UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE GRADUAÇÃO EM ARQUIVOLOGIA

VÁLBER HERMÍNIO CAETANO

GESTÃO DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS: SEGURANÇA PROPORCIONADA PELA CRIPTOGRAFIA, ASSINATURA DIGITAL E CERTIFICAÇÃO DIGITAL

JOÃO PESSOA - PB
2017

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE GRADUAÇÃO EM ARQUIVOLOGIA

VÁLBER HERMÍNIO CAETANO

GESTÃO DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS:
SEGURANÇA PROPORCIONADA PELA CRIPTOGRAFIA, ASSINATURA DIGITAL E CERTIFICAÇÃO DIGITAL

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Arquivologia do Centro de Ciências Sociais Aplicadas da Universidade Federal da Paraíba como requisito parcial para obtenção do grau de bacharel.

Orientador: Profo. Me. Luiz Eduardo Ferreira da Silva.

JOÃO PESSOA - PB
2017

Dados Internacionais de Catalogação na Publicação (CIP)

H551g Hermínio Caetano, Válber.

GESTÃO DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS: Segurança proporcionada pela criptografia, assinatura digital e certificação digital / Válber Hermínio Caetano. — João Pessoa, 2017.

31 f.

Orientador(a): Prof° Msc. Luiz Eduardo Ferreira da Silva. Trabalho de Conclusão de Curso (Arquivologia) — UFPB/CCSA.

1. Criptografia. 2. Gestão documental. 3. Documentos digitais. 4. Segurança da Informação. I. Título.

UFPB/CCSA/BS CDU:930.25(043.2)

Gerada pelo Catalogar - Sistema de Geração Automática de Ficha Catalográfica do CCSA/UFPB, com os dados fornecidos pelo autor(a)

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE GRADUAÇÃO EM ARQUIVOLOGIA

VÁLBER HERMÍNIO CAETANO

GESTÃO DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS: SEGURANÇA PROPORCIONADA PELA CRIPTOGRAFIA, ASSINATURA DIGITAL E CERTIFICAÇÃO DIGITAL

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Arquivologia do Centro de Ciências Sociais Aplicadas da Universidade Federal da Paraíba como requisito parcial para obtenção do grau de bacharelado.

Aprovado em: 12 / 04 /2017.

BANCA EXAMINADORA

Profo. Me. Luiz Eduardo Ferreira da Silva
(Orientador – DCI/UFPB)

Profa. Ma. Maria Meriane Vieira rocha
(Examinadora – DCI/UFPB)

Profa. Ma. Vanessa Alves Santana
(Examinadora – DCI/UFPB)

GESTÃO DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS: Segurança proporcionada pela criptografia, assinatura digital e certificação digital

Válber Hermínio Caetano[1]

RESUMO

Apresenta um estudo teórico bibliográfico do processo de gestão documental com foco na segurança da informação arquivística através de métodos de criptografia, assinatura digital e certificação digital na proteção de documentos em suporte digital. A necessidade desse estudo surgiu a partir da percepção da deficiência dos graduandos em arquivologia da UFPB quanto ao tema em pauta. Objetiva mostrar o nível de segurança e autenticidade das informações proporcionado pela criptografia, assinatura digital e certificação digital em documentos arquivísticos de suporte digital e qual a contribuição dessas ferramentas para a arquivologia. Buscou-se dados de como surgiu à criptografia e como ela pode ser utilizada em conjunto com outras ferramentas para ajudar na proteção da informação na arquivística, passando pelos tipos de criptografias usadas, destacando seus pontos fortes e suas fraquezas, tentando assim mostrar qual melhor algoritmo se encaixa em sua necessidade. Também apresenta uma visão normativa através da análise da ISO 15489 e o e-ARQ que dispõem das informações necessárias para a implantação de um sistema informatizado de gestão de documentos digitais. Esse estudo mostrou que as ferramentas de proteção à informação aqui em pauta vieram para somar e trouxeram inúmeros benefícios ao campo da arquivologia.

Palavras-chave: Criptografia. Gestão documental. Documentos digitais. Segurança da Informação.

[1] Válber Hermínio Caetano, Graduando do curso de Bacharelado em Arquivologia pela Universidade Federal da Paraíba – UFPB. E-mail: valberhe@gmail.com

1 INTRODUÇÃO

A evolução da tecnologia melhorou o fluxo de documentos e aumentou a celeridade dos trabalhos nas repartições públicas e privadas, em contrapartida facilitou também os trabalhos de falsificação, os tornando cada vez mais “idênticos” aos originais. Na área de segurança da informação e documentação surge a criptografia digital como método que garante a autenticidade do documento e que mantém as características originais, pois nenhum documento criptografado pode ser modificado sem que sua autenticidade seja alterada, isso garante segurança aos portadores e receptores.

De forma geral, criptografia significa a utilização de uma técnica de camuflagem da mensagem que está sendo transmitida, com o propósito de garantir que apenas o destinatário e o remetente possuam conhecimento do teor desta mensagem através da utilização de uma chave secreta de decriptação. Em conformidade com a Câmara Técnica de Documentos Eletrônicos (2006, p. 81) que conceitua criptografia como “um método de codificação de objetos digitais segundo um código secreto (chave), de modo que estes não possam ser apresentados por uma aplicação de forma legível ou inteligível e somente usuários autorizados podem restabelecer sua forma original”.

Diante da percepção da deficiência que os graduandos em arquivologia da Universidade Federal da Paraíba - UFPB possuem quanto ao tema Gestão documental voltado à proteção de arquivos em suporte digital através da criptografia, certificação digital e assinatura digital surgiu a necessidade de discutir-se mais sobre esse tema. Numa tentativa de explanar esta temática, buscou-se retratar os benefícios que as ferramentas tecnológicas de proteção à informação trouxeram para a área de segurança da informação e, consequentemente, para a arquivologia. Fez-se um link entre essas ferramentas e os sistemas informatizados de gestão arquivística de documentos que, dentre suas características, também é proporcionar maior proteção às informações. Diante disso, buscou-se informações para responder aos seguintes problemas: os documentos criptografados são realmente seguros? O que impede que uma terceira pessoa altere a autenticidade do documento criptografado?

A fim de responder às atuais questões este trabalho se propôs ao seguinte objetivo Geral, mostrar o nível de segurança proporcionado pela criptografia, assinatura digital e certificação digital em documentos arquivísticos de suporte digital e qual a contribuição dessas ferramentas para a arquivologia. Quanto aos objetivos

específicos buscou-se retratar a importância de um SIGAD para a segurança da informação arquivística; Mostrar como a certificação digital e a criptografia podem proporcionar maior proteção aos documentos arquivísticos.

Levando em consideração que nas últimas décadas o crescimento da informação digital foi surpreendente, no intuito de acompanhar esse ritmo várias áreas do conhecimento vêm se aperfeiçoando, principalmente a de Tecnologia da Informação (TI). Os documentos digitais tornam-se cada vez mais seguros com o uso dos algoritmos criptográficos. Para tanto, este trabalho justifica-se pela possibilidade de despertar o interesse dos graduandos em arquivologia em conhecer melhor as ferramentas tecnológicas que auxiliam na proteção da informação, e que podem ser utilizadas como mais um elemento no processo de gestão documental.

Para o desenvolvimento do presente trabalho foram utilizadas pesquisas bibliográficas. A pesquisa bibliográfica baseou-se em publicações científicas realizadas através de levantamentos de referências teóricas já analisadas e publicadas por meios escritos e eletrônicos, que segundo Moresi (2003, p.10):

> É o estudo sistematizado desenvolvido com base em material publicado em livros, revistas, jornais, redes eletrônicas, isto é, material acessível ao público em geral. Fornece instrumental analítico para qualquer outro tipo de pesquisa, mas também pode esgotar-se em si mesma. O material publicado pode ser de fonte primária ou secundária[...]

Segundo Demo (2000, p. 20), “a pesquisa teórica se configura em um método dedicado a reconstruir teoria, conceitos, ideias, ideologias, tendo em vista, em termos imediatos, aprimorar fundamentos teóricos”.

Quanto à abordagem, fez-se uso do método qualitativo, tipo de pesquisa onde se busca aprofundar-se na compreensão dos fenômenos que se estudam as ações dos indivíduos, grupos ou organizações em seu ambiente e contexto social, interpretando-os segundo a perspectiva dos participantes da situação enfocada, sem se preocupar com representatividade numérica, generalizações estatísticas e relações lineares de causa e efeito.

O seguinte artigo está estruturado em oito capítulos: um breve conceito sobre segurança da informação e a história da criptografia; definições e conceitos fundamentais de documentos; a segurança da informação na Arquivística: um olhar na ISO 15489 e no E-ARQ Brasil; Câmara Técnica de Documentos Eletrônicos-CTDE; gestão arquivística de documentos; ged versus segurança da informação;

ferramentas de proteção à informação: certificação digital - certificado digital x assinatura digital e por fim, as contribuições da criptografia e certificação digital para a arquivologia.

2 BREVE CONCEITO SOBRE SEGURANÇA DA INFORMAÇÃO E A HISTÓRIA DA CRIPTOGRAFIA

Pode-se dizer que a informação se constitui em matéria prima para tomada de decisões essenciais em qualquer setor das repartições públicas ou privadas, por isso que é plausível que exista debates sobre essa temática, segurança da informação. A partir disso será possível entender a relevância de proteger o que é importante, pois sua ausência poderá ocasionar prejuízos, financeiros, administrativos, jurídicos, culturais entre outros. Nesse contexto, segundo a Associação Brasileira de Normas Técnicas (2002), NBR ISO/IEC 17799, o aglomerado de dados é irrelevante quando estes não passam pelo processo de interpretação para que seja aproveitado algum conhecimento relevante. Sabendo-se quão valiosa é a informação, ela deve ser tratada como um ativo da empresa, sendo a essa dispensada à mesma importância que se dispensa aos bens palpáveis. Segundo Sprouse&Moonitz (1962, ARS n.3) "Ativos representam benefícios esperados, direitos que foram adquiridos pela entidade como resultado de alguma transação corrente passada".

Segundo Oliveira (1992, p. 34) diz que "informação é o dado trabalhado que permite ao executivo tomar decisões", então podemos inferir que a informação é a interpretação desses dados. Partindo desta premissa, é plausível considerar a informação como um ativo institucional cuja sua gestão e controle são medidas de prevenção tomadas pelo gestor de segurança da informação que visa gerir e controlar o acesso de funcionários, bem como definir o que cada profissional pode acessar de informação da empresa.

Segundo Wadlow (2000, p.53), “a segurança deverá ser proporcional ao valor do que está se protegendo”. A segurança da informação chegou com o propósito de proteger as informações registradas, sem se importar onde estejam situadas: impressas em papel, nos discos rígidos dos computadores ou até mesmo na memória das pessoas que as conhecem. O Decreto nº 3505, de junho de 2000, define segurança da informação da seguinte forma:

> Proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou trânsito, abrangendo, inclusive, a segurança, dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças e seu desenvolvimento. (BRASIL, 2000).

Através da modernização tecnológica no transporte, armazenamento e manipulação dos dados e informações as empresas tornaram-se mais ágeis, mas, ao mesmo tempo, tais modernizações trouxeram consigo novos riscos, tais como: Ataques de Crackers (Black hat hackers), de engenharia social, vírus, worms, negação de serviço e espionagem eletrônica são noticiadas pela imprensa frequentemente. Perante esta situação, a segurança da informação torna-se indispensável às organizações, sejam elas do setor público ou privado. A criptografia é uma ferramenta que há tempos faz parte da história humana, uma vez que sempre houve fórmulas secretas e informações confidenciais que não poderiam nem deveriam ser expostas ao público ou na mão de pessoas “erradas”.

Segundo Kahn (1967, p.65), em 1900 a. c. houve o primeiro contato do ser humano com a criptografia, esse contato ocorreu no Egito, através do arquiteto Khnumhotep II responsável por criar os monumentos do faraó Amenemhet II. O faraó armazenava uma quantidade indeterminada de tesouros, cujo trajeto para localizá-los era documentando em tabletes de argila, nem precisa dizer que, consequentemente, eles precisavam ser criptografados evitando assim que ladrões saqueassem a tumba, foi aí que:

> [...]O escriba de Khnumhotep II teve a ideia de substituir algumas palavras ou trechos de texto destes tabletes. Caso o documento fosse roubado, o ladrão não encontraria o caminho que o levaria ao tesouro - morreria de fome, perdido nas catacumbas da pirâmide. Pode ser considerado o primeiro exemplo documentado da escrita cifrada (FRANÇA, 2005,p. 2.).

Em 50 a.C, Júlio César utilizou sua cifra de substituição para criptografar comunicações governamentais. Ele modificou letras trocando-as em três posições; A por D, B por E etc. Até hoje o código de César é o único da Antiguidade ainda utilizado. Por isso, atualmente, qualquer cifra baseada na substituição cíclica das letras do alfabeto denomina-se código de César. Embora seja simples (ou exatamente por ser), esse método foi utilizado pelos oficiais na Guerra de Secessão americana e pelo exército russo em 1915. A comunicação sem fio teve início 14 anos antes da primeira utilização do código César de cifragem, no ano de 1901, apesar dos benefícios

trazidos pela comunicação de longa distância sem o uso de fios ou cabos, o sistema é aberto o que aumenta o desafio da criptologia em proteger a informação. Em 1921, Edward Hugh Hebern fundou a Hebern Electric Code, uma empresa produtora de máquinas de cifragem eletromecânicas baseadas em rotores que giram a cada caractere cifrado (TKOTZ, 2005).

Portanto, pode-se perceber o quão antigo é a técnica de criptografar, e que apesar da evolução da tecnologia proporcionar o seu aperfeiçoamento, não mudou sua essência e seu objetivo principal: garantir a segurança e inviolabilidade de informações importantes. Para a arquivologia a criptografia documental figura como sendo uma ferramenta essencial no apoio a proteção dos documentos arquivísticos digitais dentro de um sistema informatizado de gestão documental, uma vez que se deve considerar que uma das propostas da gestão documental é garantir a integridade do documento até a sua destinação final.

2.1 O Que é Criptografia?

A palavra criptografia vem do grego kryptos, oculto, e graphein, escrita. Há muitos relatos de possíveis modos de codificar/cifrar mensagens como mecanismos de segurança. Segundo Fubah (2010) em 1500 a. c. a criptografia na Mesopotâmia estava bem avançada com relação à criptografia egípcia. A criptografia para a Câmara Técnica de Documentos Eletrônicos (2006, p. 81) “é um método de codificação de objetos digitais segundo um código secreto (chave), de modo que estes não possam ser apresentados por uma aplicação de forma legível ou inteligível e somente usuários autorizados podem restabelecer sua forma original”. Portanto, pode-se inferir que criptografar significa se utilizar de uma técnica de camuflagem da mensagem que está sendo transmitida, com o propósito de garantir que apenas o destinatário e o remetente possuam conhecimento do teor desta mensagem através da utilização de uma chave secreta de decriptação.

O nível de segurança da criptografia é medido em bits, quanto mais bits, mais forte é a criptografia. Sendo assim, destacamos os 3 tipos de criptografia, vamos começar falando sobre a criptografia Hash, que é responsável por pegar dados de qualquer tamanho e transformá-lo em dados de tamanho fixo, que é chamado de valor de Hash e, geralmente, é formado por 16 ou 20 bytes. O primeiro registro encontrado

de tal codificação foi de uma fórmula de esmaltes para cerâmica, que foi encontrada às margens do rio Tigre em um tablete de argila que continha símbolos que podiam ter inúmeros significados. Algumas dúvidas surgiram sobre a veracidade de alguns supostos métodos de proteger mensagens,

> Se é que realmente existiu, o scytalae espartano ou bastão de Licurgo era um bastão de madeira ao redor do qual se enrolava firmemente uma tira de couro ou pergaminho, longa e estreita. Escrevia-se a mensagem no sentido do comprimento do bastão e, depois, desenrolava-se a tira com as letras embaralhadas (FUBAH, 2010, p. 1.).

A criptografia é usada desde os primórdios da humanidade, isso já foi exposto, mas o que poucos sabem é que ela teve um papel fundamental nas guerras travadas durante toda nossa história, a fim de proteger as mensagens, caso fossem interceptadas pelo inimigo, os exércitos começaram a proteger suas mensagens codificando-as, um bom exemplo disso foi o uso da Enigma pelo exército Alemão em 1926.

> Desenvolvida por Arthur Scherbius em 1918, a Enigma levantou um grande interesse por parte da marinha de guerra alemã em 1926, quando passou a ser usado como seu principal meio de comunicação e ficaram conhecidas como Funkschlüssel [...] "(CASTELLÓ, 2012, p. 2.).

Em 1928, o exército viu, que a Enigma era um bom meio de proteger sua comunicação de inimigos que pudessem interceptá-las, sendo assim, foi criada uma versão exclusiva para o exército Alemão, que foi chamada de Enigma G e que, em pouco tempo, já estava sendo usada por todo ele, suas chaves eram trocadas mensalmente. Segundo Castelló (2013), a título de curiosidade, os aliados só conseguiram decifrar os códigos do enigma graças ao roubo de uma dessas máquinas, e que graças à engenharia reversa, foram construídas máquinas capazes de ler e codificar os códigos alemães, os Colossus. A criptografia foi fortemente usada para vários fins, principalmente durante épocas de guerra onde a segurança das mensagens transmitidas entre os soldados era de vital importância

> [...] tal como durante a Guerra Fria, onde Estados Unidos e União Soviética usaram esses métodos a fim de esconder do inimigo suas ações e movimentações, criptografando-as e impedindo que outros que não possuíssem a chave pudessem ler, forçando-os a usar diversos métodos para quebrar os códigos de criptografia (CASTELLÓ, 2012, p. 2.).

Assim, vários tipos de criptografia foram surgindo com o decorrer do tempo, tanto por chave simétrica, chave assimétrica ou por Hash. Atualmente, a criptografia é comumente usada na internet, principalmente na proteção de transações financeiras, em segurança e acesso em comunicação. Com o uso da internet surgiram novas aplicações como o comércio eletrônico e o home-banking. Nestas aplicações, informações confidenciais como cartões de crédito, transações financeiras, etc. são enviadas e processadas em meios não confiáveis. Enquanto meios de comunicações suficientemente seguros para proteger este tipo de informação não surgem, a criptografia aparece como uma boa alternativa para proteção de dados. Com a criptografia e assinatura digital, três características importantes para segurança de informações são alcançadas. São elas: Privacidade: Proteger contra o acesso de intrusos; Autenticidade: Certificar-se de que, quem é o autor de um documento é quem diz ser; Integridade: Proteger contra modificação dos dados por intrusos.

2.2.1 Tipos de Criptografía

Basicamente existem dois tipos de criptografia, a de chave simétrica, onde a cifragem e decifragem são feitos com uma única chave, ou seja, tanto quem envia quanto quem recebe a mensagem usam a mesma chave. No entanto, esse tipo de criptografia possui suas desvantagens, pois em algoritmos simétricos, como, por exemplo, o DES (Data Encription Standard), existe o “problema de distribuição de chaves”. Considerando que a chave de decifragem é a mesma que foi utilizada para cifrar, a chave tem de ser enviada para todos os usuários autorizados, e essa ação resulta num atraso de tempo e possibilita que a chave chegue a pessoas não autorizadas. O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), afirma que:

> Uma mensagem codificada por um método de criptografia deve ser privada, ou seja, somente aquele que enviou e aquele que recebeu devem ter acesso ao conteúdo da mensagem. Além disso, uma mensagem deve poder ser assinada, ou seja, a pessoa que a recebeu deve poder verificar se o remetente é mesmo a pessoa que diz ser e ter a capacidade de identificar se uma mensagem pode ter sido modificada.

Com a chegada da criptografia assimétrica o problema da distribuição de chaves foi resolvido mediante o uso de chaves públicas. Neste novo sistema, cada

usuário autorizado possui um par de chaves denominado chave pública e chave privada, sendo que a chave pública é divulgada, já a chave privada é mantida em segredo. Se uma pessoa quiser enviar uma mensagem privada, o transmissor cifra a mensagem usando a chave pública do destinatário pretendido, que deverá usar a sua respectiva chave privada para conseguir recuperar a mensagem original.

3 DEFINIÇÕES E CONCEITOS FUNDAMENTAIS: Documento x Documento arquivístico

Entender o conceito de documento e suas características é fundamental, principalmente no mundo arquivístico, onde o manuseio e o lidar com diversos tipos de documentos, dos mais diversos suportes, são constantes.

Para o Dicionário Brasileiro de Terminologia Arquivística (2005, p.73), “documento é a unidade de registro de informações, qualquer que seja o formato ou o suporte”. Numa visão complementar, Gomes (1967, p. 5) informa que o documento é considerado “[...] peça escrita ou impressa que oferece prova ou informação sobre um assunto ou matéria qualquer”. Podemos entender, então, nitidamente, que os conceitos de documento apresentados acima se atrelam a materiais palpáveis que de certa forma são registrados. Tão importante quanto conhecer o conceito de documento de uma forma mais ampla, é conhecer o conceito e as características de documento arquivístico para que assim se abre a possibilidade de enxergar os pontos que marcam as diferenças entre os dois tipos.

Segundo o CONARQ (2006), todo documento produzido e recebido no decorrer das atividades de um órgão ou entidade, independentemente do suporte em que se apresentem, registram suas políticas, funções, procedimentos e decisões. Por isso, o CONARQ estabelece que só serão reconhecidos como documentos arquivísticos aqueles que conferem aos órgãos e entidades a capacidade de:

- Conduzir as atividades de forma transparente, possibilitando a governança e o controle social das informações;
- Apoiar e documentar a elaboração de políticas e o processo de tomada de decisão;
- Possibilitar a continuidade das atividades em caso de sinistro;
- Fornecer evidência em caso de litígio;
- Proteger os interesses do órgão ou entidade e os direitos dos funcionários e

dos usuários ou clientes;

- Assegurar e documentar as atividades de pesquisa, desenvolvimento e inovação, bem como a pesquisa histórica;
- Manter a memória corporativa e coletiva.

Logo é perceptível que há uma obrigatoriedade de que para um documento comum ser considerado um documento de arquivo ele precisa estar ligado direto ou indiretamente à atividade que o gerou e tal fato lhe remete a outros pontos essenciais, que são as características singulares, tais quais segundo Bellotto (2006, p.35-43), são “unicidade, organicidade, indivisibilidade, Integridade, autenticidade e heterogeneidade de seu conteúdo”.A partir da análise das informações anteriores pode-se inferir que qualquer documento, seja ele emitido por pessoa física ou jurídica, será considerado documento de arquivo desde que mantenham um elo com a atividade que o gerou, elo esse, que lhe atribui algumas características únicas e essenciais.

3.2 Documentoarquivístico digital

A globalização e o desenvolvimento da tecnologia estão fazendo com que os documentos em suporte tradicional (papel) aos poucos diminuam dando espaço ao aumento de documentos em outros suportes como os de plataforma digital. Tal fato aponta para um futuro onde grande parte dos documentos será criado, manuseado, acondicionado, tratado, ou seja, gerenciado - partindo para uma linguagem coloquial arquivística - através de programas e softwares de computadores, cabendo ao profissional arquivista ser preparado para tal evolução.

A formação do arquivista deve ser focada numa visão global acerca da documentação arquivística digital, ou seja, de modo a familiarizar-se com todas as ferramentas de criação e gestão de tais documentos, gestão num contexto amplo, desde como o documento deve ser criado, manuseado, preservado, disponibilizado para acesso, até sua destinação final, visando maior segurança e dando maior credibilidade às informações contidas em tais documentos de plataforma digital. Mas o que é documento arquivístico digital? Trata-se do documento digital reconhecido e tratado como um documento arquivístico, codificado em dígitos binários, acessível e interpretável por meio de sistema computacional, (CONARQ, 2011, p. 128). Pode-se

inferir, então, que as cadeias de bits que contêm dados de forma, de conteúdo formam a composição do documento digital.

Segundo Flores (2016, p.118), quando se refere à aparência e a composição de documentos digitais, não se pode esquecer seus ambientes custodiadores, pois é através das cadeias de custódia, dos ambientes de produção e preservação de documentos que se pode garantir a inalterabilidade dos documentos de arquivo. É fácil entender então, que a cadeia de custódia documental nada mais é que o ambiente no qual perpassa o ciclo de vida dos documentos. Em palavras mais simples, é através dela que se define o responsável por aplicar os princípios e as funções arquivísticas à documentação. Flores (2016, p.118)aponta ainda que é por meio de uma linha ininterrupta que se mantém a custódia confiável de documentos arquivísticos tradicionais, compreendendo-se as três idades do arquivo, quais são: corrente, intermediária e permanente. Sendo assim, é importante que se perceba que a credibilidade e confiança nas informações dos documentos é obtida através da qualidade dos serviços da própria instituição, pois é nesse espaço que acontece a produção, gestão, preservação e se provê acesso aos seus documentos.

4 A SEGURANÇA DA INFORMAÇÃO NA ARQUIVÍSTICA: um olhar na ISO 15489 e no E-ARQ Brasil

No meio arquivístico existem várias formas e suportes de registros de informação, a informação pode estar em suporte de papel, em meios eletrônicos (imagens, áudios ou vídeos), documentos impressos etc. Mas em qual suporte a informação está registrada é o que menos importa quando se está falando de segurança da informação, uma vez que, independentemente de onde esta esteja registrada ou difundida, o mais importante é que ela esteja segura, ou seja, recomenda-se a utilização de ferramentas e métodos que auxiliem adequadamente um sistema que vise proteger da melhor forma possível a informação. No entanto, Espirito Santo (2010, p.2) aponta que, infelizmente, na maioria das vezes não se é dispensada a importância necessária à informação e só conseguem perceber o quão ela é importante para o funcionamento da instituição quando a informação é destruída, perdida ou roubada.

Como forma e tentativa de evitar que tais situações aconteçam, principalmente

em arquivos com um vasto volume de informações, onde tais informações são de suma importância, portanto devem ser preservadas e difundidas, as instituições têm o dever de realizar ações que possibilitem o cuidado e principalmente a segurança das informações em âmbito arquivístico. Inquestionavelmente, a criação de um projeto estratégico de segurança da informação se faz necessário quando o assunto é garantir a integridade dos documentos de arquivos digitais, para isso, deve constar controles de acesso e métodos de segurança que garantam tal feito. Para conseguir manter os preceitos básicos de segurança e gestão da informação algumas normas essenciais devem ser obedecidas, vamos aqui nos pautar em duas, tais quais: ISO 15489, e-ARQ.

O controle de acesso também é citado nessas normas, que fazem referência a esse requisito esclarecendo que se adotado de forma eficaz e cuidadosa pode evitar vários danos à massa documental e à própria instituição. De acordo com o Instituto dos Arquivos Nacionais/Torre do Tombo (2000, p.47)

> O controle de acesso são regras das quais “as organizações têm de poder controlar quem está autorizado a aceder aos documentos de arquivo e em que circunstâncias o acesso é permitido, dado que os documentos podem conter informação pessoal, comercial ou operacionalmente sensível”

Sfreddo (2008) corrobora que para a segurança de informações arquivística, o controle de acesso é um dos fatores que contribuem para monitorar as ações realizadas na instituição e assim proteger as informações. Regulamentando esta mesma temática, apesar de se tratar de norma estrangeira, a ISO 15489-1 é bastante utilizada e pautada pelos profissionais do setor arquivístico nacional. No que se refere à gestão documental esta é a primeira norma criada com fins específicos e requisitos necessários para dar suporte a um sistema de gestão de documentos. Ela é dividida em duas partes, a primeira é composta pelos pressupostos gerais, tais como: os requisitos necessários para dar sustentação a um sistema de gestão de documentos, e a segunda parte, que abrange as diretrizes necessárias para a aplicação dos princípios citados na primeira.

5 CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS

A CTDE é formada por profissionais de várias áreas do conhecimento, ou seja,

tem uma formação multidisciplinar e tem como objetivo definir e apresentar ao Conselho Nacional de Arquivos normas, diretrizes, procedimentos técnicos e instrumentos legais sobre gestão arquivística e preservação dos documentos digitais, isto é, produzidos em formato digital, processados e armazenados por computador, em conformidade com os padrões nacionais e internacionais. E para subsidiar o desenvolvimento desses trabalhos desenvolve estudos e análises sobre as iniciativas internacionais e a literatura especializada

E uma das principais Normas internacionais que define como realizar a inserção de um programa de gestão documental é a ISO 15489 - estabelecendo que os documentos de arquivo devem apresentar as seguintes características (princípios) para uma maior credibilidade: autenticidade, confiabilidade, integridade e disponibilidade - Conforme a Norma citada, a implantação de uma política de gestão de documentos que permita gerar documentos autênticos deve ser precedida de uma conscientização por parte da instituição no que se refere a seus recursos, as atividades que desenvolve e de sua responsabilidade perante a sociedade e o usuário do arquivo, seja ele usuário interno ou externo.

Por tanto, a norma ISO 15489 é de grande relevância para o contexto arquivístico uma vez se refere a uma ferramenta de grande valor para qualquer profissional desta área do conhecimento que pretenda intervir ativamente na gestão documental, além de prestar uma contribuição significativa para o aumento da eficiência e credibilidade organizacional.

> Credibilidade de um documento arquivístico enquanto uma afirmação do fato. Existe quando um documento arquivístico pode sustentar o fato ao qual se refere, e é estabelecida pelo exame da completeza da forma do documento e do grau de controle exercido no processo de sua criação (CONARQ, CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS, 2011).

Através do desenvolvimento de um processo de Gestão documental a instituição está se resguardando não apenas quanto à guarda e a preservação das informações documentais, mas também no controle e prevenção das ameaças e risco de furto, de falsificações documentais e outros procedimentos que coloquem em temeridade a confiabilidade das informações que serão recebidas pelos usuários. Quando uma instituição arquivística, produtora ou mantenedora de acervos documentais, cria mecanismos de ações para robustecer a segurança do acervo documental ela está garantindo a sua própria segurança institucional.

> Considera-se gestão documental o conjunto de procedimentos e operações técnicas referentes à sua produção, tramitação, uso, avaliação e arquivamento em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente (BRASIL, 1991).

A gestão de documentos traz inúmeros benefícios à instituição, tais como: organização e a recuperação dos documentos produzidos e recebidos controlando o fluxo da massa documental, esses procedimentos são muito importantes, pois evita o acúmulo de documentos desnecessários que causam a obstrução do espaço físico do arquivo, independentemente da plataforma, obstruções essas que podem se tornar um risco aos princípios da segurança da informação. Segundo o e-ARQ para que seja garantido que os princípios daconfidencialidade, integridade e disponibilidade sejam mantidos, o sistema de gestão arquivística de documentos deve estabelecer três requisitos, quais sejam: controle de acesso, trilhas de auditoria e cópias de segurança.

Partindo do princípio de que o controle de acesso se constitui como um dos componentes que contribuem para a segurança da informação em uma instituição, tal componente, segundo o e-ARQ (2006) deve estabelecer algumas garantias mínimas, como:

- Restrição de acesso aos documentos;
- Exibição dos documentos, criptografados ou não, e dos metadados somente aos usuários autorizados;
- Uso e intervenção nos documentos somente pelos usuários autorizados.

Tal restrição de acesso é muito importante para que se mantenha o documento inalterado, pois o manuseio dos documentos por usuários despreparados, no sentido mais amplo da palavra – tecnicamente despreparado oumal-intencionado quanto ao uso das informações contidas nos referidos documentos – pode desencadear vários problemas para a instituição.

> e-ARQ é uma especificação de requisitos que estabelece um conjunto de condições a serem cumpridas pela organização produtora/recebedora de documentos, pelo sistema de gestão arquivística e pelos próprios documentos a fim de garantir a sua confiabilidade e autenticidade, assim como seu acesso (CONARQ, CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS, 2006, p.5).

Portanto, percebe-se o quão importante é o papel do e-ARQ Brasil dentro do processo de gestão documental, pois são através deste que surgem as especificações e condições que devem ser cumpridas pelas instituições produtoras/recebedoras de

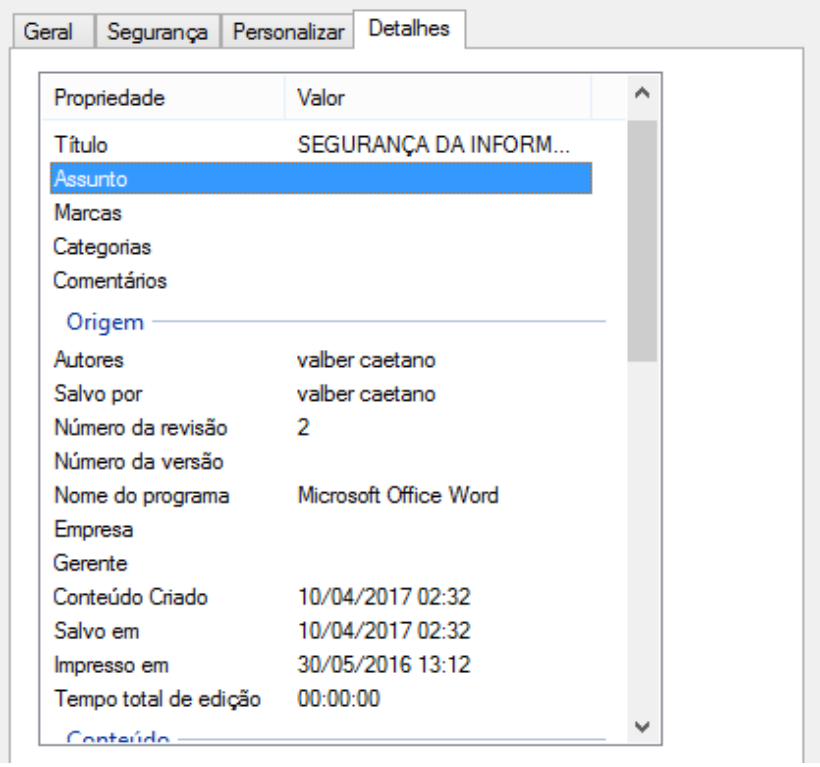
documentos, especificações estas que visam garantir que as informações são confiáveis, autênticas e, principalmente, que o acesso a elas será garantido, com certo nível de controle, ao longo do tempo. O CONARQ através de sua CTDE indica que o controle do acesso pode ser feito por meio do cadastro dos usuários (identificador de usuário), crachá de identificação (credenciais de autenticação) ou até mesmo pela restrição do espaço do acervo a uso exclusivo dos funcionários autorizados (autorização de acesso).

Todavia, não se pode lembrar controle de acesso e esquecer-se de classificação da informação quanto ao seu grau de sigilo, pois a seleção e restrição do acesso se darão a partir das informações obtidas desse processo de classificação. Uma vez que esse processo de classificação tem o objetivo de definir qual o grau de sigilo que possui cada documento arquivístico. Que são três, conforme a lei de acesso à informação, BRASIL lei 12.527, de 18 de novembro de 2011: Ultra-secreta, que possui prazo de restrição de acesso de 25 anos; Secreta: com prazo de restrição de acesso de 15 anos; e reservada que deve ser mantida sobre restrição de acesso por um período de 5 anos. Nesses casos de documentos cujo grau de sigilo não permite o acesso ostensivo, as instituições devem atentar e redobrar os cuidados quanto ao acesso.

Ainda sobre controle de acesso, segundo Flores, Sfreddo (2012), a Norma ISO 15489-1, em resumo, relata que as instituições devem criar normas ou regras formalizadas que direcionem as restrições, permissões e condições de acesso às informações. Além disso, o sistema de controle de acesso deve conter mecanismos de restrição de acesso não apenas aos usuários externos, mas também aos internos (funcionários) e tais níveis de acesso devem ser revisados periodicamente, podendo variar conforme o tempo, para que a segurança da informação seja garantida.

Quanto a Trilha de auditoria, é o conjunto de informações registradas que permite o rastreamento de intervenções ou tentativas de intervenção no documento arquivístico digital ou no sistema computacional (SIGAD), portanto, a trilha de auditoria deve registrar o movimento e o uso dos documentos arquivísticos dentro de um SIGAD (captura, registro, classificação, indexação, arquivamento, armazenamento, recuperação da informação, acesso e uso, preservação e destinação), informando quem operou a data e a hora, e as ações realizadas.

Exemplo de trilha de auditoria



Fonte: Microsoft office WORD, 2016.

A trilha de auditoria tem o objetivo de fornecer informações sobre o cumprimento das políticas e regras da gestão arquivística de documentos do órgão ou entidade (CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS, 2006).

6 GESTÃO ARQUIVÍSTICA DE DOCUMENTOS: SIGAD, GED E SEGURANÇA DA INFORMAÇÃO

A partir do entendimento do conceito de gestão documental pode-se criar um sistema de gestão arquivística de documentos que, segundo o e-ARQ (2006) “é o conjunto de procedimentos e operações técnicas cuja interação permite a eficiência e a eficácia da gestão arquivística de documentos”. Um programa de gestão documental, conforme orientações do e-ARQ Brasil, deve ser capaz de garantir que os documentos sejam confiáveis, acessíveis e compreensíveis. Portanto, os órgãos produtores e/ou mantenedores possuem a responsabilidade de garantir, através do processo de gestão arquivística de documentos que os arquivos produzidos sejam o reflexo fiel das suas atividades e que os documentos em fase permanente sejam devidamente recolhidos às instituições arquivísticas.

6.1Sistema Informatizado de Gestão Arquivística de Documentos – SIGAD

O Conselho Nacional de Arquivos (CONARQ), através de sua Câmara técnica de documentos eletrônicos, regulamenta aplicação do e-ARQ Brasil, recomendando adoção do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - SIGAD - é um software que foi desenvolvido para produzir, receber, armazenar, dar acesso e destinar documentos arquivísticos. Um SIGAD pode ser composto por software único ou vários softwares integrados, adquiridos ou encomendados. O CONARQ, através de sua Câmara Técnica de Documentos Eletrônicos, recomenda:

6.1.1 Um Sigad deve Abranger:

I· Documentos arquivísticos convencionais (analógicos),

II· Documentos arquivísticos digitais (convencionais ou dinâmicos, inclusive bancos de dados e páginas web).

Percebe-se que um SIGAD deve ser capaz de abranger os mais diversos tipos de documentos, seja ele codificado de forma analógica, como por ex.: os executáveis em aparelho de vídeo cassete ou filmadora; ou os codificados de forma digital caracterizado pela codificação em dígitos binários e acessado por meio de sistema computacional.

6.1.2 Quais as ações Básicas de um Sigad?

I· O registro das referências dos documentos convencionais, podendo incluir imagens digitalizadas,

II· A captura, armazenamento e promoção do acesso aos documentos digitais.

O registro e a captura dos documentos são ações fundamentais, que devem ser executadas pelo sistema informatizado de gestão documental através da incorporação de um documento ao sistema, que a partir daí passará seguir as rotinas de tramitação e arquivamento. O registro vem logo depois como forma de formalizar a captura do documento arquivístico através da atribuição de um número identificador

e de uma descrição informativa.

6.1.3 O Sigad possui algumas tarefas essenciais:

I· Captura, armazenamento, indexação e recuperação de todos os tipos de documentos arquivísticos e de todos os componentes digitais do documento arquivístico, como por exemplo um relatório com0 os anexos em diferentes arquivos;
II· Integração entre documentos digitais e não digitais;
III· Gestão dos documentos a partir do plano de classificação;
IV· Avaliação dos documentos e aplicação da tabela de temporalidade e destinação para recolhimento e preservação dos que tenham valor permanente;
V· Exportação dos documentos para transferência e recolhimento;
VI· Armazenamento seguro para garantir a autenticidade dos documentos;
VII· Instrumentos para gestão de estratégias de preservação dos documentos;
VIII· Implementação de metadados***** para descrever os contextos documentais:**[a]** jurídico administrativo; **[b]** de proveniência; **[c]** de procedimentos; **[d]** documental; **[e]** tecnológico.

Considerando as recomendações do CONARQ, através da câmara técnica de documentos eletrônicos, pode-se perceber que um SIGAD deve iniciar o processo de gestão documental desde a captura do documento, controlando todos os procedimentos meio, tais como: armazenamento, indexação, preservação etc., através da utilização de ferramentas de controle, sempre com o propósito principal de facilitar o processo de acesso e recuperação de todos os tipos de documentos arquivísticos de forma que garanta a segurança e a inviolabilidade dos documentos gerenciados.

No que se refere ao GED, primando pela interdisciplinaridade e com o intuito de tirar proveito da evolução tecnológica, trazendo-a para o campo da arquivística, especificamente para o da gestão documental, é de grande importância a instalação de um programa de Gerenciamento eletrônico de documentos, que o e-ARQ (2006) define como sendo o conjunto de tecnologias utilizadas para organização da informação não-estruturada de um órgão ou entidade, que pode ser dividido nas

seguintes funcionalidades: captura, gerenciamento, armazenamento e distribuição. As normas de gestão mais recentes já fazem referência a esse requisito, pois, quando adotado de forma eficaz e cuidadosa pode evitar vários danos à massa documental e à própria instituição.

Segundo Silva (2011), um sistema de Gerenciamento Eletrônico de Documentos (GED) desempenha um papel essencial quando se refere ao assunto segurança da informação documental, pois, tal sistema combina várias ferramentas em uma só plataforma, facilitando o armazenamento, o manuseio e uma rápida e eficiente recuperação de imagens e textos, além disso, pode-se restringir o tipo de acesso através da diferenciação das permissões para cada usuário num determinado documento, por exemplo: usuário 1 pode ter acesso para apenas visualização, usuário 2 pode ter acesso para visualização e impressão, enquanto o usuário 3 pode ter acesso completo, ou seja, além dessas funções tem acesso a edição do documento, contribuindo assim, demasiadamente, para uma maior segurança e confiabilidade da informação. Ainda como ferramenta que contribui para um maior nível de segurança da informação, o GED possui *workflow* integrado ao sistema de gerenciamento de documentos, isso significa um maior controle eletrônico das atividades do ciclo de vida dos documentos, porque através destes *workflows* pode-se, antecipadamente, estipular quem são os usuários que realizarão cada atividade e quais os prazos que cada um dispõe para conclui-las.

> Workflow é o conjunto de softwares e serviços que aplicados a uma estrutura de fluxo de trabalho, não somente para o movimento da informação, como também para a interação de processos de negócios e processos de trabalho humano que geram informação (CASONATO, 1995).

Normalmente, quando nos referimos a instituições que lidam com fluxo de trabalho, especificamente dos trabalhos e procedimentos executados pelos profissionais que atuam com documentos digitais, aqui se inclui os profissionais arquivistas, a tecnologia workflow ganha um espaço relevante. Não poderia ser diferente, pois, o workflow facilita muito e dar celeridade ao andamento do trabalho uma vez que permite que grupos de pessoas trabalhem ao mesmo tempo, de forma cooperativa, com o mesmo arquivo ou documento para que possam atingir o mesmo objetivo. Vale salientar ainda, que o sistema workflow possui distintos modelos entre si, de maneira que cabe identificar qual modelo se ajusta melhor às necessidades da instituição no que se refere ao trabalho arquivístico.

7 FERRAMENTAS DE PROTEÇÃO À INFORMAÇÃO: Certificação Digital - Certificado Digital X Assinatura Digital

Ainda há certa confusão quando o assunto é distinguir certificado digital de assinatura digital. Ambas são ferramentas utilizadas para proteger documentos eletrônicos, mas desempenham funções distintas dentro desse processo de proteção, vejamos: Através da definição dada pela Medida Provisória nº 2.200-2 de 2001, deve-se entender que certificado digital é um documento eletrônico assinado digitalmente por uma autoridade certificadora, e que contém diversos dados sobre o emissor e o seu titular, deve ficar claro também que a função precípua do certificado digital é a de vincular uma pessoa ou uma entidade a uma chave pública. Já a assinatura digital é uma modalidade de assinatura eletrônica, resultado de uma operação matemática que utiliza algoritmos de criptografia assimétrica e permite constatar, com segurança, a origem e a integridade do documento. Infere-se que certificado digital e assinatura digital são elementos que compõem a certificação digital e possuem como base a criptografia, técnica que codifica dados, e a união desses dois elementos proporciona a comprovação da identidade de uma pessoa ou site, ou seja, dar mais segurança e evita fraudes de documentos eletrônicas. Reforçando tais explicações conceituais e objetivas através de autores conceituados, pode-se dizer que:

> Certificação Digital é um conjunto de técnicas e processos que propiciam mais segurança às comunicações e transações eletrônicas, permitindo também a guarda segura de documentos.
> Permite que informações transitem pela Internet com maior segurança. É baseada na existência de Certificados Digitais emitidos por uma Autoridade Certificadora (AC), considerada confiável pelas partes envolvidas. (Silva, AT EL., 2008 p.X) Garantindo o conteúdo de mensagens ou textos, sua autoria e data em que foi assinada. Baseia-se no princípio da terceira parte confiável, que oferece confiabilidade entre partes que se utilizem de Certificados Digitais. Para isso utiliza-se de uma Infra-estrutura de chaves públicas, cuja principal função é definir técnicas e procedimentos.
> A Medida Provisória 2.200-2, de agosto de 2001 estabelece a Infra- estrutura de Chaves públicas Brasileira – ICP-Brasil (SILVA at el., 2008, p.XII).

Os documentos eletrônicos recebem a aprovação da Secretaria da Receita Federal através de inúmeras ferramentas de segurança e passam pela fiscalização do Governo Federal por meio do Instituto de Tecnologia da Informação e do Instituto de Chaves Públicas do Brasil, com o intuito de assegurar a confiabilidade do sistema. Para isso, a emissão do certificado digital deverá ser realizada por uma autoridade de certificação (AC), através de assinatura com sua chave privada. Os certificados digitais devem dispor de algumas informações essenciais sobre seu proprietário, tais

como: A Chave Pública do proprietário, O nome do proprietário, A data de vencimento da Chave Pública, Nome do emissor (a AC que emitiu a Identificação Digital), O número de série da Identificação Digital e A assinatura digital do emissor.

8 CONTRIBUIÇÕES DA CRIPTOGRAFIA E CERTIFICAÇÃO DIGITAL PARA A ARQUIVOLOGIA

Essa avalanche de crescimento de documentos nesse novo formato, digital, principalmente nas repartições públicas, despertou na arquivologia a necessidade de incorporar e conhecer melhor as ferramentas utilizadas para proteger este tipo de documento. Sabe-se que, legalmente, a assinatura digital garante a autenticidade e a integridade das informações em documentos digitais, no entanto, sob a ótica da arquivística e da diplomática, a autenticidade dos documentos não depende apenas da assinatura, mas sim de todo um conjunto de elementos relacionados ao processo de produção e tramitação desse documento. Contudo, são inúmeros os benefícios trazidos pela tecnologia da informação, especificamente pelas ferramentas aqui em pauta, para a arquivologia, refletindo-se também em benefícios para a sociedade, logo abaixo uma pequena amostra:

<table>
<tr><td colspan="2">I - O avanço na garantia de segurança proporcionada aos documentos arquivísticosque contém informações de cunho particular:</td></tr>
<tr><td></td><td>● Comissões da Força Aérea Brasileira, nos Estados Unidos e em Londres utiliza o apoio da criptografia através da certificação digital para garantir mais segurança e otimização nos sistemas de licitações</td></tr>
<tr><td></td><td>● A Globo investe em tecnologia de certificação Digital para barrar a falsificação de documentos importantes.</td></tr>
<tr><td colspan="2">II - A celeridade na recuperação e disponibilização de informações de teor ostensivo ou particular pelas instituições públicas:</td></tr>
<tr><td></td><td>● A adoção da certificação digital do prontuário eletrônico de paciente pelo Hospital São Vicente de Paulo diminuiu o uso de papel e facilitou o acesso à informação.</td></tr>
<tr><td colspan="2">III - e o auxílio na desobstrução de arquivos compostos de documentos em suporte</td></tr>
</table>

de papel:
● *Com o uso da certificação digital, a telefônica elimina o consumo anual de 2,3 milhões de folhas de papel.*
● *Na Sul América Saúde, 1,1 milhão é o número de folhas de papel que esta instituição de saúde deixou de utilizar em 2010 com a certificação digital das apólices relativas a 85 prestadores de serviços.*

Fonte: ICP-Brasil, 2017.

Percebe-se através da ilustração da tabela anterior que tais ferramentas têm demonstrado eficácia no que se propõem a fazer, proteger e dar celeridade aos trâmites institucionais. Como informação complementar cabe saber que a própria Receita Federal do Brasil - RFB é um dos órgãos públicos federais que mais faz uso da certificação digital como alternativa para dar agilidade e comodidade ao contribuinte, além de proporcionar a garantia do sigilo das informações fiscais dos mesmos.

9 CONSIDERAÇÕES FINAIS

Tal estudo nos mostra que a tecnologia atual nos disponibiliza várias ferramentas eficazes de proteção à informação arquivística, principalmente aquelas em suporte digital. Constatou-se que os algoritmos de criptografia vêm evoluindo constantemente, com isso, assinatura digital e certificado digital, os documentos digitais podem ser considerados legítimos, pois se torna possível provar sua autenticidade, validando assim esses documentos diante de qualquer pessoa física ou jurídica. Os documentos digitais que estão criptografados não podem ser alterados sem que percam sua autenticidade, facilitando assim o trabalho do arquivista na hora de verificar se o documento é ou não legítimo.

Amparado pelos motivos expostos sugestiono a utilização da criptografia para aumentar o nível de segurança no processo de controle de acesso nos sistemas informatizados de gestão documental, pois se caracteriza como uma boa alternativa à proteção dos bancos de dados das informações sobre usuários e senhas, visto que, em caso de invasão do sistema os dados não serão decifrados. Cabe também a nós, futuros ou profissionais da informação, saber aproveitar tais ferramentas da melhor forma possível dentro de um sistema de gestão documental. Tal aproveitamento só será possível pelos graduandos em Arquivologia a partir de uma formação arquivística amparada por disciplinas e componentes curriculares atualizados conforme as novas tecnologias voltadas à segurança da informação em
suportes digitais.

A segurança desses documentos traz para nós arquivistas uma forma de diminuir o espaço físico do arquivo, pois quanto mais seguros estiverem os documentos digitais menos precisaremos de documentos físicos (papel), facilitando a organização do arquivo. Em tempos modernos, muitos estudiosos da área acham um ultraje dizer que os documentos em suporte de papel serão extintos e mostram diversos argumentos contra tal fato; Eu concordo! porém, ao meu ver, fica claro que a cada dia que passa os documentos digitais vem ganhando espaço e com a proteção desses documentos, feita por algoritmos de criptografia que além de proteger comprovam a autenticidade dos mesmos, fica visível que o futuro da arquivologia serão os arquivos híbridos com predominância dos documentos em suportes digitais, pois a viabilidade, comodidade e custo benefício que esses arquivos proporcionam ao usuário são bem superiores se comparado aos “arquivos tradicionais”.

MANAGEMENT OF DIGITAL ARCHIVAL DOCUMENTS: Security provided by encryption, digital signature and digital certification

[**GESTÃO DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS:** Segurança proporcionada pela criptografia, assinatura digital e certificação digital]

Valber Herminia Caetano[2]

ABSTRACT

The present paper is brought a bibliographic study about the process of document management. It focuses on archival information security, by means of methods of cryptography, digital signature and digital certification in the protection of documents on digital media. The need of this study emerged from the perception of the deficiency of Archival Science undergraduates of the UFPB in relation to the theme. It aims to show the level of security and authenticity of information that are proportioned by cryptography, digital signature and digital certification in archival documents of digital media and what is the contribution of these tools to Archival Science. It was looked for data about how cryptography has emerged and how it can be used together with other tools to help in the protection of archival information, passing by the types of cryptography that are used, highlighting their strengths and weaknesses, in order to try to show which algorithm is better according the need. The paper also presents a normative view by means of the analysis of the ISO 15489 and the e-ARQ, which have the needed information to the implementation of a computerized system of digital document management. This study showed that the tools of information protection above mentioned have come to add up and have brought innumerable benefits to the field of Archival Science.

Keywords: Cryptography. Document management. Digital documents. Information Security.

[2] Válber Hermínio Caetano, Graduando do curso de Bacharelado em Arquivologia pela Universidade Federal da Paraíba – UFPB. E-mail: valberhe@gmail.com

REFERÊNCIAS

ARQUIVO NACIONAL. **Dicionário Brasileiro de Terminologia Arquivística**. Rio de Janeiro: Arquivo Nacional, 2005. 232 p. (Publicações Técnicas; n 51).

ARQUIVO NACIONAL (Brasil) **Dicionário brasileiro de terminologia arquivística**. Rio de Janeiro, 2005, p.73.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS**. NBR ISO/IEC 17799**: Tecnologia da informação: código de prática para a gestão da segurança da informação. Rio de Janeiro, 2002.

BELLOTTO, Heloisa Liberalli. **Arquivos Permanentes:** tratamento documental. 4. ed. Rio de Janeiro: FGV, 2006. Cap.2, p.35-43.

BRASIL. Decreto nº 3.505, de 13 de junho de 2000. **Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal**. Poder Executivo, Brasília, DF, 26 jun. 2001. Seção 1, p. 1.

_____. Medida Provisória nº 2.200-2, de 24 de agosto de 2001. **Institui a infraestrutura de chaves públicas brasileiras – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências**. Brasília, DF, 2006. Disponível em: <https://www.planalto.gov.br/ccivil-03/MPV/Antigas-2001/2200-2.htm> . Acesso em: 17 fev. 2017.

CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS. **Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos**: e-ARQ. Rio de Janeiro: Conarq, 2006, p.81. Disponível em: <http://www.conarq.arquivonacional.gov.br/Media/publicacoes/ earqbrasilv1. pdf>. Acesso em: 26 abr. 2017

CASONATO, R. **Enterprise Work Management:** Myth or Reality? Part 1, Research Note, IDOM, KAWFL-136, Gartner Group, nov.1995.Disponível em: <http://www.ufrgs.br/gianti/files/artigos/1996/1996_041_PPGA_UFRGS.pdf> Acesso em: 16 fev 2017.

CASTELLÓ; Thiago in outros. **Assinatura Digital**. GTA/UFRJ. 2008. Disponível em: <http://www.gta.ufrj.br/grad/07_1/ass-dig/index.html> Acesso em: 10 abr. 2016.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **Modelo de requisitos para sistemas informatizados de gestão arquivística de documentos**. Câmara técnica

de documentos eletrônicos. E-ARQ, 2006. p. 5. Disponível em: <http://www.uel.br/cch/cdph/arqtxt/downloads_e_ARQ.pdf> Acesso em: 14 fev 2017.

DEMO, Pedro. **Metodologia do Conhecimento Científico**. São Paulo: Atlas, 2000.

ESPÍRITO SANTO, Adrielle Fernanda Silva do. **Segurança da Informação**. Departamento de Ciência da Computação - Instituto Cuiabano de Educação (ICE). Cuiabá – MT – Brasil, 2010. Disponível em: <http://www.ice.edu.br/TNX/storage/webdisco/2011/03/11/outros/2bc3b892c73868cf712dcf084ed96b8a.pdf>. Acesso em: 13 fev. 2017.

FLORES, D. **Cadeia de custódia digital de documentos arquivísticos**: do Sigad ao RDC-Arq. Brasília, DF: Instituto de Patrimônio Histórico e Artístico Nacional (Iphan), 2016, 122 slides, color, padrão.

FRANÇA, Waldizar Borges de Araújo. **Criptografia**. Universidade Católica de Brasília,DF, 2005. Disponível em: <http://www.ucb.br/sites/100/103/TCC/22005/WaldizarBorgesdeAraujoFranco.pdf>. Acesso em: 05 abr. 2016.

FUBAH, Felipe. **Criptografia**. Faculdade de Tecnologia de Taquaritinga. 2010. Disponivel em: <http://www.ebah.com.br/content/ABAAABeUMAI/criptografia> Acesso em: 05 abr. 2016.

GOMES, F. Araújo. **Arquivo e documentação**. Rio de Janeiro: [s.n.], 1967. p.5

INSTITUTO DOS ARQUIVOS NACIONAIS/TORRE DO TOMBO; INSTITUTO DE INFORMÁTICA – **Recomendações para a gestão de documentos de arquivo electrónicos:** contexto de suporte. Lisboa: Instituto dos Arquivos Nacionais/Torre do Tombo, 2000. p.47.

KAHN, David. **The Codebreakers, The Story of Secret Writing**. Abreviada peloautor. Nova Yorque: The Macmillan Company, 1967, P.65.

MORESI, Eduardo. **Metodologia da Pesquisa.** Universidade Católica de Brasília. 2003. p.10. Dísponivel em: <http://ftp.unisc.br/portal/upload/com_arquivo/1370886616.pdf>Acesso em: 11 abr. 2016

OLIVEIRA, Djalma de Pinho Rebouças de. **Sistemas de informações gerenciais**: estratégicas, táticas, operacionais. São Paulo: Atlas, 1992, P.34.

SFREDDO, Josiane Ayres. **O controle de acesso na percepção dos profissionais de arquivo:** uma questão de segurança das informações institucionais. Universidade Federal de Santa Maria, 2008.

SILVA, Edilberto M. **Políticas de Segurança e Planos de Continuidade de Negócios**: texto base da disciplina da Pós-Graduação Segurança da Informação FACSENAC/DF, 2011. Disponível em: <http://www.edilms.eti.br/?cat=44>. Acesso em: 24 fev. 2017.

SILVA, Luiz Gustavo Cordeiro da. et al. **Certificação Digital** – Conceitos e Aplicaçoes: Modelos Brasileiro e Australiano. Rio de Janeiro: Ciência Moderna, 2008.

SPROUSE, Robert T.; MOONITZ, Maurice. **A tentative set of broad accounting principles for business enterprises**.New York: AICPA, 1962.

TKOTZ, Viktória. **Criptografia**: segredos embalados para viagem. São Paulo: Novatec, 2005.

WADLOW, Thomas. **Segurança de Redes.** Rio de Janeiro: Campus, 2000.