UNIVERSIDADE FEDERAL DA PARAÍBA

CENTRO DE CIÊNCIAS SOCIAIS APLICADAS

CURSO DE GRADUAÇÃO EM ARQUIVOLOGIA

KAWAN DE SOUZA PACOTE

DOCUMENTOS ARQUIVÍSTICOS DIGITAIS: Métodos para uma eliminação segura

JOÃO PESSOA
2015

KAWAN DE SOUZA PACOTE

DOCUMENTOS ARQUIVÍSTICOS DIGITAIS: Métodos para uma eliminação segura

Artigo apresentado ao Curso de Graduação em Arquivologia, da Universidade Federal da Paraíba como requisito parcial para a obtenção do título de Bacharel em Arquivologia, sob orientação do Prof. Dr. Wagner Junqueira de Araújo.

JOÃO PESSOA
2015

KAWAN DE SOUZA PACOTE

DOCUMENTOS ARQUIVÍSTICOS DIGITAIS: Métodos para uma eliminação segura

Artigo apresentado ao Curso de Graduação em Arquivologia, da Universidade Federal da Paraíba como requisito parcial para a obtenção do título de Bacharel em Arquivologia, sob orientação do Prof. Dr. Wagner Junqueira de Araújo.

Aprovado em _____/_____2015.

BANCA EXAMINADORA

_____

Prof. Dr. Wagner Junqueira de Araújo (Orientador)

Universidade Federal da Paraíba

_____

Prof. Dr. Marckson Roberto Ferreira de Sousa

Universidade Federal da Paraíba

_____

Profª. Me. Patrícia Maria da Silva

Universidade Federal da Paraíba

DOCUMENTOS ARQUIVÍSTICOS DIGITAIS: Métodos para uma eliminação segura

PACOTE, Kawan[1]

RESUMO: Seguindo a popularização dos computadores, certas atividades como a criação de documentos digitais tornaram-se comuns tanto para os usuários, quanto para as empresas ou instituições públicas. Para os Arquivistas que, normalmente lidam com documentos arquivísticos em meio físico, a criação de documentos arquivísticos no âmbito digital gerou inúmeras possibilidades, dentre elas, a dinamização no seu acesso e uso. Entretanto, a fragilidade inerente ao suporte e a maneira como o documento arquivístico digital será eliminado, requer um maior cuidado por parte daqueles que lidam com este, pois a eliminação incorreta do documento o torna passível de recuperação para fins alheios a sua criação. O presente artigo tem como objetivo identificar e disseminar, métodos, modelos e ferramentas para eliminação segura do documento arquivístico em formato digital.

PALAVRAS-CHAVES: Documento Arquivístico Digital. Gestão de Documentos. Sanitização. Segurança da Informação.

[1] Graduando em Arquivologia pela Universidade Federal da Paraíba. E-mail: kawan.souza@gmail.com

1 INTRODUÇÃO

O Arquivista é um profissional que possui os documentos como objeto de trabalho, entretanto este não lida com um documento qualquer, mas sim com o documento arquivístico. Devido aos adventos tecnológicos o documento arquivístico passou a coexistir no âmbito digital resultando no que é denominado como documento arquivístico digital. Para o desenvolvimento deste trabalho é necessário conhecer os conceitos sobre do que venha a ser um documento e um documento arquivístico, para então abordar o documento arquivístico digital na gestão de documentos e os métodos para a sua eliminação. Desta maneira, o artigo foi elaborado a partir de uma revisão de literatura. A revisão de literatura para Echer (2001) é de suma importância para a elaboração de um artigo, pois permite ao pesquisador situar-se entre os problemas que já foram e os que necessitam ser estudados. Portanto, foi necessário No presente artigo a revisão foi realizada através de artigos, dissertações, livros e periódicos no portal da CAPES e na plataforma do Google Acadêmico. Esta revisão foi desenvolvida de modo a identificar os métodos, modelos e ferramentas existentes almejando uma forma segura de eliminar o documento arquivistico digital.

Belloto (2007, p. 35) apresenta um conceito abrangente sobre os documentos:

> [...] documento é qualquer elemento gráfico, iconográfico, plástico, ou fônico pelo qual o homem se expressa. É o livro, o artigo de revista ou jornal, o relatório, o processo, o dossiê, a carta, a legislação, a estampa, a tela, a escultura, a fotografia, o filme, o disco, a fita magnética, o objeto utilitário etc., enfim, tudo o que seja produzido, por motivos funcionais, jurídicos, científicos, técnicos, culturais ou artísticos, pela atividade humana.

Por outro lado, o Dicionário de Terminologia Arquivística define o documento como uma “unidade de registro de informações, qualquer que seja o suporte ou formato” (ARQUIVO NACIONAL, 2005, p. 73). Por sua vez o projeto de Pesquisa Internacional em Registros Autênticos e Permanentes em Sistemas Eletrônicos (*The*

International Research on Permanent Authentic Records in Electronic Systems - INTERPARES) em seu glossário define como “uma unidade indivisível de informação constituída por uma mensagem fixada num suporte (registrada) com uma sintaxe estável. Um documento tem forma fixa e conteúdo estável”. (INTERPARES, 2015, *online*).

Por outro lado, o documento arquivístico possui características distintas e de maneira sucinta é definida pela autora Duranti como:

> [...] qualquer documento criado (produzido ou recebido e retido para ação ou referência) por uma pessoa física ou jurídica ao longo de uma atividade prática como instrumento e subproduto dessa atividade. (DURANTI, 2005, p. 07).

A definição de Duranti se assemelha ao do Conselho Nacional de Arquivos – CONARQ – no qual o define como “um documento produzido e/ou recebido e mantido por pessoa física ou jurídica, no decorrer das suas atividades, qualquer que seja o suporte, e dotado de organicidade” (CONARQ, 2011, p. 09). Assim como as definições vistas anteriormente, a definição do Modelo de Requisitos para a Gestão de Documentos Eletrônicos (MOREQ) também destaca a relação orgânica do documento com quem os produziu ao dizer que é o “documento criado, recebido ou mantido como prova e informação de uma pessoa ou um grupo no exercício de suas funções estatutárias ou na condução de seus negócios” (EUROPEAN COMISSION, 2008, p. 67, tradução nossa). [2]

O documento arquivístico digital é descrito pelo e-ARQ como um “um documento digital que é tratado e gerenciado como um documento arquivístico, ou seja, incorporado ao sistema de arquivos” (CONARQ, 2011 p. 09). O INTERPARES (2015, *online*) apresenta um conceito similar ao do e-ARQ ao afirmar que

[2] Na versão original: “[...]documents créés, reçus et préservés àtitre de preuve et d’information par une personne physique ou morale dans l’exercice de sés obligations légales ou la conduite de son activité”.

“documento digital reconhecido e tratado como documento arquivístico”. Rondinelli por outro lado conceitua o documento arquivístico digital como uma junção de outros conceitos:

> Podemos dizer que o documento arquivístico digital é um documento, isto é, ‘uma unidade indivisível de informação constituída por uma mensagem fixada num suporte (registrada), com uma sintática estável’, [...] produzido e/ou recebido por uma pessoa física ou jurídica, no decorrer das suas atividades, [...] codificado em dígitos binários e interpretável por um sistema computacional, em suporte magnético, ótico ou outro (RONDINELLI, 2011. p. 227).

O processo de definição e consolidação de um termo é um processo lento, a pesar dos conceitos apresentados pelos diferentes órgãos e autores caminharem em um mesmo sentido, ainda há espaço para o aperfeiçoamento destes.

2 GESTÃO DE DOCUMENTOS ARQUIVISTICOS

A Gestão de Documentos regula toda a prática arquivística realizada em uma instituição. Ela abrange o documento por todo o seu ciclo vital, ou seja, desde o momento em que o documento é criado, assim como a sua posterior eliminação ou caso este apresente valor secundário para a instituição mantenedora, o recolhimento para a guarda permanente.

A criação do conceito e ascensão da Gestão de Documentos é atribuída à necessidade na qual, a Administração Pública dos países ingressos na Segunda Guerra mundial possuía, em contornar as massas documentais acumuladas ocasionadas pela corrida armamentista.

> A atividade denominada *records management*, originalmente cunhada em inglês e posteriormente traduzida como gestão de documentos, não surgiu da prática ou teoria dos arquivos, mas por uma necessidade da administração pública (RODRIGUES, 2006, p.103).

Para Bernardes e Delatorre (2008), a gestão de documentos não é só importante para a administração pública, mas também para a democracia, este que é um direito da sociedade. As atividades da administração pública estão refletidas em seus documentos e a transparência exigida pela sociedade nada mais é do que a consequência da gestão de documentos.

> Ao definir normas e procedimentos técnicos referentes à classificação, avaliação, preservação e eliminação de documentos públicos, a gestão documental contribui decisivamente para atender às demandas da sociedade contemporânea por transparência nas ações de governo e acesso rápido às informações (BERNARDES; DELATORRE, 2008, p. 06).

No Brasil a Gestão de Documentos está disposta na constituição federal em seu artigo de nº 216 no qual aponta que “cabem à administração pública, na forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem”. (BRASIL, 1988). E posteriormente a matéria foi regulamentada pela lei de nº 8.159, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências, na qual considera a gestão como um “conjunto de procedimentos e operações técnicas referentes à sua produção, tramitação, uso, avaliação e arquivamento em fase corrente e intermediaria, visando a sua eliminação ou recolhimento para guarda permanente” (BRASIL, 1991).

A nível internacional existe a ISO 15489-1:2001 destinada a todos que lidam diretamente ou indiretamente com os documentos. Ela foi elaborada pela Organização Internacional para a Padronização (International Organization for Standardization) também conhecida como ISO. A Norma Internacional recebeu o título de **Informação e Documentação - Gestão de documentos de arquivo** e apesar dos seus quase quinze anos de existência ainda serve de subsídio para a instauração da gestão de documentos. A ISO elenca algumas das atividades de uma gestão documental:

- Criação e estabelecimento de políticas e normas;

- Alocação de responsabilidades e competências;
- Fixação de procedimentos e diretrizes;
- O projeto, implementação e a administração de sistemas especializados;
- Integração do sistema da gestão de documentos aos outros sistemas da organização.

Todavia, se faz necessário acrescentar que o conceito da Gestão de Documentos não é estático, e esse por sua vez podem variar de acordo com a tradição arquivística de cada país.

> Não se pode falar de gestão de documentos como um conceito único e de aplicação universal, uma vez que de sua elaboração e desenvolvimento participaram fatores determinantes, em que se destaca uma dada e específica tradição arquivística, e também administrativa, e um contexto histórico e institucional (INDOLFO, 2007, p. 33).

Ao elaborar um plano de gestão de documentos deve se atentar para que este possua os requisitos mínimos, neste caso, que ele possua as três fases básicas da gestão de documentos. Partindo de autores como Jardim (1987) e Paes (1997) pode-se distinguir as principais características de cada fase. Em sua primeira fase a **produção,** estabelece diretrizes acerca da criação do documento, almejando a padronização. Auxilia na escolha, e na utilização dos recursos materiais e tecnológicos utilizados. Também delimita tanto a criação dos documentos essenciais à instituição quanto na concepção e implementação dos sistemas utilizados. Em seguida temos a **utilização** na qual são estabelecidas normas para a utilização, acesso e recuperação da informação. Assim como as possíveis alterações e a manutenção dos sistemas utilizados. E por último a mais complexa fase a **destinação.** A destinação consiste na avaliação e destinação de documentos nos quais esses recebem os seus devidos prazos de guarda. Esta fase determina quais documentos devem ser eliminados ou preservados com base em seu valor de prova.

Cada uma dessas etapas requer ao profissional que lida com essas informações um cuidado específico. Haja vista, o cuidado necessário para a devida

implantação, a ISO assenta uma série de princípios a serem seguidos de modo que este seja abrangente ao ponto de suprir as necessidades da instituição.

> - Determinar os documentos de arquivo que devem ser criados e as informações que devem ser incluídas nestes documentos;
> - Decidir a forma e a estrutura em que deve criar e incorporar o sistema dos documentos de arquivo tal como a tecnologia utilizada;
> - Determinar os metadados que devem ser criados junto ao documento de arquivo e ao longo dos processos relacionados com o mesmo. Assim como os metadados serão vinculados e geridos ao longo do tempo;
> - Determinar os requisitos para recuperar, utilizar e transmitir documentos de arquivo durante as atividades da instituição e outros possíveis usuários e os prazos necessários para cumpri-los;
> - Decidir como organizar os documentos de arquivo de maneira que se cumpram os requisitos necessários;
> - Avaliar os riscos resultantes da perca de documentos de arquivo que testemunhem atividades realizadas;
> - Preservar os documentos de arquivo e permitir o acesso ao mesmo ao longo do tempo com o objetivo de satisfazer as necessidades da organização e as expectativas da sociedade;
> - Cumprir os requisitos legais e regulamentários, as normas aplicáveis e a política de organização;
> - Garantir que os documentos de arquivo sejam conservados em um ambiente seguro;
> - Garantir que o documento de arquivo seja conservado durante o período de tempo necessário e requerido;
> - Identificar e avaliar formas de melhorar a efetividade, eficácia e a qualidade dos processos, decisões e ações que podem resultar em uma melhor criação e gestão dos documentos de arquivo.
>
> (ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN, 2001, p. 8 Tradução nossa).

Logo, a utilização desses princípios possibilita a aplicação da gestão de documentos em consonância com a teoria das três idades. Teoria essa que divide o ciclo de vida dos documentos em três idades a partir da sua frequência de uso. Estas idades são definidas no Dicionário Brasileiro de Terminologia Arquivística (2005, *online,* grifo nosso) como:

> **Corrente** o ‘Conjunto de documentos, em tramitação ou não, que, pelo seu valor primário, é objeto de consultas frequentes pela entidade que o produziu, a quem compete a sua administração’. **Intermediário**: ‘Conjunto de documentos originários de arquivos correntes, com uso pouco frequente,

> que aguarda destinação' **Permanente**: 'Conjunto de documentos preservados em caráter definitivo em função do seu valor'.

Ressalta-se a importância do controle dos documentos em cada fase e sua forma diferente de organizar e disponibilizar as informações. Bem como, no acesso a estas, uma vez que o contexto de cada fase muda não só o modo de acondicionamento, guarda e conservação, mas também a finalidade e os usuários que irão acessá-las. No arquivo corrente e intermediário essas informações são de uso exclusivo da unidade/pessoa que o produziu, e são utilizadas para cumprimento das tarefas administrativas das instituições, enquanto na fase permanente é utilizado para fins diversos daquele que lhe deu origem, como por exemplo, a pesquisa e extensão.

3 GESTÃO DE DOCUMENTOS ARQUIVISTICOS DIGITAIS: A ELIMINAÇÃO DO DOCUMENTO DIGITAL

Dentro dos modelos de gestão de documentos apresentados, o descarte de documentos em formato digital merece atenção por dois motivos. Primeiro pela fragilidade inerente ao suporte, segundo que o descarte só vem sendo tratado em trabalhos mais recentes. Quando realizado de maneira imprópria pode ocasionar diversos problemas. Ao contrário dos documentos analógicos, os digitais deixam vestígios passíveis de serem recuperados. Estes vestígios são conhecidos como a remanência de dados. A remanência de dados aliada à prática das instituições públicas em doar ou leiloar computadores, notebooks e outras mídias de suporte consideradas desfasadas tornam as informações da instituição alvo de pessoas mal intencionadas. Portanto percebe-se a necessidade do uso da Segurança da Informação (SI) nos processos de descarte ao analisarmos a eliminação do documento digital.

Esse contexto Beal (2008, p. 07) alerta ao dizer que:

> São relativamente comuns os casos de descoberta de informações sigilosas ou dados pessoais sujeitos a normas de privacidade em computadores usados quando estes são transferidos de área, doados ou vendidos durante um processo de renovação do parque de computadores da organização.

No âmbito digital, a eliminação de forma corriqueira seguiria o seguinte procedimento: o documento é selecionado para em seguida ser eliminado utilizando a tecla *delete* ou clicando sobre o documento e escolhendo a opção excluir**.** Os documentos eliminados desta maneira podem ser encontrados na Lixeira até que esta seja esvaziada. Ainda existe outra forma que é a combinação da tecla *shift* mais *delete* que apesar do Sistema Operacional (SO) garantir a eliminação permanente, não impede que o documento seja passível de recuperação.

Além destes, existem outras maneiras que podem ser utilizadas com o intuito de eliminar os documentos, como por exemplo a inserção de uma nova imagem ou a formatação. Estes dados podem ser recuperados através de *softwares* gratuitos como ***EASEUS Data Recovery Wizard*** (http://www.easeus.com/datarecoverywizard/free-data-recovery-software.htm), ***Recuva*** (https://www.piriform.com/recuva) ou o ***PC Inspector File Recovery*** **(**http://www.pcinspector.de/).

Ainda nesta mesma linha de considerações, temos o Recuva como exemplo de um software gratuito e intuitivo. O software permite que o usuário escolha o Português Brasileiro dentre outros idiomas, porém esse não está totalmente traduzido restando poucas frases em inglês. O que torna o Recuva intuitivo é o seu assistente. O uso do assistente não é obrigatório e indicado para aqueles que não sabem ao certo o que, onde e como procurar os arquivos eliminados. Caso aceite a ajuda do assistente ele irá questionar o tipo de arquivo que deseja recuperar. O usuário possui a liberdade de escolher todos os tipos ou limitar a uma simples imagem. Após selecionar o tipo é preciso escolher o local. Dentre as alternativas podemos escolher desde uma busca em todo computador a um pendrive. E por fim, se o usuário deseja uma verificação superficial ou profunda. É necessário alertar que

o tempo de verificação pode variar de forma drástica conforme as escolhas feitas anteriormente e o local a ser verificado. Por fim, é preciso selecionar quais arquivos devem ser recuperados e os locais que estes devem ser salvos.

Esses são programas que possuem a interface intuitiva, encontrados facilmente na *web* e não necessitam como pré-requisito de conhecimentos técnicos acerca da prática.

Da mesma forma que existem programas que recuperam os documentos digitais também existe métodos e programas que impeçam a recuperação destes. A prática de evitar a recuperação de dados ao eliminar os documentos é conhecida como sanitização de dados.

A sanitização, terminologia aplicada ao processo, ocorre no meio digital e segue a premissa da eliminação de um documento convencional, porém, com métodos diferentes. Conforme Queiroz e Vargas (2010, p.85) " a sanitização de dados é simplesmente uma eliminação de dados de forma que eles não possam ser encontrados novamente." Entretanto, é necessário frisar que a sanitização não deve ser encarada como um meio para eliminar os dados, mas realizar tal tarefa de modo na qual a mídia que até então os conservara possa ser reutilizada de uma maneira segura. Ou seja, sem que seja possível a recuperação dos dados. " A sanitização é definida como um processo de remover os dados da mídia antes de reutilizar a mídia em um ambiente que não fornece um nível de proteção aceitável aos dados que estavam na mídia antes da sanitização". (United States Department of Defense, 2006, p. 74, tradução nossa).

Nota-se uma grande falha por parte daqueles que eliminam os documentos sem a devida sanitização nos locais onde esses estão armazenados. Como por exemplo as duas formas de eliminação anteriormente ditas. A inserção de uma nova imagem e a formatação.

> As empresas acreditam que por uma nova imagem no disco rígido durante o processo de clonagem ou ghost vai sanitizar o disco rígido. Portanto, um disco rígido será usado por inúmeras pessoas durante o seu ciclo de vida.

> Teoricamente, isso indica que um HD que só foi feita a inserção de uma nova imagem como parte da prática de sanitização pode conter dados de muitas pessoas no fim do seu tempo útil de vida. (Amari, 2006 apud Podhradsky; Streef, 2011, p.49, tradução nossa). [...]Outro equívoco popular é que formatar um disco rígido irá sanitiza-lo. O que em teoria é tão falho quanto o uso da imagem. A formatação de um disco simplesmente prepara a unidade para o seu uso inicial (Davis, 2008 apud Podhradsky; Streef, 2011, p.49, tradução nossa)

A sanitização possui diversos métodos e pode ser realizada através da contratação de empresas especializadas, ou através de softwares, sejam esses pagos ou gratuitos. Não existe um único método destinado a todas as mídias, assim como não é aconselhável essa prática, pois cada situação é única.

Logo, a sanitização pode ser realizada não só em discos rígidos, mas na memória interna de celulares, drives removíveis (Pendrive / HD Externo) ou até mesmo fitas magnéticas que ainda é utilizada como uma forma de backup. Outro fator determinante para a sanitização é o sigilo da informação. Por exemplo, podemos imaginar um escritório contábil que ao decorrer dos anos acaba por acumular uma grande quantidade de informações e possui o dever de resguarda-las. Os documentos encontrados podem vir a ser desde uma declaração de imposto de renda, a um holerite.

> Uma empresa com 50 empregados deverá gerir um arquivo de 1.400 arquivos eletrônicos somente relativos a salário e 13º, por exemplo. Fora os demais para as férias, rescisões, avisos prévios, atestados médicos, advertências, suspensões, afastamentos, acidentes de trabalho e muitos outros". (Oliveira, 2014)

Cada documento possui valor único no contexto em que foi gerado, e por isso o mesmo valor a eles atribuído determinará a escolha do método de sanitização a ser adotado. *O National Institute of Standards and Technology* (NIST) é o Instituto Nacional de Padrões e Tecnologia dos Estados Unidos. O NIST divide a sanitização em três categorias:

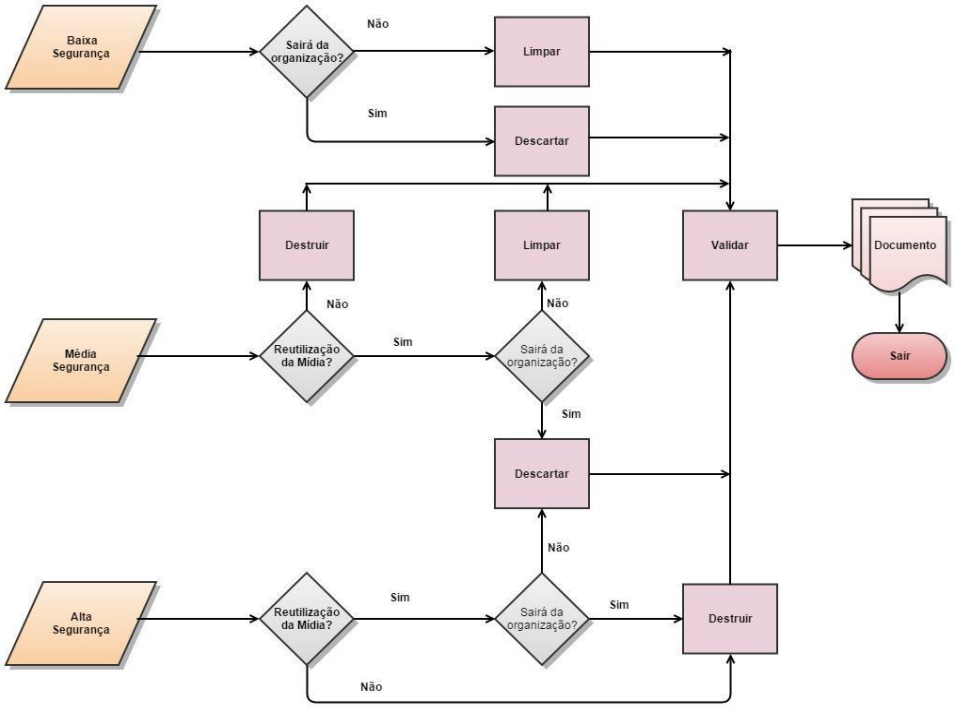
> **Limpar**: Utiliza um método que higieniza os locais de armazenamento estabelecido pelo usuário. No caso de um computador ele iria voltar ao seu estado de fábrica. Comumente utilizado quando existe a reutilização do computador.
> **Descartar**: Este método remove os documentos de forma que não possa ser recuperado por qualquer técnica ou em laboratório. Comumente utilizada quando existe a necessidade de descartar ou doar o computador.
> **Destruir**: A destruição quando realizada apropriadamente torna inviável a recuperação dos dados e impossibilita a utilização da mídia, porém, dependendo da forma que ela foi destruída os dados podem ser recuperados utilizando técnicas de laboratórios (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 2014, p. 09, tradução nossa).

Além das três categorias apresentadas, existem métodos específicos utilizados como contramedidas para evitar a remanência de dados. A Criptografia, Desmagnetização e Substituição. Eles são evidenciados no artigo dos Fundamentos de Sistemas de Informação sobre Segurança / Sistema de Controle de Acesso (WIKIBOOKS, 2015, *online*, tradução nossa):

> **Substituição**: Sobrescreve os documentos com novos dados. Este método se enquadra na categoria “limpar” vista anteriormente e é comumente aceitável, pois não agride ou destrói o local onde o dado está armazenado.
> **Desmagnetização**: A desmagnetização utiliza um aparelho feito para apagar os dados removendo ou reduzindo o campo magnético dos hard drives (HD) ou similares, mas pode ocorrer do pulso magnético destruir partes ou o mesmo.
> **Criptografia**: A criptografia pode atenuar os riscos de recuperar os dados, mas para isso é necessário que os documentos sejam criptografados antes de serem eliminados. A criptografia embaralha os dados de forma que sem a chave não seja possível recupera-los.

O NIST (2014) ainda apresenta um fluxo para auxiliar no processo, conforme demonstrado na Figura 1.

FIGURA 1 - FLUXO DE DECISÃO PARA SANITIZAÇÃO

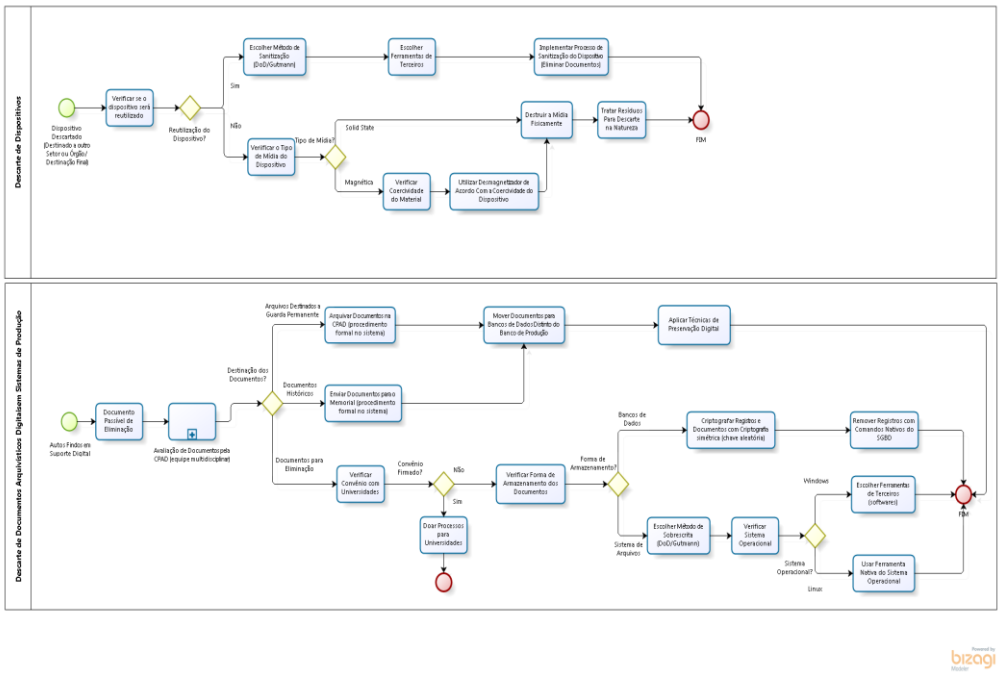


Fonte: National Institute of Standards and Technology, 2014, p.17, tradução nossa.

O fluxo do NIST aborda o descarte de documentos e da mídia utilizada levando em conta três níveis diferentes de segurança da informação. Foi criado com o intuito de orientar no processo de descarte e por não possuir nenhuma especificidade na qual restrinja outra organização de utiliza-lo, este se torna universal. O único requisito para utilizar o modelo é uma reflexão acerca do grau de sigilo do documento, se existe a reutilização da mídia e se essa sairá da organização.

Por outro lado, temos um fluxo elaborado por Silva (2015, p. 95) no qual contempla outros aspectos além da eliminação como a guarda permanente dos documentos. Estas singularidades demonstram a indispensabilidade de que cada país ou agências governamental possua a sua.

FIGURA 2 – MODELO FINAL DE DESCARTE SEGURO DE DOCUMENTOS EM SUPORTE DIGITAL



Fonte: Silva ,2015, p. 95.

O Modelo de Silva foi elaborado especificamente para atender as necessidades do Órgão da Justiça Trabalhista da Paraíba a partir de suas necessidades. Ele aborda o descarte de documentos e da mídia ao dividi-lo em duas atividades. A primeira atividade é o descarte de dispositivo que oferece método específico para sanitização e verifica qual mídia será descartada. A segunda atividade refere-se ao descarte de documentos arquivístico digitais. Neste aspecto o modelo contempla não só os documentos a serem eliminados, mas também aqueles que são de guarda permanente, que possuem caráter histórico e como estão armazenados.

Em uma análise entre os dois modelos, a primeira e talvez maior diferença seja o intuito para o qual estes foram criados. O modelo do NIST por ser de uma instituição de padronização não contempla as particularidades concernentes a cada organização. Já a elaborada por Silva (2015) moldado de acordo com a realidade e necessidades específicas da Justiça Trabalhista Paraibana. A segunda diferença é

que em seu fluxo de decisão para sanitização o NIST não esclarece quais métodos específicos deveram ser utilizados para sanitização e em quais tipos de mídias. O modelo de Silva (2015) já especifica os tipos de mídias a serem encontrados e os métodos de sanitização utilizados.

Ao adentrarmos as similaridades notamos que ambos os modelos possuem a mesma preocupação com a mídia e se esta será reutilizada. Os dois modelos atingem os seus objetivos, seja de um modo geral ou específico.

Esses dois modelos são exemplos dos diferentes métodos utilizados para a destruição de documentos digitais. É comum que cada país tenha a sua, percebe-se pelo quadro que são em maior parte provenientes da América do Norte.

QUADRO 1 – NORMAS DE ELIMINAÇÃO

País	Método	Link
Austrália	ISM 6.2.92	http://www.asd.gov.au/infosec/ism/index.htmhttp://www.asd.gov.au/infosec/ism/index.htm
Canadá	CSEC ITSG-06	https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsg06-eng.pdfhttps://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsg06-eng.pdf
Estados Unidos da América	DoD 5220.22-M	http://www.dtic.mil/whs/directives/corres/pdf/522022m.pdf
Estados Unidos da América	AFSSI-5020	http://cryptome.org/afssi5020.htm
Estados Unidos da América	AR 380-19	http://fas.org/irp/doddir/army/r380_19.pdf
Estados Unidos da América	NAVSO P-5239-26	http://fas.org/irp/doddir/navy/5239_26.htmhttp://fas.org/irp/doddir/navy/5239_26.htm http://fas.org/irp/doddir/navy/5239_26.htm
Estados Unidos da América	NIST 800-88	http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf
Nova Zelândia	NZISM	http://www.gcsb.govt.nz/assets/GCSB-Documents/NZISM-2011-Version-1.01.pdf

Fonte: Dados da pesquisa, 2015.

É importante frisar que existem outras normas além das supracitadas, porém devido a barreira linguística encontrada tornou-se inviável a descrição das mesmas. A exemplo da norma Russa na qual não foi encontrada outra versão em outro idioma além do russo. As normas foram concebidas para auxiliar o governo ou agências governamentais a resguardar informações sigilosas através de diretrizes, manuais ou políticas de segurança da informação. Em uma análise dos seus objetivos nota-se que estes em sua maioria são similares. Os cernes de suas preocupações estão voltadas a evitar o acesso indevido a informações, sejam governamentais ou de terceiros.

ISM 6.2.92: O Manual de Segurança da Informação do Governo Australiano foi concebido para auxiliar as agências governamentais a proteger seus sistemas de informações e tecnologia da informação e comunicação.

CSEC ITSG-06: Esta diretriz busca auxiliar as autoridades governamentais de Tecnologia Da Informação do Canadá na seleção de métodos para preparar os dispositivos de armazenamento eletrônico para desclassificação, reutilização ou eliminação.

DOD 522022M: O manual foi emitido em conformidade com o Programa Nacional de Segurança Industrial. Ele prescreve os requisitos, restrições e outras salvaguardas para prevenir a divulgação não autorizada de informações sigilosas.

AFSSI-5020: Esta instrução implementa o Programa de Segurança da Computação da Força Aérea, abordando os requisitos na área da segurança da remanência. Especificamente essa instrução fornece: Uma discussão sobre as ameaças e vulnerabilidade associados a limpeza, sanitização e destruição da mídia; Procedimentos para uma limpeza de mídia e as restrições para a reutilização da mídia; Procedimentos para sanitizar a mídia; E técnicas aprovadas para a destruição de mídias, fitas e etc.

AR380-19: Este regulamento estabelece a política de segurança do sistema de informação do exército. Prescreve a política de segurança do sistema de informação para a proteção de informações sigilosas ou não classificadas, armazenadas ou transmitidas através de um sistema de informação automatizado.

NAVSO P-5239-26:Fornece métodos e procedimentos para evitar a divulgação de informações sigilosas e / ou não classificadas para aqueles que o acesso não está autorizado.

NIST 800-88: O objetivo desta publicação especial é auxiliar na tomada de decisão quando existir a necessidade da mídia ser eliminada, reutilizada ou deixará a organização.

NZISM: O objetivo deste manual é garantir que seja aplicada um gerenciamento de riscos de segurança cibernética dentro do governo.

A partir das normas vistas anteriormente é possível identificar os métodos utilizados no descarte. Para cada necessidade de descarte é possível aplicar um método. Estes métodos como por exemplo o de sobrescrita, implementadas por diferentes ferramentas de *software*. Tais funcionalidades podem ser encontradas em programas específicos ou até mesmo em antivírus como o **Kaspersky**. Os programas específicos como **DBAN**, **ErAce** e o mais conhecido **File Shredder** são gratuitos e podem possuir um único ou diversos métodos. Uma das maiores vantagens é a liberdade em que o usuário tem de escolher qual método utilizar, mas isso é viável apenas enquanto o usuário possuir conhecimento sobre os métodos existentes e qual se adequa a sua necessidade.

Por exemplo, caso o usuário deseje utilizar o File Shredder para sanitizar um disco rígido, um conjunto de documentos ou um único documento, ele deverá seguir estes passos. Em um primeiro momento, é importante frisar que o software é gratuito e não oferece a escolha de um idioma. Isto pode gerar uma barreira linguística para o usuário que não possua um conhecimento básico de Inglês. Após a instalação e inicialização do programa, o usuário poderá escolher o método para sanitizar ao

clicar na opção Shredder Settings e em seguida na aba Algorithms. O método padrão é o DOD 5220-22.M, entretanto, existem outros como o de Guttman. Para sanitizar é preciso selecionar o documento, pasta ou disco rígido. A seleção do documento ou pasta pode ocorrer através do software ao clicar na opção Add File(s) ou Add Folder. Também é possível selecionar o documento e o arrastar (Drag and Drop) até que esteja posicionado sob a interface do software. Após a seleção é preciso clicar na opção Shred Files Now e confirmar o desejo de sanitizar o documento ou pasta. Outra maneira é selecionar o item a ser sanitizado, clicar com o botão direito do mouse, procurar pela opção File Shredder e por fim, selecionar a opção Secure Delete Files. Por outro lado, a sanitização de um disco rígido é viável exclusivamente através do software. É preciso selecionar a Opção Shred Free Disk Space para em seguida determinar o disco e o método que será utilizado.

A tomada de decisão, deve ser acompanhada de um planejamento e de procedimentos registrados. Estes são um dos maiores empecilhos para a utilização destes *softwares* em comparação aos de recuperação de documentos os quais possuem interface intuitiva, e um único objetivo. Contudo com o devido treinamento e estudo é possível à inserção desta prática nas instituições, sejam estas públicas ou privadas, regulando o uso dos documentos digitais e a sua confidencialidade.

4 CONSIDERAÇÕES FINAIS

Em nosso cotidiano, aquele que detém mais informações consequentemente irá se sobressair sobre os que não a possuem. Tornou-se comum nos depararmos com notícias acerca de empresas semelhantes falirem enquanto outras prosperam. Venda de informações privilegiadas. Aquisição de documentos pessoais de terceiros para transações fraudulentas. O que torna tudo isso possível são as informações.

O arquivista enquanto profissional da informação está acostumado a lidar com as informações presentes nos documentos arquivísticos sob a sua posse, pois faz parte da sua rotina não só resguardar, mas torna-las acessíveis. Entretanto, o

ingresso do documento arquivístico digital modifica este cenário, logo que, na visão do autor, o arquivista passa a lidar com dois tipos de documentos. O primeiro, no qual ele tem um maior controle e possui registros sobre quem o acessa ou o modifica. E o segundo, um documento oculto para o arquivista no qual ele não conhece quem o criou, qual a finalidade de sua criação e quais os riscos que este documento pode trazer para a sua entidade mantenedora. Com este artigo espera-se disseminar o que vem a ser a sanitização de arquivos digitais no âmbito da arquivologia, discutir os métodos utilizados e ressaltar a necessidade de que a segurança da informação venha atuar em consonância por todo o ciclo de vida do documento arquivístico digital. Além de servir como estimulo para que os arquivistas possam produzir novos trabalhos ou discutirem acerca da temática.

DIGITAL RECORDS: Methods for a safe elimination

ABSTRACT

Following the computers popularity certain activities such as create digital records have become common for both ordinary users and companies or government institutions. For the Archivists who normally deals with common records, the creation of the records in the digital context has generated plenty possibilities, among them, boosting their access and use. However, the inherent fragility of the support and the way the digital record are deleted requires great care on the part of those who deal with this because the incorrect elimination of the document makes recoverable for other purposes besides their creation. Therefore, this article seeks to disseminate the methods, models and tools for safe disposal of record in the digital context. The methods used on this article was the literature review, the results show that existing methods are generic and are designed to specific needs and suggest that the theme needs further study focused on the characteristics and peculiarities of archival activity.

Keywords: Digital Record. Records Management. Sanitization. Security Information.

REFERÊNCIAS

AIR FORCE SYSTEM SECURITY (Estados Unidos da America). **AIR FORCE SYSTEM SECURITY INSTRUCTION 5020:** Remanence Security. [S.l.: s.n.], 1996. Disponível em: <http://cryptome.org/afssi5020.htm>. Acesso em: 04 mar. 2015.

ARQUIVO NACIONAL (Brasil). **Dicionário Brasileiro de Terminologia Arquivística**. Rio de Janeiro, 2005. Disponível em: <http://www.portalan.arquivonacional.gov.br/Media/Dicion%20Term%20Arquiv.pdf>. Acesso em: 04 mar. 2015.

AUSTRALIAN SIGNALS DIRECTORATE. **Information Security Manual.** 2015. Disponível em: <http://www.asd.gov.au/infosec/ism/index.htm>. Acesso em: 04 mar. 2015.

BEAL, Adriana. **Segurança da informação:** Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações. São Paulo: Atlas, 2008.

BELLOTTO, Heloísa Liberalli. **Arquivos permanentes: tratamento documental**. FGV Editora, 2004

BERNARDES, Ieda Pimenta; DELATORRE, Hilda. **GESTÃO DOCUMENTAL APLICADA**. São Paulo: Arquivo Público do Estado de São Paulo, 2008. Disponível em: <http://www.arquivoestado.sp.gov.br/site/assets/publicacao/anexo/gestao_documental_aplicada.pdf>. Acesso em: 05 ago. 2015

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988.

_____. Lei nº 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. **Diário Oficial da República Federativa do Brasil**. Brasília, DF, 9 jan. 1991. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8159.htm>. Acesso em: 04 mar. 2015.

COMMUNICATIONS SECURITY ESTABELISHMENT. **IT Security Guidance:** Clearing and Declassifying Eletronic Data Storage Devices, 2006. Disponível em: < https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsg06-eng.pdf >. Acesso em: 04 mar. 2015.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **E-ARQ Brasil**: Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivístico de Documentos. Rio de Janeiro: [s.n.], 2011. Disponível em: <http://www.documentoseletronicos.arquivonacional.gov.br/media/e-arq-brasil-2011-corrigido.pdf >. Acesso em: 04 mar. 2015.

DBAN. Disponível em: http://www.dban.org/download Acesso em: 04/03/15.

DEPARTMENT OF THE NAVY (Estados Unidos da America). **NAVAL INFORMATION SYSTEMS MANAGEMENT CENTER:** NAVSO P-5239-26. WASHINGTON, D.C: [s.n.], 1993. Disponível em: <http://fas.org/irp/doddir/navy/5239_26.htm>. Acesso em: 04 mar. 2015.

DURANTI, Luciana. Rumo a uma teoria arquivística de preservação digital: as descobertas conceituais do Projeto InterPARES**. Arquivo & Administração. Rio de Janeiro: Associação dos Arquivistas Brasileiros**, v. 4, n. 1, p. 5-18, 2005.

ECHER, Isabel Cristina. A revisão de literatura na construção do trabalho científico. **Revista gaúcha de enfermagem. Porto Alegre. Vol. 22, n. 2 (jul. 2001), p. 5-20**, 2001.Disponível em: http://www.lume.ufrgs.br/handle/10183/23470. Acesso em: 13 de Jan. 2016.

ERACE. erase hard drive, wipe hdd. Disponível em: http://sourceforge.net/projects/erace/ Acesso em: 04/03/15

EUROPEAN COMMISSION. **Exigences types pour la maîtrise de l'archivage électronique**, 2008.
Disponível em :<http://www.archivesdefrance.culture.gouv.fr/static/2094>. Acesso em: 05 ago.2015.

FEDERATION RUSSIAN. **GOST 50739-95**: Computers technique, Information protection against unauthorised access to information, General technical

requirements, 1995. Disponível em: <http://protect.gost.ru/document.aspx?control=7&id=134268>. Acesso em: 04 mar. 2015.

FILESHREDDER. Disponível: http://www.fileshredder.org/ Acesso em: 04/03/15.

FINSLAB. **A Eliminação de Dados**, 2015. Disponível em: <http://finslab.com/enciclopedia/letra-a/a-eliminacao-de-dados.php>. Acesso em: 04 mar. 2015.

FISHER, Tim. **Data Sanitization Methods**. [2015?]. Disponível em: <http://pcsupport.about.com/od/toolsofthetrade/g/data-sanitization-method.htm>. Acesso em: 04 mar. 2015.

FISHER, Tim. **HMG IS5**, [2015?]. Disponível em: <http://pcsupport.about.com/od/termshm/g/hmg-is5.htm>. Acesso em: 04 mar. 2015.

GOVERNMENT COMMUNICATIONS SECURITY BUREAU (Nova Zelândia). . **New Zeland Information Security:** Manual. Nova Zelândia: [s.n.], 2011. Disponível em: <http://www.gcsb.govt.nz/assets/GCSB-Documents/NZISM-2011-Version-1.01.pdf>. Acesso em: 04 mar. 2015.

HEADQUARTERS DEPARTMENT OF THE ARMY. **Information Systems Security**. Washington: [s.n.], 1998. Disponível em: <http://fas.org/irp/doddir/army/r380_19.pdf>. Acesso em: 04 mar. 2015.

INDOLFO, Ana Celeste. Gestão de documentos: uma renovação epistemológica no universo da arquivologia. **Arquivística. net,** Rio de Janeiro, v. 3, n. 2, p. 28 - 60, 2007. Disponível em: <http://www.brapci.inf.br/_repositorio/2011/06/pdf_59336b505e_0003553.pdf> . Acesso em: 05 ago. 2015.

INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS (INTERPARES). **Terminology Database**, [2015] Disponível em: <http://www.interpares.org/ip3/ip3_terminology_db.cfm?team=4&status=glossary>. Acesso em: 05 ago. 2015

JARDIM, José Maria. O conceito e a prática de gestão de documentos. **Acervo**, Rio de Janeiro, v. 2, n. 2, p. 36 - 43, 1987. Disponível em: < http://arquivar.com.br/site/wp-content/uploads/2007/09/O-Conceito-e-a-Pratica-de-Gestao-de-Documentos.pdf> Acesso em: 05 ago. 2015

KASPERSKY LAB. Disponível em: <http://brazil.kaspersky.com/downloads/versoes-de-teste/productos-para-usuarios-domesticos Acesso em: 04/03/15.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Guidelines for Media Sanitization**: Recommendations of the National Institute of Standards and Technology Special Publication Draft 800-88r1. Maryland: U.S Government Printing Office, 2014. Disponível em: <http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf>. Acesso em: 04 mar. 2015.

OLIVEIRA, Ronaldo Dias. **Guardar documentos é tão importante quanto pagar impostos**. Disponível em: < http://www.contabeis.com.br/noticias/18362/guardar-documentos-e-tao-importante-quanto-pagar-impostos/> Acesso em: 15 nov.2015.

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. **Norma Internacional ISO 15489-1.** Ginebra: ISO, 2001. Disponível em: < http://www.informacionpublicapgr.gob.sv/descargables/sia/normativa-internacional/GEStexto1(CS).pdf>. Acesso em 04 mar. 2015.

PAES, Marilena Leite. **Arquivo:** teoria e prática. 3. ed. Rio de Janeiro: FGV Editora, 1997. Disponível em: <http://pcsupport.about.com/od/termshm/g/hmg-is5.htm>. Acesso em: 10 mar. 2015

PODHRADSKY, Ashley L.; STREFF, Kevin. Testing Data Sanitization Practices of Retired Drives with The Digital Forensics Data Recovery Project. **Journal of Information Privacy and Security,** v.7, n. 3, p. 46-63, 2011. Disponível em: <http://www.tandfonline.com/doi/abs/10.1080/15536548.2011.10855917> Acesso em: 03 de nov.2015

QUEIROZ, Claudemir; Vargas, Raffael. Investigação e Perícia Forense Computacional. **Brasport. Rio de Janeiro**, 2010.

RODRIGUES, Ana Márcia Lutterbach. A teoria dos arquivos e a gestão de documentos. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 11, n. 1, 2006. Paginação irregular. Disponível em: < http://www.scielo.br/pdf/pci/v11n1/v11n1a09>. Acesso em: 05 ago. 2015

RONDINELLI, Rosely Curi. **O conceito de documento arquivístico frente à realidade digital: uma revisitação necessária, 2011, 270f**. 2011. Tese de Doutorado. Tese (Doutorado em Ciência da Informação) –Instituto de Arte e Comunicação Social, Universidade Federal Fluminense, Niterói.

SANTOS, Vanderlei Batista dos; INNARELLI, Humberto Celeste; SOUSA, Renato Tarciso Barbosa de. **Arquivística Temas Contemporâneos:** classificação, preservação digital, gestão do conhecimento. 2. ed. Distrito Federal: SENAC, 2008 p.223

SILVA, Silvio Lucas da. **O DESCARTE SEGURO DE DOCUMENTOS ARQUIVÍSTICOS EM SUPORTE DIGITAL:** um estudo de caso na Justiça Trabalhista Paraibana. 2015. 118 f. Dissertação (Mestrado em Ciência da Informação) - Centro de Ciências Sociais Aplicadas, Universidade Federal da Paraíba, João Pessoa, 2015.

THE FEDERAL OFFICE FOR INFORMATION SECURITY (Alemanha). **BSI-Standards**, [2015?]. Disponível em: <https://www.bsi.bund.de/EN/Publications/BSIStandards/standards.html>. Acesso em: 04 mar. 2015.

UNITED STATES DEPARTMENT OF DEFENSE. **DoD 5220.22-M.** 2006. Disponível em: <http://www.dtic.mil/whs/directives/corres/pdf/522022m.pdf>. Acesso em: 04 mar. 2015.

WIKIBOOKS CONTRIBUTORS. **Fundamentals of Information Systems Security/Access Control Systems**, 2015. Disponível em: <http://en.wikibooks.org/w/index.php?title=Fundamentals_of_Information_Systems_Security/Access_Control_Systems&oldid=2758750>. Acesso em: 10 mar. 2015.