UNIVERSIDADE FEDERAL DO MARANHÃO
CENTRO DE CIÊNCIAS SOCIAIS
CURSO DE BIBLIOTECONOMIA

ISABELLE CRISTINE MARCOS RODRIGUES

SEGURANÇA DA INFORMAÇÃO NO CAMPO ARQUIVISTICO: o estudo da integridade em documentos de arquivo

São Luís
2021

ISABELLE CRISTINE MARCOS RODRIGUES

SEGURANÇA DA INFORMAÇÃO NO CAMPO ARQUIVISTICO: o estudo da integridade em documentos de arquivo

Monografia apresentada ao curso de Biblioteconomia da Universidade Federal do Maranhão, como requisito para a obtenção do título de Bacharel em Biblioteconomia.
Orientadora: Profa. Dra. Dirlene Santos Barros

São Luís
2021

Ficha gerada por meio do SIGAA/Biblioteca com dados fornecidos pelo(a) autor(a). Diretoria Integrada de Bibliotecas/UFMA

Rodrigues, Isabelle Cristine Marcos. SEGURANÇA DA INFORMAÇÃO NO CAMPO ARQUIVISTICO : o estudo da integridade em documentos de arquivo / Isabelle Cristine Marcos Rodrigues. - 2021.
51 p.

Orientador(a): Dirlene Santos Barros.
Monografia (Graduação) - Curso de Biblioteconomia, Universidade Federal do Maranhão, São Luis, 2021.

1. Arquivistica. 2. Autenticidade. 3. Documento digital. 4. Integridade. 5. Segurança da Informação. I. Barros, Dirlene Santos. II. Título

ISABELLE CRISTINE MARCOS RODRIGUES

SEGURANÇA DA INFORMAÇÃO NO CAMPO ARQUIVISTICO: o estudo do "pilar" integridade em documentos de arquivo

Monografia apresentada ao curso de Biblioteconomia da Universidade Federal do Maranhão, como requisito para a obtenção do título de Bacharel em Biblioteconomia.
Orientadora: Profª Drª Dirlene Silva Barros

Aprovado em:_____/_____/_____.

BANCA EXAMINADORA

_____
Profa. Dirlene Santos Barros (Orientadora)
Doutora em Ciência da Informação
Universidade Federal do Maranhão

_____
Prof. Dr. Roosewelt Lins Silva
Doutor em Informática na Educação
Universidade Federal do Maranhão

_____
Profa. Dra. Jaciara Januário da Silva
Doutora em Ciência da Informação
Universidade Federal do Maranhão

São Luís
2021

'"Se vi mais longe foi por estar de pé sobre ombros de gigantes."
Isaac Newton (1676, não paginado)

AGRADECIMENTOS

Em primeiro lugar, a Deus, por me acompanhar nesses caminhos tortuosos e que me ensinaram a ser o que eu sou hoje;

A minha orientadora, profa. Dirlene Santos Barros, a qual sou muito grata por ter aceitado esse desafio, pela paciência e pelas novas ideias, sou eternamente grata;

A o prof. Roosewelt Lins e a profa. Jaciara Januário pelas importantes contribuições na pré-banca que possibilitaram com que esta pesquisa ficasse mais clara e concisa;

A minha mãe, Rosalia de Fatima e meu pai, Wathonas Hylo, pelo apoio incondicional, e por ser meu farol numa tempestade;

A minha irmã, Gabrielli Rodrigues, por me apoiar em tudo e por ter me apoiado quando eu mais precisei para finalizar este trabalho;

Ao meu amor Marcos Paulo Moraes por ter me dado forças, carinho e me ajudado de modo indireto nos meus estudos;

Aos meus amigos de longa data, Lucas Ewerton, Thalia Rios e Uriel Ewerton por estarem comigo quando eu mais precisei;

À Universidade Federal do Maranhão e aos professores do curso de Biblioteconomia, que foram fundamentais para a minha formação como profissional, pesquisadora e cidadã;

Agradeço aos meus colegas do Curso de Biblioteconomia em especial, João Mateus, Danyelle Lobo e Jacira Soares, levarei vocês por toda a vida.

RESUMO

Segurança da Informação no âmbito arquivístico com foco na integridade. Objetiva estudar modelos de segurança da informação existentes a partir do pilar Integridade para garantia da autenticidade das informações arquivísticas. Para que fosse possível, houve um levantamento bibliográfico em bases de dados além da utilização de normas e diretrizes; trata-se ainda de uma pesquisa exploratória e descritiva. Apresentou-se os modelos HIDPS (Sistema de Detecção e Prevenção de Intrusão Baseada em Host) e *blockchain* como os mais adequados para assegurar a integridade dos sistemas e o uso de marca d'água para a autenticidade. Conclui-se que ainda são necessários mais estudos envolvendo a Arquivística e da área da Segurança da Informação para que se possa adequar esses modelos para uso, de modo que seja alcançada a autenticidade.
Palavras-chave: segurança da informação. Arquivística. documento digital. integridade. autenticidade.

ABSTRACT

This present work presents Information Security in the archival scope with a focus on the "pillar" of integrity. The research's objective was to find Information Security models that can be applied in archiving to ensure the integrity and therefore the authenticity of digital archival documents. This is descriptive research, where, to understand Information Security and Archival Science, a description of its characteristics and relationships was necessary. Also has exploratory research, where there was an expansion in digital archival documents and their characteristics, as well as in Information Security models. To make it possible, there was a bibliographic survey in databases in addition to the use of norms and guidelines. The HIDPS (host based IDPS) and blockchain models were presented as the most adequate to ensure the integrity of the systems, while the watermark focused on authenticity. It is concluded that archival studies are still needed in the area of Information Security so that these models can be adapted for use so that authenticity is achieved.

Keywords: Information Security. Archival Studies. Digital Records. Integrity. Authenticity.

SUMÁRIO

1 INTRODUÇÃO **11**

2 A SEGURANÇA DA INFORMAÇÃO ARQUIVÍSTICA NA CONFIABILIDADE DOS ARQUIVOS **15**

2.1 O documento arquivístico: da gênese à sua autenticidade **16**

2.2 Segurança da informação **25**

2.2.1 Política de Segurança da Informação **32**

2.3 Diretrizes para a segurança da informação arquivística: ABNT NBR ISO/IEC 27002 e ISO/IEC 27001 e o Conselho Nacional de Arquivos **35**

3 A SEGURANÇA DA INFORMAÇÃO ARQUIVÍSTICA: a garantia da autenticidade pelo pilar da integridade **43**

4 CONSIDERAÇÕES FINAIS **49**

REFERÊNCIAS **50**

1 INTRODUÇÃO

A segurança da informação é uma temática que faz parte dos debates acadêmicos, do exercício profissional de várias áreas do conhecimento e do cotidiano das pessoas. Esse cenário, real e preocupante, é resultante da presença massificada das Tecnologias de Informação e Comunicação (TIC) no cotidiano das pessoas através da gama de informação produzida, disseminada e usada e/ou consumida para a tomada de decisões em vários âmbitos, por muitas vezes, sem saber a integridade dessas informações.

Ao se tratar dos documentos arquivísticos digitais, esse cenário se torna mais problemático por se relacionar às informações produzidas e/ou recebidas do exercício do fazer administrativo, jurídico e legal, cuja produção é considerável e, por vezes, gera a chamada massa documental acumulada, que se perde em meio ao caos, gerando prejuízos para as organizações no tocante a tomada de decisões.

Dessa forma, pensar e implementar sistemas de informação arquivística que armazene as informações garantindo a sua integridade é uma questão da gestão de uma organização. Isto porque com o uso da TIC, o documento arquivístico digital mantém as características de um documento físico, porém, a informação ali contida, pode sofrer alterações caso não haja uma segurança adequada.

Essa segurança consiste no processo de garantir a integridade, disponibilidade e confidencialidade das informações, protegendo-as de ameaças. A integridade, disponibilidade e confidencialidade da informação são conhecidos como os três pilares que garantem que a informação contida no documento seja restrita, autêntica e disponível a quem precisa.

Nesse sentido, esta pesquisa se originou em função à preocupação com as informações disponíveis no meio digital, surgindo diversos questionamentos referente a veracidade dessas informações, como a autenticidade e a autenticação dessas informações de modo que não sofram nenhuma modificação.

Em adição a isso, teve o estímulo da disciplina de Arquivística, que durante o período fez com que surgisse dúvidas quanto ao armazenamento e disponibilidade de documentos em meio web, considerando os riscos que este meio apresenta; ao interesse pessoal, pelo conhecimento que será adquirido durante o processo das experiências profissionais; ao conhecimento que será atribuído a área de Arquivística, Biblioteconomia e Documentação, devido a escassa produção científica nessa área, o que dificulta a visibilidade e não destaca a sua importância.

Outro aspecto decisivo para a escolha desta temática foram as pesquisas desenvolvidas em bases de dados como Scielo, Biblioteca Digital de Teses e Dissertações do Instituto

Brasileiro de Ciência e Tecnologia, Bibliotecas digitais da Universidade Federal do Maranhão, Universidade de São Paulo, Universidade de Brasília que possuem poucas pesquisas sobre segurança da informação em arquivos.

A partir de então, a seguinte indagação norteou esta pesquisa: "Os modelos de segurança da informação existentes garantem a autenticidade das informações arquivísticas a partir do pilar da Integridade?"

Para tanto, tem-se como objetivo geral estudar modelos de segurança da informação existentes a partir do pilar Integridade para garantia da autenticidade das informações arquivísticas e, como objetivos específicos: estudar os pilares da segurança da informação; caracterizar a gestão dos documentos arquivísticos digitais e verificar o pilar integridade nos modelos de segurança da informação para a informação arquivística.

A escolha do pilar "Integridade" é pautada na constante manipulação da informação contida em qualquer que seja o sistema de informação em âmbito mundial e nacional. A integridade está ligada à autenticidade do documento, ou seja, a informação contida no documento não tenha sofrido nenhum tipo de alteração.

É necessário enfatizar que na maioria das organizações, a ausência de recursos, seja financeiro, humano, tecnológico dentre outros acaba por não permitir que se dê o espaço adequado para a segurança da informação. Em consequência a isso, o problema se agrava por falta de conhecimento sobre a temática.

O desenvolvimento desta pesquisa se constituiu em um desafio que se apresentou ora como claro, ora como duvidoso e intrigante. Houve a sensação de não se saber para onde caminhar. À proporção que se avançava nas leituras sobre a temática foi se tateando o caminho a seguir.

O objeto de pesquisa se insinuava, se mostrava e se definia; os tipos de pesquisas se desenharam; os dados se mostraram para as técnicas de coleta para, então, serem analisados. Esse processo ocorreu de forma natural, embora, cheio de desafios, tensões e cansaço.

O levantamento bibliográfico desenvolvido foi fundamental para sanar a falta de informação referente a segurança da informação, suas implicações para a manutenção da integridade dos documentos de arquivos. Estes frutos de decisões, fazeres que norteiam uma organização, cuja manutenção da autenticidade da informação arquivística é primordial para o seu prosseguir.

Assim, esta pesquisa de caráter qualitativo, caracterizada pela pesquisa bibliográfica feita em livros, periódicos, teses, dissertação e trabalhos de conclusão de cursos recuperadas em diversas bases de dados de universidades públicas brasileiras já apresentadas.

A pesquisa documental também foi fundamental para o levantamento das Normas Nacionais e Internacionais que tratam sobre a segurança da informação, bem como das resoluções do Conselho Nacional de Arquivo (Conarq) referente a autenticidade de documentos arquivísticos dentre outros.

Soma-se a isso, a pesquisa descritiva que, de acordo com Gil (2011, p. 28) "[...] têm como objetivo primordial a descrição das características de determinada população ou fenômeno ou o estabelecimento de relação com variáveis.", ou seja, a compreensão da segurança da informação, do documento arquivístico dentre outros aspectos foram compreendidos a partir da descrição de suas características, elementos legais e as relações entre eles.

Além da pesquisa descritiva, teve a pesquisa exploratória que possibilitou aprofundar a segurança da informação no contexto dos documentos arquivísticos digitais, bem como os requisitos necessários para esta segurança, uma vez que, esse tipo de pesquisa "[...] tem como principal finalidade desenvolver, esclarecer e modificar conceitos e ideias, tendo em vista a formulação de problemas mais precisos ou hipóteses pesquisáveis para estudos posteriores." (GIL, 2011, p. 27).

Prodanov e Freitas (2013, p. 52) afirmam que a utilização dessa pesquisa facilita a delimitação do tema e elencam três itens que essa pesquisa envolve, são eles: "[...] levantamento bibliográfico; entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado e análise de exemplos que estimulem a compreensão.". No caso da pesquisa em tela, o levantamento bibliográfico e análise de modelos de segurança da informação foram essenciais para se apropriar da temática.

A coleta de dados ocorreu por meio da pesquisa bibliográfica, principalmente, de autores internacionais que apresentam dois modelos de segurança da informação, o *HIDPS* e *blockchain*, onde se verificou os requisitos contidos que possibilitem essa segurança e que possa ser aplicado no contexto arquivístico.

A partir de então, desenvolveu-se a análise desses dados baseado no referencial teórico trabalhado na pesquisa, nos modelos apresentados e nas considerações que a pesquisadora fazia a partir do que apreendeu.

A pesquisa em tela está estruturada em cinco seções: a primeira é a introdução, onde se apresenta o porquê da pesquisa, sua contextualização e objetivos. Em seguida, a seção dois é constituída pela fundamentação teórica sobre a segurança da informação, a informação arquivística digital, normas e legislações sobre a integridade e a política de segurança da informação.

A terceira seção enfoca a metodologia utilizada na construção da pesquisa a partir do levantamento bibliográfico e documental em âmbito nacional e mundial, bem como a técnica utilizada para a coleta de dados e tratamento desses dados.

Por conseguinte, tem-se a seção quatro com a apresentação dos dados coletados a parti da pesquisa bibliográfica e documental em relação a dois sistemas de segurança da informação, onde estuda-se o seu uso para a garantia do pilar Integridade para os documentos arquivísticos digitais seguida da quinta seção com as considerações finais.

Assim, espera-se que esta pesquisa sirva de referencial teórico sobre segurança da informação em documentos arquivísticos na garantia da Integridade, a fim de contribuir para gerar novas pesquisa e como material bibliográfico para a Arquivologia, Biblioteconomia e Ciência da Informação, uma vez que as pesquisas voltadas para este tema são ainda poucas.

2 A SEGURANÇA DA INFORMAÇÃO ARQUIVÍSTICA NA CONFIABILIDADE DOS ARQUIVOS

A Arquivística é a área que compreende o estudo da informação arquivística, bem como as técnicas, processos e sistemas de gestão. É deveras importante ressaltar que o documento arquivístico já detinha valor antes da contemporaneidade como Schellenberg (2006, p.25) explicita "[...] os arquivos como instituição, provavelmente, tiveram origem na antiga civilização grega [...]", disponibilizados em espaços concebidos como santuários.

Embora, sua gênese esteja ligada antes da Antiguidade Clássica, urge enfatizar que o desenvolvimento da Arquivística, como prática e teoria dos arquivos, se inicia

> Como apontam Ketelaar, Horsman & Thomassen (2003, p. 249, tradução nossa) em artigo publicado referente ao centenário do manual holandês, 'O manual de arranjo de descrição de arquivos (1898)' é geralmente referenciado como o ponto inicial da teoria Arquivística e de sua metodologia. (BARROS, 2013, p.145).

O Manual do Arquivistas Holandeses foi o ponto alto dentro da prática arquivística, sendo considerado uma das bases pela comunidade arquivística internacional. Barros (2013) diz que essa publicação sintetizou e instaurou um discurso da arquivística ligada ao acesso e desenvolvimento de políticas arquivísticas. O arquivo passou por muitas transformações e cada uma delas teve uma contribuição importante para o que conhecemos hoje. Isto ocorreu devido ao crescimento das instituições de caráter administrativo e o interesse de outras instituições na preservação da cultura e, como consequência desse cenário, precisaram aprimorar suas técnicas para responder as demandas de cada arquivo.

Com isso, o desenvolvimento da gestão de documentos permitiu uma organização mais precisa, visto que o aumento da massa documental era uma realidade. Essa gestão é definida pelo Dicionário Brasileiro de Terminologia Arquivística (2005, p. 100) como o "Conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento (1, 2) de documentos em fase corrente e intermediária, visando sua eliminação ou recolhimento." Trata-se, portanto, de práticas e técnicas empregadas para garantir a autenticidade, confiabilidade e integridade da informação arquivística de forma a ser recuperada e utilizada pelos seus usuários.

Nessa perspectiva, é salutar destacar que a gestão de documentos implementada racionaliza processos, otimiza tempo e espaço e potencializa as tomadas de decisões ao possibilitar a Segurança da Informação. Essa acontece em função da autenticidade, confiabilidade e integridade da informação arquivística serem partes integrantes da gestão de documentos, de forma a garantir e proteger os documentos contra ações maliciosas que podem

colocar em risco a integridade de qualquer instituição. Contudo, para que isto transcorra de forma eficaz, é preciso que a organização

> [...] antes de elaborar medidas que garantam a segurança da informação é necessário que a instituição elabore uma política ou um programa de gestão de documentos e, dentro desse, um dos objetivos deve ser dar acesso ou tornar acessíveis os documentos aos usuários. (SFREDO; FLORES, 2012, p.168).

Conforme enfatiza a citação, o desenvolvimento de uma política de gestão de documentos deve levar em conta as necessidades institucionais e ser distribuída para todos da instituição, visto que a sua implementação pressupõe para Vianez *et. al* (2008, p. 35) a necessidade "[...] que se tenha um documento que declare o comprometimento da direção e estabeleça o enfoque da organização para gerenciar a política." Dessa forma, priorizando a necessidade da organização em garantir a segurança da informação em seus espaços, evitando quebras de confidencialidade, autenticidade e integridade do documento arquivístico.

2.1 O documento arquivístico: da gênese à sua autenticidade

Ao se abordar concepções no campo científico, observa-se que há contrassensos e consensos como resultado do processo de investigação, reflexão, debate e amadurecimento entre os pares que conduzem posicionamentos teóricos e metodológicos.

A Arquivologia não foge a esta regra, uma vez que, ela é a área que produz conhecimento a partir do seu *córpus*, documento arquivístico demarcando sua atuação, sua relação interdisciplinar e sua conjectura teórica.

No tocante a compreensão do documento arquivístico, ele é resultante de uma atividade laboral, de ordem administrativa com característica probatória. Todavia, há de se que considerar essa característica como meio de prova transcende os documentos administrativos, contemplando os documentos testemunhais e jurídicos, em seu formato impresso e eletrônico.

Para a autora Paes (2004, p. 26) o documento é demarcado por ser um meio de prova seja pela pessoa física ou jurídica, pública ou privada que deve ser conservado e preservado de modo que a informação contida não sofra alteração. "[...]- l. Aquele que, produzido e/ou recebido por uma instituição pública ou privada, no exercício de suas atividades, constitui elemento de prova ou de informação 2. Aquele produzido e/ou recebido por pessoa física no decurso de sua existência.".

Essa concepção é asseverada no Código de Processo Civil Brasileiro em seu artigo 332 "[...] Todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, provar a verdade dos fatos, em que se funda a ação ou a defesa." (BRASIL, 2001, não paginado).

Percebe-se assim, a manutenção do caráter probatório ao conceber como o que há previsto e em conformidade com a legislação. Essa afirmação permanece, dentro de um contexto mais atual e reflete a sua gênese: “A origem do arquivo, portanto, obedecendo a imperativos de ordem prática, corresponde à necessidade de constituir e conservar registros de ações e de fatos, a título de prova e informação.” (CAMARGO; MACHADO, 2000, p. 13). Assim, o documento de arquivo traz em sua gênese a veracidade de fatos e decisões de ordem prática que refletem os dizeres e fazeres em tempo e espaço determinados.

Nesse sentido, o documento de arquivo é originário dos processos de dentro das organizações, são os registros das informações sobre a organização, de suas atribuições, ações dentre outros, sejam órgãos públicos, sejam privados, cujo produtor deste documento terá um vínculo com o estado probatório.

É importante destacar, nesse contexto, que os documentos de arquivo se originam através de uma acumulação natural “[...] onde seu conteúdo e significado só podem ser compreendidos na medida em que se possa ligar o documento ao seu contexto mais amplo de produção, às suas origens funcionais.” (RODRIGUES, 2010, p. 176). Essa acumulação põe em voga a necessidade de uma compreensão acerca da contextualização deste documento, de onde ele se encontra e com o que se relaciona, de modo que a relação entre o produtor e o documento de arquivo seja clara.

Essa relação para Duranti (1994, p. 52) é chamada de Inter-relacionamento, pois sua relação ocorre de forma interna e externa entre si, embora eles sejam interdependentes devido ao seu conteúdo e características probatórias, “[...] os documentos estão ligados entre si por um elo que é criado no momento em que são produzidos ou recebidos, que é determinado pela razão de sua produção e que é necessário à sua própria existência, à sua capacidade de cumprir seu objetivo, ao seu significado, confiabilidade e autenticidade.”

De acordo com Rondinelli (2011, p.223)[1] documento arquivístico “[...] se constitui em registro de ações humanas independentemente da forma em que se apresenta e da base em que se encontra afixado.”. A autora demarca essa concepção a partir do estudo-de diferentes autores, desde os clássicos aos contemporâneos.

[1] Rosely Cury Rondinelli em sua tese de doutorado “O Conceito de documento arquivístico frente à realidade digital: uma revisitação necessária” de 2011 defendida no Programa de Pós-Graduação em Ciência da Informação.

Dentre os clássicos, como Jenkinson e Schellenberg que discutiram abertamente a definição de documento de arquivos, dentre outros para apresentarem a compreensão deles sobre arquivo, como bem ilustra o Quadro 1:

QUADRO 1- Sistematização do conceito de documento arquivístico a partir dos clássicos

AUTORES	ANO	TERMO ADOTADO	IDEIAS CENTRAIS
Associação dos Arquivistas Holandeses	1898	Arquivo	• Natureza dos arquivos: pessoas jurídicas • Organicidade • Forma documental • Anexos
Jenkinson	1922	Arquivo	• Natureza dos arquivos: pessoas jurídicas • Organicidade (implícita) • Imparcialidade • Autenticidade • Forma documental • Anexos • Custódia ininterrupta • Uso pelo órgão produtor • Preservação
Schellenberg	1956	Documento arquivístico (record) Arquivo (archives)	• Natureza dos arquivos: pessoas jurídicas e intervenção do arquivista • Organicidade (implícita) • Evidência • Seleção • Uso secundário
Casanova	1928	Arquivo	• Natureza dos arquivos: pessoas físicas e jurídicas • Organicidade (implícita) • Ordenação • Uso pelo órgão produtor • Uso secundário
Cencetti	1937	Arquivo	• Natureza dos arquivos: pessoas físicas e jurídicas • Organicidade (implícita) • Uso pelo órgão produtor
Brenneke	1953	Arquivo	• Natureza dos arquivos: pessoas físicas e jurídicas • Organicidade (implícita) • Evidência
CONVERGÊNCIA			
• Natureza dos arquivos: pessoas jurídicas* • Organicidade (*Em relação a Shellenberg, há divergência entre os autores quanto à sua concepção sobre anautreza dos arquivos).			

Fonte: Rondinelli (2011, p. 168)

É compreendido que o documento arquivístico sofreu mudanças dentro de suas concepções de modo que fosse se adaptando a realidade do espaço. Nota-se que a característica "Natureza dos arquivos: pessoas jurídicas" e "organicidade" se mantiveram mesmo que implícita ou acompanhada de outros fatores. Isso se dá, devido a origem da massa documental, que registram ou atestam fatos. Estes ligados a organizações além da organicidade, onde reflete a estrutura e atividade da organização nos conjuntos documentais.

Dito isso, apresenta-se definições mais contemporâneas por Rondinelli (2011) que, também faz, uma análise e destaca elementos do documento arquivístico, conforme a Quadro 2.

QUADRO 2 - Sistematização do conceito de documento arquivístico a partir de autores contemporâneos

AUTORES	ANO	TERMO ADOTADO	IDEIAS CENTRAIS
Associação dos Arquivistas Franceses	1973	Arquivo	• Natureza dos arquivos: pessoas físicas e jurídicas • Organicidade
Carucci	1983	Arquivo	• Natureza dos arquivos: pessoas físicas e jurídicas • Organicidade
Cortes Alonso	1989	Arquivo	• Natureza dos arquivos: pessoas físicas e jurídicas • Organicidade (implícita) • Naturalidade • Unicidade • Integridade • Autenticidade • Imparcialidade • Uso pelo órgão produtor • Uso secundário
Heredia Herrera	1991	Arquivo Documentos arquivísticos Documento de arquivo	• Natureza dos arquivos: pessoas físicas e jurídicas • Naturalidade • Organicidade • Ordenação • Uso pelo órgão produtor • Uso secundário
Martín-Pozzuelo Campillos	1996	Documento de arquivo	• Natureza dos arquivos: pessoas físicas e jurídicas • Organicidade (implícita) • Contexto de produção • Unicidade • Autenticidade • Multiplicidade de conteúdo • Interdependência
Rodriguez Bravo	2002	Documento de arquivo	• Natureza dos arquivos: pessoas jurídicas • Naturalidade • Organicidade

Duranti	1994	Documento arquivístico	• Natureza dos arquivos: pessoas físicas e jurídicas • Imparcialidade • Autenticidade • Naturalidade • Organicidade • Unicidade
Duranti	2002	Documento arquivístico	• Natureza dos arquivos: pessoas físicas e jurídicas • Organicidade • Instrumento • Subproduto
Eastwood	2009	Documento arquivístico	• Natureza dos arquivos: pessoas físicas e jurídicas • Imparcialidade • Autenticidade • Naturalidade • Organicidade • Unicidade
Mckemmish e Upward	1991 1994 2001 2005 2010	Documento arquivístico contínuo	• Natureza dos arquivos: pessoas físicas e jurídicas • Documento contínuo • Evidência • Transação • Contexto
Yeo	2007 2008	Documento arquivístico	• Natureza dos arquivos: pessoas físicas e jurídicas • Organicidade (implícita) • Representação • Persistência • Atividades • Ocorrência • Doc. protótipo • Doc. limítrofe
CONVERGÊNCIAS			
• Natureza dos arquivos: pessoas jurídicas • Organicidade			

Fonte: Rondinelli (2011, p. 194-195)

Compreende-se, assim, a demarcação por duas características em todas as concepções, porém novos fatores emergem como a autenticidade, imparcialidade, naturalidade e unicidade. Características estas, indispensáveis para garantir a veracidade do documento, sua singularidade, sua ordenação e sua neutralidade em qualquer ambiente em que o documento arquivístico esteja armazenado.

É importante ressalva que armazenar e preservar documentos arquivísticos digitais são uma questão de preocupação para os estudiosos da área, devido a fatores que combinados, podem ser grandes riscos para as informações ali contidas.

O documento arquivístico digital é composto por forma e conteúdo e uma cadeia de custódia ininterrupta, considerada imprescindível, que garante sua autenticidade. Este modelo de documento é o mais comumente usados devido a sua facilidade de armazenamento e de custo. Santos e Flores (2016, p. 166) refletem que:

> Os documentos digitais possuem diversas facilidades no que tange ao modo de criar, editar e difundir conteúdo. Em meio a sua demanda, observa-se que estes registros também estão sendo produzidos de maneira orgânica e consequentemente, vêm constituindo parte dos acervos. Assim, há necessidade de refletir sobre as mudanças de ordem teórica e prática, ocasionadas pelas tecnologias da informação na Arquivística.

Há, nessa afirmação, a necessidade em rever as bases da Arquivística em função da proliferação do uso de TIC nos processos e fluxos informacionais. Isto faz com que organizações demandem por *softwares* e os demais artefatos para produção e gerenciamento de seus processos. No entanto, se destaca uma preocupação com a manutenção, armazenamento e preservação desses documentos.

Um aspecto importante, nesse cenário, a ressaltar são sete funções arquivísticas que, Rousseau e Couture (1998), abordaram dentro do contexto do documento digital arquivístico a saber: produção, avaliação, aquisição, conservação, classificação, descrição e difusão.

A produção "[...] resultado de atividades derivadas de funções, as quais são exercidas de forma natural no âmbito da instituição a fim de atingir seus objetivos." (SANTOS; FLORES, 2011, p. 167). É nele que o documento nasce, seja recebido e/ou produzido como consecução dos objetivos da organização que o gerou. Acentua-se a importância de o arquivista ter conhecimento sobre a instituição e sua missão e objetivo, tecnologias disponíveis que poderão ser utilizadas durante o processo de produção de documentos, além do tipo de documento a ser utilizado pela organização, pois isto contribui para o fluxo de informação. Soma-se a isso, a atenção ao formato do documento, principalmente quando se trata de migração de documentos, preservação e acesso por um período limitado para que não haja perda de informação.

A segunda função consiste na avaliação voltada para a análise da massa documental identificada dentro do arquivo como corrente e intermediário. Essa função ocorre por meio da tabela de temporalidade de documentos, um dos instrumentos de gestão de documentos, que auxilia o processo de transferência e recolhimento ou eliminação da documentação contribuindo para a produtividade rotineira administrativa e preservando os documentos, não obstante de apurar o valor probatório, social, legal e históricos que estes carregam consigo.

A avaliação tem como objetivo verificar quais documentos podem ser eliminados e/ou recolhidos e, para isso, é preciso avaliar seus valores para saber se de fato tem importância para a instituição (por tanto, deve-se conhecer a fundo a organização). Por isso, é necessário "[...] que estes estejam inseridos em um sistema informatizado que contemple requisitos como uma tabela de temporalidade para definir os prazos de guarda e a destinação final." (SANTOS; FLORES, 2011, p.168). Esta Tabela de Temporalidade é elaborada por uma Comissão multidisciplinar denominada Comissão Permanente de Avaliação Documental (CPAD) que tem arquivista como um dos profissionais com participação obrigatória.

A aquisição é a forma em que serão adquiridos os documentos de arquivo podendo ser por compra ou doação em qualquer uma das idades do arquivo, sendo a guarda destes documentos de responsabilidade do custodiador do acervo documental. Para os documentos arquivísticos digitais, é preciso entender se o acervo que está sendo adquirido está dentro da confiabilidade, isto é, se o acervo atesta a credibilidade enquanto sustenta uma afirmação do fato que carrega, assim como "Da mesma forma, o novo custodiador deverá demonstrar que os documentos adquiridos serão armazenados de forma confiável, mantendo a integridade e a autenticidade." (SANTOS; FLORES, 2011, p. 169)

Para que seja possível garantir a confiabilidade destes documentos, recomenda-se a utilização de repositórios digitais e a inserção de novos padrões de metadados, considerando as normas, diretrizes, padrões e recomendações - por exemplo, Conarq, onde o custodiador atual deve se atualizar de modo que "O processo como um todo deve manter um alto nível de confiabilidade, tendo em vista as vulnerabilidades dos documentos digitais no que tange a sua adulteração[...]." (SANTOS, FLORES, 2011, p. 169)

Por conseguinte, tem-se a classificação onde se destaca por ser puramente intelectual e lógica, pois é nesta que haverá a organização dos documentos de acordo com o Código de Classificação com os fundos arquivísticos, não obstante do princípio da organicidade. Tal função é asseverada por Santos e Flores (2011, p. 169) quando "Observa-se que a classificação é composta pela criação e utilização do plano de classificação de documentos, então elaborado a partir da análise dos documentos produzidos frente ao arquivo corrente, sendo esta uma das formas de organização hierárquica." Esta etapa colabora diretamente com a questão da eliminação de documentos não necessários à entidade produtora, e melhora a recuperação da informação destes documentos.

Dentro dos documentos arquivísticos digitais, devido ao seu caráter de produção excessivo, a organicidade se perde, uma vez que, a massa documental está acumulada e o meio digital é abstruso, o que pode atrapalhar na recuperação deste documento: "A ausência de

procedimentos de classificação afetará diretamente nos procedimentos simultâneos e posteriores como avaliação, descrição, preservação e acesso.". (SANTOS; FLORES, 2011, p. 170). Torna-se uma problemática por atrapalhar os outros processos fazendo com que o documento perca sua autenticidade, integridade e confiabilidade, principalmente, a disponibilidade, que é o acesso facilitado à informação contida nesse documento.

Após o processo de criação desse documento é necessário que se faça a classificação com vistas a evitar a perda dos documentos no meio digital. Outra solução é a criação na estrutura de metadados do sistema, um campo para a inserção do Código de Classificação - por exemplo, a disponibilizada pelo Conarq, que irá assegurar a recuperação do documento e auxiliar nas outras etapas.

A descrição tem como objetivo a recuperação do documento, ou seja, a forma que este documento estará caracterizado irá implicar neste objetivo. Geralmente, há a elaboração de instrumentos como guias e catálogos, que auxilia nesse processo além da utilização da indexação e de metadados. Santos e Flores (2011, p. 170) afirmam que "A padronização da descrição proporciona maior agilidade, otimiza o trabalho e diminuir os custos. Além disso, as normas agilizam as atividades do pesquisador no uso de instrumentos de pesquisa."

Quando se trata de documento arquivístico digital, deve-se atentar para o software a ser utilizado: se ele está de acordo com a ISAD(G), Norma Geral Internacional de Descrição Arquivística, que auxilia na criação de campos de metadados ou na atualização destes.

De acordo com Santos e Flores (2011, p. 170) "[...] a descrição está relacionada a outras diversas funções arquivística inserindo informações referentes às possíveis transformações do documento, o que irá corroborar na sua presunção de autenticidade." Os metadados são a melhor ferramenta para a descrição, pois permitem - através dos padrões de metadados - a criação de campos, estes vão expressar as características desses documentos, facilitando a recuperação e otimizando o acesso.

Outra função é a conservação, considerada uma grande preocupação quando se trata de documentos arquivísticos. Proteger os documentos de ações adversas de forma que haja o mínimo de interferência no documento, fazer o reparo e manter este documento para que outros possam acessar é uma tarefa laboriosa. Santos e Flores (2011, p. 171) afirma que a conservação "[...] visa proteger os documentos de fatores internos, externos e sinistros. A conservação compreende a manutenção de condições ideais, pequenos reparos e até mesmo, grandes intervenções nos documentos."

Para que se tenha uma preservação documental é necessário ter uma equipe que fará fazer uma política institucional voltada a atividades, são baseadas "[...] no valor agregado da

informação orgânica, na demanda de uso e nas vulnerabilidades presentes no acervo [...]" (SANTOS; FLORES, 2011, p. 171). E, dentro disso, é necessário estudar diferentes suportes para conhecer a forma de preservação de cada um e quais são as ameaças mais comuns para preparar melhor o documento que será um guia dentro da organização.

Como os documentos digitais estão sendo cada vez mais manuseados pelas organizações devido a sua facilidade de acesso, logo, a preocupação com a manutenção desse documento se torna pertinente. Desse modo, é necessário se utilizar de estratégias de preservação de documentos e entre outros para manter o documento digital dentro dos parâmetros da preservação. Segundo Santos e Flores (2011, p.172) o repositório digital consiste em uma forma de preservação devido "[...] conformidade com normas e recomendações amplamente aceitas e difundidas pela comunidade de preservação, como, por exemplo, o modelo *Open Archival Information System* (OAIS).

Não obstante, esse documento digital deve estar em um ambiente autêntico, ter seus processos confiáveis de modo que se crie estrutura de metadados para garantir a autenticidade. A preservação é a parte mais sensível quando se trata de documentos digitais, pois é neste em que a informação contida dentro do documento não deve sofrer alteração. O documento digital, enquanto objeto físico, é expresso por cadeia de *bits* e estas garantem a autenticidade. E este é o verdadeiro desafio, manter essas cadeias de *bits* intocáveis. Todavia, há métodos que podem ser utilizados, porém a obsolescência tecnológica é uma grande ameaça, é certo que a partir de uma revolução tecnológica na área da preservação poderá melhorar ou atualizar os métodos de preservação.

Por último, a difusão é o momento em que a informação contida no documento será levada ao público, de acordo com as leis e os prazos estabelecidos nestes. Com o crescimento tecnológico, atualmente, é possível optar pela digitalização que é uma estratégia facilitadora do acesso e disseminação da informação. Santos e Flores (2011, p. 173) afirmam em relação ao documento digital:

> Para os documentos digitais produzidos diretamente em meio digital (born digital) há uma abordagem diferenciada, em virtude de sua natureza e forma de representação. Não é preciso digitalizá-los, pois já nasceram em meio digital, no entanto, o acervo deve difundi-los, e proporcionar condições de acesso a estes registros. Isto implica em se usar sistemas de acesso intuitivos e disponibilizar os documentos em formatos de arquivo amplamente difundidos pela comunidade de usuários.

Em outras palavras, a utilização de um sistema que permita que o usuário acesse e, em alguns casos, faça o download para que a informação ali contida seja disseminada. A preservação digital com seus procedimentos, pode causar alteração na forma do documento, o

que pode dificultar o acesso para alguns usuários. Dito isto, temos os metadados que funcionam como auxiliadores no processo de recuperação da informação. Destaca-se pela variedade de tipos, onde se destaca os metadados descritivos, pois se cria campos que variam desde autor até palavras-chaves, aumentando assim a exatidão da busca e neles estão contidas informações sobre o documento como data da criação e data da última modificação (caso o documento sofra alguma modificação).

Quadro 3 – Padrão de metadados Dublin Core versão simples

Identifier	Definition
Title	A name given to the resource.
Creator	An entity primarily responsible for making the content of the resource.
Subject	The topic of the content of the resource.
Description	An account of the content of the resource.
Publisher	An entity responsible for making the resource available.
Contributor	An entity responsible for making contributions to the content of the resource.
Date	A date associated with an event in the life cycle of the resource.
Type	The nature or genre of the content of the resource.
Format	The physical or digital manifestation of the resource.
Identifier	An unambiguous reference to the resource within a given context.
Source	A reference to a resource from which the present resource is derived.
Language	A language of the intellectual content of the resource.
Relation	A reference to a related resource.
Coverage	The extent or scope of the content of the resource.
Rights	Information about rights held in and over the resource.

Fonte: Sugimoto, Baker e Weibel (2002, não paginado)

Os documentos digitais precisaram se apoiar nos antigos métodos da arquivística e os especialistas das áreas tiveram que se adequar às novas realidades. Por serem extremamente fáceis de acessar e manter, os documentos digitais estarão entre nós por muito tempo e até lá é esperado que as tecnologias sofram renovações para que as informações neles contidas não se percam nessa aglomeração de informações geradas a todos os instantes.

2.2 Segurança da informação

O uso intensivo das TIC por várias organizações proporciona a concentração de um denso volume de informações em um único ambiente. Esse contexto, embora se apresente, em um primeiro olhar, como uma vantagem em função do aparente controle sobre as informações produzidas e recebidas, tem se tornado uma problemática para a segurança da informação.

Desse modo, é importante explicitar que a informação é fator imprescindível para a determinação de estratégia, uma vez que as organizações fazem uso da informação para atribuir sentido às mudanças do contexto externo, principalmente, para tomar decisões (CHOO, 2004). Para Setzer (1999, não paginado, grifo do autor) "*Informação* é uma abstração informal (isto é, não pode ser formalizada através de uma teoria lógica ou matemática), que representa algo significativo para alguém através de textos, imagens, sons ou animação." Em outras palavras, a informação sai do campo de dados para se validar através de comunicação informal, de modo que haja uma inclusão a aqueles que não abstraem informação de modo formal.

Por conseguinte, a informação solidificou como valiosa e poderosa, tornando-se no principal ativo de uma organização e servindo a qualquer interesse - seja ele de cunho pessoal ou coletivo. Em função disso afirma-se que as organizações (públicas ou privadas) interessam-se em manter essa informação restrita e em desenvolver sistemas automatizados devido a modernização de processos, que podem afetar seus ambientes caso não sejam atualizados.

Posto isso, a história da segurança da informação se desperta com a segurança de computadores, que se identifica por proteção, *hardware* e *software* de ameaças. Whitman e Mattford (2012) fazem uma linha do tempo bem detalhada dividindo-o em 10 anos.

O primeiro problema de segurança documentado aconteceu antes dos anos 1960, quando o sistema utilizado, ao mesmo tempo, por dois administradores sofreu um *glitch,* isto é, misturou os arquivos causando uma falha na segurança pois e imprimindo em um dos arquivos a senha de acesso ao sistema. [2]

Durante o ano de 1960, enquanto acontecia a guerra fria, a Agência de Projetos de Pesquisa Avançada do Departamento de Defesa começou a analisar a possibilidade de um sistema de comunicação em rede para ajudar a troca de informação entre os militares. Em 1968 nasceu a ARPANET, considerada por muitos o antecessor da internet.

Já nos anos 1970 e 1980, devido ao rápido crescimento da utilização da ARPANET, Robert M. Metcalfe, em dezembro de 1973 descobriu falhas fundamentais na segurança da ARPANET. De acordo com Whitman e Mattford (2012, p.5, tradução nossa) alguns problemas foram encontrados" [...] vulnerabilidade da estrutura e formatos da senha; falta de procedimentos de proteção para conexões discadas; e não existência de identificação e autorização do usuário para o sistema.".

[2] WHITMAN, Michael E.; MATTORD, Herbert J.. **Principles of Information Security**. 4. ed. Boston: Course Technology, 2012. 658 p.

Os autores constataram que a falha de segurança era tão grande ao ponto de *hackers* invadirem o sistema por conta de números de telefone que naquela época eram deixados em cabines de ligação. Em 1978 um estudo chamado "Analise de proteção: Relatório Final" foi publicado com foco em um projeto proposto pela ARPA para descobrir as vulnerabilidades no sistema de segurança. Como citado por Whitman e Mattford (2012, p.6, tradução nossa)

> Bisbey e Hollingworth publicaram seu estudo 'Análise de proteção: Relatório final", discutindo o projeto de análise de proteção criada pela ARPA para melhor entender as vulnerabilidades de operação de segurança do sistema e examinar as possibilidades de técnicas automatizadas de detecção de vulnerabilidades em software de sistema existente.'[3]

Enquanto nos anos 1990, as redes de computadores se tornaram mais comuns, ocasionando uma necessidade de conectar essas redes entre si. Desse modo, a internet se tornou disponível para o público em geral e trouxe consigo acesso para todos os computadores através da Local Area Network (LAN) ou rede local. Apesar disso, o desdobramento da internet definiu a segurança como prioridade baixa.

Os autores supracitados também discutem que os problemas que ocorrem na época atual com os e-*mails* na internet são resultantes dessa falta de segurança. Naquela época, os *emails* não eram encriptados ou codificados visto que os usuários eram considerados confiáveis. Como o uso de computadores conectados diretamente a redes se tornaram frequentes, a segurança física foi perdida e a informação que ficava guardada em banco de dados foi exposta a ameaças.

Os autores ressaltam que, nos anos de 2000 até hoje, a Internet ainda traz muitas redes de computadores inseguras e que ainda se comunicam entre si. Devido ao crescimento de ataques cibernéticos, a preocupação com a defesa contra esses ataques fez com que as empresas e governos buscassem uma infraestrutura mais avançada e políticas mais eficazes.

Embora os autores Whitman e Mattford (2012) fizessem um resgate histórico a partir de 1960, há registros que a preocupação com a informação vem desde 1918, com a Primeira Guerra Mundial, onde Arthur Scherbius[4] inventou um dispositivo de cifras, porém, somente em 1923, que foi oficialmente comercializado com o nome de Enigma. A máquina passou por diversas

---

[3] Bisbey and Hollingworth publish their study "Protection Analysis: Final Report," discussing the Protection Analysis project created by ARPA to better understand the vulnerabilities of operating system security and examine the possibility of automated vulnerability detection techniques in existing system software.

[4] Arthur Scherbius (1878-1929) foi engenheiro elétrico alemão criador e patenteador da Máquina Enigma para cifrar mensagens. CASTELLÓ, Thiago; VAZ, Verônica. **História da Criptografia**. Disponível em: https://www.gta.ufrj.br/grad/07_1/ass-dig/HistriadaCriptografia.html. Acesso em: 21 fev. 2021.

alterações até que em 1928, os alemães passaram a chamá-la de Enigma G, um dispositivo mais aprimorado para decodificar e codificar mensagens.

Lattaro (2016, p. 56) traz de modo resumido os resultados obtidos pelo uso da Enigma G:

> Enquanto nos anos 90, as redes de computadores se tornaram mais comuns, ocasionando uma necessidade de conectar essas redes entre si. Desse modo, a internet se tornou disponível para o público em geral e trouxe consigo acesso para todos os computadores através da Local Area Network (LAN) ou rede local. Apesar disso, o desdobramento da internet definiu a segurança como prioridade baixa.

Os autores supracitados também discutem que os problemas que ocorrem na época atual com os e-*mails* na internet são resultantes dessa falta de segurança. Naquela época, os *e-mails* não eram encriptados ou codificados visto que os usuários eram considerados confiáveis. Como o uso de computadores conectados diretamente a redes se tornaram frequentes, a segurança física foi perdida e a informação que ficava guardada em banco de dados foi exposta a ameaças.

Os autores ressaltam que, nos anos 2000 até hoje, a Internet ainda traz muitas redes de computadores inseguras e que ainda se comunicam entre si. Devido ao crescimento de ataques cibernéticos, a preocupação com a defesa contra esses ataques fez com que as empresas e governos buscassem uma infraestrutura mais avançada e políticas mais eficazes.

Embora os autores Whitman e Mattford (2012) fizessem um resgate histórico a partir de 1960, há registros que a preocupação com a informação vem desde 1918, com a Segunda ou primeira? Guerra Mundial, onde Arthur Scherbius[5] inventou um dispositivo de cifras, porém, somente em 1923, que foi oficialmente comercializado com o nome de Enigma. A máquina passou por diversas alterações até que em 1928, os alemães passaram a chamá-la de Enigma G, um dispositivo mais aprimorado para decodificar e codificar mensagens.

Lattaro (2016, p. 56) traz de modo resumido os resultados obtidos pelo uso da Enigma G:

> Entretanto, resumindo a história, alguns matemáticos e mestres em xadrez, como Newman e Turing, conseguiram quebrar o código. Dizem os historiadores que a Segunda Guerra Mundial terminou um ano antes do' previsto' por conta deste fato. Sendo assim, os alemães criaram a primeira máquina a utilizar a 'one time pad' (cifra de chave única), e os ingleses criaram o primeiro computador digital programável, chamado de Colossus.

[5] Arthur Scherbius (1878-1929) foi engenheiro elétrico alemão criador e patenteador da Máquina Enigma para cifrar mensagens. CASTELLÓ, Thiago; VAZ, Verônica. **História da Criptografia**. Disponível em: https://www.gta.ufrj.br/grad/07_1/ass-dig/HistriadaCriptografia.html. Acesso em: 21 fev. 2021.

Esse contexto denota como o progresso da ciência no desenvolvimento da tecnologia altera o curso de alguns fatos. A exemplo, tem-se o fenômeno da Globalização[6] que expandiu a atuação da Segurança da Informação em função da internet e dos dispositivos de acesso.

Abordar segurança, de maneira geral, há de se considerar as várias concepções, cujo emprego do sentido ocorre conforme o contexto em que é empregada, como por exemplo, a manutenção de um cofre seguro dentro de um banco. A segurança é, assim, um conjunto de padrões para um único objetivo, manter o acesso restrito em diferentes ambientes como dentro de uma organização.

Para Caruso e Steffen (1999, p.5) a segurança "[...] mais que estrutura hierárquica, homens e equipamentos, é postura gerencial em uma organização, o que ultrapassa a tradicional abordagem dada à segurança na maioria das empresas.". Ou seja, a segurança pressupõe mais que recursos humanos, técnicas materiais, envolvendo, também, a gestão de todos os ativos de uma organização de forma a evitar que ameaças externas adentrem no ambiente interno e garanta a sua eficiência. A segurança em si, nada mais é que um conjunto de regras onde a gestão atua para garantir o máximo de seguridade dentro de um ambiente.

Assim, a Segurança da Informação se faz presente dentro das organizações visto que a automatização dos sistemas se modernizou e trouxe consigo uma preocupação acerca dos dados que eram gerados e distribuídos. O Glossário de Segurança da Informação (2019, p.42) conceitua a segurança da informação como "[...] ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.". Ela pode ser vista como um conjunto de regras que garante o controle sobre os dados que são disponibilizados.

Já Beal (2005, p.1) afirma que "A Segurança da Informação pode ser entendida como o processo de proteger informações das ameaças para a sua integridade, disponibilidade e confidencialidade". É importante ressaltar que os dois conceitos se divergem quando um é visto como um objetivo e o outro como um processo. A diferença é que um é uma atividade fim - no caso o conceito do Glossário de Segurança da Informação - enquanto o outro é visto como um processo, isto é, cíclico.

A ISO/IEC 17799 (2005, p.1) põe em voga a concepção de Segurança da Informação como a "[...] preservação da confidencialidade, da integridade e da disponibilidade da

[6] CASTELLS (1999a), por sua vez, considera que o momento atual é percebido através da mudança em nossa cultura material, como resultado do novo paradigma tecnológico que se organiza em torno da tecnologia da informação. RODRIGUES, Ana Maria da Silva; OLIVEIRA, Cristina M. V. Camilo de; FREITAS, Maria Cristina Vieira de. Globalização, cultura e sociedade da informação. **Perspect. Cienc. Inf.**, Belo Horizonte, v. 6, n. 1, p. 97-105, jan./jun. 2001.

informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas."

É interessante observar que esse conceito também se iguala às concepções acima referenciadas, porém é mais completa, abrangendo novos termos como "não repúdio" e "responsabilidade". Implica afirmar que a Segurança da Informação - dentro do contexto das organizações - pode assumir dois papéis, pois varia de acordo com a necessidade das instituições.

Percebe-se que há um item essencial dentro dos sistemas de informação chamados de ativos. Os ativos são qualquer coisa que tenha valor para a organização. Nesse caso, trabalha-se a concepção de ativos de informação de acordo com o postulado pelo Glossário de Segurança da Informação (2019, p. 7) que os concebe como:

> [...] os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso; [...]

Os ativos de informação podem ser um banco de dados, arquivos, contratos e entre outros. Esses ativos precisam ser protegidos contra perda, furto, alterações em seu conteúdo que podem afetar de forma negativa uma organização.

Nesse contexto, é importante destacar que a instalação e, em outros casos, a manutenção de sistemas de segurança da informação são essenciais para manter esses ativos seguros e sem alteração ou distribuição. Beal (2005, p.10) vai mais a fundo e defende que é necessário a adoção de controles de segurança, que consistem em medidas de proteção "[...] que abrangem uma grande diversidade de iniciativas, indo dos cuidados com os processos de comunicação à segurança de pessoas, mídias e componentes de TI".

Dessa forma, a segurança da informação é algo que toda organização deve adotar, pois os riscos existem e os ativos são suscetíveis a sofrer ameaças. Ressalta-se que toda organização deve ter uma visão das suas necessidades - inclusive segurança - garantindo assim medidas mais organizadas e mais apropriadas, considerando o fator econômico de modo que minimize ou elimine os riscos para a organização. Estimando também os três pilares (que foram muito citados pelos autores): Confidencialidade, Integridade e Disponibilidade.

Para a compreensão sobre a Segurança da Informação tem-se como ponto de partida o estudo aprofundado sobre os seus três pilares que compreendem em: Confidencialidade, Integridade e Disponibilidade (CID) ou os três pilares da segurança da informação (BEAL, 2005).

A confidencialidade dentro da Segurança da informação é demonstrada como uma forma de manter o acesso restrito a usuários de dentro e fora do sistema, de forma que a informação contida ali não sofra tanta interferência.

Yinka (2011, p.663, tradução nossa) a define como "[...] o termo usado para prevenir a liberação de informação para pessoas ou sistemas não autorizados."[7]. Dessa forma, a ausência da confidencialidade é o primeiro passo para a invasão de sistemas por hackers ou pessoas de má índole. Logo, ela afeta a privacidade, como por exemplo, o vazamento de informações pessoais[8].

Whitman e Mattford (2012) listam que para proteger a confidencialidade de informação, pode ser utilizado algumas medidas como: classificação da informação, armazenamento seguro de documentos., aplicação de políticas gerais de segurança e educação de guardiões de informações e usuários finais. Os autores classificam a relação da confidencialidade sendo interdependente com outras características da informação, sendo mais próxima da privacidade, onde, os usuários estão sempre conectados de modo que em algum momento deixamos pedaços de nossas informações espalhadas pelo universo da internet. Assim, apreende-se que numa sociedade onde a informação tem valor, significa que uma empresa pode perder milhões em ações quando uma informação importante é vazada.

A confidencialidade trabalha junto com o grau de sigilo, que por sua vez é definido como uma atribuição a qualquer dado e depende da sua natureza e/ou conteúdo para ser classificado. Quanto ao documento ostensivo, isto é, documento cujo acesso é garantido por lei no qual seu conteúdo não é prejudicial, a confidencialidade se faz presente, porém, devido ao grau de sigilo que é mínimo ou não existe, as normativas variam de acordo com a instituição.

Quanto à integridade, ela se posiciona em relação a informação que não deve ser modificada. Beal (2008, p.1) afirma que ela é a "[...] garantia da criação legítima e da consistência da informação ao longo do seu ciclo de vida: em especial, prevenção contra criação ou destruição não autorizada de dados e informações.". A Integridade engloba a autenticidade, que por sua vez, se define como informação livre de adulteração.

Os autores Whitman e Mattford (2012) complementam que a integridade do documento pode ser quebrada enquanto a informação está sendo transmitida ou armazenada. Tanto vírus,

---

[7] [...] the term used to prevent the disclosure of information to unauthorized individuals or system.

[8] Vazamento de dados do ebay em 2014 onde dados de 145 milhões de usuários foram vazados incluindo nomes, endereços e senhas criptografadas. SWINHOE, Dan. **Os 15 maiores vazamentos de dados do século 21**. 2020. Disponível em: https://computerworld.com.br/seguranca/os-15-maiores-vazamentos-violacoes-de-dados-do-seculo-21/. Acesso em: 21 fev. 2021.

quanto hackers ou até mesmo o próprio sistema podem fazer com que a informação seja corrompida e essa informação pode voltar a circular entre os sistemas caso não seja verificada. Os autores apontam o método de chave de segurança, pois além de detectar a presença de vírus também utiliza um *hashing* de arquivo, onde esse arquivo é lido por um algoritmo que usa o valor dos Bits existentes para identificar um número, chamado de *hashing* de valor, onde essa combinação é única. Se a informação sofrer alguma alteração, a sequência muda indicando que aquela informação sofreu uma mudança.

De acordo com o Conarq (2012, p.2) a Autenticidade é a "[...] qualidade de um documento ser exatamente aquele que foi produzido, não tendo sofrido alteração, corrompimento e adulteração.". É a manutenção do conteúdo do documento em seu estágio original, sem sofrer qualquer mudança, de forma a representar a fidedignidade da informação.

Apesar das definições serem bem parecidas, a Integridade se caracteriza por utilizar dos parâmetros da autenticidade para garantir a originalidade da informação. Assim, quando há quebra da confidencialidade, como por exemplo o vazamento das informações, a violação da integridade por sua vez é a alteração dessa informação disponibilizada de forma ilegítima ou em outro contexto, a inserção de informações falsas em um sistema.

A Disponibilidade está relacionada ao acesso à informação, porém há um controle direcionado a quem pode acessar e quais informações podem obter; quando ocorre a violação da disponibilidade, significa que a restrição existente já não tem mais efeito e a informação em si sofre interferências. Yinka (2011, p.663, tradução nossa) afirma que "[...] implica que os sistemas de computação costumavam guardar e processar a informação, os controles de segurança costumavam proteger eles e os canais de comunicação costumavam acessar."[9]

A Disponibilidade caminha junto com a Confidencialidade pois de acordo com o sigilo do documento implica diretamente na disponibilidade dessa informação contida no documento, sendo assim, os três pilares constituem um processo cíclico, onde variam de acordo com as necessidades das organizações e dos documentos, garantindo normas que devem cumprir o papel de proteção dessas informações e assim diminuindo o risco de ameaças.

2.2.1 Política de Segurança da Informação

A gestão eficaz e segura da informação tem como condição ímpar o planejamento de medidas de segurança com vistas a inibir o acesso não autorizado e propiciar o uso de informações confiáveis na e pela organização.

[9] This implies that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.

Esse cenário se torna um imperativo devido a crescente utilização de tecnologia de informação na produção, manuseio, uso e disseminação de informação pelas instituições. Isto porque, é ciente que a informação é um ativo, ou seja, ela tem valor. Logo, a perda desse ativo acarreta uma série de consequências que constantemente não há reversão.

Para evitar a concretização desse cenário, o desenvolvimento de uma política organizacional se apresenta como uma solução por representar um documento que agrega um conjunto de orientações que servem para controlar o ambiente e garantir o sucesso da organização. Assim, quando se fala em segurança da informação, deixa-se bem explícito que a necessidade maior é assegurar que o ativo da organização esteja protegido.

A política de segurança da informação é um documento direcional, informativo em relação a necessidade de proteger e garantir a confiabilidade no referido ativo, que deve ser feito de acordo com a necessidade da organização, fazendo um documento original que atenda de forma positiva os aspectos relacionados ao acesso, manuseio, uso e proteção dos dados e do sistema de informação e que esteja em consonância com objetivos e metas empresariais, para que estes, seja gerenciado com base na segurança e que faça parte da estratégia da organização.

A implementação de um sistema de segurança deve contemplar o ordenamento jurídico vigente e as regulamentações da própria instituição. Dentre a legislação, tem-se os requisitos recomendados pela NBR ISO 27001 que é uma norma que foi elaborada no intuito de acordo com a ABNT (2013) "[...] prover requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI).", cuja descrição deve ser clara, objetiva e disseminada a todos os colaboradores da empresa.

O conhecimento da Política de segurança da informação pelos que compõem a organização é fundamental por nela está contida diretrizes, normas e procedimentos. As diretrizes têm o papel estratégico pelo fato da alta direção estar envolvida. Afinal, eles irão definir o valor que a informação tem dentro da organização, enquanto as normas terão o papel tático. Semôla (2003. p. 106) exemplifica como:

> Critérios normatizados para admissão e demissão de funcionários; criação e manutenção de senhas; descarte de informação em mídia magnética; desenvolvimento e manutenção de sistemas; uso da Internet; acesso remoto; uso de notebook; contratação de serviços terceirizados; e classificação da informação são bons exemplos de normas de uma típica política de segurança.

Dessa forma, as normas serão acompanhadas de situações para melhor aplicação da política em si, orientando também para alcançar os objetivos explícitos no documento. Como os procedimentos têm o papel operacional, de modo que eles são mais detalhados e explicativos para os devidos processos de acordo com a necessidade da organização. Geralmente, estão

presentes em grande quantidade devido ao caráter detalhado e, dessa forma, garantindo a implementação dos controles de forma bem-sucedida.

Coelho, Araújo e Bezerra (2014) adicionam mais dois tópicos a essa política: Instruções e Evidências. O primeiro consiste no detalhamento das operações que irão executar a implementação dos controles e, o segundo, trata-se do monitoramento a partir do uso de mecanismos de coleta de dados a fim de contestar se a aplicabilidade dos controles foi eficiente e eficaz.

Urge destacar que a elaboração dessa política, ressalta-se a importância da participação de todos os funcionários da organização, de forma a entender as suas necessidades, ou seja, compreender o coletivo beneficia quando o documento for aplicado pois não haverá resistência. Sêmola (2003, p.108) destaca que o "[...] importante é dar o pontapé inicial e formar um grupo de trabalho com representantes das áreas e departamentos mais representativos, integrando visões, percepções e necessidades múltiplas que tenderão a convergir e gerar os instrumentos da política."

A política da segurança da informação tem como aliado a disseminação da informação, desde a sua origem até a sua aplicabilidade, possibilita a organização ficar ciente dos processos e diretrizes. Para tanto, a solicitação de um processo de divulgação é importante para que os funcionários se sintam responsáveis pela política e, assim, se responsabilizam pela sua implementação.

Para garantir uma política de segurança da informação efetiva é preciso, também, que o seu *layout* seja agradável, a sua escrita e organização estejam em harmonia.

Hone e Elof (2002) defendem que essa política deve combinar com a cultura da organização para que se evite o risco em confundir com os outros documentos, por exemplo, regulamentos de processos não correlacionados e colocando em evidência a informação de forma que ela não seja estranha aos olhos dos funcionários.

O seu desenvolvimento geralmente é feito por indivíduos da área técnica, que não têm contato direto com o usuário. Logo, o documento fica muito detalhado e extenso, fazendo com que os funcionários de outras áreas não consigam entender ou achar cansativo a leitura. Por isso, é impreterível que haja participação ativa dos funcionários durante o processo de desenvolvimento.

Outro elemento importante na construção de uma política de segurança da informação é a forma do documento que deve ser dinâmica, com uso de gráficos e imagens, além da sua escrita ser direta ao ponto, nem curto e nem longo, para que a organizações existente naquela organização entenda a proposta da política. É interessante também, desenvolver outros

documentos para apoio da política principal detalhando, caso necessário, alguns tópicos. Além de sempre destacar a importância da segurança da informação e a sua função estratégica para a empresa.

Uma das partes principais para a eficácia da política de segurança da informação é o compromisso. Isto exige uma mudança de comportamento por parte dos funcionários e o diretor da organização. Para que a política surta efeito, a direção da organização deve começar a mudar seus padrões, aplicando o que está na política, de forma que os outros níveis sigam esse comportamento. Em conjunto, deve-se disseminar as informações contidas na política aos funcionários de todos os níveis, utilizando diversos métodos como panfletos, e-*mails* e *posters* ou outro que julgar mais conveniente.

A política de segurança da informação deve estar sempre atrelada a missão e visão da organização. Por conseguinte, esse documento é um "documento vivo", ele estará sempre em crescimento vistas a apoiar os objetivos da organização e, por ser um documento vivo, a sua atualização deve ser contínua e de acordo com os ciclos da organização, deixando espaço para novas ideias surgirem.

Advoga-se que a efetividade da política de segurança da informação é um processo contínuo, com a participação de diversos níveis organizacionais, garantir uma aplicação de sucesso, por meio de uma série de benefícios advindos dessa efetividade e sendo ativo no critério estratégico e competitivo. Assegurar que o ativo da informação não sofra interferências ou ameaças é um dever das organizações como um todo, de modo que haja ganhos, e a organização cresça. Daí ser imprescindível o desenvolvimento de uma política de segurança da informação, conforme se enfatizará na próxima seção, a partir das diretrizes referentes para o seu desenvolvimento com base em normas existentes no Brasil.

2.3 Diretrizes para a segurança da informação arquivística: ABNT NBR ISO/IEC 27002 e ISO/IEC 27001 e o Conselho Nacional de Arquivos

Para garantir que a política de Segurança da Informação seja cumprida, a criação de normas e diretrizes foram de extrema necessidade. Em âmbito brasileiro, a Associação Brasileira de Normas Técnicas (ABN) traduziu a Norma ISO/IEC 27001:2013 e 27002:2013 com complemento da norma 27701:2019, para a prática de gestão da Segurança da Informação. Em relação a Conarq em sua Resolução nº 37 intitulada "Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais" esclarece que dentro da autenticidade, a integridade é uma parte dela.

Em relação à norma ABNT ISO/IEC 27001:2013, é importante situar que ela foi feita no intuito de “[...] prover requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI). A adoção de um SGSI é uma decisão estratégica para uma organização.” (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013, não paginado). Dito isso, para manter um sistema de segurança da informação funcionando é necessário encabeçar as necessidades, os requisitos de segurança e os objetivos da organização juntamente com os processos organizacionais e o espaço físico, pois são fatores de influência.

> É importante que um sistema de gestão de segurança da informação seja parte de, e esteja integrado com os processos da organização e com a estrutura de administração global, e que a segurança da informação seja considerada no projeto dos processos, sistemas de informação e controles. É esperado que a implementação de um sistema de gestão de segurança da informação seja planejada de acordo com as necessidades da organização. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013, p.vi)

Um sistema de segurança da informação está ligado diretamente com a confidencialidade, integridade e disponibilidade, de modo que preserve essa informação com a gestão de riscos, além que essa norma pode ser aplicada para “[...] avaliar a capacidade da organização em atender aos seus próprios requisitos de segurança da informação.” (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013, p.vi). Também ~~diz~~ afirma que os requisitos ali expostos podem ser aplicados independente da ordem que irá aparecer na norma.

Essa é a norma principal. Nela há a exposição detalhada por onde iniciar e por fim, sua aplicação e melhoria. Referente a autenticidade, é apontado nas áreas de controle e seus objetivos onde se trata da criptografia como controle criptográfico com o intuito de "[...] assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.” (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013, p.18).

Já a norma 27002:2013 é um código de prática para os controles da norma anterior, sendo mais extensa e bem mais detalhada,

> [...] projetada para as organizações usarem como uma referência na seleção de controles dentro do processo de implementação de um sistema de gestão da segurança da informação (SGSI), baseado na ABNT NBR ISO/IEC 27001 ou como um documento de orientação para as organizações implementarem controles de segurança da informação comumente aceitos. Esta Norma é também usada no desenvolvimento de organizações e indústrias específicas de gerenciamento de segurança da informação, levando em consideração os seus ambientes de risco de segurança da informação específicos. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013, p. x).

Essa norma resgata o conceito de segurança da informação e de ativo da informação, sendo este o valioso objeto dentro da organização. Por este motivo, a criação de uma política da segurança da informação ou até mesmo um reforço em políticas já existentes são benéficas para a proteção deste ativo contra ameaças, uma vez que, estas se aproveitam de vulnerabilidades, como por exemplo, mudança de sistemas, processos e até alterações dentro do quadro de colaboradores. Logo, "Uma segurança da informação eficaz reduz estes riscos, protegendo a organização das ameaças e vulnerabilidades e, assim, reduzindo o impacto aos seus ativos." (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013, p. x).

Outro aspecto que essa norma engloba é o desenvolvimento dos requisitos necessários para uma política por fornecer "[...] diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização." (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013, p. 1). A observância dos riscos se torna condição ímpar para que se estabeleça as normas de segurança.

A norma contém 14 seções de controle sendo 35 objetivos de controles e 114 controles, tangendo para a seção de número 10, onde se trata da criptografia como meio de garantir a autenticidade, confidencialidade e integridade da informação.

Dentro das diretrizes para a aplicação é ressaltado que é possível utilizar diversos controles criptográficos para a alcançar os objetivos da segurança da informação, destacando a autenticidade, através de "[...] assinaturas digitais ou códigos de autenticação de mensagens (MAC) para verificar a autenticidade ou integridade de informações sensíveis ou críticas, armazenadas ou transmitidas [...]"(ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013, p. 36). As assinaturas digitais consistem em um processo assimétrico de criptografia, onde há dois tipos de chaves: pública e privada que cifram a mensagem onde somente quem tiver a chave poderá decodificar.

A autenticação são as técnicas para garantir a autenticidade da informação ou - no caso de sistemas - usuários, por exemplo, caso estes queiram ter acesso ao sistema. Por conta disso, se faz necessário um gerenciamento de chaves para que haja a autenticação do usuário e, consequentemente, sua entrada seja permitida.

> Além do gerenciamento seguro de chaves secretas e privadas, convém que a autenticidade de chaves públicas seja considerada. Este processo de autenticação pode ser conduzido utilizando-se certificados de chaves públicas que são normalmente emitidos por uma autoridade certificadora, a qual recomenda-se que seja uma organização reconhecida, com controles

> adequados e procedimentos implantados com o objetivo de garantir o requerido nível de confiança. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013, p. 37).

O processo de transferência de informação é tratado na da organização e com quaisquer entidades externas: quando se trata de sistemas, é reforçado que nenhum sistema é seguro, e as ameaças podem ser tanto externas quanto internas. Os riscos existentes quando há migração de informações de um sistema para o outro, por exemplo, pode corromper os arquivos, vazamentos e até ataque através de algum vírus. Dessa forma, as técnicas de criptografia irão garantir que a autenticidade destes não seja perdida durante a transferência de informação usando as chaves de ordem pública ou privada.

Importante frisar, que, embora não exista uma tecnologia de segurança 100%, mas as existentes são constantemente aperfeiçoadas, buscam inibir ataques cada vez mais visíveis a ameaças existentes nesse espaço, que podem comprometer os objetivos para/com a informação.

> A autenticidade dos documentos arquivísticos digitais é ameaçada sempre que eles são transmitidos através do espaço (entre pessoas e sistemas ou aplicativos) ou do tempo (armazenagem contínua ou atualização/substituição de hardware/software usados para armazenar, processar e comunicar os documentos). (CONSELHO NACIONAL DE ARQUIVO, 2012, p. 1)

Sabe-se que a tecnologia utilizada sofre o processo de obsolescência em função da produção acelerada de softwares e hardwares. Então, para que fosse mais bem avaliada esta questão ligada aos documentos digitais, a autenticidade se volta a identidade e integridade, de modo que foram utilizados procedimentos administrativos atrelado às tecnologias que minimizem em algum ponto, mudanças nos documentos, caso haja migração de sistemas ou este documento seja salvo várias vezes por diferentes usuários.

> A presunção de autenticidade dos documentos arquivísticos sempre fez parte do processo tradicional de avaliação desses documentos e é fortemente apoiada na análise de sua forma e de seu conteúdo, que nos documentos não digitais estão inextricavelmente ligados ao suporte – isto é, forma, conteúdo e suporte são inseparáveis. (CONSELHO NACIONAL DE ARQUIVO, 2012, p. 1)

A autenticidade é um processo que verifica se a informação contida naquele documento é verídica e quando se trata de autenticidade, temos a figura da diplomática. Esta faz uma análise desde data, espécie, conteúdo e proveniência, por exemplo, que está ligada a documentos mais antigos, enquanto a autenticidade, aqui estudada, está voltada a documentos digitais, analisando a forma - aparência do documento - e o conteúdo - informação contida no documento - sendo estes significativo para a presunção da autenticidade considerando a cadeia de custódia ininterrupta definida pelo Conselho Nacional de Arquivo (2012, p, 1) como a "[...] linha

contínua de custodiadores de documentos arquivísticos (desde o seu produtor até o seu legítimo sucessor) pela qual se assegura que esses documentos são os mesmos desde o início, não sofreram nenhum processo de alteração e, portanto, são autênticos." Se caso este documento migrar entre sistemas ou parar em outros usuários, sua autenticidade começa a ser duvidosa.

Como toda informação disponível no meio digital, além das ameaças referentes a vírus e ataques *hackers*, a autenticidade pode ficar comprometida. O Conarq (2013, p. 1) exemplifica que

> Os documentos arquivísticos digitais apresentam dificuldades adicionais para presunção de autenticidade em razão de serem facilmente duplicados, distribuídos, renomeados, reformatados ou convertidos, além de poderem ser alterados e falsificados com facilidade, sem deixar rastros aparentes.

A resolução nº 37 de autoria do conarq informa que as características físicas dos documentos digitais podem mudar, sendo essas características o suporte e a cadeia de *bits*. O suporte, por não estar ligado a forma e ao conteúdo, não muda a autenticidade dos documentos, e a cadeia de *bits* está relacionado da seguinte forma: o documento após ser salvo se desmancha em cadeias. Estas representam dados referentes à composição, o conteúdo e forma, sendo utilizado como estratégia dentro da preservação digital. No entanto, deixa-se bem claro que documento arquivístico digital é um objeto conceitual, pois ele precisa de um dispositivo de saída para que seja exibido como, por exemplo, o monitor.

Quando se trata de documentos arquivísticos, leva-se em consideração três aspectos para a devida autenticidade: legal, diplomático e histórico de acordo com a resolução 37 do conarq

a) legal: são documentos que para garantir a sua genuinidade, precisam dar testemunhos sobre si, ou seja, precisa atestar a fidedignidade de que tal informação ali contida durante ou depois de sua produção de fato é verossímil perante uma autoridade pública representativa.
b) Diplomáticos: foram escritos e neles se encontram a data e lugar com assinatura das pessoas ou pessoa que produziu-o, como por exemplo, documentos manuscritos antigos.
c) Histórico: atestam fatos ou informações verdadeiras.

Os três independem, entre si, ao ponto que um documento pode ser autenticamente histórico e diplomático, porém não é um documento legal. O aspecto histórico e a diplomática se complementam, e se importam com o conteúdo e a veracidade deste. Por esse motivo, é considerado o conceito de autenticidade da diplomática. De acordo com o Conselho Nacional de Arquivo (2012, p. 4)

> Observa-se uma relação entre o aspecto histórico da autenticidade e o conceito diplomático de confiabilidade no sentido de que ambos se referem à

> veracidade do conteúdo do documento. Já no que tange ao ponto de vista da diplomática, a autenticidade se refere a não alteração do documento após sua produção, mesmo que o conteúdo não seja verdadeiro. Para fins destas diretrizes será considerado o conceito de autenticidade da diplomática.

Quando se trata de presunção da autenticidade, é importante considerar que há algumas particularidades a serem destacadas, iniciando-se pelo ambiente de produção, este contém "[...] procedimentos de controle, o sistema informatizado e o próprio produtor e/ou custodiador dos documentos [...]" (CONSELHO NACIONAL DE ARQUIVO, 2012, p. 4). Desmembrando-o pelo primeiro, estes procedimentos de controle abarcam quem produz os documentos e salvaguarda-os, além de descrever como essas ações acontecem. Inicialmente se preocupa com o "como" e quem irá executar essas práticas. O Conarq (2012, p. 4) exemplifica:

> Assim, é preciso que se definam direitos de acesso, espaços de trabalho (produção, recebimento, alteração, classificação, registro de metadados, arquivamento e destinação), conjunto de metadados e procedimentos de preservação.

Um sistema informatizado deve ser confiável, isto é, deve ser protegido contra exposição por indivíduos não autorizados ou sistemas. Para tanto, é preciso que as normas e diretrizes sejam implementadas e acessos autorizados (direitos e privilégios) somente para aqueles habilitados.

O Conselho Nacional de Arquivo (2012, p. 4) expõe "[...] é preciso que se definam direitos de acesso, espaços de trabalho (produção, recebimento, alteração, classificação, registro de metadados, arquivamento e destinação), conjunto de metadados e procedimentos de preservação."

Por último, a entidade produtora ou custeadora deve "[...] possuir reputação idônea, demonstrar capacidade e conhecimento específico para gerenciar os documentos e, consequentemente, inspirar a confiança dos usuários." (CONSELHO NACIONAL DE ARQUIVO, 2012, p. 4). Este último, é bem relacionado com a confiabilidade, para que se tenha um sistema seguro, deve-se atentar ao fator humano, no caso, quem é o possuidor ou mantenedor da instituição, isso ajuda a evitar brechas ou vazamento de informações. Quando se trata de usuário, é necessário criar um padrão de comportamento a ser seguido, porém deve-se começar pelos diretores e CEO, seguindo a hierarquia. É estratégico ter os usuários seguindo o padrão para evitar acessos indevidos e quebra na segurança.

Outra ênfase dada pelo Conselho Nacional de Arquivo (2012, p. 5) consiste na implementação, "[...] sempre que possível, técnicas de autenticação apoiadas em políticas e procedimentos administrativos e arquivísticos independentes de tecnologia e/ou neutros.". As organizações devem ter documentos administrativos-jurídicos como políticas, diretrizes e

normas pois estas regulamentam e efetivam os objetivos, de modo que a sociedade existente na organização entenda e aplique, garantindo assim, o sucesso daquele documento.

E dentro dessas políticas estarão também ferramentas de autenticação para declarar a autenticidade dos documentos digitais. A autenticação é definida como "[...] declaração de autenticidade de um documento arquivístico, num determinado momento, resultante do acréscimo de um elemento ou da afirmação por parte de uma pessoa investida de autoridade para tal." (CONSELHO NACIONAL DE ARQUIVOS, 2012, p. 2). Esta faz parte da autenticidade, sendo um mecanismo de atestado de veracidade, por uma pessoa autorizada para isso, como por exemplo, diplomas de ensino superior.

Porém, esta declaração nem sempre garante a autenticidade como explica o Conselho Nacional de Arquivo (2012, p. 5):

> Enquanto declaração, a autenticação não garante necessariamente a autenticidade do documento, na medida em que se pode declarar como autêntico algo que não é. Da mesma forma, um documento pode ser considerado autêntico sem que nele conste uma autenticação.

Assim, quando se fala de autenticação, começa-se a pensar em métodos muito conhecidos, como QR code, códigos de verificação, *links* enviados por sites ao e-mail para autorizar acesso e assim por diante. Porém, quando se trata de documentos digitais, um outro método também utilizado, é a assinatura digital.

A assinatura digital, é concebida pelo Conselho Nacional de Arquivo (2012, p.5) como "[...] resultado de um cálculo matemático que envolve a cadeia de bits do documento e a chave da assinatura digital.". Logo, se essa cadeia sofrer alguma alteração, significa que a informação contida naquele documento foi alterada e não poderá ser assegurada a autenticidade. Sabe-se que os trâmites da informação devem ocorrer, e por isto, é necessário se atentar ao sistema, pessoas, aplicativos que vão estar nesse meio, de modo que garanta a confiabilidade destes.

Quanto mais se converte, mais cadeias de bits aparecem, invalidando assim a assinatura digital. Porém, para que se garanta a autenticidade caso isso ocorra, pode-se utilizar outros métodos como a inserção de metadados, isto é, inserir mais informações sobre o documento, informações relevantes e relacionadas com o autor do documento até palavras-chaves.

> Ao se receber um documento assinado digitalmente, deve-se registrar, como metadado de integridade, a informação indicando que o documento foi recebido com tal assinatura e que esta foi verificada. Da mesma maneira, nas sucessivas conversões de formatos, deve-se registrar, também como metadado, o evento de conversão. (CONSELHO NACIONAL DE ARQUIVO, 2012, p. 6).

Verifica-se assim, que apesar dos métodos utilizados, os documentos correm o risco de não serem autênticos devido a uma série de fatores como sistema, técnicas de autenticidade e

entre outros. Como documentos digitais dependem de certo modo, da tecnologia, ele acaba sendo exposto a questão da obsolescência tecnológica, pois *softwares* e *hardwares* tem uma validade.

3 A SEGURANÇA DA INFORMAÇÃO ARQUIVÍSTICA: a garantia da autenticidade pelo pilar da integridade

O avanço das TIC possibilita conectar e transmitir informação de modo rápido, porém, nem sempre seguro. Essa preocupação com a segurança ocorre devido a inúmeros casos de invasão ou roubo de informações institucionais, públicas e/ou pessoais privilegiadas.[10]

Esta seção apresentará dois modelos de segurança da informação com ênfase no pilar da integridade para as informações arquivísticas a partir do referencial teórico pesquisado, lido e analisado. Embora a Segurança da Informação e a Arquivística serem áreas distintas, o caráter interdisciplinar de ambas, permite o diálogo voltado para a segurança do documento digital, sua autenticidade e sua integridade.

Tal afirmativa é situada ao se trazer a segurança da informação para o campo da Arquivística. Onde se considera no documento digital, a sua forma e conteúdo, cuja apresentação ocorre por códigos binários e cadeias de *bits* e sua utilização é respaldada no acesso facilitado através dos aparatos tecnológicos dentre outras razões.

Nesse sentido, ao se falar de informação, compreende-a como um aglomerado lógico de ideias que possibilita a geração de conhecimento a diversos segmentos da sociedade. E, quando esta informação é trabalhada por sistemas, ameaças podem ocorrer, como a sua perda ou não ser tão inteligível a ponto de quem for acessá-la não a entender. O pilar da integridade quando aplicado obedecendo aos requisitos de proteção necessários podem garantir a segurança dessa informação e, como consequência, a garantia da autenticidade de um documento digital arquivístico por um sistema.

Ressalta-se que nenhum sistema é seguro e que ele pode sofrer uma cominação a ponto de prejudicar uma organização como um todo, principalmente, quando se volta para os objetos no meio digital e o modo como eles estão disponibilizados. Para que os riscos, rupturas e roubos, voltado para controles que possam melhorar a autenticidade, dentro dos sistemas e nos documentos arquivísticos.

Sabe-se que já existem alguns processos para garantir a integridade do documento como a assinatura digital, cadeia de *bits* e outros processos mais detalhados pelo Conarq. Todavia, a integridade é fundamental para que os sistemas armazenem a informação, a mantenha sem modificação e, assim, garanta a autenticidade.

[10] O adjetivo privilegiado é atribuído a este contexto pelo fato do ativo da informação ser um insumo estratégico.

Nesse contexto, é importante destacar o formato do arquivo das informações arquivísticas que deve ser em *Portable Document Format* (PDF) por ser considerado o padrão de documentos digitais por instituições públicas em função de atribuir integridade ao conteúdo informacional. Seu uso é reforçado pelo fato de ter compatibilidade com vários sistemas operacionais e compactar os arquivos como explicitado por Santos e Flores (2016).

Assim, para que se exerça o controle da segurança da informação arquivística é necessário que sistemas de informação adotem alguns requisitos com vistas a sua integridade como as cópias de segurança, sistemas de autenticação digital, bem como, alguns sistemas de informação que possibilitam o controle da segurança.

Para esta pesquisa, selecionou-se dois modelos. O primeiro chamado de Sistema de Detecção e Prevenção de Intrusão Baseada em Host[11] (HIDPS) também chamado de sistema de verificação de integridade "[...] porque eles fazem um *benchmark* e monitoram o status dos principais arquivos do sistema e detectam quando um invasor cria, modifica ou exclui arquivos monitorados."[12] (WHITMAN, MATTFORD, 2011, p. 302, tradução nossa). Ele está localizado em um só computador ou sistema, o que permite a verificação através do fluxo informacional indo para o *host*[13], além de possibilitar a leitura de mensagens encriptadas que estão na rede.

Algo interessante, nesse modelo, é que o sistema salva os tamanhos, localização ou quaisquer outras características acerca dos arquivos, atestando, caso haja alguma modificação nos documentos, em conjunto e consegue ver os *logs* no sistema de forma a prever alguns eventos.

> O HIDPS tem um alerta quando ocorre um desses eventos: atributos do arquivo mudam, novos arquivos são criados, ou arquivos existentes são deletados [...] O HIDPS examina estes arquivos e *logs* para determinar se um ataque está a caminho ou se já ocorreu e se o ataque está ocorrendo ou foi bem-sucedido. (WHITMAN; MATTFORD. 2011, p. 303, tradução nossa)[14]

Mas, como esse sistema responde ao pilar da integridade para as informações arquivísticas? A resposta para esta indagação é que ele se localiza dentro da integridade por manter o acesso restrito a alguns usuários, por classificar os arquivos de modo que caso algo

[11] Na língua inglesa identificado somente pela sigla host-based IDPS (HIDPS) (WHITMAN;MATTFORD, 2011)

[12] [...] because they benchmark and monitor the status of key system files and detect when an intruder creates, modifies, or deletes monitored files"

[13] Um computador ligado a internet que recebe as informações que são geradas

[14] The HIDPS triggers an alert when one of the following occurs: file attributes change, new files are created, or existing files are deleted. [...] The HIDPS examines these files and logs to determine if an attack is underway or has occurred and if the attack is succeeding or was successful.

mude, terá um alerta emitido para o administrador. Isto é fundamental para manter a autenticidade dos documentos e, por consequência, a sua integridade.

Em relação ao contexto do ativo informacional, o HIDPS terá somente um fluxo corrente e um único administrador, e este avaliará os arquivos que estão passando pelo sistema.

Tratando-se dos documentos em si, vê que algumas técnicas estão bem mais atualizadas e alinhadas diretamente com a criptografia. Esta se mostrou viável quando se trata de autenticidade e integridade, como uso de marcas d'água para averiguar se a informação é verdadeira ou não.

Esse procedimento ocorre pelo uso de marca d'água alinhada com a criptografia que permite esconder uma chave *hash*, cuja identificação será possível pelo sistema que gera essa informação.

No tocante a autenticidade, observa-se que tanto sistemas quanto documentos partem do pressuposto único de como garantir veracidade as informações que são apresentadas e como elas podem ser benéficas a organização. Dessa forma, técnicas de criptografia são utilizadas para tentar assegurar que a informação que chega até o usuario é de fato verídica, íntegra desde a sua produção até o seu acesso, ou seja, a autenticidade é garantida.

Outro aspecto importante em relação a segurança da informação é desuso dos artefatos tecnológicos, a famosa obsolescência tecnológica. Um modo de evitar que os documentos sejam perdidos, caso armazenados em um *software*, é a migração de sistemas. Neste caso, pode-se perder o formato – por exemplo, saindo de um DOCX para PDF – durante a transferência menos o conteúdo armazenado.

A migração de dados, presente no modelo HIDPS requer que

> os funcionários tenham conhecimento dos formatos antigos tanto quanto os novos, a habilidade de analisar e recomendar os melhores novos formatos, o tempo para implementar e testar programas pilotos de migração, e a capacidade de desenvolver e refinar continuamente o processo de migração.[15] (LIN; RAMAIAH; WAL, 2003, p. 120, tradução nossa)

Outra opção é realizar periodicamente ou de acordo com a necessidade *backups*, que se definem como cópias de segurança dos documentos que podem ser armazenadas em nuvem ou não.

> As cópias de segurança em computadores são instrumentos importantes para compensar - ou tentar sanar - problemas advindos de hardware, como, por

[15] Digital migration requires the staff to have knowledge of the old formats as well as the new, the ability to analyse and recommend the best of new formats, the time to implement and test migration pilot programs, and the capacity to develop and continually refine migration process.

> exemplo, uma pane no disco rígido, ou de software, como a invasão do sistema por hackers, ataques de vírus, perda acidental de arquivos, conflitos no sistema operacional etc. (FIALHO JUNIOR, 2007, não paginado).

Comumente, os *hardwares* usados para armazenar os documentos estão expostos a ameaças como as citadas acima. O *backup* é uma segurança de que terá cópias armazenadas que poderão ser recuperadas. Quando se trabalha com sistema de gestão de documentos, principalmente quando esses documentos estão voltados a guarda permanente, deve-se ter uma diretriz pronta com os períodos do *backup* a serem realizados, devido ao crescimento de volume destes documentos por serem digitais.

> Outra vantagem do backup em nuvem para empresas é sua fácil manutenção, que acaba economizando gastos extras com manutenção ou até mesmo substituição de equipamentos. Também foi descoberto que um método de backup que ainda é muito utilizado pelas empresas é o backup em fitas magnéticas ou fitas LTO, por terem um custo muito baixo, possibilitando uma fácil substituição caso necessário. (SCOPEL; FIORESE; CERVINSKI; CARLESSO; XAVIER; TISOTT; ZANANDREA; SILVA; CAMARGO, 2018, p. 9).

A citação acima expõe que há dois métodos de fazer o *backup*, em nuvem, onde o acesso seria ainda mais facilitado, porém, custo mais elevado, o valor do espaço em nuvem é referente a quantidade de armazenamento que será utilizado e quanto tempo (assinatura mensal ou anual). Enquanto o físico, seria armazenado em fitas LTO ou HD externo [16]cujo acesso não é tão facilitado e a duração deles é reduzida, e o valor é menor comparado ao armazenamento em nuvem, pois se está falando em grandes volumes de dados.

Kavuri, Kancherla e Bobba (2014) afirmam que se o armazenamento em nuvem for utilizado, pede que seja gerado um *hash* antes, isto é, um código criptografado, pois quando a informação for enviada para ser armazenada, ela irá em forma de "chave" de modo que quem for acessar, conseguirá verificar a informação.

O segundo modelo é o *blockchain* que apesar de ser utilizado para transações bancárias, atualmente, é usado para documentos digitais, sendo concebido:

> [...] uma espécie de livro contábil distribuído, no qual informações são registradas e compartilhadas para servidores espalhados por toda a rede, onde esses dados são verificados e validados em forma de consenso, criando um histórico transparente e imutável de todos os registros inseridos na plataforma. Os registros dessas transações são formados por uma série de blocos criptografados, distribuídos através de uma rede peer-to-peer (de ponto a ponto), e encadeados ao bloco anterior formando uma cadeia de blocos, correntes de blocos, ou como mais conhecida, Blockchain. (NASCIMENTO; DORNELES, 2020, p. 27).

[16] Fitas LTO (Linear Tape-Open) são fitas magnéticas de armazenamento e o HD externo (hard disc) é um dispositivo de armazenamento via USB (universal serial bus).

O *blockchain* pode ser visto como uma base de dados, mas o concebemos, nesta pesquisa, como um modelo de segurança da informação com possibilidades de arquivar todo tipo de informação "[...] indelével, sustentável e descentralizada [...] de maneira segura, rápida, com prova criptográfica e atualizações próximas do tempo real, viabilizando acesso à informação de forma transparente e compartilhada." (NASCIMENTO; DORNELES; 2020, p. 27)

Trata-se, portanto, de um modelo de validação de dados que garante a autenticidade. Funciona da seguinte forma: se um documento foi gerado, ele terá uma assinatura digital, esta ao ser inserida no *blockchain* será validada com um *timestamp*, uma espécie de carimbo de tempo que registra o momento em que o documento foi validado e essa assinatura não será mais removida.

Esse modelo foi retirado da área dos *Bitcoins*, e por isso, ainda está em desenvolvimento, além de ser pouco utilizada no Brasil e no mundo. Os autores Nascimento e Dorneles (2020) desenvolveram em sua pesquisa "Recomendações para o uso de documentos arquivísticos digitais nas plataformas do tipo *blockchain*" e fizeram um quadro com as empresas e como elas utilizam o *blockchain*, conforme ilustrado no Quadro 3:

QUADRO 4 - Casos de utilização de tecnologia do tipo blockchain

PLATAFORMA	SERVIÇOS	DESCRIÇÃO
Bitnation	Provimento de serviços de cartório em âmbito internacional.	Desenvolvem e fornecem soluções avançadas de *software* e *hardware* necessárias para empresas, governos, organizações e indivíduos moverem ativos com segurança pelo *blockchain*. (Fonte: *website* da empresa)
Factom	Protocolo de publicação descentralizado para a construção de sistemas de registros imutáveis e verificáveis de forma independente.	Fornecem uma plataforma *Blockchain* como serviço para soluções de proveniência e integridade de dados construídas no *blockchain* da empresa. Ajudam clientes e parceiros a criar aplicativos prontos para negócios que preservam evidências, demonstram conformidade, aumentam a transparência do processo, agilizam auditorias, reduzem custos e automatizam transações. (Fonte: *website* da empresa)
Uniproof	Registro de documentos eletrônicos em cartório e *blockchain*.	Registram em cartório e em *blockchain* qualquer arquivo eletrônico. Assim elimina documentos em papel e evita ir até o cartório, obtendo validade jurídica e fé pública em seus documentos, a partir do seu computador. Basta acessar a plataforma, enviar seus arquivos e aguardar o retorno dos documentos registrados em forma eletrônica. (Fonte: *website* da empresa)

Bitfury	Soluções avançadas de *software* e *hardware* através de sistema de *Blockchain*	Desenvolvem e fornecem soluções avançadas de *software* e *hardware* necessárias para empresas, governos, organizações e indivíduos moverem ativos com segurança pelo *Blockchain*. (Fonte: *website* da empresa)
OriginalMy	Validação de identidade, assinatura eletrônica e certificação de documentos digitais.	Por meio de uma plataforma totalmente automatizada e segura, é coletada evidência pública sobre conteúdo on-line, como sites e redes sociais, certificando-os em *blockchain* e autenticando-os no cartório. Também é possível certificar e verificar a autenticidade de documentos e arquivos digitais, incluindo contratos. Além da autenticação de informações, e a empresa fornece a identidade do *Blockchain*. É uma forte validação de dados de identidade digital que permite a assinatura digital de arquivos com prova de autoria. (Fonte: *website* da empresa)

Fonte: Nascimento; Dorneles (2020, p. 37)

Os usos do *blockchain* vão desde registro em cartório até validação de identidade, em alguns casos, a empresa elimina os documentos físicos deixando somente no meio digital – economizando espaço e custo – e outras, autentica em duas fases, cartório e em *blockchain* de modo que a segurança é reforçada.

Expressa-se que esse modelo apesar dos pontos positivos apresentados, se faz necessário que haja uma visão arquivística baseada em suporte, conteúdo e forma, pois estes são importantes para assegurar a autenticidade, e sugere-se a inserção de metadados para melhor desmembrar o documento e assim, acessá-lo.

Assim, apreende-se que segurança da informação é um processo para proteger os objetos informacionais das ameaças de forma que garanta a sua Confiabilidade, Integridade e Disponibilidade constituem-se, por assim dizer, na trindade que mantém a informação de forma restrita a alguns usuários ou sistema, sem sofrer qualquer tipo de alteração, estando disponível a usuários ou sistemas autorizados.

4 CONSIDERAÇÕES FINAIS

A finalização de uma pesquisa representa novos começos. Isto porque, o processo vivenciado gera novos questionamentos e novas direções. Não se constitui em uma tarefa fácil, sobretudo, quando parar e se parou no momento adequado.

Durante a realização da pesquisa, foi-se encontrado os seguintes problemas: a literatura brasileira é trivial e repetitiva. Em relação a literatura internacional, esta por sua vez, trouxe novas visões, porém a barreira linguística foi um empecilho durante a realização do estudo. A pesquisa em base de dados internacionais foi necessária visto que as bases de dados brasileiras estão desprovidas de tal conteúdo.

Dessa forma, esta pesquisa trilhou um percurso para responder a seguinte indagação "Os modelos de segurança da informação existentes garantem a autenticidade das informações arquivísticas a partir do pilar da Integridade?". De certo, a resposta é oriunda do estudo de dois modelos: HIDPS e *blockchain* utilizados por organizações que foram apresentadas na seção 4 com aplicabilidade no contexto do documento arquivístico.

Dentre os resultados alcançados e que respondem ao problema da pesquisa é a necessidade de os modelos terem os três pilares da segurança da informação presente em seus processos e para isto, é necessário que todo e qualquer modelo tenha a participação do arquivista em sua concepção e implementação.

Além disso, a manutenção da integridade garantirá que a segurança da informação arquivística mantenha o documento ou sistema sem modificação; de forma íntegro durante o seu ciclo de vida documental. A autenticidade, apesar de ter quase a mesma concepção que a integridade, é mais voltada para as técnicas que irão autenticar o documento.

No entanto, explicita-se que ainda não é possível garantir que a informação em si é autêntica, mesmo com os usos das técnicas, pois nenhum sistema é seguro e embora utilize antivírus e todos os cuidados possíveis, ainda assim, a segurança é quebrada com muita facilidade.

Dito isso, espera-se que a partir desse trabalho, irrompam pesquisas para a utilização dos modelos apresentados para a integridade de documentos de arquivos digitais e criação de políticas de segurança da informação voltadas para documentos digitais.

É necessário, portanto, que haja um estudo da área da Arquivística em conjunto da Segurança da Informação para que se possa escolher requisitos, que de fato irão contribuir de forma positiva, desenvolvendo assim, novas perspectivas para os documentos arquivísticos digitais.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 17799**: Técnicas de segurança e código de práticas para a gestão de segurança da informação. Rio de janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001**: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro: Abnt, 2013. 99 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 27002**: Tecnologia da Informação, técnicas de segurança e código de prática para controles de segurança da informação. Rio de janeiro, 2013.

A KAVURI, Satheesh K s V; KANCHERLA, Gangadhara Rao; BOBBA, Basaveswara Rao. Data authentication and integrity verification techniques for trusted/untrusted cloud servers. In: 2014 INTERNATIONAL CONFERENCE ON ADVANCES IN COMPUTING, COMMUNICATIONS AND INFORMATICS (ICACCI), 2014, Dehi. **2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI).** [S.L.]: Ieee, 2014. p. 2590-2596. Disponível em: https://ieeexplore.ieee.org/document/6968657/authors#authors. Acesso em: 04 abr. 2020.

ARQUIVO NACIONAL. **Dicionario Brasileiro de terminologia arquivística**. Rio de Janeiro: Arquivo Nacional, 2005. 232 p.

AYRES SFREDDO, Josiane; FLORES, Daniel. Segurança da informação arquivística: o controle de acesso em arquivos públicos estaduais. **Perspectivas em Ciência da Informação**, [S.l.], v. 17, n. 2, p. 158-178, maio 2012. ISSN 19815344. Disponível em: <http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/1290>. Acesso em: 12 set. 2021

BARROS, T. H. B. Por uma arqueologia da arquivística: elementos históricos de sua constituição. **Informação Arquivística**, v. 3, n. 2, 2014. DOI: 10.18377/2316-7300/informacaoarquivistica.v3n2p% Acesso em: 12 set. 2021.

BEAL, Adriana. **Segurança da Informação**. São Paulo: Atlas, 2008. 175 p.

BELLOTTO, Heloísa Liberalli. A diplomática como chave da teoria arquivística. **Archeion Online**, João Pessoa, v.3, n.2, p.04-13, jul./dez. 2015.

BRASIL. Lei nº 13.105 de 16 de março de 2015. **Institui o Código de Processo Civil**. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13105.htm> Acesso em: 07 abr. 2021

CAMARGO, Ana Maria de Almeida; MACHADO, Helena Correa. **Como implantar arquivos municipais**. São Paulo: Arquivo do Estado / Associação de Arquivistas de São Paulo, 2000 (Projeto Como Fazer, v. 3).

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em Informática e de Informações**, São Paulo: Editora SENAC São Paulo, 1999.

CHOO, Chun Wei. **Preenchendo as lacunas cognitivas**: como as pessoas processam as informações. In: Dominando a gestão da informação. Porto Alegre: Bookman, 2004.

COELHO, Flávia Estélia Silva; ARAÚJO, Luiz Geraldo Segadas; BEZERRA, Edson Kowask. **Gestão da Segurança da Informação NBR 27001 e NBR 27002**. Rio de Janeiro-RJ: RNP/ESR, 2014.

CONSELHO NACIONAL DE ARQUIVOS – CONARQ (Brasil). **Legislação arquivística brasileira e correlata**. Rio de Janeiro: Arquivo Nacional, 2017. 195 p.

CONSELHO NACIONAL DE ARQUIVOS – CONARQ (Brasil). Câmara Técnica de documentos eletrônicos. **Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais**. Rio de Janeiro: Arquivo Nacional, 2012. Disponível em: http://conarq.gov.br/publicacoes-ctde/167-diretrizes-para-apresuncao-de-autenticidade-dedocumentos-arquivisticos-digitais.html. Acesso em: 30 mar. 2020.

DURANTI, Luciana. **Registros documentais contemporâneos como prova de ação**. Tradução Adelina Novaes Cruz. Estudos Históricos, Rio de Janeiro, v. 7, n. 13, p. 49 – 64, 1994.

FIALHO JUNIOR, Mozart. **Guia Essencial do Backup**. São Paulo: Digerati Books, 2007. 128 p.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. São Paulo: Atlas, 2011. 200 p.

GABINETE DE SEGURANÇA INSTITUCIONAL. **Glossário de Segurança da Informação**. Brasília: Assessoria de Comunicação Social do Gsi, 2020. 50 p. Disponível em: https://dados.gov.br/dataset/glossario-de-seguranca-da-informacao. Acesso em: 29 jun. 2021.

HÖNE, Karin; ELOFF, J.H.P. What Makes an Effective Information Security Policy? **Network Security**, [S.L.], v. 2002, n. 6, p. 14-16, jun. 2002. Mark Allen Group. http://dx.doi.org/10.1016/s1353-4858(02)06011-7. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1353485802060117. Acesso em: 12 maio 2021.

LATTARO, Alex. Uma breve viagem ao desenvolvimento da Segurança da Informação: passado, presente e futuro. **Desenvolvimento da Segurança da Informação**: passado, presente e futuro, São Paulo, v. 19, n. 11, p. 55-61, ago. 2016.

LIN, Lim Siew; RAMAIAH, Chennupati K.; WAL, Pitt Kuan. Problems in the preservation of electronic records. **Library Review**, [S.L.], v. 52, n. 3, p. 117-125, abr. 2003. Emerald. http://dx.doi.org/10.1108/00242530310465924.

NASCIMENTO, Cynthia Giovania Fernandes do; DORNELES, Sânderson Lopes. Recomendações da Diplomática para o uso de documentos arquivísticos digitais nas plataformas do tipo blockchain. **Archeion Online**, [S.L.], v. 7, n. 2, p. 26-42, 30 jun. 2020. Portal de Periodicos UFPB. http://dx.doi.org/10.22478/ufpb.2318-6186.2020v7n2.52500.

PAES, Marilena Leite. **Arquivo:** teoria e prática. Rio de Janeiro: Editora PGV, 2004. 228 p.

PRODANOV, Cleber Cristiano. **Metodologia do trabalho científico**: métodos e técnicas da pesquisa e do trabalho acadêmico. 2. ed. Novo Hamburgo: Feevale, 2013. 277 p.

RODRIGUES, Ana Célia. Natureza do documento de arquivo: vínculo e estrutura. In: FREITAS, Lídia Silva de; MARCONDES, Carlos Henrique; RODRIGUES, Ana Célia. **Documento**: gênese e contextos do uso. Niterói: Eduff, 2010. p. 175-192.

RONDINELLI, Rosely Curi. **O Conceito de documento arquivístico frente à realidade digital**: uma revisitação necessária. 2011. 270 f. Tese (Doutorado) - Curso de Ciência da Informação, Universidade Federal Fluminense, Niterói, 2011.

ROUSSEAU, Jean-Yves; COUTURE, Carol. **Os Fundamentos da disciplina arquivística**. Lisboa: Publicações Dom Quixote, 1998

SANTOS, H. M. D.; FLORES, D. O documento digital no contexto das funções arquivísticas. **Páginas A&B, Arquivos e Bibliotecas (Portugal)**, n. 5, p. 165-177, 2016. Disponível em: http://hdl.handle.net/20.500.11959/brapci/65458. Acesso em: 12 set. 2021.

SCHELLENBERG, T. R. **Arquivos modernos**. *Princípios e técnicas*. Rio de Janeiro: FGV, 1973. Traduzido em 2006 para o português, por Nilza Teixeira Soares - G.E. D – FGV.

SCOPEL, Eduardo Longhi; FIORESE, Breno Carra; CERVINSKI, Natan Susin; CARLESSO, Guilherme Cavalheiro; XAVIER, Nícolas Lamb; TISOTT, Priscila Bresolin; ZANANDREA, Gabriela; SILVA, Eduardo Robini da; CAMARGO, Maria Emilia. Importância da Segurança da Informação e Backup. In: MOSTRA DE INICIAÇÃO CIENTIFICA, PÓS-GRADUAÇÃO, PESQUISA E EXTENSÃO, 17., 2018, Caxias do Sul. **Anais [...] .** Caxias do Sul: Ucs, 2018. p. 1-10.

SÊMOLA, Marcos. **Gestão da segurança da informação**: visão executiva da segurança da informação. Rio de Janeiro: Elsevier, 2003.

SETZER, V.W. **Os Meios Eletrônicos e a Educação**: Uma Visão alternativa. São Paulo: Editora Escrituras, Coleção Ensaios Transversais Vol. 10, 2001.

SUGIMOTO, Shigeo; BAKER, Thomas; WEIBEL, Stuart L.. Dublin Core: process and principles. **Lecture Notes In Computer Science**, [S.L.], p. 25-35, 2002. Springer Berlin Heidelberg. http://dx.doi.org/10.1007/3-540-36227-4_3.

VIANEZ, Marcos de S.; SEGOBIA, Roberta H.; CAMARGO, Vander. Segurança de Informação: aderência à norma ABNT NBR ISO/IEC n. 17.799:2005. **Revista de Informática Aplicada**, São Caetano do Sul, v. 4, n. 3, p. 33-44, jan. 2008. Semestral. Disponível em: https://seer.uscs.edu.br/index.php/revista_informatica_aplicada/article/view/307. Acesso em: 24 maio 2021.

YINKA, Akintunde Michael. DATA AND INFORMATION SECURITY. In: 1ST INTERNATIONAL TECHNOLOGY, EDUCATION AND ENVIRONMENT CONFERENCE, 1., 2011, Omoku. **Proceedings [...]** . Paquistão: Human Resource Management Academic Research Society, 2011. p. 661-666. Disponível em: https://hrmars.com/index.php/pages/detail/Proceeding2. Acesso em: 25 maio 2021.

WHITMAN, Michael E.; MATTORD, Herbert J.. **Principles of Information Security**. 4. ed. Boston: Course Technology, 2012. 658 p.