Universidade Presbiteriana Mackenzie

Pós-Graduação

Computação Forense

O Impacto do Cloud Computing no Processo de Perícia Digital

Legislação Aplicada a Perícia Forense
Professora: Vera Kaiser Sanches Kerr

Robson da Silva Ramos
T.I.A. Nº 70970580
robsramos@ig.com.br

Nicholas Istenes Eses
T.I.A. Nº 70957878
nistenes@gmail.com

RESUMO

O presente artigo tem como objetivo apresentar aos leitores os impactos e desafios trazidos ao processo de perícia forense digital de acordo com o novo cenário de Cloud Computing, bem como uma análise dos problemas trazidos a este processo no Brasil de acordo com a legislação atualmente aplicada para esta prática sugerindo a adoção de alguns procedimentos para minimização dos problemas que poderão surgir.

Introdução

A tecnologia evolui cada vez mais rápida trazendo diversos benefícios a todos os setores e também, como conseqüência, a necessidade de se revisar ou até mesmo adaptar alguns processos. Uma importante revolução que está acontecendo no meio digital é a introdução do conceito de *Cloud Computing* que trará vários benefícios e novos serviços aos seus clientes e com a evolução, conforme dito, a inevitável revisão de processos e conceitos atuais. O presente artigo tem como objetivo apresentar resumidamente o que é *Cloud Computing*, os desafios atuais e o impacto que o mesmo trará no processo de perícia forense focando, especificamente, nas leis que regem este processo, organizado da seguinte forma: o capítulo um apresenta a definição sobre *Cloud Computing;* no capítulo dois são apresentados os desafios atuais, em relação à questão de segurança, do *Cloud Computing*, bem como a apresentação de iniciativas de destaque sobre o estudo do tema; no capítulo três temos a apresentação sobre o surgimento de uma nova modalidade de crime: o crime eletrônico e a descrição do que é perícia forense e técnicas utilizadas pela tal, ressaltando-se a importância do processo de cadeia de custódia; No capítulo quatro ~~4~~ uma apresentação sobre os desafios e problemas trazidos pelo *Cloud Computing* à perícia digital conforme feita hoje de acordo com a legislação aplicada no Brasil para estes procedimentos. Por fim, a conclusão com as iniciativas que entendemos serem necessárias para minimizar os problemas trazidos por este novo cenário.

1. *Cloud Computing*

O *Cloud Computing* ou "computação nas nuvens"[1] - tradução literal para o português - parece ser o novo paradigma da informática que, conforme alguns especialistas, pode levar ao fim, no futuro, dos computadores pessoais em relação a forma que funcionam hoje, funcionando estes, a partir de então, apenas como autênticos terminais "burros" com os dados e o processamento na nuvem. Google, Microsoft, Yahoo já oferecem ao público serviços baseados neste conceito. Mas afinal, o que é *Cloud Computing*?

Segundo definição do NIST[2], *Cloud Computing* é: "... um modelo que possibilita acesso, de modo conveniente e sob demanda, a um conjunto de recursos computacionais configuráveis (por exemplo, redes, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente adquiridos e liberados com mínimo de esforço gerencial ou interação com provedor de serviços".(NIST/2009). Em resumo, *Cloud Computing* pode ser entendido como um conceito que consiste em, basicamente, ter acesso a serviços, estrutura e ferramentas hoje presentes nos computadores pessoais ou locais através da Internet. Este conceito está associado, de maneira geral, a três subdivisões de acordo com a característica dos serviços providos. São elas:

---

[1] A nuvem neste caso, é uma metáfora para a Internet ou infra-estrutura de comunicação entre os componentes arquiteturais, baseada em uma abstração , o que oculta a complexidade de infra-estrutura. Baseado em **Computação em Nuvem: Conceitos, Tecnologias, Aplicações e Desafios** de Souza, Flávio R. C., Moreira, Leonardo O., Machado, Javam C. Universidade Federal do Ceará.

[2] NIST – *National Institute of Standards and Techonology* – agência governamental não-regulatória de administração de tecnologia do Departamento de Comércio dos Estados Unidos.

- Software como serviço: permite que *softwares* ou aplicativos sejam utilizados de forma remota por múltiplos usuários. Um exemplo deste caso é o *Google Docs*.[3]
- Plataforma como serviço: consiste em disponibilizar plataformas de desenvolvimento e de distribuição de aplicações. Um exemplo deste caso é o *Microsoft Windows Azure*.[4]
- Infraestrutura como serviço: disponibilização de recursos de hardware como capacidade de processamento e opções de armazenamentos de dados. Um exemplo neste caso é o *Amazon S3*.[5]

A oferta dos três tipos de serviços acima citados traz uma gama de oportunidades e benefícios não só para usuários comuns como também para as empresas. Os principais benefícios que podemos citar são:

- Escalabilidade.
- Redução de custos.
- Melhor Desempenho.
- Pagamento de taxa quando somente do uso do software ao invés da compra de uma licença para uso, o que é normalmente mais caro.
- Facilidade no compartilhamento dos dados e, por conseguinte, no trabalho corporativo.
- Proporcionar as empresas um foco maior nos negócios em que atuam.

Com todos estes benefícios e ainda aqueles que poderão ser disponibilizados por esta nova tendência, o *Cloud Computing* se consolida como um paradigma que tende a crescer e dominar os investimentos nos próximos anos. O CEO da Microsoft, Steve Ballmer, em palestra na Universidade de Washington em Seattle (EUA), revelou que "Das 40 mil pessoas que desenvolvem produtos na Microsoft, 70% estão projetando exclusivamente para a nuvem, ou são conduzidas pela inspiração de servirem à nuvem de alguma forma. (...). E daqui a alguns anos esse porcentual será de 90%". (COMPUTERWORLD, 2010).

Desta forma, o processo de migração para o uso de serviços através do *Cloud Computing* parece ser cada vez mais irredutível. Porém, pelo fato de ser algo teoricamente ainda "novo", há ainda muito a ser definido e estudado em relação a vários aspectos, principalmente no que se refere à segurança.

2. Problemas de Segurança no Cloud Computing

Uma das maiores preocupações entre profissionais de TI relativas à implantação e utilização do *Cloud Computing* refere-se ao quesito segurança. Resultados preliminares de entrevistas feitas pela empresa TheInfoPro com profissionais de segurança das mil maiores empresas americanas apontam que 53% deles estão “muito

[3] *Google Docs* é um pacote de aplicativos Web que oferecem serviços de edição de texto, planilha eletrônica entre outros.
[4] O *Microsoft Azure* é uma plataforma para a implementação de computação em nuvem que oferece um conjunto específico de serviços para desenvolvedores.
[5] *Amazon S3 (Simple Storage Service)* é um serviço de armazenamento on-line oferecido por *Amazon Web Services*.

preocupados" com a adoção de soluções hospedadas em nuvem (INFO ONLINE, 2009). Toda está preocupação demonstrada está baseada, geralmente, a questões de privacidade das informações que estão na nuvem, a existência de planos de contingência caso a infra-estrutura da nuvem entre em colapso e o possível início de uma "onda" de ataques direcionadas à própria nuvem que poderá se iniciar quando da utilização em larga escala do *Cloud Computing*.[6]

Em relação a todas estas questões, cria-se a necessidade de ações, estudos e debates de forma a estabelecer as melhores práticas e padrões para as empresas que oferecem serviços de *Cloud Computing*, proporcionando assim um ambiente cada vez mais seguro para comportar os dados e aplicações de empresas e também a manutenção da privacidade dos dados de usuários comuns. Neste contexto, podemos citar como uma iniciativa de destaque da ENISA (European Network and Information Security Agency)[7] que publicou, em novembro de 2009, o relatório "*Cloud Computing: Benefits, risks and recomendation for information security*" feito por especialistas na área de *Cloud Computing* da indústria, acadêmicos e membros governamentais. Neste relatório, destacamos a lista que contém os principais problemas de segurança, as vulnerabilidades e os riscos, as recomendações para garantir a segurança de clientes de empresas que oferecerão serviços de *Cloud Computing*, as recomendações legais para a utilização e oferecimentos do serviço e, por último, as recomendações sobre a criação de mecanismos específicos para auditoria, coleta de evidências e análise forense.

3. Crimes Eletrônicos X Perícia Forense

3.1 Crimes Eletrônicos

No tópico anterior, na qual foram abordados os problemas de segurança de *Cloud Computing,* foi citada a preocupação com os possíveis ataques que *crackers* poderão realizar na nuvem. Porém, a preocupação com os crimes eletrônicos não está relacionada apenas a nuvem e aos profissionais de TI e sim estendida a todas as tecnologias, arquiteturas, mecanismos, usuários e profissionais envolvidos com o "universo digital". Esta nova modalidade de crime, que pode ser assim descrito, faz-se do uso dos meios computacionais como meio ou fim para as práticas de atividades ilícitas e já no ano de 2006, segundo pesquisa conduzida pela IBM, 100% dos usuários temiam mais o cibercrime do que os delitos físicos (CORIOLANO, 2008). Pesquisas mais recente mostram, inclusive, que a receita do cibercrime já é mais lucrativa do que a do narcotráfico (ITWEB, 2009), o que mostra que a incidência deste tipo de crime tende a aumentar.

Este aumento no número de ocorrências está provocando, no Brasil, um impacto, não apenas em relação à discussão quanto a criação ou não de novas leis para tipificação dos crimes eletrônicos[8], mas, principalmente, no que se refere a perícia forense.

---

[6] Segundo Mark Nicolett, vice-presidente de pesquisas da Gartner: "A computação em nuvem atrai *hackers* [*crackers*, seria o mais correto], porque há muito dado corporativo em um único lugar" (INFO ONLINE,2009).

[7] ENISA é uma agência que têm, como um dos objetivos, desenvolver a segurança da informação na União Européia.

[8] Há mais de 10 anos tramita no Congresso o projeto de Lei nº 84/1999 para Crimes Eletrônicos.

3.2 Perícia forense digital: a adoção da cadeia de custódia para garantir a integridade das evidências

Pode-se entender como perícia forense a atividade realizada, geralmente por um especialista nesta, objetivando a produção de assertivas fundamentadas sobre o fato investigado. A pericia forense digital neste contexto, pode ser entendida como mais um ramo da perícia forense e definida segundo Dan Farmer[9] como: "(..) a captura e análise de evidências tanto quanto possível livres de estarem distorcidas ou tendenciosas, de tal forma a reconstruir determinados dados ou o que aconteceu num sistema do passado".

Para a guarda destas evidências que constituem o material probatório, entendemos que a cadeia de custódia é uma técnica fundamental a ser utilizada na perícia forense de forma que a justiça não tenha motivos para considerá-lo, no futuro, como fonte de uma prova ilícita.

Mas o que seria uma cadeia de custódia? A cadeia de custódia é um procedimento aplicável a todos os tipos de perícia, inclusive a digital, e pode ser definida como: um processo usado de forma a comprovar que o material probatório não sofreu nenhum tipo de alteração desde a sua apreensão e durante todo o processo judicial, registrando, de forma a prover um histórico da movimentação ou manuseio, todas as ocorrências de sua tramitação. Isto é muito importante, porque caso haja qualquer indício de que o material sofrera algum tipo de alteração pode fazer com que o seu valor probatório seja questionado e, desta forma, trazer consequências muito graves para o andamento do processo.

Segundo consenso entre especialistas, a cadeia de custódia em meios digitais possui alguns passos mínimos a serem seguidos para garantir a integridade do material fruto da investigação. São eles:

- A perícia deve ser realizada na cópia da mídia e o seu original deve ser preservado. Alguns especialistas recomendam neste caso até mesmo duas cópias de segurança, uma para análise e outra a ser utilizada caso a primeira apresente algum tipo de problema.
- Primeiramente, deve-se calcular o *hash*[10], de preferência utilizando para isso dois tipos de algoritmos, da mídia original antes de copiá-lo.
- Após realizar a cópia da mídia, em que devem ser adotados alguns cuidados, comparar o *hash* da mídia original com os das cópias. É recomendável que se faça uma ata notarial[11] com o *hash* de cada uma das cópias e o registro que o *hash* das cópias é o mesmo *hash* da mídia original.
- A cada novo contato com as cópias, deve-se registrar quem a acessou, data e hora.

---

[9] Citação extraída de **Conceitos para perícia forense computacional** de Cansian, Adriano Mauro. UNES. Dan Farmer é um renomado pesquisador americano em segurança de computadores.

[10] *Hash* é uma sequência de bits produzidos por um algoritmo computacional que permite, dentre outras coisas, a identificação única de uma informação ou arquivo.

[11] Ata notarial é um instrumento que consiste em uma narração objetiva dos fatos observados e presenciados por um Tabelião. A ata notarial permite que se dê credibilidade ao fato observado, já que o Tabelião possui fé pública.

No entanto, no Brasil, os procedimentos a serem seguidos para garantir a cadeia de custódia em meios digitais não são formais ou legais, em termos jurídicos, o que se aplica também a outras técnicas usadas na pericia digital. Entendemos que a presença, pelo menos mínima, de procedimentos formais ou previstos na lei para a produção da prova pericial seria fundamental e evitaria muitos dos questionamentos e dúvidas apontadas pela partes durante o processo judicial. A falta de procedimentos formais tende a se agravar ainda mais com o *Cloud Computing* que trará ainda outras dificuldades e problemas para a forma que a perícia forense computacional é feita hoje. Abordaremos este assunto a seguir.

4. O processo de pericia forense sobre a nova ótica de *Cloud Computing*

4.1 Cloud Computing e os novos desafios para a pericia forense digital

A ausência atual de normas formais previstas contratualmente na oferta de serviços de Cloud Computing cria um ambiente de apreensão não só para profissionais da perícia forense, mas em todos envolvidos na busca da verdade processual. Para reforçar ainda mais este clima de apreensão e dúvidas Jeff Barr[12], em outubro de 2008, foi incapaz de responder a perguntas sobre quais "cuidados" os vendedores estão tendo para permitir que futuras investigações forenses no ambiente de *Cloud Computing* procedam de forma eficaz. (ZDNET, 2009). Entretanto, esta falta de aspectos formais na oferta deste tipo de serviço é apenas uns dos desafios atuais, neste novo cenário, para a perícia digital.

Há uma tendência para que em um futuro próximo, conforme já dito, tenhamos os dados, os softwares e também a infraestrutura localizados na nuvem[13] em servidores que são propriedade de terceiros e não mais de "forma local". Desta forma, o perito poderá não ter mais, em muitas ocasiões, o acesso ao disco rígido, infraestrutura e o controle sobre a rede do ambiente a ser investigado, o que hoje são requisitos fundamentais em muitas das perícias a serem realizadas para obter-se um laudo pericial completo e fundamentado.

4.2 Legislação Brasileira aplicada ao processo de perícia forense e os problemas relacionados ao surgimento dos novos desafios

No Brasil temos, tanto no código penal como no cível, alguns artigos que ditam como as perícias devem ser realizadas. A seguir, iremos analisar alguns dos artigos do decreto de lei 3689/41, do Código de Processo Penal, que determinam o processo de perícia e, de acordo com esses, os problemas relacionados aos novos desafios trazidos pelo *Cloud Computing*.

Do Capítulo II - Do Exame do Corpo de Delito e das Perícias em Geral

Artigo 158. Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado.

---

[12] Jeff Barr é um profissional de *Web Services* da Amazon.

[13] Segundo John Herlihy, executivo do Google, em três anos os computadores pessoais serão irrelevantes.

Artigo 167. Não sendo possível o exame de corpo de delito, por haverem desaparecido os vestígios, a prova testemunhal poderá suprir-lhe a falta.

Podemos resumir e entender os artigos acima como a necessidade da realização da perícia, quando da ocorrência de um crime, mesmo com o conhecimento da autoria e se, ao comprovar o desaparecimento dos vestígios, terem-se o testemunho como seu substituto. Com o novo cenário de *Cloud Computing*, podemos relacionar os seguintes problemas:

- Conforme já citado, não temos formalização quanto as normas contratuais na oferta de serviços de *Cloud Computing*, desta forma não estão previstas atualmente ferramentas e a garantia de que os dados ainda estarão disponíveis para a realização da perícia o que pode impossibilitar o exame de corpo de delito. Para apoiar esta preocupação segundo a consultoria Gartner: "Serviços de *Cloud* são especialmente difíceis de investigar, porque os logs e dados de vários clientes podem estar localizados conjuntamente e também estar distribuídos com uma constante mudança no conjunto de máquinas e *data centers*. Se você não conseguir um compromisso contratual para apoiar formas específicas de investigação - juntamente com evidências de que o vendedor já tenha apoiado com sucesso tais atividades - então a sua única suposição segura é de que os pedidos de investigação e descoberta serão impossíveis."(ZDNET UK,2009, nossa tradução).[14]

- Conforme exposto, com a possibilidade de não ser possível o exame de corpo de delito a prova testemunhal poderá suprir-lo falta. Porém é muito complicado em meios digitais, devido à volatilidade das informações e a necessidade muitas vezes do conhecimento técnico para a narrativa dos fatos, se fazer o testemunho de forma que as informações constantes do tal não sejam questionadas quanto a sua veracidade.

Por último, analisamos o impacto para os seguintes artigos:

Artigo 159. Parágrafo Sexto. Havendo requerimento das partes, o material probatório que serviu de base à perícia será disponibilizado no ambiente do órgão oficial, que manterá sempre sua guarda, e na presença de perito oficial, para exame pelos assistentes, salvo se for impossível a sua conservação. (Incluído pela Lei nº 11.690, de 2008)
Artigo 169. Para o efeito de exame do local onde houver sido praticada a infração, a autoridade providenciará imediatamente para que não se altere o estado das coisas até a chegada dos peritos, que poderão instruir seus laudos com fotografias, desenhos ou esquemas elucidativos.
Art.169. Parágrafo único. Os peritos registrarão, no laudo, as alterações do estado das coisas e discutirão, no relatório, as conseqüências dessas alterações na dinâmica dos fatos. (Incluído pela Lei nº 8.862, de 28.3.1994)

[14] Citação original: "Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation—along with evidence that the vendor has already successfully supported such activities—then your only safe assumption is that investigation and discovery requests will be impossible".

Resumindo o que está descrito nos artigos citados acima, o material fruto da investigação deve ser preservado. Uma boa prática para isso é, conforme visto, a cadeia de custódia, porém o *Cloud Computing* também traz problemas à preservação deste material, como o que segue:

- Com esta nova tendência, o material probatório estará armazenado em servidores de terceiros. Desta maneira, como será feito a cadeia de custódia quando este material estiver na nuvem? Basicamente, conforme já exposto, a cadeia de custódia consiste em verificar a cada passo da investigação a integridade do material através do *hash*, porém, quando este estiver armazenado na rede, muitas vezes não haverá a capacidade de acesso, seja de forma lógica ou mesma física, que poderá impossibilitar desta maneira uma cadeia de custódia adequada.

Conclusão

O *Cloud Computing* é uma tendência que crescerá nos próximos anos, conforme vimos, proporcionando as empresas economia de recursos e foco em seus negócios e aos usuários comuns comodidade e menos gastos na utilização de softwares do dia-a-dia.

E como ocorre para quase todas as novas tendências tecnológicas, assim como telefones celulares, rede sem fio e novos tipos de criptografia, a computação nas nuvens está trazendo mais complexidade e novos desafios que exigirão uma adaptação e também a evolução tanto para o processo de perícia digital como também tudo envolvido a ele.

No Brasil, esta evolução justifica-se pela análise dos artigos abaixo da lei 3689/41 do nosso código penal:

Título VII - Da Prova, Capítulo I - Disposições Gerais

Art. 157. São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais. (Redação dada pela Lei nº 11.690, de 2008).
Parágrafo Primeiro. São também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo de causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras. (Incluído pela Lei nº 11.690, de 2008).

Do Capítulo II - Do Exame do Corpo de Delito e das Perícias em Geral

Art. 181. No caso de inobservância de formalidade ou no caso de omissões, obscuridades ou contradições, a autoridade policial ou judiciária mandará suprir a formalidade ou completar ou esclarecer o laudo.
Parágrafo único. A autoridade poderá também ordenar que se proceda a novo exame, por outros peritos, se julgar conveniente.
Art. 182. O juiz não ficará adstrito ao laudo, podendo aceitá-lo ou rejeitá-lo, no todo ou em parte.

Analisando estes artigos comprova-se a preocupação com a preservação, e a adoção de procedimentos adequados na produção da prova pericial de forma que a mesma não seja questionada, considerada como ilícita ou mesmo rejeitada pelo juiz.

Concluímos que, para que isto não aconteça e ao mesmo tempo haja a possibilidade da produção de uma prova pericial completa e fundamentada são necessários:

- A formalização dos procedimentos, pelo menos os globais, que são utilizados na produção da prova pericial digital e também, principalmente, dos que se referem à garantia da cadeia de custódia levando-se em conta as mudanças trazidas pelo *Cloud Computing.*
- Um tratado internacional de colaboração em investigação de crimes digitais assinado, de preferência, pela maior parte dos países. Com isto, poderão ser evitados problemas legais nos casos em que a investigação possa ferir a jurisdição de um país onde está localizada fisicamente a nuvem bem como facilitar a captura e preservação das evidências. Citamos como iniciativa de destaque o Tratado de Budapeste na qual o Brasil ainda não é signatário.
- E uma presença cada vez maior de iniciativas como o da ENISA e outros órgãos para promover, entre outras coisas, a formalização das normas contratuais na oferta destes tipos de serviço garantindo a preservação e acesso adequado às evidências, de forma a não violar a privacidade de outros usuários da nuvem.

Referências Bibliográficas

AMAZON WEB SERVICES. **Amazon Simple Storage Service.** Disponível em: <http://aws.amazon.com/s3/>. Acesso em: 04 mar. 2010.

BIGSEY. **Cloud Computing & The Impact On Digital Forensic Investigations**. Disponível em: <http://www.zdnet.co.uk/blogs/cloud-computing-and-the-impact-on-digital-forensic-investigations-10012285/cloud-computing-and-the-impact-on-digital-forensic-investigations-10012286/>. Acesso em 07 mar. 2010.

BLUM, Renato Opice, JARDIM, Victor E. M. Costa.. **Os avanços nacionais no combate aos crimes eletrônicos**. Disponível em: <http://www.revistaagente.com.br/os-avancos-nacionais-no-combate-aos-crimes-eletronicos/>. Acesso em 10 mar. 2010.

CANSIAN, Adriano Mauro. **Conceitos para perícia forense computacional**. UNESP.São José do Rio Preto. Disponível em: <http://www.acmesecurity.org/~adriano/docs/eri2001/artigo-adr-icmc-2001.pdf>. Acesso em: 20 mar. 2010.

ENISA. **Cloud Computing - Benefits, risks and recommendations for information security**. 20 nov. 2009. Disponível em: <http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment>. Acesso em 07 mar. 2010.

GOOGLE INC. **Welcome to Google Docs.** Disponível em: < http://docs.google.com/>. Acesso em: 04 mar. 2010.

ITWEB**. Receita do cibercrime supera a do comércio mundial de drogas**. Disponível em: <http://www.itweb.com.br/voce_informa/interna.asp?cod=2967>. Acesso em: 08 mar. 2010.

ITWEB, **Segurança na nuvem: é preciso identificar os problemas**. Disponível em: <http://www.itweb.com.br/noticias/index.asp?cod=62822>. Acesso em: 03 mar. 2010.

JUSBRASIL. **Código Processo Penal - Decreto-lei 3689/41 | Decreto-lei Nº 3.689, de 3 de outubro de 1941**. Disponível em: <http://www.jusbrasil.com.br/legislacao/91622/codigo-processo-penal-decreto-lei-3689-41>. Acesso em: 09 mar. 2010.

LOPES, M., GABRIEL, M. M., BARETTA, G. M. S.. **Cadeia de Custódia: Uma abordagem preliminar**. Disponível em: <http://calvados.c3sl.ufpr.br/ojs2/index.php/academica/article/viewArticle/9022. Acesso em: 13 mar. 2010.

MICROSOFT. **Windows Azure Platform.** Disponível em: <http://www.microsoft.com/windowsazure/>. Acesso em 04 mar. 2010.

MOREIRA, Daniela. **Computação em nuvem preocupa empresas**. Disponível em: <http://info.abril.com.br/professional/seguranca/computacao-em-nuvem-preocupa-ti.shtml>. Acesso em 04 mar. 2010.

NIST. **The NIST Definition of Cloud Computing.** 2009. Disponível em: <csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc> Acesso em 04 mar. 2010.

NOGUEIRA, Matheus Cadori, PEZZI, Daniel da Cunha. : **A Computação agora é nas nuvens**.

SANTOS, Corioloano A. A. C.. **Atual Cenário dos Crimes Cibernéticos no Brasil**. 2008.

SENASP. **Busca e Apreensão - Aula 1 Conceitos e Enfoques Básicos**. Disponível em: <http://senasp.dtcom.com.br/modulos/educacional/material_apoio/aula1.pdf>. Acesso em 12 mar. 2010.

SHIPLEY, Todd. **Collection of Evidence from the Internet, Part 2**. Disponível em: <http://www.dfinews.com/articles.php?pid=790>. Acesso em: 10 mar. 2010.

SOUZA, Flávio R. C., MOREIRA Leornardo O., MACHADO Javam C.. **Computação em Nuvem: Conceitos, Tecnologias, Aplicações e Desafios**. UFC. Disponível em: <http://www.es.ufc.br/~flavio/files/Computacao_Nuvem.pdf>. Acesso em: 16 mar. 2010.

TEIXEIRA,Alexandre, ESES Nicholas I., CABRAL, Carlos, RAMOS, Robson da S.. **Robustez da Prova Digital. A importância do Hash no Processo Judicial**. Universidade Presbiteriana Mackenzie. 2010.

TUTIKIAN, Cláudia Fonseca. **O instrumento da ata notarial no processo trabalhista**. Jus Navigandi, Teresina, ano 9, n. 733, 8 jul. 2005. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=6975>. Acesso em: 20 mar. 2010.

WIKIPEDIA. **Computação em nuvem**. Disponível em: <http://pt.wikipedia.org/wiki/Computa%C3%A7%C3%A3o_em_nuvem>. Acesso em: 07 mar. 2010.

WIKIPEDIA. Dan Farmer. Disponível em: <http://en.wikipedia.org/wiki/Dan_Farmer>. Acesso em: 13 mar. 2010.

WIKIPEDIA. **European Network and Information Security Agency**. Disponível em: http//en.wikipedia.org/wiki/European_Network_and_Information_Security_Agency. Acessom em 12 mar. 2010.

WIKIPEDIA**. Hash**. Disponível em: <http://pt.wikipedia.org/wiki/Hash>. Acesso em 14. Mar.2010.

ZMOGINSKI, Felipe. **Em três anos desktops serão irrelevantes**. Disponível em: <http://info.abril.com.br/noticias/tecnologia-pessoal/em-tres-anos-desktops-serao-irrelevantes-04032010-36.shl>. Acesso em 15 mar. 2010.