a mais diante da sua dinamicidade, volatilidade e facilidade de alteração e interceptação.

Devemos ainda levar em consideração que os sistemas que produzem informação digital estão se desenvolvendo em ritmo mais rápido, trazendo assim à gestão de documentos, uma gama de dados digitais produzidos em âmbito particular ou institucional, que se multiplicam tanto no que tange sua tipologia, como sua complexidade.

Por conseguinte, é necessário primeiramente se distinguir segundo relatório publicado em 1990, intitulado *United Nations, Advisory Committe for the co-ordination of Information System* (ACCIS), Management of Electronic Records:Issues and Guidelines citado por RONDINELLI (2013), quais são documentos arquivístico e quais não são. Segundo a Câmara Técnica de Documentos Eletrônicos, temos documentos arquivísticos como "documento produzido ou recebido por uma pessoa física ou jurídica, no decorrer das suas atividades, qualquer que seja o suporte, e retido para ação ou referência" CTDE (2012, p.2), a mesma também define documento arquivístico digital como: "documento digital reconhecido e tratado como um documento arquivístico" CTDE (2012,p.3).

Diante da realidade em que vivemos, em que dados, informações, documentos, podem estar sendo criados sem controle, temos uma tarefa difícil, mas, o arquivista responsável pela instituição deve entender a importância de, primeiramente, fazer esta diferenciação, pois sem esta, a gestão de documentos será inviável diante da quantidade de documentos para gerir, perdendo assim, uma de suas características que é a de controlar a produção e a guarda ou eliminação de documentos, assegurando o descarte dos mesmos sem valor probatório, legal

ou para futuras pesquisas científicas, e a instituição terá assim uma simples armazenagem de uma massa documental.

O desafio de manter a segurança da informação, preservando as características de um documento arquivístico, como: organicidade, unicidade, confiabilidade, autenticidade e acesso, definidas pelo EARQ-Brasil (2011), torna-se algo extremamente importante para a Arquivologia, diante do novo cenário arquivístico no qual, os documentos digitais nos inserem.

Cenário este que podemos notar, nos novos suportes, nas novas tipologias, metadados, processo de criação por sistema, informações escritas em linguagem alfabética, porém armazenadas em dígitos binários.

A Arquivologia utiliza-se da interdisciplinaridade para poder abarcar todos os aspectos referentes à gerência da informação. Princípios e técnicas foram criados para solucionar problemas advindos do grande acúmulo de massa documental encontrado na maioria das instituições públicas e privadas de um modo geral. Dentro deste gerenciamento, nasce também a necessidade de estabelecer políticas que venham trazer segurança à informação.

A produção do documento digital trouxe mais dificuldade para manutenção da segurança, diante do desafio de manter o documento digital autêntico e fidedigno. Assim, a Arquivologia busca desenvolver, juntamente com outras áreas da ciência da informação, mecanismos para controle do documento digital arquivístico. Métodos, procedimentos, tecnologias, dispositivos de armazenamento, processos informáticos, controles de segurança emergiram nos últimos anos trazendo à Arquivologia a necessidade de se adaptar e expandir seus conceitos para o controle da gestão de documentos digitais.

Diante disto, traçamos como principal questionamento para o presente trabalho, a seguinte problemática: **Quais são as formas e mecanismos de segurança da informação utilizadas pela Arquivologia, para conferir segurança às informações arquivísticas digitais?**

Para tanto, buscando responder a problemática supramencionada partimos da hipótese de que existem formas para conferir aos documentos arquivísticos digitais as qualidades de autenticidade, segurança e fidedignidade, uma vez que nos utilizemos das formas corretas de controle da segurança da informação.

Por esta razão e frente a tal indagação, tendo como referência os conhecimentos advindos do campo da Arquivologia, construídos e adquiridos ao longo de nosso curso da graduação, traçamos como objetivo geral de nossa pesquisa: Compreender os mecanismos ou formas utilizadas para conferir segurança às informações arquivísticas digitais, analisando de

acordo com o aporte teórico encontrado em nossos estudos bibliográficos e identificando na opinião dos diversos autores estudados, que e quais são as formas de segurança aqui discutidas.

Tendo como objetivos específicos: descrever os conceitos de documento analógico, digital, arquivístico e arquivístico digital; buscando, pois distinguir os conceitos de segurança da informação digital, bem como os mecanismos de segurança da informação digital, para só então apresentar aos arquivistas, assim como, aos analistas de sistemas, cientistas da computação e informação, as formas para assegurar a segurança dos documentos arquivísticos digitais. E por fim, contribuir para que novos estudos surjam tratando desta temática.

Assim, com uma visão de futuro profissional arquivista, este trabalho justifica-se pela necessidade de aprimorar conhecimentos adquiridos no meio acadêmico, diante do crescimento exponencial e da volatilidade que informações digitais passam a ter diante das novas tecnologias da informação.

Em relação a anseios acadêmicos, esta pesquisa proporcionará aos profissionais da informação o esclarecimento necessário acerca da gestão de documentos em organizações, com foco na segurança das informações arquivística digital, apresentando e investigando, mecanismos de segurança digital encontrados na literatura nacional e internacional, de modo a contribuir com a ampliação da literatura quanto à proposição evidenciada, considerando o ainda pouco expressivo estudo da área no Brasil.

À sociedade, evidencio a importante contribuição, por apresentar o tema proposto chamando a atenção ao meio arquivístico, no sentido de estimulá-los ao crescimento do conhecimento na área, enfatizando a necessidade de manutenção de arquivos autênticos e fidedignos, cumprindo assim, seu papel social.

Apresenta-se neste trabalho o primeiro capítulo, introduzindo os leitores ao tema da importância da segurança da informação digital para a Arquivologia. A metodologia é abordada no capitulo dois, bem como suas definições. O referencial teórico é apresentado no capítulo três, fazendo a análise dos dados referentes a conceitos de documentos, documentos arquivísticos, documentos digitais, segurança da informação, expondo mecanismos de segurança digital e apresentando algumas características que podem ser usadas nas políticas de segurança. Já o capítulo quatro traz as conclusões advindas do presente trabalho. Por fim, são apresentadas as referências utilizadas nesta monografia.

2. METODOLOGIA

Partindo da premissa que segundo Prodanov e Freitas (2013, p.14):

> A metodologia é a aplicação de procedimentos e técnicas que devem ser observados para construção do conhecimento, com o propósito de comprovar sua validade e utilidade nos diversos âmbitos da sociedade. (PRODANOV, 2013, p14)

E com o objetivo de trazer melhor compreensão ao leitor, traçamos a presente pesquisa de acordo com os seguintes critérios: quanto à natureza, abordagem, objetivo e procedimentos utilizados.

Desse modo, primamos por uma pesquisa básica quanto à sua natureza a qual "objetiva gerar conhecimentos novos, úteis para o avanço da ciência sem aplicação prática prevista. Envolve verdades e interesses universais" (PRODANOV e FREITAS, 2013, p. 51). Por também compreendermos que esta "procura os princípios, os fundamentos do mundo, das coisas, do seu funcionamento; sua intenção é desvendar características, propriedades básicas dos fundamentos" (MICHEL, 2009, p.43).

Foi adotado o método de pesquisa descritiva e de fundo qualitativo. Pretendeu-se aprofundar e ampliar o conhecimento atualmente disponível sobre o objeto de estudo e áreas relacionadas. O desenvolvimento teórico esteve baseado na pesquisa qualitativa orientando-se pelo tema e assuntos delimitados.

Para Gil (2008) a pesquisa descritiva apresenta características de determinadas populações ou fenômenos. Utiliza-se de técnicas padronizadas de coletas de dados tais como o questionário e a observação sistemática.

O que em nossa perspectiva nos permitirá debruçar-nos de um modo mais profundo sobre o tema, dando-nos, pois a oportunidade de descrever tal fenômeno com mais propriedade, uma vez que a cada novo dado coletado ou aprendizado alcançado, tais conhecimentos nos farão corroborar ou não com as hipóteses por nós previamente traçadas.

A fim de adentrarmos melhor neste campo científico, utilizamos a pesquisa bibliográfica, uma vez que nossa pesquisa fora elaborada "a partir de material já publicado, constituído principalmente de: livros, revistas, publicações em periódicos e artigos científicos, jornais, boletins, monografias, dissertações, teses..." (PRODANOV e FREITAS, 2013, p. 54). Cabendo ressaltar que para estes autores, nesta modalidade de pesquisa o objetivo principal seria o de "colocar o pesquisador em contato direto com todo material já escrito sobre o assunto da pesquisa". (PRODANOV e FREITAS, 2013, p. 54).

No que se refere à pesquisa bibliográfica, corroboramos com a caracterização que Minayo et al. (2010) faz da mesma, ao descrevê-la como: disciplinada, crítica e ampla. Sendo esta disciplinada, devido à criticidade com as quais escolhemos os textos bem como os autores que nortearão nossa pesquisa, crítica devido ao diálogo que estabeleceremos entre as teorias elencadas e o nosso objeto de investigação, e por fim ampla, haja vista que "espera-se que o pesquisador saiba dizer o que é o consenso sobre o assunto em debate e o que é polêmico, o que já é tido como conhecido e o que ainda pouco se sabe. (MINAYO et al., 2010, p. 36).

Em se tratando de sua finalidade, vemos que segundo Lakatos e Marconi (2008, p.185) espera-se pois:

> Colocar o pesquisador em contato direto com tudo o que foi escrito dito ou filmado sobre determinado assunto, inclusive conferencias seguidas de debates que tenham sido transcritos por alguma forma, quer publicadas, quer gravadas.

Em contrapartida, cabe ressaltar que para tais autores a pesquisa bibliográfica apesar de ser fundamentada em fontes já escritas e publicadas por autores da área, não é meramente uma repetição do que já foi dito, mas, um exame de um tema sob um novo enfoque ou abordagem, chegando a novas conclusões sobre o problema.

Assim, tendo este como um trabalho monográfico, e, portanto científico, tentamos na perspectiva de Prodanov e Freitas (2013), questionar e articular o discurso com consistência lógica e, portanto, capaz de convencer.

Em se tratando do método de abordagem, utilizamos o método indutivo, o qual, segundo este autor "surgiu e serviu para que os estudiosos da sociedade abandonassem a postura especulativa e se inclinassem a adotar a observação como procedimento indispensável para atingir o conhecimento científico" (PRODANOV E FREITAS, 2013, p29).

Por fim, ratificamos que seus fins são de cunho descritivo, pois nos provemos de procedimentos bibliográficos, baseados em materiais já elaborados e cujos principais instrumentos foram às fontes bibliográficas cuja confiabilidade fora reafirmada pelas escolhas dos autores utilizados, os quais são de fato, referência no assunto.

3. DOCUMENTO

A Arquivologia é uma área do conhecimento que lida diretamente com a organização, armazenamento, e disseminação da informação registrada, produzida em função de atividades de uma pessoa física ou jurídica. Neste sentido é interessante, iniciarmos com o conceito, de documento e, em seguida, o de documento arquivístico e documento arquivístico digital.

Utilizando-se como referência a área do Direito, cito Almeida (2012, p.1), para conceituar documento segundo a mesma como:

> O vocábulo **documento** é oriundo do latim *documentun*, do verbo *docere*, que significa ensinar, instruir, mostrar. Na doutrina encontramos vários conceitos: para *Moacyr Amaral dos Santos* a prova documental é a coisa representativa de um fato e destinada a fixá-lo de modo permanente e idôneo, reproduzindo-o em juízo;*Arruda Alvim* diz que é tudo aquilo destinado a fixar duradouramente um fato; para *Humberto Theodoro Junior*, a prova documental é o resultado de uma obra humana que tenha por objetivo a fixação ou retratação material de algum acontecimento.

Para a área da História, trago a definição de Le Goff (1996, p.538), que diz:

> O documento não é inócuo. É, antes de mais nada, o resultado de uma montagem, consciente ou inconsciente, das sociedades que o produziram, mas também das épocas sucessivas durantes as quais continuou a viver, talvez esquecido, durante as quais continuou a ser manipulado, ainda que pelo silêncio. O documento é uma coisa que fica, que dura, e o testemunho, o ensinamento (para evocar a etimologia) que ele traz devem ser em primeiro lugar analisados, desmitificando-lhe o seu significado aparente. O documento é monumento. Resulta do esforço das sociedades históricas para impor ao futuro – voluntária ou involuntariamente – determinada imagem de si próprias. No limite, não existe um documento verdade. Todo documento é mentira. Cabe ao historiador não fazer o papel de ingênuo. Os medievalistas, que tanto trabalharam para construir uma crítica – sempre útil, decerto – do falso, devem superar essa problemática, porque qualquer documento é, ao mesmo tempo, verdadeiro – incluindo talvez sobretudo os falsos – e falso, porque um monumento é em primeiro lugar uma roupagem, uma aparência enganadora, uma montagem. É preciso começar por desmontar, demolir esta montagem, desestruturar esta construção e analisar as condições de produção dos documentos-monumentos.

Segundo Bellotto (2006, p.35), documento pode ser conceituado como "qualquer elemento gráfico, iconográfico, plástico ou fônico pelo qual o homem se expressa". Documento, comumente falando, temos em mente informação registrada independentemente de seu suporte.

De acordo com Rondinelle (2013, apud DURANTI, 1998, p.41) documento "tradicionalmente se refere à multiplicidade de fontes de evidência" pode ser também entendido como documento escrito, que por sua vez é definido como "evidência produzida num suporte (papel, fita magnética, disco, placa, etc.) por meio de um instrumento de escrita (caneta, lápis, máquina de escrever etc.) ou de um aparato para fixação de dados, imagens e/ou vozes".

Vale ressaltar que dentre as definições o suporte torna-se algo mais em segundo plano, conforme Rondinelle (2013, p.53) "há de ressaltar, não significa o atrelamento da entidade documental a determinado tipo de suporte, mas à necessidade de estabilidade e permanência desse mesmo conteúdo". Logo, o suporte é importante para o acesso, mas não tem em si tanta importância para a consistência da informação.

Conforme o dicionário de terminologia arquivística (2005, p.73), a definição de documento é "Unidade de registro de informações, qualquer que seja o suporte ou formato." Nesta definição vemos a contemporaneidade da definição, pois esta, abrange todos os suportes, inclusive os novos que a cada dia surge com a informatização de sistemas de informação.

Conforme Duranti (2008, p.32) documento pode ser definido como "unidade indivisível de informação constituída por uma mensagem fixada num suporte (registrada) com uma sintaxe estável. Um documento tem forma fixa e conteúdo estável".

Diante do exposto sobre documento, as definições mais contemporâneas tratam deste de maneira genérica, como informação registrada, importante é a permanência da sintaxe, a estabilidade do conteúdo e a permanência deste possibilitando a guarda.

3.1 DOCUMENTO ARQUIVÍSTICO

O objeto da Arquivologia consiste em informações "produzidas por uma entidade pública ou privada ou por uma família ou pessoa no transcurso das funções que justificam sua existência como tal, guardando esses documentos relações orgânicas entre si" (BELLOTTO, 2006, p.37).

Um documento será considerado arquivístico segundo o e-ARQ Brasil (2011) quando este for produzido e/ou recebido por pessoa, seja física ou jurídica, e dotado de organicidade.

Para Paes (1997, p.47), documento de arquivo pode ser definido como "1.Aquele que, produzido e/ou recebido por uma instituição pública ou privada, no exercício de suas atividades, constitua elemento de prova ou de informação.2.Aquele produzido e/ou recebido por pessoa física no decurso de sua existência."

Conforme Bellotto (2006, p.37),

> Os documentos de arquivo são os produzidos por uma entidade pública ou privada ou por uma família ou pessoa no transcurso das funções que justificam sua existência como tal, guardando esses documentos relações orgânicas entre si. Tratam sobretudo de provar, de testemunhar alguma coisa.

O documento arquivístico também pode ser definido como “documento produzido e/ou recebido por uma pessoa física ou jurídica, no decorrer de suas atividades, qualquer que seja o suporte” (CTDE,2010, p.11). Ao conceito de documento acrescentamos a proveniência e a função administrativa, legal ou histórica.

O documento de arquivo possui a característica de ser criado pela necessidade administrativa, e não através de coleção. Este, também é acumulado de forma natural, possuindo assim uma relação única entre ele, seu antecessor e seu subsequente, ele é único onde se encontra, mesmo que existam cópias elas também terão seu valor único diante da organicidade à qual pertença.

Para Rondinelle (2013, p. 231), o documento de arquivo “constitui o registro de ações humanas independentemente da forma como se apresenta e da base em que se encontra afixado”. A autora também acrescenta em sua obra que “documentos digitais gerados no curso de atividades desempenhadas por pessoas físicas e jurídicas e em suportes tão diferentes como magnéticos e ópticos, também podem ser documentos arquivísticos”. (RONDINELLE 2013, p.232)

A autora supracitada traz a Arquivologia uma visão contemporânea da definição de documento arquivístico frente aos documentos digitais, os quais, atualmente tomam cada vez mais uso nas instituições, lembrando que, as novas definições trazem uma visão mais ampla sobre os documentos arquivísticos, porém, todas as características às quais pertencem ao documento arquivístico analógico, também devem permanecer no documento digitalizado ou digital.

Quando falamos em documento de arquivo, lembramos de acordo com algumas definições, - além de outras características - de informações registradas em um suporte, este último, Bellotto (2010, p.36) afirma que:

> A forma/ função pela qual o documento é criado é o que determina seu uso e seu destino de armazenamento futuro. É a razão de sua origem e de seu emprego, e não o suporte ao qual está constituído, que vai determinar sua condição de documento de arquivo, de biblioteca, de centro de documentação ou de museu.

O documento arquivístico analógico como também o digital se difere do documento propriamente dito, por apresentar características às quais, do ponto de vista diplomático, são:

> Forma fixa, conteúdo estável, relação orgânica, contexto identificável, ação e o envolvimento de cinco pessoas, autor, redator, destinatário, originador e produtor. Há que ressaltar que entre essas cinco pessoas, pelo menos as três primeiras têm de estar presentes num documento arquivístico. (RONDINELLI, 2013, p.235).

Do ponto de vista arquivístico, as características de organicidade, unicidade, confiabilidade (fidedignidade), autenticidade e acessibilidade são exigências a serem

encontrados nos documentos arquivísticos conforme o EARQ-Brasil (2006), tanto no analógico, como no digital.

Tratando-se do documento arquivístico como entidade individual, temos a Diplomática, que em muito auxilia quanto aos métodos utilizados para entender o documento arquivístico seja na composição física ou intelectual. Já a Arquivologia utilizando-se também da Diplomática estuda o conjunto de documentos com suas relações orgânicas.

3.1.1 Composição Física e Intelectual do Documento Arquivístico – Diplomática

O entendimento da composição física e intelectual do documento de arquivo é de suma importância, no sentido de compreendermos os elementos que compõe o documento para assim, através de estudos diplomáticos podermos independentemente do suporte garantir sua fidedignidade e autenticidade trazendo ao documento de arquivo um de seus aspectos principais que é o seu valor de prova.

A Diplomática é a disciplina que nos norteia sobre a veracidade e autenticidade do documento. Foi com esta área de conhecimento que adveio a noção de documento arquivístico como fonte de prova, esta se constitui segundo Duranti e MacNeil (1996, p,47) como:

> Um corpo de conceitos e métodos, originalmente desenvolvidos nos seculos XVIII, "com o objetivo de provar a fidedignidade e a autenticidade dos documentos". Ao longo do tempo ela "evoluiu para um sistema sofisticado de ideias sobre a natureza dos documentos, sua origem e composição, suas relações com as ações e pessoas a eles conectados e com o seu contexto organizacional, social e legal".

Segundo Duranti (1998, p.5), a Diplomática "foi feita para olhar os documentos retrospectivamente, como fonte de prova de fatos que precisavam ser demonstrados".

O documento arquivístico, tanto para a Arquivologia como para a Diplomática, fica claro que é fonte de prova, mas, não prova em si; para Duranti (1998) esse potencial advém de algumas características do documento de arquivo, as quais Fonseca(1998) interpreta como: a autenticidade, ou seja um documento que seja capaz de provar de onde vem e que não foi modificado e se sim quem fez a alteração; a naturalidade, todo documento arquivístico é criado de modo natural nas administrações ou famílias, não de forma artificial, são acumulados de maneira contínua e progressiva, de forma orgânica; inter-relacionamento, todos os documentos são criados para assumir uma função e todos estão ligados por um elo que é criado no momento de sua criação e unicidade, todo documento é único na estrutura documental da instituição da qual pertença, podem até existir cópias deste documento, mas cada uma será única em seu lugar, cada uma com uma função.

Para constatar que um documento é verídico, os diplomatistas utilizam-se de evidências internas e externas ao documento embutidas em sua forma física e intelectual diferentemente da antiguidade a qual se baseava em evidências externas ao documento, como testemunhas e outras.

Rondinelli (2013, p.51) em estudo realizado com base na Diplomática, afirma que esta última,

> "Descobriu que os elementos identificados pelos primeiros diplomatas como necessários à criação de um documento – a saber, sistema jurídico, ato, pessoas, procedimentos e forma documentaria (que reúne todos estes elementos e mostra suas relações) – são tão importantes para os documentos contemporâneos quanto o eram para os documentos medievais, apenas se manifestam de maneira diferente".

Atualmente, documentos arquivísticos, seja qual for o suporte, possuem os mesmos elementos constitutivos, estes elencados segundo Bellotto (2010, p.47) como:

- Suporte, forma física do documento;
- Conteúdo, mensagem transmitida pelo documento;
- Forma, regras de apresentação do conteúdo seja numa forma física ou intelectual, na forma física encontramos as fontes utilizadas, logomarcas, símbolos aspectos visíveis sem a necessidade de interpretação do texto, e forma intelectual elementos que digam pra que foi criado aquele documento, qual sua função administrativa, como exemplos saudações, data, exposição do assunto, marcações ao decorrer de sua fase corrente dentre outras;
- Ação, o ato ou ação que o origina;
- Pessoas, tratando-se de documento em suporte físico, o autor, o destinatário e o escritor, em se tratando de documentos digitais acrescenta-se ainda o criador, o proprietário do fundo ao qual o documento está sendo produzido, para garantir assim o princípio da proveniência e o originador, para ficar registado mesmo quando o autor seja diferente quem o originou;
- Relação orgânica, todo documento possui função única e está relacionado ao seu anterior e subsequente na medida em que resulta de uma mesma atividade;
- Contexto, jurídico-administrativo, de proveniência, de procedimentos e documentário.

A possibilidade de integração dos princípios e técnicas segundo Rondinelli (2007) é vista para os arquivistas como o caminho mais seguro para o bom gerenciamento arquivístico de hoje.

A perspectiva da Diplomática ampliou-se. Hoje o documento arquivístico é analisado de forma ampliada, o estudo tipológico atualmente compreende perspectivas contextualizadas do documento, entendendo suas atribuições intrínsecas ligadas a sua criação, sua função, seu propósito e sua relação com a entidade autora/geradora.

Com esta nova perspectiva contemporânea de estudo da diplomática, surge a necessidade da interdisciplinaridade da Arquivologia com a mesma, frente ao novo, que ainda nos traz indagações a respeito do manter das características de um documento arquivístico em um documento digital.

3.2 DOCUMENTO DIGITAL

No presente momento em que vivemos, podemos observar o gigantesco crescimento da informática, da ciência da computação e juntamente com eles, cada vez mais, sistemas de informação automatizados adentram as instituições, criando cada vez mais documentos digitais. Estes últimos definidos como "informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional." CTDE (2012, p.3)

Com o avanço das tecnologias, a tendência é que o uso de documentos digitais cresça exponencialmente. Com isto, tanto a Arquivologia como a Diplomática vem se atualizando, e adaptando para os novos desafios impostos pela dinamicidade dos documentos digitais, pois eles podem ser criados indiscriminadamente, modificados, duplicados, acessados sem autorização, interceptados, renomeados, reformatados tudo isto deixando rastros, entretanto que, visíveis somente por especialistas e quando sabendo do problema entram em investigação.

As várias definições utilizadas nesta pesquisa acerca de documento arquivístico, mostram que os mesmos podem se apresentar em qualquer suporte, assim consequentemente inserindo-se também os documentos digitais, desde que possuam as características de documento de arquivo.

Porém, o documento digital, possui várias peculiaridades, como a armazenagem em linguagem binária, a necessidade de *software* com a mesma sofisticação tecnológica para garantir o acesso através de *hardware* também específico, a tramitação por *intranet/internet*, ou através da mudança do suporte que o armazena para assim poder seguir para o destinatário, e também a volatilidade tanto do *software* como do *hardware* aos quais tem como base. Sobre este, Rondinelle (2013, p.231) explica:

> Na verdade, nesse novo ambiente, o documento foge totalmente aos padrões mais conhecidos, como a linguagem alfabética, registrada em papel e de leitura direta, bem como sua relação inextricável com o suporte. No mundo digital tudo é codificado em linguagem binaria e, para se tornar acessível aos olhos humanos, precisa da intermediação de programas computacionais igualmente codificados em bits, numa sofisticação tecnológica que passa despercebida à maioria dos usuários. Juntem-se a isso as tecnologias de rede com sua alta capacidade comunicacional.

Ao final de sua citação supracitada, Rondinelle (2013, p.231), fala da "alta capacidade comunicacional", e pensando nisto, devemos também lembrar da responsabilidade do profissional arquivístico em controlar a produção documental, pois, sem isto, uma instituição, que se utilize de sistemas informatizados de gestão de documentos poderá estar criando

documentos indiscriminadamente e juntamente com eles documentos sem valor administrativo, legal, ou histórico, não permitindo assim uma gestão arquivística de documentos pois os fundos não terão valor de prova, organicidade, e o volume documental crescerá imensuravelmente.

3.2.1 Documento arquivístico digital

Documento digital é uma informação codificada em dígitos binários, o documento arquivístico digital é segundo o EARQ-Brasil (2006, p.4) "um documento arquivístico codificado em dígitos binários, produzido, tramitado e armazenado por sistema computacional".

Dentre as peculiaridades do documento digital, segundo Rondinelle (2013), na sua produção podem existir até cinco pessoas, o autor, redator, destinatário, originador e produtor. Ainda de acordo com a autora supracitada, estes devem apresentar as seguintes características: "forma fixa, conteúdo estável, relação orgânica, contexto identificável, ação" (RONDINELLI, 2013, p.235). A forma fixa e conteúdo estável é um desafio, que diante da "facilidade" de manipulação de dados digitais faz com que a cada dia formas e mecanismos de controle de segurança garantam que o documento mantenha a mesma apresentação que tinha quando armazenado após a criação.

Além das informações que o documento digital apresenta referente à sua criação, a sua ação na instituição, algumas outras informações serão encontradas nestes, estas, informações chamadas de metadados – os quais serão apresentados a frente, terão a prerrogativa de contribuir para a fidedignidade e autenticidade dos documentos digitas.

A vulnerabilidade do documento digital é notável, assim, os profissionais da Arquivologia devem estar atentos e juntamente com a Diplomática e profissionais da computação construírem sistemas informatizados que tragam ao documento arquivístico digital o valor de prova, que garantam ao documento todos os princípios que lhes são necessários para serem considerados documentos arquivísticos, pois de outra forma, estaremos criando, armazenando e utilizando documentos que não possuem nenhum valor legal.

3.2.2 Características dos Documentos Arquivísticos

Para que documentos digitais sejam considerados arquivísticos digitais, estes devem possuir as mesmas características legais de um documento convencional. Diante disto, iremos

elencar algumas destas para podermos entender um pouco mais sobre o desafio que a Arquivologia tem frente a gestão do documento digital.

Vale salientar que estas características apresentadas de maneira isolada, estão no documento de modo integrado, tendo em vista que um documento autêntico tem que ser integro e fidedigno.

3.2.2.1 Autenticidade

Para tratarmos sobre a autenticidade, temos que definir qual temos em foco, pois a mesma pode ser definida em três formas, a histórica, a legal e a diplomática. Segundo Duranti (1998, p.45), as três podem ser definidas como:

> Documentos legalmente autênticos son aquellos que soportan uma prueba sobre sí mismos, a causa de la intervención durante o después de su creación, de um representante de uma autoridad pública que garantiza su genuinidad.
> Documentos diplomaticamente autênticos son aquellos que fueron escritos de acuerdo a las práticas del tempo y lugar indicados em el texto y firmados com el o los nombres de las personas competentes para crearlos.
> Documentos historicamente autênticos son los que atestiguan que sucedió lo que verdaderamente tuvo lugar o informan lo que es verdade.

Um documento pode ter a característica de ser legalmente autêntico e não ser diplomaticamente, pode ser historicamente e não legalmente, ou seja, todos são independentes, não necessariamente por ser autêntico em uma área será em todas. Para fins desta pesquisa utilizaremos as definições de autenticidade diplomática.

A autenticidade segundo MacNeil (2000, apud RONDINELLI, 2005,p.66) é "a capacidade de se provar que um documento arquivístico é o que diz ser".

Para EARQ-Brasil (2006, p.22),

> Um documento arquivístico autentico é aquele que é o que diz ser, independente de se tratar de minuta, original ou cópia, e que é livre de adulterações ou qualquer outro tipo de corrupção. Enquanto a confiabilidade está relacionada ao momento da produção, a autenticidade está ligada a transmissão do documento e à sua preservação e custódia.

Como compreendido, o manter de um documento autêntico está relacionado à sua produção, tramitação e guarda seguras, preservando nele as informações registradas no ato de produção sem alterações, complementações ou qualquer outro tipo de marcação que não sejam autorizadas, e se houver tais marcações registradas, estas devem ser um documento autêntico, principalmente o digital, devendo este ser controlado desde sua criação até sua destinação final preservando e registrando nele todas as trilhas de tramitação, alteração e acesso.

Se por um lado um documento convencional deve haver controles como restrição de acesso físico, marcações físicas nos documentos dentre outros, por outro, os documentos digitais devem ser com sistemas de gestão arquivística elaborados por arquivistas em parceria com outros profissionais da tecnologia da informação que viabilizem a criação por autor autorizado, controle na tramitação com mecanismos de segurança que impossibilitem a interceptação e alteração de documentos, controles de acesso, registros de modificações ou complementações de documentos através de metadados, e a garantia de armazenamento seguro e acessível sempre que necessário.

Para um documento digital diante de sua facilidade de adulteração sem deixar rastros, faz-se um desafio ao profissional da arquivística.

3.2.2.2 Fidedignidade

A fidedignidade está relacionada ao seu ato de produção, à qual MacNeil(2000, apud RONDINELLI, 2005, p.64) define do ponto de vista diplomático como "a capacidade de um documento arquivístico sustentar os fatos que atesta".

Segundo a CTDE (2004, p.4) a fidedignidade é a "capacidade de um documento arquivístico sustentar os fatos que atesta. Refere-se à autoridade e à confiabilidade de um documento. Está relacionada ao momento da produção do documento".

Quando falamos em fidedignidade temos que o documento é capaz de provar os fatos dos quais atesta, a autenticidade diz se é realmente um documento que diz ser, e fidedignidade se é seguro acreditar no que este documento atesta.

3.2.2.3 Integridade

De acordo com a NBR ISO/IEC 17799:2001, integridade é a "salvaguarda da exatidão e completeza da informação e dos métodos de processamento". Um projeto da Universidade de Bristish Columbia (1997) citado por Rondinelli (2005, p.107), subdivide à preservação de documentos digitais autênticos e fidedignos em duas partes:

1) O gerenciamento da preservação da integridade dos documentos eletrônicos pode ser cuidadosamente dividido em duas fases: uma dirigida ao controle da criação e da manutenção de documentos correntes e intermediários, fidedignos e autênticos, e outra dirigida à preservação de documentos permanentes autênticos;
2) A integridade dos documentos eletrônicos é mais bem preservada quando se atribui a responsabilidade pela sua fidedignidade ao órgão encarregado da sua criação e a responsabilidade pela sua fidedignidade pela sua autenticidade ao órgão encarregado de sua preservação.

Um documento íntegro é aquele que se mantém no transcurso de sua tramitação, sem alterações não permitidas, sendo assim, um documento produzido e enviado, seja fisicamente ou digitalmente, deverá chegar ao destinatário sem alterações, quando este chegar ao destinatário e precisar acrescentar alguma informação, esta deverá ser registrada e informada a autoria do adendo.

Para a Câmara Técnica de Documentos Eletrônicos do CONARQ[1] (2012, p.2), "Integridade é a capacidade de um documento arquivístico transmitir exatamente a mensagem que levou à sua produção (sem sofrer alterações de forma e conteúdo) de maneira a atingir seus objetivos.".

D-Lib Magazine (September 1999) diz que falando sobre documentos digitais:

> Principais processos envolvidos na gestão de objetos digitais ao longo do tempo incluem o rastreamento de autenticidade, como parte de proveniência; manutenção da integridade do objeto digital e garantir a integridade referencial de links para esse objeto (a partir de outros objetos ou a partir de registos de metadados); e entender como a reformatação impactos a integridade do objeto. Estes envolvem tanto o objeto digital e seus metadados[2].

Com relação aos documentos digitais, haverá outros tipos de informações, os metadados, estes também, os sistemas informatizados de gestão arquivística de documentos terão que assegurar sua integridade, pois através deles é que as características de autenticidade e fidedignidade serão atribuídas aos documentos digitais.

3.2.2.4 Confidencialidade

Informações são muito importantes para manter a competitividade, para servir de prova para instituições, manter e melhorar lucros dentre inúmeros benefícios. Entretanto, há de se garantir que estas sejam acessíveis somente por pessoas autorizadas, pois, de outra forma, tanto a empresa sairia em desvantagem frente à competitividade, como também as informações podem ser facilmente modificadas.

Para isso, o documento arquivístico deve preservar como característica a confidencialidade, esta, segundo a NBR ISO/IEC 17799, (2001, p.2), pode ser denominada como "garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso". Sem isso, e também o registro de quem acessou, fica difícil definir quem fez alterações ao documento, e se estas eram permitidas ou não.

Quanto ao controle do acesso aos documentos o EARQ-Brasil (2006, p.31) diz que:

---

[1] CONARQ: Conselho Nacional de Arquivos

2 Key processes involved in the management of digital objects over time include the tracking of authenticity as part of provenance; maintaining the integrity of the digital object and ensuring the referential integrity of links to that object (from other objects or from metadata records); and understanding how reformatting impacts the integrity of the object. These involve both the digital object and its metadata.

> A atribuição de restrições deve ser feita no momento da captura, com base no esquema de classificação de segurança e sigilo elaborado pelo órgão ou entidade e envolve os seguintes passos:
> - Identificar a ação ou atividade que o documento registra;
> - Identificar a unidade administrativa à qual o documento pertence;
> - Verificar a precaução de segurança e o grau de sigilo;
> - Atribuir o grau de sigilo e as restrições de acesso ao documento;
> - Registrar o grau de sigilo e as restrições de acesso no sistema de gestão arquivística de documentos;

Para que a confidencialidade seja eficaz, os profissionais arquivistas responsáveis pela instituição deverão observar nos sistemas de informação, se estes registram através de metadados todas as informações de controle de acesso do documento identificando quem poderá acessar e/ou modificar alterar um documento, observando também o grau de sigilo os quais lhe competem.

3.2.2.5 Organicidade

O documento de arquivo, diferentemente do de museu e biblioteca, é obtido através de "passagem natural, dentro do esquema das três idades" BELLOTTO (2006, p.37), em que justifica-se sua existência por fazer parte de uma entidade pública ou privada durante o transcurso de suas atividades; assim, o princípio da organicidade que segundo a Câmara Técnica de Documentos Eletrônicos (CTDE) (BRASIL, 2010, p. 18) é um "Atributo de um acervo documental decorrente da existência de relação orgânica entre seus documentos. Essencial para que um determinado conjunto de documentos seja considerado um arquivo.".

Ainda segundo a organicidade BELLOTTO (2006, p28) diz:

> O documento de arquivo só tem sentido se relacionado ao meio que o produziu. Seu conjunto tem de retratar a infraestrutura e as funções do órgão gerador. Reflete, em outras palavras, suas atividades-meio e suas atividades-fim.

Para o EARQ-Brasil (2011, p.21):

> O documento arquivístico se caracteriza pela organicidade, ou seja, pelas relações que mantem com os demais documentos do órgão ou entidade e que refletem suas funções e atividades. Os documentos arquivísticos não são coletados artificialmente, mas estão ligados uns aos outros por um elo que se materializa no plano de classificação, que os contextualiza no conjunto ao qual pertencem. Os documentos arquivísticos apresentam um conjunto de relações que devem ser mantidas.

A organicidade é de suma importância para o documento arquivístico, uma vez que, se não mantida, o documento poderá não ter função alguma e o arquivo poderá perder sua estrutura e deixar de refletir as funções e atividades da instituição.

3.2.2.6 Unicidade

Segundo BELLOTTO (2002, p. 21), é o princípio que "Não obstante forma, gênero, tipo ou suporte, os documentos de arquivos conservam seu caráter único, em função do contexto em que foram produzidos.". Mesmo enquanto cópias, estes podem possuir diferentes

funções dependendo do local e contexto onde se encontrem como diz o EARQ-Brasil (2011, p.21),

> Documento arquivístico é único no conjunto documental ao qual pertence; podem existir cópias em um ou mais grupos de documentos, mas cada cópia é única em seu lugar, porque o conjunto de suas relações com os demais documentos do grupo é sempre único.

Diante desta característica, temos que, o documento de arquivo dotado de organicidade assume papel único frente à estrutura da instituição, refletindo juntamente com o acervo as atividades da mesma.

3.2.2.7 Auditabilidade

Os documentos arquivísticos digitais, também devem apresentar a característica de Auditabilidade, pois, os metadados gerados por sistemas de informação arquivística sobre as ações envolvidas com os documentos, devem ser verificadas e assim asseguradas as características dos documentos arquivísticos.

Segundo CASSA (2015, p2), em publicação na revista Techoje, o princípio da Auditabilidade, *"significa a configuração de sistemas e bases de dados de forma a possibilitar o rastreamento de atividades físicas e lógicas"*.

De acordo com FONTES (2006, apud, Rocha 2008,p25), *"Auditabilidade: o acesso e o uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito"*.

Assim, as informações geradas pelas ações envolvidas com o documento digital terão também que ser auditadas para servir de prova e fazer o documento arquivístico digital uma prova documental.

4. SEGURANÇA DA INFORMAÇÃO: Uma visão centrada nos documentos arquivísticos digitais

A segurança da informação vem passando por uma evolução nas últimas décadas. No passado, quando não tínhamos a inserção dos documentos digitais nas empresas, a segurança era feita fisicamente, com controles de acesso, armazenamentos adequados, protocolos, dentre outros procedimentos arquivísticos. Atualmente, com a chegada dos documentos digitais fez-se necessário a criação de sistemas informatizados e de mecanismos que dessem segurança a essas informações.

Mecanismos de controle de segurança têm sido criados para automatizar a segurança das informações contidas em suportes informáticos, assim como o documento convencional, o documento arquivístico digital para que tenha valor de prova, deve manter a fidedignidade, autenticidade, integridade, confidencialidade e acesso. Para que estas características sejam garantidas, as instituições devem ter políticas de segurança da informação.

De acordo com a NBR ISO/IEC 17799:2001 (2001, p.2) a segurança da informação "é obtida a partir da implementação de uma série de controles, que podem ser políticas, práticas, procedimentos, estruturas organizacionais e funções de *software*.". Para que as informações sejam úteis, estas, precisam estar dispostas em sistemas que assegurem sua produção, uso, tramitação e guarda de forma segura e acessível.

Tendo como base neste capítulo uma visão centrada nos documentos arquivísticos digitais, e sabendo que para criar, manter e acessar estes documentos necessitamos de *software* e *hardware*, e diante do crescimento tecnológico, podemos perceber que a criação de documentos digitais atualmente vem crescendo. Novas formas de transmissão estão sendo criadas, suportes cada vez menores e com mais capacidades de armazenamento, formas de acesso cada vez mais utilizando-se de *intranet* ou *internet*, *software* com capacidades gráficas cada vez maiores, *hardware* com muita velocidade para processamento de dados.

Nisto, muitas formas de segurança tem sido pensadas e implementadas, para que também, junto com a criação do documento, haja um controle sobre quem pode criar e quem criou. Quanto à tramitação, deixando metadados – que serão tratados mais a frente, que gerem trilhas de auditoria que sejam capazes de identificar alterações, inclusões ou qualquer tipo de modificação no documento, tramitação segura quanto ao roubo de informações e ao acesso indevido, acesso facilitado, porém com controles, os quais possam criar níveis de acesso, com autorizações ou não para edição, recebimento seguro, documento autêntico, e guarda confiável, garantindo-lhe sempre o acesso a quem estiver autorizado.

Há muitas facilidades advindas do uso da informação digital, porém se estas informações não tiverem valor legal serão inúteis à instituição.

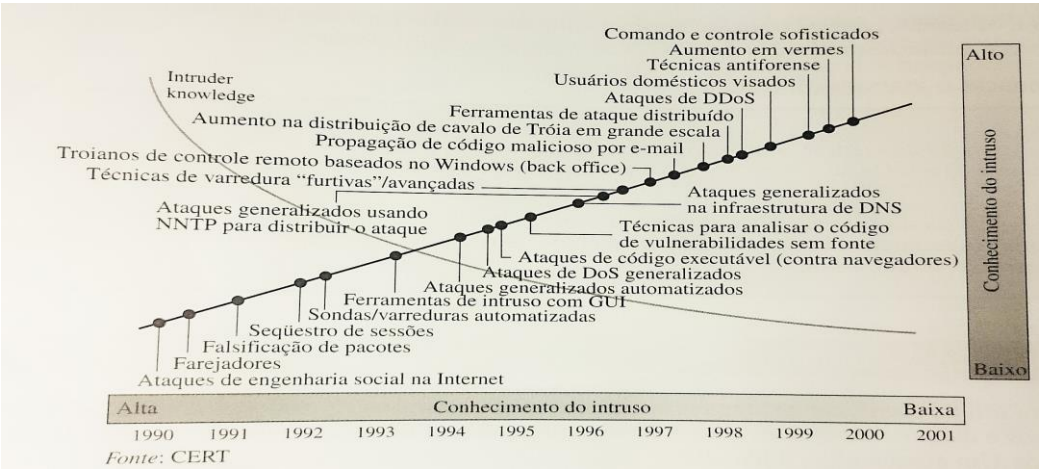
A gestão arquivística de documentos vem assim, através de suas práticas e utilizando-se de mecanismos da área da computação, garantir que todos os documentos que constituem o acervo da empresa estejam confiáveis, autênticos e fidedignos, garantindo-lhes também o seu acesso e guarda eficiente.

O desafio para a Ciência da Computação e a Arquivologia torna-se maior quando os sistemas de informação estão conectados a internet, segundo a qual William Stallings (2008, p.5) diz que:

> Ao longo do tempo, os ataques na internet e em sistemas conectados à internet se tornaram mais sofisticados, enquanto a habilidade e o conhecimento exigidos para montar um ataque diminuíram. Os ataques se tornaram mais automatizados e podem causar mais danos.

A cada dia, os ataques tornam-se cada vez mais comuns diante da facilidade de faze-los. A Figura ilustrada por William Stallings (2008, p.5) mostra isto:

Figura 1 – Tendências na sofisticação do ataque e conhecimento do intruso.



Fonte: CERT, apud, WILLIAN, 2008, p.5

Com os riscos cada vez maiores, profissionais da Arquivologia devem estar atentos a inserir em sistemas de informação mecanismos cada vez mais atualizados para eliminar as vulnerabilidades destes, quanto à segurança quando se falando em sistemas conectados a redes de computadores:

> É preciso que haja uma grande gama de tecnologias e ferramentas para agir contra a ameaça crescente. Em um nível básico, os algoritmos criptográficos para confidencialidade e autenticação assumem maior importância. Além disso, os projetistas precisam focalizar os protocolos baseados na internet e as vulnerabilidades dos sistemas operacionais e das aplicações atacadas.

Um profissional da Arquivologia deve, quanto da responsabilidade de uma instituição deve, ao fazer a gestão de documentos digitais, estar atento aos requisitos dos sistemas de informação que será utilizado, verificando e inferindo-lhes os procedimentos da gestão de documentos e verificando a capacidade destes de garantir a produção, tramitação, uso, guarda e acesso de modo que a informação seja criada por pessoas autorizadas, acessadas somente por quem de direito, transmitidas sem possibilitar roubo e acessíveis sempre que necessário, conferindo-lhes a autenticidade e fidedignidade.

Uma instituição, ao trabalhar com sistemas de informação deve analisar quais são os riscos que está correndo, verificar as ameaças às quais podem estar sujeito e identificar quais serão as consequências de possíveis falhas na segurança. Através disto, utilizar-se de mecanismos de segurança que possam corrigir as vulnerabilidades as quais os sistemas possuem.

Para ameaça e ataque utilizamos as definições apresentada pela RFC 2828(2000, apud, WILLIAN, 2008, p.6):

Quadro1 – Definições Ameaça x Ataque

Ameaça	**Ataque**
Potencial para violação da segurança quando há uma circunstância, capacidade, ação ou evento que pode quebrar a segurança e causar danos. Ou seja, uma ameaça é um possível perigo que pode explorar uma vulnerabilidade.	Um ataque à segurança do sistema, derivado de uma ameaça inteligente, ou seja, um ativo inteligente que é uma tentativa deliberada (especialmente no sentido de um método ou técnica) de burlar os serviços de segurança e violar a política de segurança de um sistema.

Fonte: RFC 2828(2000, apud, WILLIAN, 2008, p.6)

Dentre as ameaças podemos encontrar: as naturais, causadas por fenômenos da natureza como inundações, incêndios dentre outros; as ameaças causadas pelo desconhecimento dos riscos, muitas vezes praticadas inconscientemente; e as ameaças voluntárias que também podemos chamar de ataques.

Estes ataques podem capturar informações, interceptar, interromper, negar acesso, apagar informações, acrescentar informações, enviar informações personificando-as, e até excluir acervos inteiros de documentos arquivísticos se não verificados e utilizados mecanismos de controle de segurança nos sistemas informatizados de gestão dos documentos digitais.

Por conseguinte, vimos que, a segurança da informação é tão importante quanto a própria informação, pois, se estas últimas forem acessadas indevidamente, modificadas, negadas, excluídas, poderão afetar a competitividade da empresa assim como também não substanciar fatos, podendo ser tratadas como informações inverídicas.

4.1 METADADOS

Como elemento de registro das informações referente à segurança dos documentos digitais, faz-se necessário explanarmos um pouco sobre os metadados, que também são informações importantíssimas perante a necessidade de assegurá-los para o uso futuro pelas auditorias.

Manter um documento arquivístico digital seguro, preservando seu valor legal e histórico, é um desafio para as instituições, estas, através de sistemas informatizados de gestão arquivística de documentos, utilizam-se de mecanismos de segurança que irão conferir características de documentos de arquivo aos documentos digitais.

Por sua vez, estes mecanismos acabam por gerar uma gama nova de informações que serão atreladas aos documentos, estas informações serão chamadas de metadados, e estes serão responsáveis por inferir aos documentos digitais as características de autenticidade, fidedignidade, confidencialidade, integridade e organicidade.

De acordo com o glossário da Câmara Técnica de Documentos Eletrônicos, metadados são: “dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e/ou preservar documentos arquivísticos ao longo do tempo”.

Com relação ao conceito desse novo tipo de informações Rondinelle (2007, p.60) diz: “Hoje, o conceito de metadados foi totalmente assimilado pela Arquivologia, sendo o mesmo considerado elemento fundamental para a garantia da capacidade testemunhal do documento eletrônico arquivístico.”.

Analisando diplomaticamente, os metadados podem ser considerados como a parte intelectual do documento, a qual, será composta por um conjunto de informações que registram os atos, propósitos, identificando acessos, criações, modificações, registrando trilhas de tramitação, e construindo relações orgânicas entre os documentos.

> Metadados, portanto, se constituem em componentes do documento eletrônico arquivístico e em instrumentos para sua análise diplomática. É através do domínio desse tipo de análise que será possível estabelecer métodos que garantam a fidedignidade a autenticidade do documento eletrônico arquivístico. (RONDINELLE, 2007, p.62).

Muitas são as classificações dadas aos metadados, e para o EARQ-Brasil (2011), os metadados foram definidos para seis tipos de entidades, sendo a primeira "documento" em que se refere aos documentos arquivísticos que são geridos pelo Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD), em que trata da relação orgânica entre os documentos de um dossiê, processo, arquivo. Diz que todo documento tem que ser relacionada a uma "classe" no momento em que se insere no SIGAD, e todos os eventos relacionados ao documento durante a tramitação deve ser registrado.

"Evento de gestão", refere-se às ações da gestão arquivística, como, produção, tramitação, classificação, eliminação dentre outras. As "Classes" referem-se aos diferentes níveis de agregação ao plano de classificação. A entidade "Agente", refere-se a todos que tem acesso aos documentos. "Componente digital" refere-se aos arquivos que armazenam as informações de conteúdo do documento arquivístico e o "Evento de Preservação" que se referem a migrações, compressão, validação, decifração dentre outros mecanismos de preservação dos documentos digitais.

O EARQ-Brasil (2011) traz alguns elementos que segundo eles devem fazer parte dos metadados de um SIGAD, convém dizer que estes variam de acordo com as especificidades de cada instituição, porém, os apresento abaixo, para que tenhamos uma noção de quão vasta é a gama de informações encontradas nos sistemas de informação que não necessariamente será as informações consultadas pelos interessados da empresa.

Quadro 2 – Elementos de metadados.

DOCUMENTO	1. Identificador do documento 2. Número do documento 3. Numero do protocolo 4. Identificador do processo/dossiê 5. Número do processo/dossiê 6. Identificado do volume 7. Número do volume 8. Tipo de meio 9. Status 10. Identificador de versão 11. Título 12. Descrição 13. Assunto 14. Autor 15. Destinatário 16. Originador 17. Redator	18. Interessado 19. Procedência 20. Identificador do componente digital 21. Gênero 22. Espécie 23. Tipo 24. Idioma 25. Quantidade de folhas – páginas 26. Numeração seqüencial dos documentos 27. Identificação de anexos 28. Relação com outros documentos 29. Níveis de acesso 30. Data de produção 31. Classe 32. Destinação 33. Prazo de guarda 34. Localização
EVENTO DE GESTÃO	1. Captura 2. Tramitação 3. Transferência 4. Recolhimento 5. Eliminação 6. Abertura_processo – dossiê	10. Encerramento volume 11. Juntada anexação 12. Juntada apensação 13. Desapensação 14. Desentranhamento 15. Desmembramento

	7. Encerramento processo dossiê 8. Reabertura processo dossiê 9. Abertura volume	16. Classificação sigilo 17. Desclassificação sigilo 18. Reclassificação sigilo
CLASSE	1. Classe nome 2. Classe código 3. Classe subordinação 4. Registro de Reabertura 5. Registro de desativação 6. Reativação de classe 7. Registro de mudança de classe 8. Registro de deslocamento de classe	9. Registro de extinção 10. Indicador de classe ativa – inativa 11. Prazo de guarda na fase intermediaria 12. Evento que determina a contagem do prazo de guarda na fase intermediaria 13. Destinação final 14. Registro de alterações 15. Observações
AGENTE	1. Nome 2. Identificador 3. Autorização de acesso	4. Credenciais de autenticação 5. Relação 6. Status do agente
COMPONENTE DIGITAL	1. Identificador do componente digital 2. Nome original 3. Características técnicas 4. Formato de arquivo 5. Armazenamento	6. Ambiente de software 7. Ambiente de *hardware* 8. Dependências 9. Relação com outros componentes digitais 10. Fixidade
EVENTO DE PRESERVAÇÃO	1. Compressão 2. Decifração 3. Validação 4. Verificação de fixidade 5. Cálculo hash	6. Migração 7. Replicação 8. Verificação de vírus 9. Validação

Fonte: E-ARQ Brasil (2011, p.93, 94, 95)

Estes metadados apresentam-se mais como fontes da gestão arquivística eficiente de documentos digitais, porém, não estão acessíveis junto com a visualização das informações de conteúdo dos documentos, estando assim, mais a segundo plano, tratando-se da dinamicidade do documento digital de conter mais informações que simplesmente as que estão sendo visualizadas.

5. SEGURANÇA NO DESENVOLVIMENTO DE SISTEMAS DE GESTAO DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS

Um Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD) pode ser definido segundo o EARQ-Brasil (2009, p.10) como "um conjunto de procedimentos e operações técnicas, característico do sistema de gestão arquivística de documentos, processado por computador". Este sistema deve englobar tanto a gestão dos documentos convencionais como os digitais.

No desenvolvimento de SIGAD, é de suma importância a presença do profissional arquivístico, pois alguns requisitos devem fazer parte do sistema para que este possa se caracterizar um sistema arquivístico, segundo o EARQ-Brasil (2009,p.11,12) estes são:

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

Com esta preocupação de inserção dos requisitos de gestão arquivística de documentos, temos neste trabalho o foco no requisito de segurança, tanto no que se fala da formulação dos sistemas como nos mecanismos que estes terão que abarcar para conferir segurança às informações por eles geridas.

Muitos são os riscos que uma empresa terá ao implantar um sistema de informação. Porém, ao se elaborar o sistema, devem ser estudadas quais são as ameaças que iremos ter, quais os ataques que poderá sofrer, e analisar as consequências de uma proveniente falha de segurança.

Para que possamos entender sobre segurança da informação, devemos primeiramente analisar e saber gerir os riscos que a instituição estará sujeita, sobre isto, a NBR ISO/IEC (27005:2008, p.1) define riscos de segurança da informação como: "a possibilidade de uma

determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, desta maneira prejudicando a organização.”

> Uma abordagem sistemática de gestão de risco de segurança da informação é necessária para se identificar as necessidades da organização em relação aos requisitos de segurança da informação e para criar um sistema de gestão de segurança da informação (SGSI) que seja eficaz. NBR ISO/IEC (27005:2008, p.1).

As instituições devem gerir os riscos continuamente identificando-os, avaliando os prejuízos aos quais poderão vir a existir caso estes riscos se confirmem, informando a todos envolvidos da empresa com a probabilidade dos riscos, enfatizando os pontos negativos caso os riscos se transformem em realidade, tratando os riscos criando mecanismos para evitá-los.

Uma instituição que preze pela segurança da informação deve garantir recursos para implementação de mecanismos que a componham nos sistemas de informação.

Além de todos os meios que a instituição terá, um é de suma importância que é o treinamento e capacitação dos envolvidos com a segurança determinando competências e avaliando a eficácia dos processos de segurança.

Lembremos sempre que o trabalho de manutenção de segurança da informação é um trabalho preventivo, que não implicará em resultados visíveis e muitas vezes poderemos até achar que nunca algum risco se concretizará, porém, devemos ter como fundamento, pois se deixarmos vulnerabilidades com certeza teremos ataques, e estes se concentrarão nestas, pois os hackers projetam sistemas maliciosos baseados nas vulnerabilidades do sistema e não nas medidas de proteção que a instituição utiliza.

Com relação a vulnerabilidades a NBR ISO/IEC 27005 (2008, p.42) traz alguns exemplos os quais todas as empresas poderão estar sujeitas, e para dar uma noção maior sobre o que são as vulnerabilidades apresento estas ao leitor:

Quadro 3 – Exemplos de Vulnerabilidades e Ameaças.

TIPOS	EXEMPLOS DE VULNERABILIDADES	EXEMPLOS DE AMEAÇAS
Hardware	Manutenção insuficiente/instalação defeituosa de mídia de armazenamento	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
	Falta de uma rotina de substituição periódica	Destruição de equipamento ou mídia
	Sensibilidade à umidade, poeira, sujeira	Poeira, corrosão, congelamento

	Sensibilidade a radiação eletromagnética	Radiação eletro magnética
	Inexistência de um controle eficiente de controle de configuração	Erro durante uso
	Sensibilidade a variações de voltagem	Interrupção do suprimento de energia
	Sensibilidade a variações de temperatura	Fenômeno meteorológico
	Armazenamento não protegido	Furto de mídias ou documentos
	Falta de cuidado durante o descarte	Furto de mídias ou documentos
	Realização de cópias não controlada	Furto de mídias ou documentos
Software	Procedimentos de teste de *software* insuficientes ou inexistentes	Abuso de direitos
	Falhas conhecidas no *software*	Abuso de direitos
	Não execução do "logout" ao se deixar uma estação de trabalho desassistida	Abuso de direitos
	Descarte ou reutilização de mídia de armazenamento sem a execução dos procedimentos apropriados de remoção de dados	Abuso de direitos
	Inexistência de uma trilha de auditoria	Abuso de direitos
	Atribuição errônea de direitos de acesso	Abuso de direitos
	Software amplamente distribuído	Comprometimento dos dados
	Utilizar programas aplicativos com um conjunto errado de dados (referente a um outro período)	Comprometimento dos dados
	Interface de usuário complicada	Erro durante uso
	Documentação inexistente	Erro durante uso
	Configurações de parâmetro incorreta	Erro durante uso
	Datas incorretas	Erro durante uso
Rede	Inexistência de mecanismos de autenticação e identificação como, por exemplo, para a autenticação de usuário	Forjamento de direitos
	Tabelas de senhas desprotegidas	Forjamento de direitos
	Gerenciamento de senhas mal feito	Forjamento de direitos
	Serviços desnecessários permanecem habilitados	Processamento ilegal de dados
	Software novo ou imaturo	Defeito de *software*
	Especificações confusas ou incompletas para os desenvolvedores	Defeito de *software*
	Inexistência de um controle eficaz de mudança	Defeito de *software*
	Download e uso não controlado de *software*	Alteração de *software*
	Inexistência de cópias de segurança (*back-up*)	Alteração de *software*
	Inexistência de mecanismos de proteção física no prédio,	Furto de mídias ou documentos

	portas e janelas	
	Inexistência de relatórios de gerenciamento	Uso não autorizado de equipamento
	Inexistência de evidências que comprovem o envio ou o recebimento de mensagens	Repúdio de ações
	Linhas de comunicação desprotegidas	Escuta não autorizada
	Tráfico sensível desprotegido	Escuta não autorizada
	Junções de cabeamento mal feitas	Falha do equipamento de telecomunicação
	Ponto único de falha	Falha do equipamento de telecomunicação
	Não identificação e não autenticação do emissor e do receptor	Forjamento de direitos
	Arquitetura insegura da rede	Espionagem à distância
	Transferência de senhas em claro	Espionagem à distância
	Gerenciamento de rede inadequado (quanto a flexibilidade de roteamento)	Saturação do sistema de informação
	Conexões de redes públicas desprotegidas	Uso não autorizado de equipamento
Recursos Humanos	Ausência de recursos humanos	Indisponibilidade de recursos humanos
	Procedimentos de recrutamento inadequados	Destruição de equipamento ou mídia
	Treinamento insuficiente em segurança	Erro durante o uso
	Uso incorreto de software e *hardware*	Erro durante uso
	Falta de conscientização em segurança	Erro durante uso
	Inexistência de mecanismos de monitoramento	Processamento ilegal de dados
	Trabalho não supervisionado de pessoal de limpeza ou de terceirizados	Furto de mídias ou documentos
	Inexistência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens	Uso não autorizado de equipamento
Local ou instalações	Uso inadequado ou sem cuidados necessários dos mecanismos de controle de acesso físico do acesso físico a prédios e aposentos	Destruição de equipamentos ou mídias
	Localização em área suscetível a inundações	Inundação
	Fornecimento de energia instável	Interrupção do suprimento de energia
	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Furto de equipamentos
Organização	Inexistência de um procedimento formal para o registro e a remoção de usuários	Abuso de direitos

	Inexistência de processo formal para a análise crítica dos direitos de acesso (supervisão)	Abuso de direitos
	Provisões (relativas a segurança) insuficientes ou inexistentes, em contratos com clientes e/ou terceiros	Abuso de direitos
	Inexistência de procedimento de monitoramento das instalações de processamento de informações	Abuso de direitos
	Inexistência de auditorias periódicas (supervisão)	Abuso de direitos
	Inexistência de procedimentos para a identificação e análise/avaliação de riscos	Abuso de direitos
	Inexistência de realtos de falha nos arquivos (logs) de auditoria das atividades de administradores e operadores	Abuso de direitos
	Resposta inadequada do serviço de manutenção	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
	Acordo de nível de serviço (SLA – da sigla do termo em inglês) inexistente ou insuficiente	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
	Inexistência de procedimentos de controle de mudanças	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
	Inexistência de um controle formal para o controle da documentação do SGSI	Comprometimento dos dados
	Inexistência de um controle formal para a supervisão dos registros do SGSI	Comprometimento dos dados
	Inexistência de um procedimento formal para a autorização das informações disponíveis publicamente	Dados de fontes não confiáveis
	Atribuição inadequada das responsabilidades pela segurança da informação	Repúdio de ações
	Inexistência de um plano de continuidade	Falha de equipamento
	Inexistência de política de uso de correspondência eletrônica (e-mail)	Erro durante uso
	Inexistência de procedimentos para a instalação de software em sistemas operacionais	Erro durante uso
	Ausência de registros nos arquivos de auditoria (logs) de administradores e operadores	Erro durante uso
	Inexistencia de procedimentos para manipulação de informações classificadas	Erro durante uso
	Ausência das responsabilidades ligadas à segurança da informação nas descrições de cargos e funções	Erro durante uso
	Provisões (relativas a segurança) insuficientes ou inexistentes, em contratos com funcionários	Processamento ilegal de dados
	Inexistência de um processo disciplinar no caso de incidentes relacionados a segurança da informação	Furto de equipamentos
	Inexistência de uma política formal sobre o uso de	Furto de equipamentos

	computadores móveis	
	Inexistência de controles sobre ativos fora das dependências	Furto de equipamentos
	Política de mesas e telas limpas (clear desk and clear screen) inexistente ou insuficiente	Furto de mídia ou documentos
	Inexistência de autorização para as instalações de processamentos de informações	Furto de mídia ou documentos
	Inexistência de mecanismos estabelecidos para o monitoramento de violações da segurança	Furto de mídia ou documentos
	Inexistência de análises críticas periódicas por parte da direção	Uso não autorizado de equipamento
	Inexistência de procedimentos para o relato de fragilidades ligadas a segurança	Uso não autorizado de equipamento
	Inexistência de procedimentos para garantir a conformidade com os direitos de propriedade intelectual	Uso de cópias de software falsificadas ou ilegais

Fonte: NBR ISO/IEC 27005 (2008, p.42).

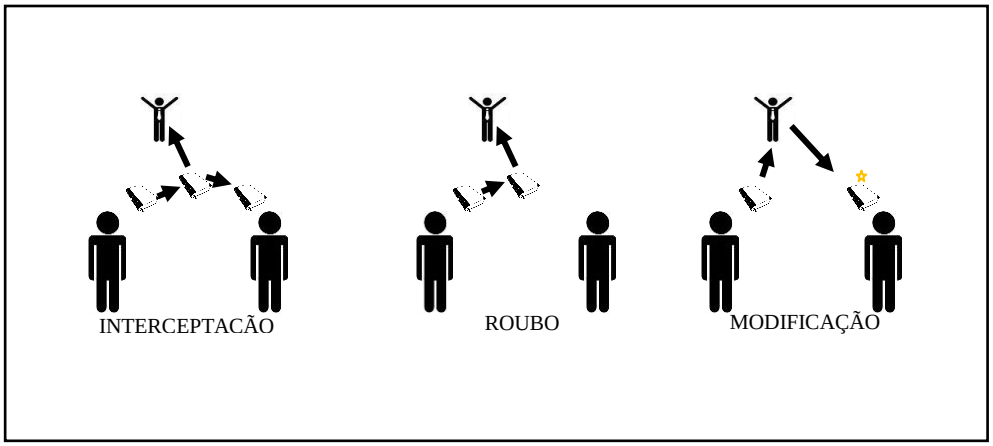
Identificados os riscos, analisadas as vulnerabilidades, a instituição deve manter o uso de mecanismo de controle da segurança da informação para assim evitar ataques, e se estes acontecerem, que não tenham sucesso.

Para o EARQ-Brasil (2009), um SIGAD deve ter mecanismos de segurança que controlem o acesso e garantam a integridade dos documentos, controle o uso e rastreamento dos documentos, identificando a permissão de acesso, o grau de sigilo dos documentos, registro de todos os acessos e tentativas de acesso, assim como o uso destes com ou sem edição. Trilhas de auditoria é o registro dos metadados, os quais trarão informações sobre acesso, uso, edições, tramitações, desde a captura ou produção do documento, ao registro classificação, indexação, arquivamento, armazenamento, recuperação da informação, preservação e destinação. Esta deverá informar quem operou, data, hora, edições ou não.

Os sistemas de informação devem garantir segurança em todas as etapas da gestão, primeiramente na produção garantindo o acesso somente de pessoas autorizadas ao sistema, registrando data e hora da produção, quem produziu, registrar onde foi produzido, qual o propósito deste, para quem diz respeito e garantir que este documento tenha uma autenticação do autor, em que possa ser conferido realmente se quem produziu a informação foi realmente o autor, evitando assim a personificação.

Na tramitação, onde um documento pode ser simplesmente capturado e as informações serem divulgadas a pessoas não autorizadas, pode ser interrompida (roubada), e também pode ser interceptada por um *hacker*, modificada, e ser dada continuidade a tramitação com documento modificado, como ilustrado na figura:

Figura 2: Formas de interceptação da informação.



Fonte: Elaborado pelo autor (2014)

Na guarda dos documentos, onde os sistemas podem sofrer ações de ataques de engenharia social, as quais englobam o uso de pessoas mal intencionadas, que coagem as outras a fazerem o errado inconscientemente, trazendo vulnerabilidades aos sistemas que depois serão alvo de ataques virtuais, com programas mal intencionados que podem negar acesso, roubar, modificar, distribuir, duplicar, apagar, acrescentar informações.

A estrutura organizacional dos arquivos pode ser comprometida por estes programas. Documentos podem ser criados por pessoas personificadas, ou seja, *hacker* se passando por outras pessoas, podem trazer prejuízos incalculáveis às instituições.

O acesso aos documentos também pode ser alvo de ataques, os sistemas muitas vezes pode ser alvo de negação de serviço, uma gama enorme de acessos podem comprometer o sistema, a área de apresentação dos documentos pode ser modificada, trazendo uma distorção do que deveria ser apresentado dentre outras inúmeras formas de ataques que atualmente crescem paralelamente ao desenvolver da informática.

Para a NBR ISO/IEC 27002 (2005, p.xii), existem controles considerados essenciais a uma organização quanto à segurança da informação os quais segundo o ponto de vista legal são:

a) “Proteção de dados e privacidade de informações pessoais;

b) Proteção de registros organizacionais;

c) Direitos de propriedade intelectual.”

Os controles considerados práticas para a segurança da informação incluem:

> a) Documento da politica de segurança da informação;
> b) Atribuição de responsabilidades para a segurança da informação;
> c) Conscientização, educação e treinamento em segurança da informação;
> d) Processamento correto nas aplicações;
> e) Gestão de vulnerabilidades técnicas;
> f) Gestão da continuidade do negócio;
> g) Gestão de incidentes de segurança da informação e melhorias.

Embora esta norma brasileira cite estes controles como exemplos para as instituições, estas últimas devem saber que, o que determina os controles a serem usados serão os riscos aos quais está exposta, assim, não há uma lista pré-elaborada a ser utilizada genericamente, pois os controles vão de acordo com as especificações de cada órgão.

Um risco pode ser qualquer incerteza quanto aos objetivos de uma instituição derivada de falhas no controle da informação. Os requisitos de segurança utilizados pelas instituições devem ser baseados nos riscos e vulnerabilidades em que estão expostas, quanto sua identificação o guia de referência para a segurança das infraestruturas críticas da informação (2010,p.29), diz:

> Para que uma organização identifique seus requisitos de segurança, ela deve basear-se em três pilares. O primeiro é o conjunto dos princípios, objetivos e necessidades para o processamento da informação que uma organização tem que desenvolver pra apoiar suas operações. O segundo é a legislação vigente, os estatutos, as regulamentações e as cláusulas contratuais que a organização, seus parceiros, contratados e prestadores de serviço têm que atender. E o terceiro, oriunda das duas anteriores, são os requisitos de segurança derivados da avaliação de riscos, processo responsável por identificar as ameaças aos ativos, as vulnerabilidades com suas respectivas probabilidades de ocorrência e os impactos aos negócios.

Um caráter preventivo é o que define a adoção de mecanismos para a segurança da informação em sistemas de gestão informatizada de documentos, estes tem o objetivo de conferir autenticidade, fidedignidade, integridade, confidencialidade, acesso e registrar tudo em forma de metadados que serão utilizados como fonte de prova para conferir o valor legal aos documentos arquivísticos digitais.

6. MECANISMOS PARA CONTROLE DE SEGURANÇA

Como apresentado anteriormente, todos os sistemas de informação estão sujeitos a ameaças e ataques, os mesmos, quando analisados os riscos e descobertas as vulnerabilidades, os profissionais responsáveis pela segurança dos sistemas utilizam-se de diversos mecanismos para eliminar as vulnerabilidades ou mesmo para diminuir o risco de ataques.

O que determina o uso ou não de mecanismos são os riscos que os sistemas estão expostos, diante disto é que os mecanismos deverão ser utilizados. Para entendermos um pouco mais sobre os mecanismos e sua aplicabilidade, apresento uma lista dos quais podem fazer parte dos sistemas de informação como recurso de segurança.

6.1 CRIPTOGRAFIA

A criptografia consiste em um "método de codificação de dados com base em algoritmo específico e chave secreta, de forma que somente os usuários autorizados possam reestabelecer a forma original dos dados." (EARQ-Brasil 2011, p.127). Este mecanismo é muito utilizado para a tramitação, envio e recebimento de documentos, possibilitando a autenticação de usuários, registrando autorias, permitindo acesso somente a autorizados e deixando a mensagem sem condições de leitura para quem não tiver as chaves de acesso.

Segundo O'Brien (2007, p. 436), "a criptografia envolve o uso de algoritmos matemáticos especiais, ou chaves, para transformar dados digitais em códigos antes de serem transmitidos e para decodificar os dados quando são recebidos.". Assim, existe o embaralhamento das informações, deixando-as serem lidas somente por quem tiver a chave de decriptografar.

A criptografia é de suma importância para a segurança da informação pois:

> Controles criptográficos podem ser usados para alcançar diversos objetivos de segurança, como, por exemplo:
> a) Confidencialidade: usando a criptografia da informação para proteger informações sensíveis ou críticas, armazenadas ou transmitidas.
> b) Integridade/autenticidade: usando assinaturas digitais ou códigos de autenticação de mensagens (MAC) para proteger a autenticidade e a integridade de informações sensíveis ou críticas, armazenadas ou transmitidas;
> c) Não-repúdio: usando técnicas de criptografia para obter prova da ocorrência ou não ocorrência de um evento ou ação.
> NBR ISO/IEC 27002, (2005, p.88).

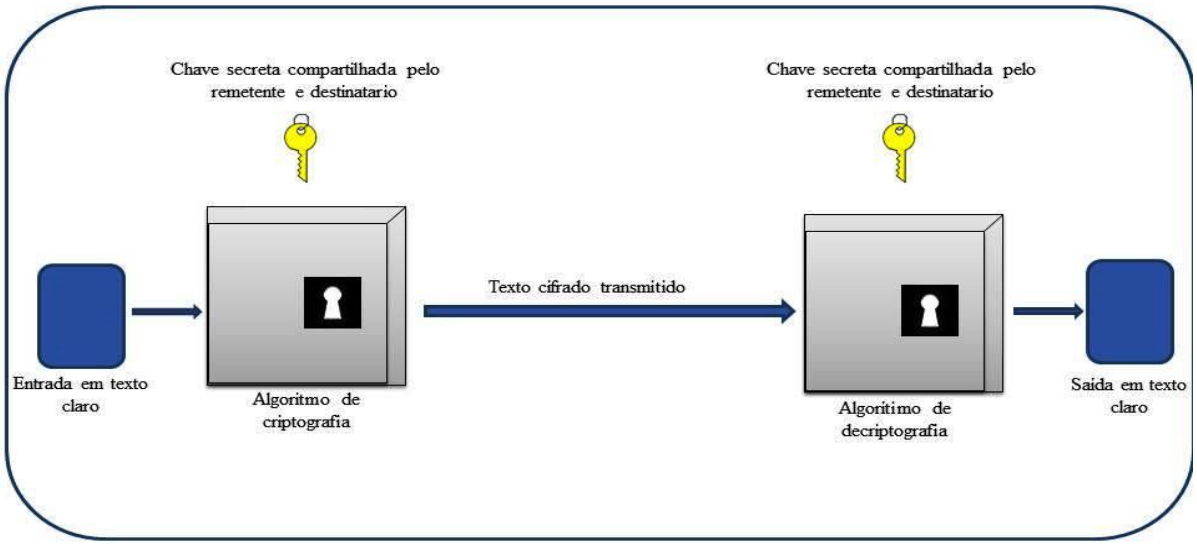
Existem dois tipos de criptografia, a simétrica em que, a chave utilizada para criptografar é a mesma para descriptografar e a assimétrica que, ao contrario da primeira,

utiliza-se de duas chaves criptográficas diferentes, a primeira para criptografar e a segunda para decriptografar.

6.1.1 Criptografia simétrica

Na criptografia simétrica o remetente e o destinatário usam a mesma chave. Um dos problemas da criptografia simétrica é que tanto "o remetente quanto o destinatário precisam conhecer a chave e mantê-la em segredo". (TURBAN, RAINER, POTTER, 2007, p.73).

Figura 3 – Criptografia Simétrica



Fonte: Stallings (2008, p.18)

Como supracitado, a criptografia simétrica utilizando-se de uma única chave para criptografar e decriptografar, oferece riscos, pois, tanto o originador quanto o receptor devem possuir a mesma chave, e assim o compartilhamento das chaves pode ser interceptado. Então, facilmente um intruso com a chave de cifragem conseguiria decriptografar uma mensagem simétrica.

Na edição número cinco da revista Segurança Digital, Oliveira (2012, p.12) diz que:

> O principal problema residente na utilização deste sistema de criptografia é que quando a chave de ciframento é a mesma utilizada para deciframento, ou esta última pode facilmente ser obtida a partir do conhecimento da primeira, ambas precisam ser compartilhadas previamente entre origem e destino, antes de se estabelecer o canal criptográfico desejado, e durante o processo de compartilhamento a senha pode ser interceptada, por isso é fundamental utilizar um canal seguro durante o compartilhamento, este independente do destinado à comunicação sigilosa, uma vez que qualquer um que tenha acesso à senha poderá descobrir o conteúdo secreto da mensagem.

Outros aspectos também podem ser considerados quando fala-se de chaves simétricas. Para uma comunicação existir com criptografia simétrica, para cada dupla de usuários deve existir uma chave, e esta, deverá ser diferente quando se muda qualquer uma das partes, assim, sabendo que a cada dupla diferente teremos que ter uma chave também diferente, teríamos assim um volume enorme de chaves privadas igual a n^2.

Também segundo a revista Segurança Digital, Oliveira (2012, p.12), "A criptografia simétrica não garante os princípios de autenticidade e não-repudiação.". O que é de suma importância para a segurança da informação por serem características dos documentos arquivísticos.

Dentre algumas vantagens que esta trás, podemos citar a velocidade, pois usa uma codificação de 128 bits, e assim pode ser processada e criptografia rapidamente.

Para a arquivologia, tanto a simétrica como a assimétrica podem ser usadas, a primeira para informações de sistema que necessitam confidencialidade entretanto não precisam de autenticidade, já na assimétrica, mecanismo diretamente usado nos documentos que podem garantir a autenticidade, confidencialidade e integridade.

6.1.2 Criptografia Assimétrica

A criptografia assimétrica utiliza chaves diferentes, uma pública e outra privada. De acordo com Turban, Rainer, Potter (2007, p.73): "A chave pública e a privada são criadas simultaneamente com a mesma fórmula matemática (algoritmo). Como as duas chaves estão matematicamente relacionadas, os dados criptografados com uma chave podem ser decriptografadas usando-se a outra chave".

Quando um usuário deseja enviar um documento criptografado a outrem, utilizando-se da criptografia assimétrica, primeiramente deverá buscar a chave pública do destinatário e assim criptografar a mensagem com ela, com isso, só quem poderá ter acesso ao conteúdo do documento será o destinatário que possui a chave privada, pois uma vez criptografado com uma chave pública, só a chave privada correspondente poderá decriptografar.

Através da criptografia assimétrica também podemos conferir autenticidade aos documentos, pois conforme diz Stallings (2008, p.73):

> Os sistemas de chave pública também mostram se uma mensagem é autêntica; ou seja, se você criptografa uma mensagem usando sua chave privada, precisa "assina-la" eletronicamente. O destinatário pode verificar se a mensagem veio de você usando sua chave pública para descriptografá-la.

A confidencialidade do documento também pode ser garantida desde que a chave privada esteja só com o destinatário, segundo isso o autor Oliveira (2012, p.12), em revista Segurança Digital, diz que:

> A grande vantagem deste sistema é permitir a qualquer um enviar uma mensagem secreta, apenas utilizando a chave pública de quem irá recebê-la. Como a chave pública está amplamente disponível, não há necessidade do envio de chaves como feito no modelo simétrico. A confidencialidade da mensagem é garantida, enquanto a chave privada estiver segura.

A desvantagem encontrada neste método criptográfico é a velocidade de processamento, por se tratar de chaves diferentes, consequentemente há uma verificação de compatibilidade das chaves, então o processo torna-se mais complexo devido a necessidade de acesso do computador ao banco de dados das chaves.

A vantagem é o alto grau de segurança por ela empregada, podendo ser utilizada também para conferir autenticidade ao documento, e admitir um alto grau de confidencialidade.

6.2 ASSINATURA DIGITAL

Assim como em um documento convencional, um documento digital precisa de um autor, ou, uma pessoa que assine aquele documento testemunhando o ato. Para documentos convencionais a assinatura era manual e tem valor legal, já como o documento digital não admite isto, por conta do seu suporte, e diante da necessidade de manter o valor legal do documento, provando-se a autenticidade deste, foi desenvolvido a assinatura digital.

Conforme Stallings (2008, p.272),

> Uma assinatura digital é um mecanismo de autenticação que permite ao criador de uma mensagem anexar um código que atue como uma assinatura. A assinatura é formada tomando o hash da mensagem e criptografando-a com a chave privada do criador. A assinatura garante a origem e a integridade da mensagem.

A assinatura digital é um modo de criptografia, quando alguém assina digitalmente um documento, um resumo do documento é criptografado e assim, para verificar a autenticidade do mesmo basta ir ao banco de chaves públicas da entidade certificadora e conferir se a chave pública de quem enviou a mensagem é a compatível com a privada que assinou o documento.

De acordo com o EARQ-Brasil (2011, p.73), “assinatura digital é uma sequência de bits que usa algoritmos específicos, chaves criptográficas e certificados digitais para autenticar a identidade do assinante e confirmar a integridade de um documento.”.

A criptografia utilizada neste método de assinatura é a assimétrica, em que utilizando-se a chave privada para criptografar o *hash* (resumo) – não mais a mensagem toda – a chave pública irá conferir a autenticidade e integridade do documento. Segundo Nascimento (2008, p.57), para a assinatura digital,

> ...é utilizada a criptografia assimétrica com a função das chaves num sentido inverso, onde o hash é criptografado usando a chave privada do remetente, sendo assim o destinatário de posse da chave pública do remetente poderá decriptar o hash. Dessa maneira garante a procedência, pois somente o remetente possui a chave privada para codificar o hash que será aberto pela sua chave pública. Já o hash gerado a partir da informação original, protegido pela criptografia, garantirá a integridade da informação.

Para que a assinatura digital tenha sentido faz-se necessário lembrar que as chaves privadas devem estar sempre em poder dos proprietários, e somente eles, pois, se não for assim, a autenticidade poderá ser contestada.

Caso algum proprietário de assinatura digital sinta que a sua assinatura não mais está segura, o mesmo poderá solicitar nova chave e assim também sua chave pública será trocada pela autoridade certificadora.

Algumas características devem ser encontradas na assinatura digital, segundo Stallings (2008, p.273) como:

- Deve verificar o autor, a data e a hora da assinatura.
- Deve autenticar o conteúdo no momento da assinatura.
- Deve ser verificável por terceiros, para resolver disputas."

Alguns requisitos também devem ser observados segundo Stallings (2008, p.273):

- "Ela precisa ser um padrão de bits que dependa da mensagem que será assinada.
- Precisa usar alguma informação exclusiva do emissor, para impedir tanto a falsificação quanto a retratação.
- Deve ser relativamente fácil produzi-la.
- Deve ser relativamente fácil reconhecê-la e verificá-la.
- Deve ser computacionalmente inviável falsifica-la, seja construindo uma nova mensagem para uma assinatura digital existente seja construindo uma assinatura digital fraudulenta para determinada mensagem.
- Deve ser prático armazenar uma cópia da assinatura digital.

Ainda sobre assinatura digital, quando falamos de criptografia assimétrica, sabemos que teremos chaves privadas e públicas, entretanto, há de ter uma entidade responsável pela criação, distribuição, armazenamento e gerenciamento das chaves de forma segura e eficiente. Esta instituição deverá ser capaz de gerir a chamada "infraestrutura de chaves públicas".

Sobre a mesma, a RFC 2828(apud, Stallings, 2008, p309) define-a como:

> O conjunto de *hardware*, software, pessoas, políticas e procedimentos necessários para criar, gerenciar, armazenar, distribuir e revogar certificados digitais com base na criptografia assimétrica. O objetivo principal para desenvolver uma PKI[2] é permitir a aquisição segura, conveniente e eficiente de chaves públicas.

Aqui no Brasil há a Instituição de Infraestruturas de Chaves Públicas Brasileira – ICP-Brasil. A mesma foi criada pelo governo federal em 24 de agosto de 2001 por meio da medida provisória de 2.200-2, e a institui para:

> ...garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras. (MP-2.200-2, 2001).

A ICP-Brasil é composta pala autoridade gestora de políticas e pela cadeia de autoridades reguladoras as quais também são compostas por Autoridade certificadora raiz, pelas Autoridades certificadoras e pelas autoridades de registro. (MP-2.200-2, 2001).

A autoridade gestora terá a função de: estabelecer políticas, adotar medidas e coordenar o estabelecimento da ICP-Brasil, homologar, auditar, fiscalizar Autoridades Certificadoras, estabelecer diretrizes, normas técnicas, normatizar. É vedada a emissão de certificados digitais ao usuário final por parte da Autoridade gestora e a Autoridade Certificadora raiz. (MP-2.200-2, 2001).

Às Autoridades Certificadoras brasileiras compete:

> ...emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações. (MP-2.200-2, 2001, art.6º).

As Autoridades certificadoras emitem certificados digitais, os mesmos podem ser relacionados com as identidades das pessoas, e conforme a Receita Federal como disposto em seu site oficial, certificado digital é :

> Um arquivo eletrônico que identifica quem é seu titular, pessoa física ou jurídica, ou seja, é um Documento Eletrônico de Identidade. Quando são realizadas transações, de forma presencial, muitas vezes é solicitada uma identificação, por meio de um registro que comprove a identidade. Na *internet*, como as transações são feitas de forma eletrônica o Certificado Digital surge como forma de garantir a identidade das partes envolvidas.

Atualmente, o uso de documentos digitais em transações financeiras e outros serviços digitais, buscam garantir autenticidade, fidedignidade, integridade, não repúdio, e é isso que o certificado digital vem trazendo as transações e serviços eletrônicos. A certificação digital

[2] PKI – Public-Key Infraestructure

para a Receita Federal, "é considerada uma ferramenta de segurança extremamente eficaz, garantindo a integridade das informações que trafegam na *internet* e identificação da origem e do destino".

A MP 2200-2, (2001, apud Receita Federal), garante validade jurídica aos documentos assinados eletronicamente com os certificados digitais emitidos dentro da infraestrutura da ICP-Brasil. Ainda também a certificação digital garante privacidade nas transações, criptografando as mensagens; integridade, não permitindo alterações/modificações; autenticidade, garantindo quem assinou o documento.

A certificação digital tem crescido e se tornado mais uma forma de documento de identificação, antes somente com assinaturas escritas manualmente agora também com assinaturas digitais, a primeira utilizada no universo dos documentos físicos e a segunda nos documentos digitais.

Com tudo o que foi supracitado, um documento digital pode ser assinado e mantido a autenticidade da informação através da assinatura digital, resolvendo assim a questão de autenticação dos documentos nos sistemas de informação.

Assim como também se caracteriza como uma criptografia assimétrica, a assinatura digital para a arquivologia é de suma importância garantindo através desta a confidencialidade, fidedignidade e autenticidade.

6.3 BIOMETRIA

Para o controle de acesso existe um mecanismo que se utiliza de características biológicas para a autenticação do usuário, a qual denomina-se biometria.

Segundo O'Brien e Marakas (2007, p.443),

> Há medidas de segurança fornecidas por dispositivos de computador que avaliam características físicas, que tornam cada indivíduo único. Isso inclui verificação de voz, digitais, geometria da mão, dinâmica de assinatura, análise de digitação, varredura da retina, reconhecimento de face, e analises do padrão genético.

Atualmente este tipo de controle de acesso tem sido muito difundido. Muitos quando falam de biometria pensam no uso das digitais, entretanto, muitas outras formas como: leitura da palma da mão, reconhecimento de face, dentre outras formas de controle biométrico são utilizadas como visto na citação de O'Brien e Marakas.

Para o TCU (2012, p.24), “Os sistemas biométricos são sistemas automáticos de verificação de identidade baseadas em características físicas do usuário. Esses sistemas têm como objetivo suprir deficiências de segurança das senhas...”. Atualmente, senhas numéricas ou alfanuméricas, tem cedido espaço ao controle biométrico diante da facilidade de roubo, em que as primeiras estão sujeitas.

Hoje, um dos maiores exemplos de controle biométrico difundido no Brasil é o da biometria nas votações. O reconhecimento das digitais dos eleitores é utilizado substituindo as assinaturas convencionais.

O Banco do Bradesco também é um exemplo para o uso da biometria, este, usou da biometria da palma da mão, que segundo a instituição em seu próprio site afirma que: “Ela faz leitura biométrica das veias da palma da mão e da corrente sanguínea ativa, e não da sua digital. Por isso, impossibilita clonagem e fraudes – nem irmãos gêmeos idênticos têm as mesmas características.” (BRADESCO, p.1, 2015).

Apesar das vantagens do uso da biometria, uma desvantagem é descrita por TCU, (2012, p.24), “Um dos problemas enfrentados pelos sistemas biométricos atuais é a alta taxa de erro, em função da mudança das características de uma pessoa com o passar dos anos, ou devido a problemas de saúde ou nervosismo, por exemplo.”. O uso da biometria, quando se utilizado em alta escala, está sempre relacionado com outro mecanismo de controle de acesso, algumas vezes para completar a segurança, outras para servir de segunda opção para a autenticação de acesso.

Nos exemplos reais que citei neste capítulo, o TSE nas votações quando não reconhecida a digital do eleitor, dispõe da assinatura convencional para que o mesmo possa votar. Já o Banco Bradesco, dispõe das senhas numéricas para autenticação do usuário.

Os controles biométricos estão se desenvolvendo rapidamente, assim, a cada dia mecanismos novos estão sendo criados e aperfeiçoados, diante disto, muitas formas hoje tem sido utilizadas ainda atreladas a outras, porém, com o avanço das tecnologias logo mais esses reconhecimentos biométricos estarão sendo utilizados podendo conferir alto grau de confiabilidade na autenticação de pessoas.

A acessibilidade, como característica do documento arquivístico, deve ser preservada e controlada. A biometria vem se tornando uma das formas muito utilizadas pelas instituições, pelo fato do controle de acesso que pode ser garantido somente o acesso de pessoas autorizadas com alto grau de confiabilidade.

6.4 FIREWALL

Atualmente há um crescente uso de redes de computadores em empresas, seja ela uma pequena ou grande empresa. Diante disto, e da necessidade de preservar a segurança das informações nelas contidas, utilizam-se de *firewall*, pois o *firewall* pode ser um dos métodos mais eficaz para manter a rede segura, tanto controlando o acesso a rede interna de computadores como regulando o acesso a redes externas.

Esta ferramenta, o *firewall*, é utilizado para controlar a transmissão de dados entre duas ou mais redes. Conforme O'Brien e Marakas (2007, p.437),

> Um *firewall* trabalha como um sistema de "porteiro" que protege as *intranet* e outras redes de computador da empresa de invasões, fornecendo um filtro e um ponto de transferência seguro para acesso a *internet* e outras redes. Ele examina as senhas e outros códigos de segurança de todo o tráfico da rede, e só permite transmissões autorizadas para dentro e para fora da rede.

O uso de redes não mais está sendo uma opção para as instituições, como as informações de maneira geral encontram-se centralizadas, as mesmas precisam utilizar tanto redes internas (*intranet*), como também a *internet*, para garantir o acesso aos autorizados quando necessário.

O *firewall* (BELL, 1994, apud Stallings, 2008) deve ter como objetivos de que todo o tráfego de dados deve passar por ele, somente tráfego autorizado pela política de segurança terá permissão de passar.

Algumas técnicas são utilizadas pelos *firewalls*, de acordo com (SMIT, 1997, apud Stallings, 2008, p.444),

> - "Controle de serviço: Determina os tipos de serviços de *Internet* que podem ser acessados, de entrada ou de saída. O *firewall* pode filtrar o tráfego com base no endereço IP e número de porta TCP; pode oferecer software de *proxy* que recebe e interpreta cada solicitação de serviço antes de passa-la adiante, ou pode hospedar o próprio software do servidor, como um serviço Web ou de correio..
> - Controle de direção: Determina a direção em que determinadas solicitações de serviço podem ser iniciadas e permitidas para fluir através do *firewall*.
> - Controle de usuário: Controla o acesso a um serviço de acordo com qual usuário está tentando acessá-lo. Essa característica normalmente é aplicada aos usuários dentro do perímetro do *firewall*. (usuários locais). Ela também pode ser aplicada ao tráfego que chega de usuários externos; esse último exige alguma forma de tecnologia de autenticação segura, como a que é fornecida no IPSec.
> - Controle de comportamento: Controla como determinados serviços são usados. Por exemplo, o *firewall* pode filtrar e-*mail* para eliminar spam ou pode permitir o acesso externo a apenas uma parte da informação em um servidor *Web* local".

Um *firewall* pode ser considerado como um controlador de dados entre duas ou mais redes, estabelecendo regras e limites, este pode ser *software* em um computador, roteador,

mainframe dentre outras possibilidades, geralmente instalado no local onde há a conexão entre as redes, local que popularmente chama-se de ponto de estrangulamento.

Quando se projeta um sistema de gestão de documentos arquivístico digitais, uma das grandes preocupações é em manter os documentos, preservando a confidencialidade e integridade, e o *firewall*, veio como mecanismo para garantir que não haja tráfego de dados maliciosos que poderiam trazer malefícios aos documentos, e que não tenha possibilidades de intrusões no sistema.

6.5 DETECTOR DE INTRUSOS

A invasão a sistemas tem se tornado uma grande ameaça a quem possui sistemas de informação. Para tentar diminuir as vulnerabilidades relacionadas, um mecanismo utilizado chama-se "sistema de detecção de intrusos (*IDS- Intrusion Detection System*)".

Para falarmos sobre IDS, devemos ter primeiramente a definição de intrusão, que segundo Mendes (2008, apud Head, Luger et al, 1990), significa "qualquer conjunto de ações que tentem comprometer a integridade, confidencialidade ou disponibilidade dos dados e/ou sistema."

O intruso pode ser dividido em três classes:

> - Mascarado: Um indivíduo que não está autorizado a usar o computador e que penetra nos controles de acesso de um sistema para explorar a conta de um usuário legítimo.
> - Infrator: Um usuário legítimo que acessa dados, programas ou recursos para os quais não tem autorização de acesso, ou que está autorizado para tal acesso, mas faz mau uso de seus privilégios
> - Usuário clandestino: Um usuário que se apodera do controle de supervisor do sistema e utiliza esse controle para escapar de auditorias e controle de acesso ou para suprimir provas parciais de auditoria.
>
> (STALLINGS, 2008, p.406)

O mecanismo de detecção de intrusos "têm sido desenvolvido para fornecer um aviso inicial de intrusão, para que a ação defensiva possa ser tomada para impedir ou minimizar danos.". (STALLINGS, 2008, p405).

O detector de intrusos busca atividades com padrões incomuns e também atividades que antes foram programadas no sistema, como atividades relacionadas à intrusão. Após serem detectadas, ou o sistema emite avisos sobre o problema ou também pode bloquear a ação do intruso.

Existem basicamente três tipos de IDS, o baseado em Host (HIDS), o baseado em Rede (NIDS) e o hibrido que utiliza os dois primeiros. Abaixo defino os tipos de IDS segundo Nassaro (2012, p.35):

Quadro 4 – Tipos de IDS

IDS baseado em Host(HIDS)	Esse sistema de detecção é baseado nas informações levantadas junto a um único computador, ignorando o trafego no restante da rede. Essa solução é adotada quando um servidor da rede necessita ser protegido, não importando muito o que acontece na sua vizinhança. O HIDS é baseado na análise de eventos do sistema e registros de *logs* ou ainda nas informações levantadas por um *software* específico. Esse meio de detecção é indicado em casos onde a segurança é focada num único servidor, porém os usuários não necessitam de muita segurança ou ainda casos onde a segurança da rede da corporação como um todo não é muito confiável, porém seu servidor necessita de maior proteção.
IDS baseado em Rede (NIDS)	Este sistema monitora e analisa o trafego dentro da rede da corporação, trabalhando com um conjunto de sensores alocados em pontos estratégicos do segmento de rede, com a finalidade de detectar atividades anormais, como os ataques de *portscan* e negação de serviço (DOS). Os NIDS são instalados em equipamentos que monitoram o conteúdo dos pacotes e do trafego e os analisam detalhadamente, principalmente seus cabeçalhos e pilhas de protocolos. Seu objetivo principal e detectar tentativas de invasões no perímetro da em- presa.
IDS híbridos	São fundamentados na união dos IDS baseados em Hosts com o IDS baseados em Rede, aumentando o controle da segurança tecnológica do ambiente.

Fonte: Nassaro (2012, p.35)

O mecanismo de detecção de intrusos deve ser uma realidade nas empresas que valorizam a informação. É necessário para combater o roubo, o acesso não autorizado, e até

mesmo intrusões que comprometam as características do documento arquivístico digital, que sejam identificados e bloqueados os acessos não autorizados a rede corporativa e até mesmo individualmente aos computadores, *smartfones*, *tablets* dentre outros equipamentos que contenham o ativo importante da informação para a empresa.

Com o uso de um IDS programado seguindo os riscos que a instituição está exposta, o intruso pode se sentir mais intimidado e desestimulado a praticar ataques aos sistemas de informação, tratando-se de uma dificuldade maior ao acesso.

Como vimos, o sistema de detecção de intrusos serve para identificar pessoas não autorizadas ao acesso, também podendo bloquear e expulsa-las da rede, assim, não devemos esquecer que este mecanismo serve para detectar intrusões, mas, preventivamente, a instituição deverá adotar mecanismos que evitem a intrusão, não deixando que qualquer um não autorizado consiga entrar no sistema de informação.

O detector de intrusos atuará juntamente com o *firewall*, fazendo com que a confidencialidade seja garantida.

6.6 TRILHAS DE AUDITORIA

Diante da necessidade de investigações futuras nos documentos digitais referentes às suas características como documento arquivístico digital, foram evidenciados a importância de manter metadados que identifiquem intervenções, tentativas de intervenções acessos, criação, tramitação dentre outros dados que demonstrem todas as ações pertinentes ao documento, a estes metadados chamamos de trilhas de auditoria.

Conforme o EARQ-Brasil (2011, p71),

> A trilha de auditoria consiste num histórico de todas as intervenções, ou tentativas de intervenções, feitas no documento e no próprio SIGAD. Nesse sentido, é também um metadado sobre os documentos arquivísticos digitais e informa sobre sua autenticidade.

A NBR ISO/IEC (27002, p.61) acrescenta que:

> Convém que os registros (*log*) de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação sejam produzidos e mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento de controle de acesso.

As trilhas de auditoria é muito importante, pois, elas devem trazer todos os registros que os usuários tentaram fazer, obtendo sucesso ou não. Através deles é que poderemos

conferir autenticidade, confidencialidade, integridade, fidedignidade, acessibilidade que são características de um documento arquivístico digital.

De acordo com o EARQ-Brasil alguns requisitos devem ser observados referente as trilhas de auditoria pelos sistemas de informação, e abaixo trazemos para entendermos mais sobre estes metadados.

Quadro 5 – Requisitos de sistema para trilhas de auditoria

REQUISITO
Um SIGAD tem que ser capaz de registrar, na trilha de auditoria, informações acerca das ações a seguir: • data e hora da captura de todos os documentos; • responsável pela captura; • reclassificação, desclassificação ou redução do grau de sigilo de um documento ou dossiê/processo, com a classificação inicial e final. • qualquer alteração na tabela de temporalidade e destinação de documentos; • qualquer ação de reavaliação de documentos; • qualquer alteração nos metadados associados a classes, dossiês/ processos ou documentos; • data e hora de produção, aditamento e eliminação de metadados; • alterações efetuadas nas permissões de acesso que afetem um dossiê/processo, documento ou usuário; • ações de exportação e importação envolvendo os documentos; • tentativas de exportação (inclusive para backup) e importação (inclusive restore); • usuário, data e hora de acesso ou tentativa de acesso a documentos e ao SIGAD; • tentativas de acesso negado a qualquer documento; • ações de eliminação de qualquer documento e seus metadados; • infrações cometidas contra mecanismos de controle de acesso; • mudanças no relógio gerador de carimbos de tempo; • todas as ações administrativas sobre os atributos de segurança (papéis, grupos, permissões etc.); • todas as ações administrativas sobre dados de usuários (cadastro, ativação, bloqueio, atualização de dados e permissões, troca de senha etc.); • todos os eventos de administração e manutenção das trilhas de auditoria (alarmes, cópias, configuração de parâmetros etc.).
Um SIGAD tem que registrar, em cada evento auditado, informações sobre a identidade do usuário, desde que essa identificação esteja de acordo com a política de privacidade da organização e a legislação vigente.
Um SIGAD deve permitir apenas ao administrador e ao auditor a leitura das trilhas de auditoria.
Um SIGAD tem que assegurar que as informações da trilha de auditoria estejam disponíveis para inspeção, a fim de que uma ocorrência específica possa ser identificada e todas as informações correspondentes sejam claras e compreensíveis.

Um SIGAD deve possuir mecanismos para realização de buscas nos eventos das trilhas de auditoria. Para facilitar a visualização do relatório, os resultados podem ser apre- sentados de modo ordenado, mas essa ordenação não pode alterar os dados incluídos na trilha.
Um SIGAD tem que ser capaz de impedir qualquer modificação na trilha de auditoria.
Somente administradores autorizados têm que ser capazes de exportar as trilhas de auditoria sem afetar a trilha armazenada, ou transferir as trilhas de auditoria de um suporte de armazenamento para outro. A trilha de auditoria não pode ser excluída antes da data indicada na tabela de temporalidade. Porém, a transferência implica a cópia da trilha para outro espaço de armazenamento, com a subsequente liberação do espaço original. A exportação é a cópia sem liberação do espaço.
Um SIGAD deve ser capaz de gerar um alarme para os administradores apropriados se o tamanho da trilha de auditoria exceder um limite preestabelecido. Esse alarme deve ser usado para indicar a proximidade do esgotamento do espaço reservado à trilha de auditoria.
Quando o espaço de armazenamento da trilha de auditoria atingir o limite preestabelecido, um SIGAD deve permitir somente operações au- ditáveis originadas por administradores. Todas as outras operações estarão bloqueadas até a liberação pelo ad- ministrador
Um SIGAD deve ser capaz de aplicar um conjunto de regras na monitoração de eventos auditados e, com base nelas, indicar a possível violação da segurança
Um SIGAD deve garantir pelo menos as seguintes regras para monitora- ção dos eventos auditados: • acumulação de um número predeterminado de tentativas consecutivas de login com erro (autenticação malsucedida), conforme especificado pela política de segurança; • ocorrência de vários login simultâneos do mesmo usuário em locais (computadores) diferentes; • login do usuário fora do horário autorizado, após logoff no período normal.
Um SIGAD tem que fornecer relatórios sobre as ações que afetam clas- ses, unidades de arquivamento e documentos, em ordem cronológica e organizados por: • documento arquivístico, unidade de arquivamento ou classe; • usuário; • tipo de ação ou operação.
Um SIGAD pode fornecer relatórios referentes a ações que afetem documen- tos e dossiês/processos organizados por posto de trabalho (nos casos em que for tecnicamente adequado), endereço de rede ou outra interface de acesso. Alguns sistemas podem oferecer diversas interfaces de acesso aos docu- mentos. Por exemplo, interface web externa, interface da *intranet* e inter- face desktop. Pode ser interessante o registro da interface de acesso usada
Somente administradores autorizados têm que ser capazes de configurar o conjunto de eventos auditáveis e seus atributos.
Somente administradores autorizados, acompanhados do auditor, têm que ser capazes de configurar o conjunto de eventos auditáveis e seus atributos.

Fonte: E-ARQ Brasil (2011, p.93, 94, 95)

Diante destes requisitos, ressalta-se a necessidade de um profissional da arquivologia no desenvolvimento dos sistemas de informação, pois, todos estes metadados são para preservar a segurança da informação, garantindo aos documentos as características de

documento arquivístico. As trilhas de auditoria como metadados serão outras informações que também os arquivistas deverão tratar, garantindo-lhes também a integridade dos mesmos.

6.7 RECURSOS HUMANOS

Muitos mecanismos, como vimos, são utilizados para conferir ao documento digital características de documento arquivístico. Estes mecanismos podem surgir com muita eficiência no mercado dos sistemas de informação, porém, todos estes devem estar relacionados e conscientizados junto com os recursos humanos da instituição, pois, muitas vezes podem não surtir efeito diante da incapacidade ou até desconhecimento de alguns sobre a prática de segurança dentro da sua área de trabalho.

Os recursos humanos da instituição não devem ser esquecidos, ao contrário, devem ser, estabelecidas responsabilidades, conscientizados, capacitados, treinados e educados para que a segurança da informação tenha êxito.

A NBR ISO/27002 (2005) atribui como responsabilidade da direção da instituição a divulgação da responsabilidade de funcionários, fornecedores e terceiros na prática da segurança da informação, conforme o estabelecido na política de segurança.

Como expressado anteriormente, os recursos humanos devem ser:

> - Sensibilizados e conscientizados: As ações de sensibilização e conscientização visam atingir os empregados de uma forma ampla. Buscam mudar o comportamento, reforçar boas praticas e focalizar a atenção na segurança, facilitando a implantação da politica de segurança da informação e comunicação.
> - Treinados: As ações de treinamento visam capacitar empregados que realizam funções específicas de segurança de acordo com a área de atuação. Geralmente, estes treinamentos são externos, realizados por fornecedores das soluções. Além disso, há a capacitação por meio de participação em seminários e congressos, cujos grupos de trabalho possibilitam exercitar a pratica e estabelecer redes de relacionamentos técnicos.
> - Educados: As ações de educação visam formar especialistas, capazes de definir estratégias de segurança, servindo de apoio ao gestor de segurança da informação e comunicação da organização, ou até mesmo atuando como Gestor da Segurança Setorial, dependendo da estrutura de segurança definida. As certificações em segurança devem servir como forma de manter gestores de segurança atualizados.
>
> (CANONGIA, GONÇALVES JUNIOR, MANDARINO JUNIOR, 2010, p.89)

Por fim, depois de estabelecidas as responsabilidade, conscientizados/sensibilizados, educados e treinados, deve ser estabelecido processo disciplinar a ser aplicado a quem descumprir as políticas de segurança da instituição, podendo sofrer punições referentes à gravidade do descumprimento. “Convém que exista um processo disciplinar formal para os

funcionários que tenham cometido uma violação da segurança da informação.” (NBR ISO/27002, 2005, p.29).

7. CONSIDERAÇÕES FINAIS

A segurança da informação digital fica evidenciada pela manutenção das características de documentos de arquivo. Os sistemas responsáveis pelo gerenciamento dos documentos arquivísticos devem abarcar mecanismos que estabeleçam segurança, garantindo suas características.

Atualmente, existem muitas formas de controle de segurança da informação. Com o desenvolver deste trabalho, ficou evidenciado que, primeiramente um profissional da arquivologia deve estar presente no desenvolver destes mecanismos, e que a instituição deve ter ciência de que deve investir em segurança para que seu ativo seja fonte probatória.

Uma análise de riscos será indispensável, para que a organização saiba quais são suas vulnerabilidades, quais os seus ativos mais importantes e como poderá sofrer ataques, para que então sejam estabelecidos mecanismos de controle da segurança da informação.

Entender as características dos documentos arquivísticos é de suma importância para o responsável pelo sistema de gestão de documentos arquivísticos, pois, entendendo o que ele deve preservar, e sabendo quais os riscos que estão relacionados às características, podem ser desenvolvidas formas de controle eficaz para resguardar os documentos arquivísticos de segurança.

Existem mecanismos de segurança que tratam de proteger o sistema, contra intrusões, danos, roubos dentre outros riscos, estes tratam de proteger contra o acesso não autorizado aos sistemas, tramitação e guarda de documentos, dos quais podemos citar o *firewall*, a assinatura digital, a biometria, o sistema de detecção de intrusos, bem como outros mecanismos tratam do documento como entidade única para segurança, como criptografia, assinatura digital.

Para que seja garantida a segurança dos documentos arquivísticos digitais, como autenticidade, fidedignidade, integridade, confidencialidade, e organicidade, utilizamos mecanismos, e para cada uma das características, temos mecanismos que as assegurem.

Para manter a segurança da informação, é necessário a conscientização da empresa, pois, mesmo se gasto fortunas para ter todos estes mecanismos em seus sistemas, mas não houver uma conscientização por parte da direção, e dos responsáveis pela política de segurança da informação, poderá se tornar um gasto em vão.

A conscientização, treinamento, e educação da equipe responsável juntamente com mecanismos de segurança específicos será o que determinará se um sistema de gestão de documentos arquivísticos digitais será seguro. Pois muitas das ameaças procuram o elo mais fraco da corrente, ou seja, mesmo o sistema estando totalmente seguro diante de dados e

pessoas externas a empresa, muitas vezes pessoas de dentro são usadas para abrir caminhos para ataques.

As características de documentos arquivísticos podem ser asseguradas em sistemas de gestão de documentos arquivísticos digitais que sigam os requisitos necessários expostos, as políticas de segurança devem começar com análises dos ativos informacionais, gerir os riscos, implementar mecanismos de segurança e gestão de documentos e conscientizar e capacitar recursos humanos para que, tenhamos um ambiente realmente seguro para o documento arquivístico.

Por fim, de acordo com os dados levantados através de normas e literatura específicas das áreas da Arquivologia, Ciência da Informação e Ciência da Computação, é possível conferir segurança tal aos documentos arquivísticos, de modo que os mesmos sejam utilizados como fonte de prova.

REFERÊNCIAS

ALMEIDA, Elizangela Santos de. Prova Documental. Conteudo Juridico, Brasilia-DF: 11 jan. 2012. Disponivel em: <http://www.conteudojuridico.com.br/?artigos&ver=2.35498&seo=1>. Acesso em: 22 jan. 2015.

ARQUIVO NACIONAL BRASIL. **Dicionário Brasileiro de Terminologia Arquivística**. Rio de Janeiro: Arquivo Nacional, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **NBR ISSO]IEC 17799 Tecnologia da informação – Código de prática para gestão da segurança da informação**. Rio de Janeiro, 2001.

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**. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **NBR ISO]IEC 27005 Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação**. Rio de Janeiro, 2008.

BELLOTTO, Heloísa Liberalli. **Arquivos permanentes – Tratamento documental**. Rio de Janeiro: FGV, 2006.

BELLOTTO, H. L. Arquivística: objeto, princípios e rumos. São Paulo: Associação dos Arquivistas de São Paulo, 2002.

BRASIL. **Guia de referência para segurança das infraestruturas críticas da informação**. Brasilia: GSIPR/SE/DSIC, 2010.

CONSELHO NACIONAL DE ARQUIVOS – CONARQ. **E-ARQ Brasil: Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos** – Câmara Técnica de Documentos Eletrônicos. 1.1 versão. Rio de Janeiro: Arquivo Nacional, 2005.

CONSELHO NACIONAL DE ARQUIVOS – CONARQ. **Glossário** – Câmara Técnica de Documentos Eletrônicos - CTDE. 5.1 versão. Rio de Janeiro: Arquivo Nacional, 2010.

CONSELHO NACIONAL DE ARQUIVOS – CONARQ. **E-ARQ Brasil: Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos** – Câmara Técnica de Documentos Eletrônicos. 1.1 versão. Rio de Janeiro: Arquivo Nacional, 2011.

CONSELHO NACIONAL DE ARQUIVOS – CONARQ. **Diretrizes para a presunção de autenticidade de documentos arquívisticos digitais** – Câmara Técnica de Documentos Eletrônicos - CTDE. 1.1 versão. Rio de Janeiro: Arquivo Nacional, 2012.

DIGITAL LIBRARY FEDERATION. A working definition of digital library, 1998. Disponível em: http://www.dlib.org/dlib/september99/09lynch.html. Acesso em: 30 de Agosto 2014.

DURANTI, Luciana. **Diplomatics: new uses for na old science**. Society of American Archivists, Marylande, 1998.

FONSECA, Maria Odila. **Informação, arquivos e instituições arquivísticas.** Arquivo e Administração. Rio de Janeiro: 1998.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2008.

LE GOFF, Jaques**. História e memória.** Campinas: Editora UNICAMP, 1996. Traduzido por Irene Ferreira, Bernardo Leitão, Suzana Ferreira Borges. Disponível em: http://w.soa.fafich.ufmg.br/hist_discip_grad/documento_monumento_legoff.pdf. Acesso em: 23 de janeiro de 2015.

MARAKAS, George M.; O'BRIEN James A. **Administração de Sistemas de Informação – Uma Introdução**. São Paulo: Mc Graw-Hill, 2007.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de Metodologia Científica**. São Paulo: Atlas, 2008.

MICHEL, Maria Helena. **Metodologia e Pesquisa Científica em Ciências Sociais**. São Paulo: Atlas, 2009.

MINAYO, Maria Cecília de Souza et al. **Pesquisa Social:** Teoria, método e criatividade. 29 ed. Petrópolis, RJ: Vozes, 2010.

PAES, Marilena Leite. **ARQUIVO Teoria e Prática**. Rio de Janeiro: Fundação Getulio Vargas, 1997.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar. **Metodologia do trabalho científico** [recurso eletrônico]: **métodos e técnicas da pesquisa e do trabalho acadêmico**. Novo Hamburgo: Feevale, 2013.

ROCHA, Paulo Cesar Cardoso. Segurança da Informação – Uma Questão não Apenas Tecnológica. Brasília, 2008.

RONDINELLI, Rosely Curi. **Gerenciamento Arquivístico de Documentos Eletrônicos**. São Paulo: Editora FGV, 2007.

RONDINELLI, Rosely Curi. **O documento arquivístico ante a realidade digital**. Rio de Janeiro: Editora FGV, 2013.

STALLINGS, Willian. **Criptografia e Segurança de Redes**. São Paulo: Pearson Prentice Hall, 2008.

TECHOJE, A importância e a implementação da segurança da informação no âmbito das atividades de negócios. 2015. Disponível em:

TURBAN, Efraim; RAINER, JR Kelly; POTTER, Richard E. **Introdução a Sistemas de Informação – Uma Abordagem Gerencial**. Rio de Janeiro: Elsevier, 2007.