SEGURANÇA DAS NUVENS COMPUTACIONAIS: UMA VISÃO DOS PRINCIPAIS PROBLEMAS E SOLUÇÕES

NELSON MIMURA GONZALEZ

CHARLES CHRISTIAN MIERS

FERNANDO FROTA REDÍGOLO

MARCO ANTÔNIO TORREZ ROJAS

TEREZA CRISTINA MELO DE BRITO CARVALHO

RESUMO

O uso da computação em nuvem traz um novo paradigma para o fornecimento de serviços computacionais, no qual não é necessário possuir todos os recursos para poder disponibilizar um serviço e, principalmente, só é preciso pagar a quantidade de recursos consumida. Contudo, o custo financeiro não é o único fator determinante para a adoção ou migração para nuvens computacionais, mas, sim, a segurança dos serviços. Este artigo tem como objetivo identificar as principais questões (problemas e soluções) de segurança relacionadas à computação em nuvem, assim como classificar e analisar quantitativamente cada uma das questões identificadas. A análise quantitativa fornece informações sobre a concentração das pesquisas relacionadas à segurança computacional das nuvens, assim como uma comparação entre os problemas e soluções identificados.

Palavras-chave: computação em nuvem, segurança computacional, classificação de segurança.

ABSTRACT

The use of cloud computing has ushered in a new paradigm for delivering computing services, the one in which one does not need to have all the resources to be able to provide a service, and mainly, it is a paradigm in which users only pay for the resources they actually use. However, financial cost is not alone the decisive factor for adopting or migrating to cloud computing, but rather the safety in the services that are provided. This article aims at identifying the primary safety issues (problems and solutions) related to cloud computing, as well as classifying and analyzing quantitatively each one of the identified issues. The quantitative analysis has yielded information on the concentration of research related to safety in computing clouds, and also a comparison between the identified problems and solutions.

Keywords: *cloud computing, computing safety, safety classification.*

INTRODUÇÃO À SEGURANÇA EM COMPUTAÇÃO EM NUVEM

O modelo de computação em nuvem tem sido visto como uma solução para as demandas crescentes dos usuários dos serviços de tecnologia da informação: serviços cada vez mais confiáveis e de melhor desempenho, disponíveis sempre que necessário, acessíveis de diferentes lugares via Internet e de diferentes dispositivos, tais como computadores, celulares e *tablets*. Dados esses benefícios, muitas organizações têm optado pelo uso de serviços de computação em nuvem, sendo que, em alguns casos, esses benefícios são obtidos a um custo inferior ao que se teria em soluções tradicionais.

O modelo de computação em nuvem, no entanto, traz consigo uma série de desafios de segurança que devem ser analisados e endereçados por todos os envolvidos no modelo (tanto usuários como provedores de serviços). A falta de entendimento e atenção às questões de segurança pode trazer reflexos negativos para as empresas e para os indivíduos que fazem uso de tais serviços. Um exemplo dessa situação foi a falha do serviço AWS (Amazon Web Services) em abril de 2011, que afetou a grande maioria dos *sites* que se utilizavam da sua infraestrutura, localizada na costa leste dos EUA. Entre os afetados estão *sites* famosos, que utilizam os recursos da AWS para oferecer os seus serviços, como: Quora, Reddit, FourSquare e Everyblock (Gilbertson, 2011).

Outro exemplo de problema de segurança associado à computação em nuvem foi o vazamento das senhas do Evernote em fevereiro de 2013, cujo impacto foi percebido pelos 50 milhões de usuários registrados no serviço, que tiveram que trocar sua senha (Cluley, 2013).

Tais problemas, porém, não são provas de que o modelo de computação em nuvem seja inerentemente inseguro. As ameaças de segurança são inerentes a ambientes *online*, independentemente da adoção ou não do modelo de computação em nuvem. Apesar de o vazamento de senhas do Evernote indicar que faltaram mecanismos para a proteção desse conteúdo (sendo, portanto, de responsabilidade da empresa), o vazamento não foi total, uma vez que os dados dos usuários armazenados no serviço não foram comprometidos. No caso do problema da Amazon, porém, a questão é diferente: por que nem todas as empresas usuárias foram afetadas? Na verdade a resposta reside em um entendimento da estrutura do serviço da Amazon: ao contratar o serviço, um usuário deve decidir em quais regiões esse serviço será executado (por exemplo, na costa leste dos EUA,

NELSON MIMURA GONZALEZ é pesquisador no Laboratório de Arquitetura e Redes de Computadores (Larc) da EP-USP.

CHARLES CHRISTIAN MIERS é professor adjunto na Universidade do Estado de Santa Catarina (Udesc).

FERNANDO FROTA REDÍGOLO pesquisador e coordenador de projetos no Larc/EP-USP.

MARCO ANTÔNIO TORREZ ROJAS é pesquisador no Larc/EP-USP.

TEREZA CRISTINA MELO DE BRITO CARVALHO é professora livre docente do Departamento de Computação e Sistemas na EP-USP, coordenadora-geral do Lassu (Laboratório de Sustentabilidade em TIC) e diretora técnica do Larc/EP-USP.

Agradecemos ao Centro de Inovação Ericsson Telecomunicações S. A. do Brasil pelo suporte e financiamento do projeto correlacionado ao tema deste artigo.

em São Paulo, na Europa, entre outros). Apesar de cada região possuir redundâncias para garantir que o serviço sobreviva à falha de alguns componentes (por exemplo, um disco ou mesmo um servidor), é possível ainda haver falhas maiores que afetem uma região inteira (o furacão Sandy, por exemplo, em 2012, deixou diversas cidades sem energia por dias, entre as quais Nova York). No caso da falha da Amazon, em 2011, as empresas que decidiram por distribuir a carga entre diferentes regiões não tiveram o seu serviço afetado de forma significativa.

A discussão sobre a segurança de um ambiente em nuvem frequentemente recai sobre uma questão de equivalência (Jansen & Grance, 2011): será que a nuvem tem o mesmo nível de segurança que a estrutura atual da minha empresa? Há, porém, outra questão que deve ser feita: será que a empresa que está contratando os serviços de nuvem tem o mesmo nível de segurança de um serviço de nuvem? Tal questão deve-se ao fato de que os provedores desses serviços podem contar com recursos e procedimentos nem sempre disponíveis ou implantados nas organizações (especialmente de pequeno e médio portes), tais como (Tompkins, 2009):

- profissionais com alto nível de capacitação técnica, incluindo especialistas em segurança;
- investimento em mecanismos sofisticados de segurança, tanto em *hardware* quanto em *software*;
- ambientes redundantes de computação; aderência a padrões de segurança;
- gerenciamento e monitoração de requisitos de segurança; e
- procedimento para identificação e resposta a incidentes de segurança.

Dessa maneira, para a adoção segura de serviços de computação em nuvem, é importante entender as principais questões de segurança associadas ao modelo, bem como o papel que os usuários e os provedores de serviço têm em relação à segurança, tanto da nuvem como do ambiente atual de computação.

VISÕES DE SEGURANÇA PARA NUVENS COMPUTACIONAIS

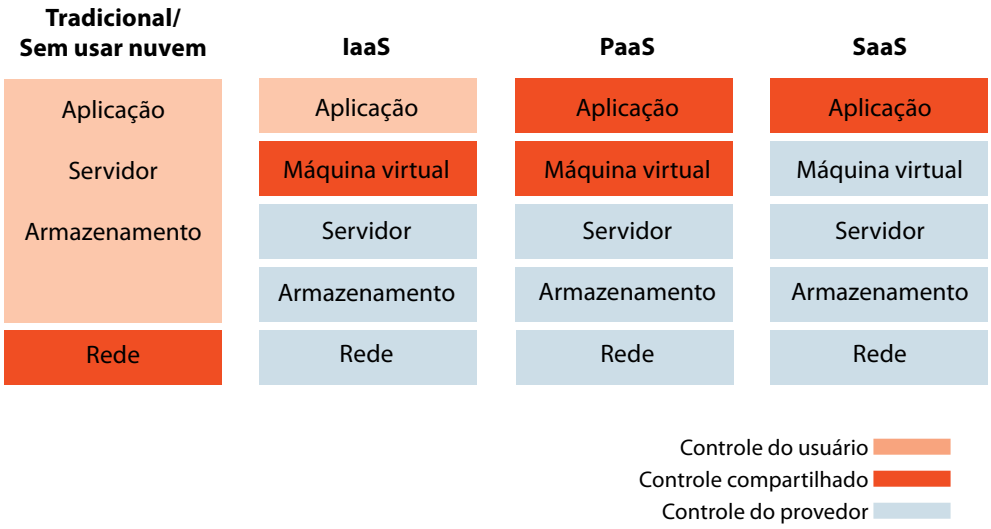
Se, por uma perspectiva, a computação em nuvem já possui dentro do seu modelo vários recursos de segurança e isso é interpretado como um benefício, também pode haver algumas características do modelo que podem ser interpretadas como problemas. Nesse sentido, é necessário que usuários e provedores de serviços de computação em nuvens tenham consciência das suas responsabilidades.

As responsabilidades pela segurança dos serviços executados em nuvens computacionais mudam de acordo com o tipo de serviço e recursos oferecidos. Contudo, sempre há responsabilidades tanto por parte do usuário como do provedor e, desse modo, nenhuma das partes é desprovida de responsabilidades no âmbito de segurança. De fato, o que ocorre em cada modelo de serviço é uma delimitação dessas responsabilidades. A Figura 1 ilustra uma visão genérica da delimitação de controle dos recursos de computação em relação a usuário e provedor com base na notação comum de modelos de serviço do National Institute of Standards and Technology – Nist (Gilbertson, 2011): IaaS – *Infrastructure as a Service*, PaaS – *Platform as a Service* e SaaS – *Software as a Service*.

A Figura 1 permite identificar que mesmo em serviços tipo SaaS ainda há responsabilidade compartilhada entre usuário e provedor. Além disso, fica evidente a parcela considerável de recursos que é de responsabilidade do provedor do serviço de nuvem em todos os modelos de serviço. Desse modo, pode-se afirmar que quem (usuário ou provedor) possui algum controle (total ou compartilhado) sobre um elemento da nuvem (rede, armazenamento, servidor, máquina virtual ou aplicação) possui também a responsabilidade sobre a segurança desse elemento. Um exemplo disso é o serviço de disco virtual do Dropbox (tipo SaaS), no qual a maior parte dos recursos é controlada pelo provedor e existe um procedimento de definição de senhas não

FIGURA 1

DELIMITAÇÃO USUAL DO CONTROLE DOS RECURSOS POR MODELO DE SERVIÇO



triviais, o que não impede o usuário de divulgar a sua senha de maneira indevida e comprometer seu serviço. A Figura 1, contudo, também possibilita uma identificação inicial das origens de alguns problemas de segurança com base nas responsabilidades do usuário e do provedor, assim como nos recursos controlados pelo mesmo usuário/provedor. As nuvens computacionais podem ser disponibilizadas usando diferentes modelos de implantação (privada, comunitária, pública e híbrida) sendo que o modo como os recursos são acessados é essencialmente similar.

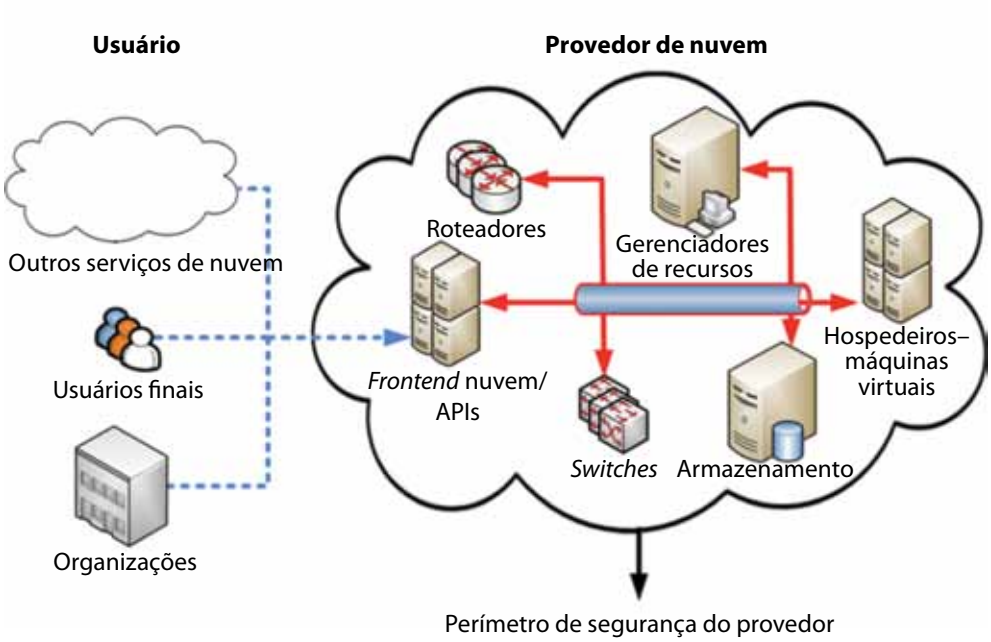
A Figura 2 apresenta uma visão, sob a ótica da organização lógica da infraestrutura das redes de computadores, do acesso aos recursos computacionais fornecidos por uma nuvem computacional do tipo privado.

A Figura 2 permite identificar que o acesso do lado do usuário (linhas de cor azul/tracejada) aos serviços do provedor de nuvem necessita ultrapassar o perímetro de segurança do provedor, que é comumente bem controlado e provido de recursos de segurança. Continuando a análise dessa figura, também é possível perceber que, dentro do provedor de nuvem, há várias interações que acontecem (linhas contínuas dentro da nuvem/cor vermelha) a fim de gerir a própria nuvem e fornecer os serviços solicitados pelos usuários. Nesse sentido, os mecanismos e controles de segurança normalmente não são acessíveis (ou até mesmo visíveis) por parte do usuário. Tal fato leva o usuário do serviço de nuvem a confiar que a segurança é tratada satisfatoriamente dentro dela.

As perspectivas mostradas nas figuras 1 e 2 permitem identificar, de um modo geral, as responsabilidades pelos recursos e, por consequência, pela sua segurança. Outro aspecto a ser considerado sobre as nuvens computacionais é a sua composição baseada em conjuntos de serviços já existentes (por exemplo, virtualização, serviços de gerenciamento de rede, etc.), que já trazem consigo questões de segurança oriundas de sua natureza individual e outras oriundas da associação desses recursos. Nesse sentido, é relevante identificar e classificar as principais questões de segurança (problemas e suas possíveis soluções) de modo a poder ter uma percepção das questões de segurança envolvidas na computação em nuvem.

FIGURA 2

VISÃO DE ACESSO AOS RECURSOS DA NUVEM
POR PARTE DE USUÁRIO E PROVEDOR



CLASSIFICAÇÃO DOS PRINCIPAIS PROBLEMAS DE SEGURANÇA EM NUVENS COMPUTACIONAIS

Instituições de pesquisa como a Cloud Security Alliance – CSA (Simmonds, Rezek & Reed, 2011) e a European Network and Information Security Agency - Enisa (Catteddu & Hogben, 2009) destacam diversos problemas de segurança que precisam ser tratados no contexto de computação em nuvem, não apenas para tornar as soluções mais seguras como também para aumentar o grau de adoção da tecnologia tanto por parte do ambiente acadêmico como também pelo mercado.

Com o objetivo de facilitar o estudo dos problemas de segurança em computação em nuvem, é relevante classificá-los. A classificação empregada para esse fim possibilita uma rápida identificação dos aspectos fundamentais de segurança e permite identificar de maneira mais clara os esforços de pesquisa realizados em cada categoria. A classificação apresentada está dividida em sete categorias (segurança de rede, interfaces, segurança de dados, virtualização, governança, conformidade e questões legais), que se subdividem em categorias menores (Gonzalez et al., 2012).

Segurança de rede

Nesta classificação, a categoria de segurança de rede refere-se a problemas de segurança associados às redes de comunicações, bem como às interações entre os elementos de processamento e armazenamento da nuvem. Neste contexto devem ser consideradas as seguintes subcategorias:

- transferências: arquiteturas distribuídas, compartilhamento de recursos em larga escala e sincronização de máquinas virtuais implicam maior fluxo de dados dentro da nuvem, o que requer a utilização de

mecanismos de proteção dessas informações (por exemplo, através de VPN – *virtual private networks*) contra ataques que exploram vulnerabilidades nos meios de comunicação;

- *firewalls*: oferecem proteção da infraestrutura do provedor da nuvem contra ataques externos e também internos. Esses mecanismos de controle de acesso também permitem isolamento, filtragem de endereços e portas de acesso, prevenção de ataques de negação de serviço (DoS – *deny of service*) e detecção de procedimentos de análise de segurança;
- configurações de segurança: incluem configurações de protocolos, sistemas e tecnologias, de modo a oferecer diferentes níveis de segurança e privacidade tanto para o provedor como para os seus usuários.

Interfaces

As interfaces de acesso às nuvens são os meios que permitem a utilização do serviço por parte dos usuários, bem como a execução de tarefas administrativas e de controle do sistema. Neste contexto devem ser consideradas as seguintes subcategorias de interfaces:

- API: interfaces de programação (*application programming interfaces*) que permitem a integração de sistemas e programas em termos de código. Constituem um elemento fundamental para PaaS e IaaS, pois permitem o acesso aos recursos virtualizados e aos sistemas oferecidos na nuvem e que devem ser protegidos contra o uso malicioso ou indevido (Rose, 200);
- administração: interfaces de acesso que permitem realizar a administração/gerenciamento de recursos da nuvem. Isso representa o gerenciamento de recursos de um IaaS, do desenvolvimento de plataformas oferecidas por um PaaS, ou das aplicações e respectivas configurações de um SaaS;
- usuário: interfaces oferecidas ao usuário final para utilização dos recursos e ferramentas oferecidos através da nuvem (o que representa o serviço propriamente dito) e, que requerem, portanto, a adoção de medidas de segurança adequadas (Espiner, 2007.);
- autenticação: interfaces de protocolos que possibilitam realizar a autenticação para acesso à nuvem, por exemplo, OpenID (Li et al., 2009). A maioria dos serviços utiliza métodos baseados em contas simples com usuário e senha e estão mais suscetíveis a ataques cujas consequências são potencializadas pelo modelo de hospedagem múltipla (*multi-tenant*) e pelo compartilhamento de recursos inerente ao modelo de nuvem.

Segurança de dados

Está relacionada à proteção dos dados com referência à confidencialidade, disponibilidade e integridade. Com base nesses conceitos, é possível destacar as seguintes subcategorias de mecanismos de segurança de dados:

- criptografia: trata-se de um mecanismo essencial para a proteção de dados sigilosos através de técnicas de cifragem (Musthaler, 2009), largamente empregado em serviços e requerido por padrões legais e de mercado (Yan, Rong & Zhao, 2009);
- redundância: corresponde a um mecanismo básico para evitar a perda de dados e garantir a disponibilidade de serviços. Para esse fim, ao menos as informações críticas de negócio devem ser protegidas em termos de integridade e disponibilidade (Tech, 2010);
- descarte ou remoção dos dados: deve ser completo e definitivo, ao contrário da maioria das técnicas disponíveis (por exemplo, Ext3, NTFS), que apenas removem as entradas dos índices do arquivo na tabela de alocação do sistema de arquivos (Dorion, 2010). Resquícios de dados podem constituir um sério problema de segurança caso as informações sejam sigilosas.

Virtualização

Técnicas de virtualização são empregadas para dividir e organizar os recursos físicos da infraestrutura da nuvem, per-

mitindo separá-los e distribuí-los entre vários clientes através de serviços e aplicações. Esta categoria subdivide-se em:

- isolamento: apesar de existir uma divisão lógica entre os recursos de cada recurso virtualizado (por exemplo, máquina virtual), o *hardware* é essencialmente o mesmo (Jaeger, Sailer & Sreenivasan, 2007). Consequentemente, é possível explorar brechas de segurança que burlem o isolamento entre as máquinas, possibilitando capturar dados de outras máquinas da nuvem;
- *hypervisor*: é o elemento de *software* responsável pela virtualização da infraestrutura. As falhas de isolamento exploradas normalmente incluem falhas de segurança desse elemento, permitindo o acesso ao espaço de disco e à memória de outras máquinas;
- vazamento de dados: ao se explorar vulnerabilidades do *hypervisor*, é possível acessar dados de outros usuários e máquinas, afetando, portanto, a integridade e a confidencialidade dos mesmos (Bakshi & Yogesh, 2009);
- identificação de máquinas virtuais: refere-se à falta de controles de identificação e autorização de máquinas virtuais e outras entidades da nuvem (Krautheim, 2009.);
- ataques entre máquinas virtuais: também denominados *cross-VM attacks*, são tentativas de estabelecer canais de comunicação entre máquinas virtuais para facilitar a obtenção de dados por vias não autorizadas (Ristenpart et. al., 2009).

Governança

Esta categoria inclui problemas relacionados à perda de controle administrativo e de segurança sobre os recursos e os dados à medida que decisões dessa natureza (administrativa/segurança) são incumbidas ao provedor da nuvem (Chow et al., 2009):

- controle de dados: mover os dados para a nuvem significa perder autonomia sobre eles. Embora o usuário tenha certo nível de controle sobre seus arquivos e informações pessoais, o controle nunca é tão assertivo quanto no caso de utilização local;
- controle da segurança: outro ponto da utilização de soluções em nuvem é a perda de controle sobre os níveis de segurança adotados e as respectivas configurações, de modo que o usuário passa a depender integralmente das políticas adotadas pelo provedor.
- *lock-in*: está relacionado ao potencial de dependência de um cliente/usuário em relação a um serviço em particular. Ao adotar o serviço de nuvem, todo um modelo de negócio passa a depender desse serviço (Briscoe & Marinos, 2009). Caso o serviço seja descontinuado ou migrado, diversas consequências em relação aos dados e processos de uma empresa ou usuário em geral podem ser observadas.

Conformidade

Nesta seção são apresentados requisitos de conformidade com diferentes níveis de serviço, disponibilidade, transparência e auditoria (Brandic et al., 2010). Esta categoria subdivide-se em:

- nível de serviço ou *service level agreements* (SLA) (Andrzejak, Yi & Kondo, 2010): estabelece políticas relacionadas a requisitos de disponibilidade de serviço e dos dados, procedimentos de segurança a serem adotados e possíveis relações com requisitos legais;
- disponibilidade: interrupções no fornecimento do serviço não são exclusivas de serviços da nuvem, porém a dependência entre serviços torna esse problema ainda mais grave (Gong et al., 2010);
- auditoria: as análises de segurança e disponibilidade de serviço são baseadas em políticas de auditoria preestabelecidas. Métodos transparentes e eficazes são necessários para avaliar as condições de serviço (Gadia, 2009), e normalmente são requisitos contratuais básicos;
- conformidade de serviço: trata de problemas relacionados às obrigações contratuais estabelecidas para um serviço e seus usuários.

Questões legais

Apresentam-se aspectos relacionados a requisitos legais em geral. Aqui é importante ressaltar que nem sempre todos os aspectos legais de um país são aplicáveis a uma nuvem, visto que algumas nuvens possuem abrangência internacional. Esta categoria subdivide-se em:

- localização dos dados: a localização precisa dos dados na nuvem é incerta, os dados podem estar distribuídos em diversos centros computacionais (por exemplo, *data centers)*, em diferentes países e sob diferentes jurisdições. Essa situação pode gerar conflitos ao se moverem dados de uma localização geográfica para outra (Agarwal, 2010);
- *e-Discovery*: como resultado de uma decisão judicial, os dispositivos de armazenamento podem ser recolhidos para análise forense em uma investigação. Contudo, todos os usuários do serviço cujos dados estão armazenados nesses dispositivos terão seus dados expostos, comprometendo a confidencialidade dos mesmos (Nelson & Simek, 2011);
- privilégios do provedor: o provedor do serviço tem controle parcial ou total sobre sua infraestrutura, além de acesso físico ao *hardware*. Usuários internos maliciosos podem conduzir atividades que comprometam gravemente a integridade e a confiabilidade do serviço como um todo;
- legislação: problemas legais relacionados aos novos conceitos e paradigmas introduzidos pelas tecnologias de computação em nuvem (Pavolotsky, 2010).

ESTADO DOS PRINCIPAIS PROBLEMAS/SOLUÇÕES DE SEGURANÇA PARA NUVENS COMPUTACIONAIS

Ter visão clara dos principais problemas envolvendo computação em nuvem, e como eles podem ser classificados, é a primeira etapa para compreender o contexto de segurança das nuvens computacionais. Com o objetivo de fornecer essa visão, foram pesquisadas mais de duzentas referências (relatórios técnicos, artigos científicos, manuais e outras fontes relevantes), identificando nessas referências cada menção a uma das categorias e subcategorias listadas na seção anterior. Foi adotada uma abordagem quantitativa para identificar o interesse sobre cada categoria, usando o total de referências sobre cada uma. Cada referência foi analisada com o objetivo de identificar quaisquer problemas de segurança em computação em nuvem mencionados, assim como soluções para os mesmos. Desse modo, uma mesma referência pode produzir mais de uma entrada em cada categoria especificada. Vale ressaltar que o objetivo desta análise não é determinar ou afirmar se cada uma das soluções apresentadas resolve completamente um problema. O objetivo é a identificação da quantidade de referências existentes sobre cada questão (problema ou solução) que fornece informação relevante sobre quais as questões que vêm recebendo mais atenção da comunidade e quais ainda não foram tão extensivamente estudadas.

Principais problemas

Os resultados obtidos pela identificação da quantidade de citações sobre os tipos de problemas de segurança em computação em nuvem podem ser observados nas figuras 3 e 4

Analisando-se a Figura 3, percebe-se que os três principais problemas identificados com mais citações são relacionados a questões legais, conformidade de serviço, perda de governança sobre os dados, somando quase um terço das citações encontradas. O primeiro problema técnico de fato encontrado é o de isolamento dos dados e recursos, com 7% das citações. Os problemas menos citados são questões de configuração de serviços, disponibilidade e segurança das interfaces de serviço.

Na Figura 4 fica evidente a predominância de citações relacionadas a questões

FIGURA 3

PROBLEMAS DE SEGURANÇA NA COMPUTAÇÃO EM NUVEM
AGRUPADOS POR SUBCATEGORIA

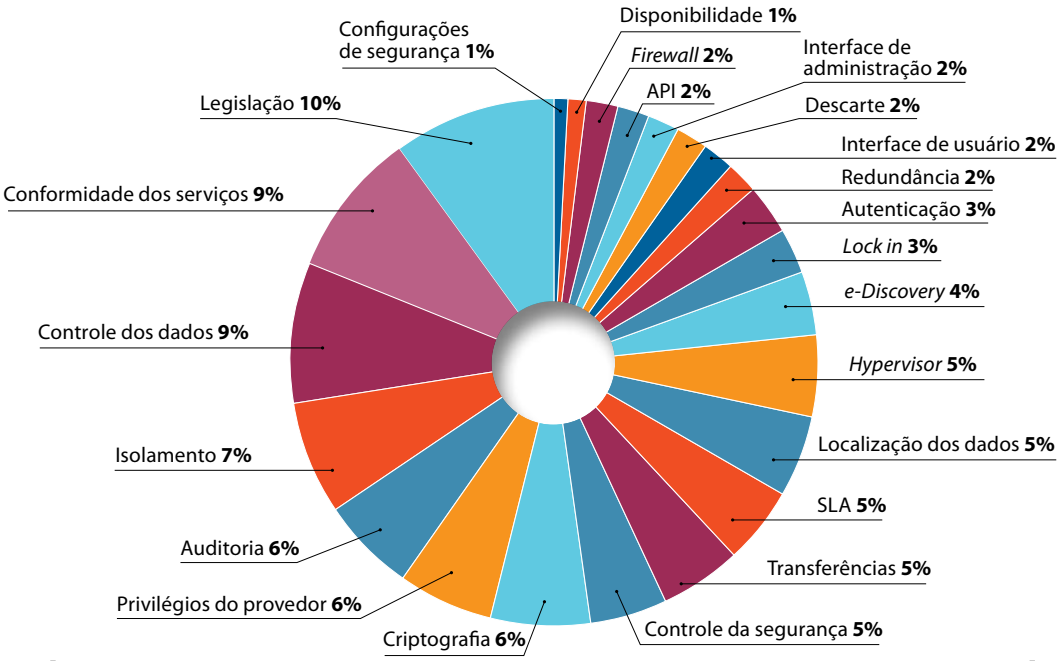
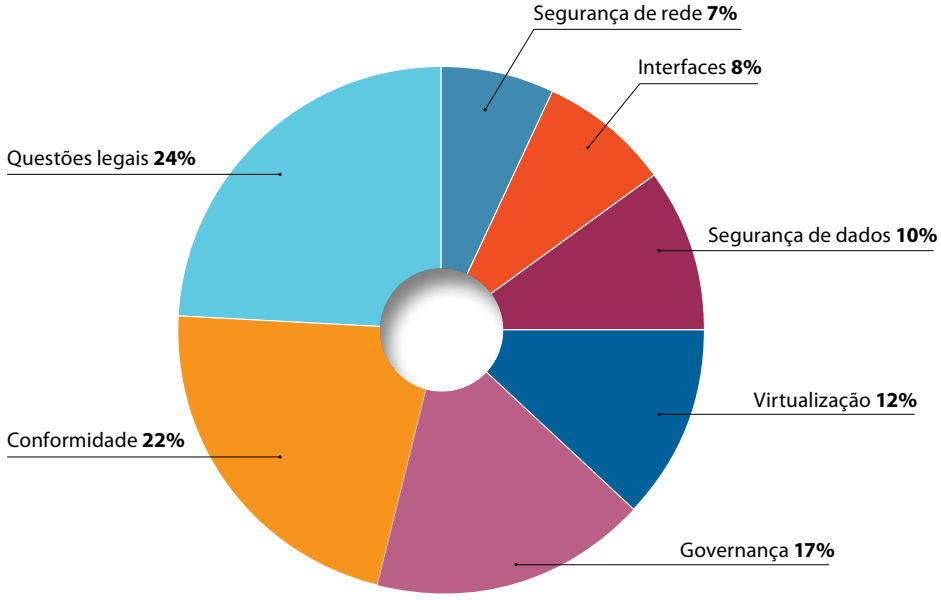


FIGURA 4

PROBLEMAS DE SEGURANÇA NA COMPUTAÇÃO EM NUVEM
AGRUPADOS POR CATEGORIA



legais, conformidade e governança (perda de controle sobre a infraestrutura e sobre o modo como os dados são administrados na nuvem). Dentre as questões técnicas, a de maior impacto é a de virtualização, com 12% das citações. Ao todo, os problemas mais relacionados às tecnologias utilizadas correspondem a 37% do total de citações.

Principais soluções

Para a análise de soluções foi adotada a mesma estratégia: análise das referências buscando citações sobre soluções para os problemas de segurança aqui listados. Os resultados são apresentados nas figuras 5 e 6, em que se constata que o montante de citações de soluções para questões legais ou de conformidade também representa uma grande porção das referências analisadas. Embora exista uma grande preocupação com esses problemas, também há um grande trabalho já em andamento para suprir as necessidades nessas áreas. O mesmo não ocorre com as questões técnicas analisadas anteriormente. Questões relacionadas à virtualização, isolamento de recursos e suas vulnerabilidades possuem poucas citações. Em outras palavras, problemas como este e outros recebem atenção considerável, porém são pouco explorados em termos de pesquisa e desenvolvimento.

Observando-se a figura 6, fica visível a distinção entre a quantidade de citações de problemas e de soluções para cada categoria. Enquanto na análise de problemas a categoria virtualização correspondia a 12% das citações, em termos de soluções a mesma categoria apresenta apenas 3%, uma diferença considerável. Já outras categorias apresentaram um percentual maior de soluções do que de problemas, o que leva à conclusão de que essas áreas estão sendo ativamente exploradas não apenas pela academia, mas também por soluções de mercado já existentes e atualizadas.

FIGURA 5

SOLUÇÕES DE SEGURANÇA NA COMPUTAÇÃO EM NUVEM
AGRUPADAS POR SUBCATEGORIA

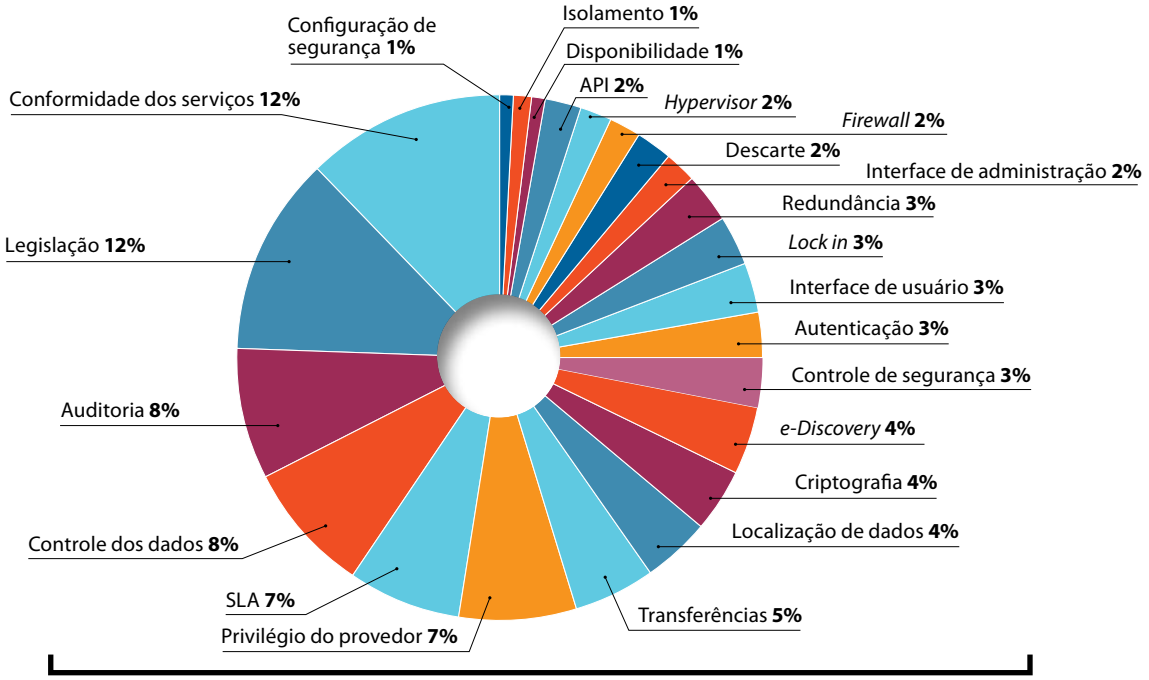


FIGURA 6

SOLUÇÕES DE SEGURANÇA NA COMPUTAÇÃO EM NUVEM
AGRUPADAS POR CATEGORIA

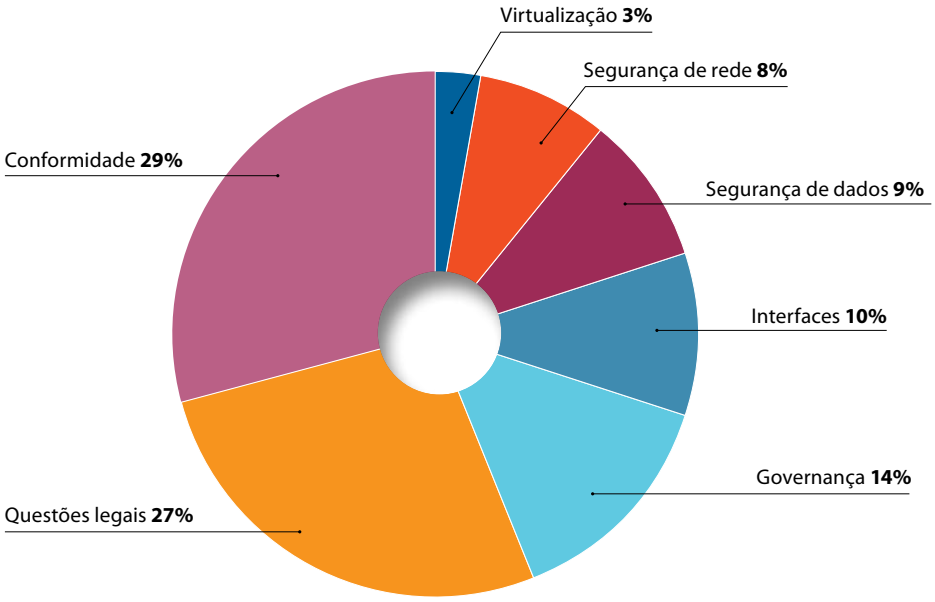
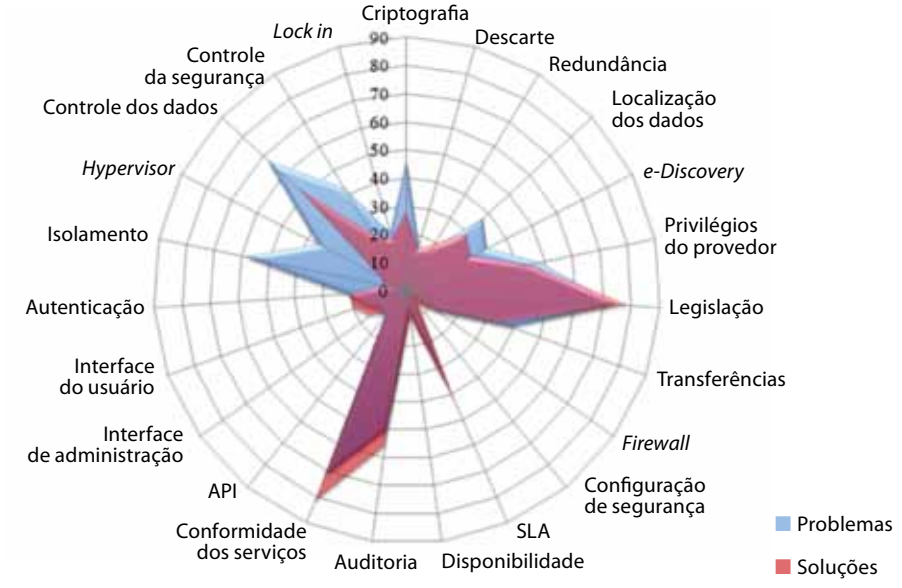


FIGURA 7

RELAÇÃO PROBLEMAS *VERSUS* SOLUÇÕES DE SEGURANÇA
PARA COMPUTAÇÃO EM NUVEM AGRUPADOS EM SUBCATEGORIAS



Análise de problemas *versus* soluções

Para comparar os resultados de cada análise foram gerados gráficos que revelam a discrepância entre citações de cada tipo. O gráfico para as categorias completas é apresentado nas figuras 7 e 8. Os valores nos eixos correspondem à quantidade de citações (de problemas ou soluções) para uma determinada categoria ou subcategoria.

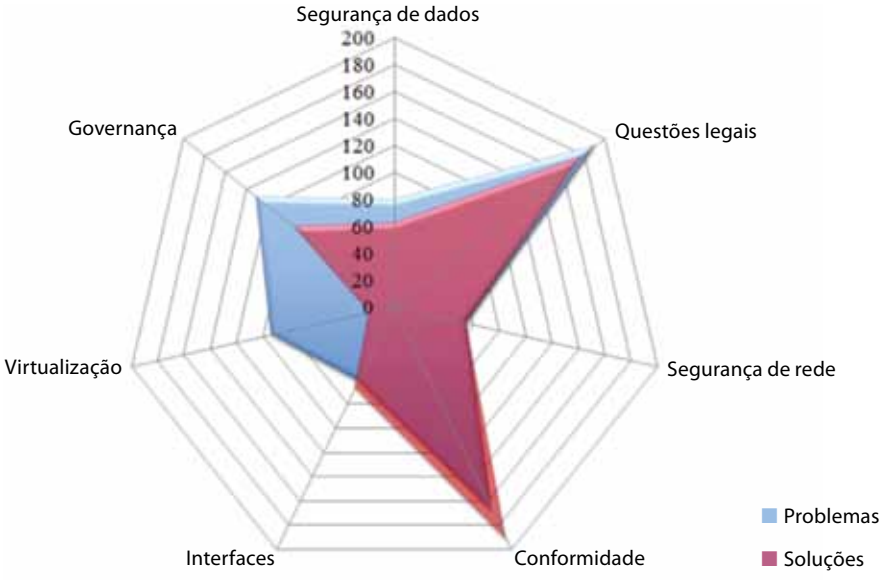
Com estas informações, pode-se inferir que categorias como conformidade de serviço, questões legais e níveis de serviço (SLA) possuem uma grande base de conhecimento existente, com equilíbrio ou até mesmo vantagem no número de soluções em relação ao de citações de problemas. Já algumas áreas técnicas, como isolamento de dados e recursos, vulnerabilidades de aplicações de virtualização e controles de segurança precisam receber atenção para que os problemas sejam resolvidos adequadamente.

CONSIDERAÇÕES FINAIS

A segurança da computação em nuvem é compartilhada tanto por usuários como pelos provedores de nuvem, sendo que a definição das responsabilidades é delimitada

FIGURA 8

RELAÇÃO PROBLEMAS *VERSUS* SOLUÇÕES DE SEGURANÇA PARA COMPUTAÇÃO EM NUVEM AGRUPADOS EM CATEGORIAS



- Estão expressas as citações de problemas. A predominância azul representa áreas nas quais existem mais citações retratando problemas na categoria do que soluções propriamente ditas. Trata-se, portanto, de áreas que ainda precisam ser pesquisadas e em que devem ser desenvolvidas novas soluções.
- Estão expressas as citações de soluções. Áreas com predominância vermelha indicam categorias com mais citações de soluções do que de problemas. São categorias que já possuem uma grande base de conhecimento desenvolvida, bem como soluções já sendo utilizadas ativamente.
- Indica as áreas onde ocorre sobreposição. Áreas com predominância nessa cor indicam equilíbrio entre citações, portanto são categorias que estão relativamente e quantitativamente balanceadas em termos de pesquisas.

principalmente pelo controle dos recursos, que muda de acordo com o tipo de serviço oferecido (IaaS, PaaS e SaaS). Nesse sentido, reforça-se o fato de que o uso de um provedor de nuvem pode tanto melhorar os aspectos de segurança como comprometê-la e que cada caso necessita ser analisado individualmente para uma decisão mais precisa.

De modo geral, pode-se dizer que usuários finais e pequenas organizações podem tirar proveito dos recursos de segurança de uma nuvem, visto que usualmente esses usuários/organizações não possuem muitos recursos para investir e manter a segurança. Por outro lado, essa afirmação parte da premissa de que a nuvem possui um nível de segurança adequado, o que nem sempre pode ser verdade e implica averiguar as condições de segurança do provedor de nuvem.

Independente do porte dos usuários, tipo de serviço ou provedor de nuvem, fica óbvio que os problemas de segurança podem estar tanto no modo como os usuários acessam os recursos da nuvem como na maneira como a nuvem realiza internamente as suas tarefas. Sendo assim, o fato de usar recursos em nuvem não exime o usuário de sua parcela de comprometimento em manter o nível de segurança dentro dos limites desejados.

Com base na análise quantitativa dos aspectos de segurança em computação em nuvem, é possível perceber que muitos problemas computacionais podem estar dentro da própria nuvem, principalmente na virtualização, que é um dos pilares da computação em nuvem. Sob essa perspectiva, resta aos usuários escolher com cautela os provedores de serviços de nuvem que irão utilizar e também levar em consideração que parte do gerenciamento dos serviços não está mais sob sua responsabilidade e sim do provedor de nuvem. Também cabe aos provedores de nuvem selecionar criteriosamente as soluções que utilizam para disponibilizar os seus serviços e alertar os usuários de sua parcela de responsabilidade.

BIBLIOGRAFIA

AGARWAL, A. "The Legal Issues Around Cloud Computing", julho/2010. Disponível em: http://www.labnol.org/internet/cloud-computing-legal-issues/14120.

ANDRZEJAK, A.; KONDO, D.; YI, S. "Decision Model for Cloud Computing Under SLA Constraints", in *Modeling, Analysis Simulation of Computer and Telecommunication Systems* (Mascots), IEEE International Symposium on. [S.l.: s.n.], 2010, pp. 257-66.

BAKSHI, A.; YOGESH, B. "Securing Cloud from ddos Attacks Using Intrusion Detection System in Virtual Machine", in *Communication Software and Networks*, 2010. ICCSN '10. Second International Conference on. [S.l.: s.n.], Feb., pp. 260-4.

BRANDIC, I. et al. "Compliant Cloud Computing (C3): Architecture and Language Support for User-driven Compliance Management in Clouds", in *Cloud Computing (Cloud)*, 2010 IEEE 3rd International Conference on [S.l.: s.n.], 2010, pp. 244-51.

BRISCOE, G.; MARINOS, A. "Digital Ecosystems in the Clouds: Towards Community Cloud Computing", in *Digital Ecosystems and Technologies*, 2009. DEST '09. 3rd IEEE International Conference on. [S.l.: s.n.], 2009, pp. 103-8.

CATTEDDU, D.; HOGBEN, G. *Benefits, Risks and Recommendations for Information* Security, novembro/2009.

CHOW, R. et al. "Controlling Data in the Cloud: Outsourcing Computation Without Outsourcing Control", in *Proceedings of the 2009 ACM Workshop on Cloud Computing Security.* New York, USA, ACM, 2009, (CCSW '09), pp. 85–90.

CLULEY, G. Evernote Hacked – "Almost 50 Million Passwords Reset After Security Breach". Disponível em: nakedsecurity.sophos.com/2013/03/02/evernote-hacked-almost-50-million-passwords-reset-after-security-breach. Acesso em: 15/3/2013.

DORION, P. "Data Destruction Services: When Data Deletion Is Not Enough", 2010. Disponível em: http://searchdatabackup.techtarget.com/tip/Data-destruction-services-When-data-deletion-is-not-enough.

ESPINER, T. "Salesforce Tight-lipped after Phishing Attack, 2007. Disponível em: http://www.zdnet.com/salesforce-tight-lipped-after-phishing-attack-3039290616.

GADIA, S. "Cloud Computing: An Auditor's Perspective", *in Isaca Journal*, v. 6, 2009.

GENOVESE, S. "Akamai Introduces Cloud-based Firewall", 2009. Disponível em: http://cloudcomputing.sys-con.com/node/1219023.

GILBERTSON, S. "Lessons From a Cloud Failure: It's Not Amazon, It's You". Disponível em: http://www.wired.com/business/2011/04/lessons-amazon-cloud-failure. Acesso em: 15/3/2013.

GONG, C. et al. "The Characteristics of Cloud Computing", in *Parallel Processing Workshops (ICPPW),* 2010 39th International Conference on [S.l.: s.n.], Sept., pp. 275-79.

GONZALEZ, N.; MIERS, C.; REDÍGOLO, F.; SIMPLÍCIO, M.; CARVALHO, T.; NÄSLUND, M.; POURZANDI, M. "A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing", in *Journal of Cloud Computing – Advances, Systems and Applications*, v. 1, 2012.

JAEGER, T.; SAILER, R.; SREENIVASAN, Y. "Managing the Risk of Covert Information Flows in Virtual Machine Systems", in *Proceedings of the 12th ACM Symposium on Access Control Models and Technologies.* New York, ACM, 2007, (SACMAT'07), pp. 81–90.

JANSEN, W.; GRANCE, T. SP 800-144. *Guidelines on Security and Privacy in Public Cloud Computing*. Gaithersburg, National Institute of Standards & Technology, 2011.

JENSEN, M. et al. "On Technical Security Issues in Cloud Computing", in *IEEE. Cloud Computing*, 2009. Cloud'09. IEEE International Conference on. [S.l.], 2009, pp. 109–16.

KRAUTHEIM, F. J. "Private Virtual Infrastructure for Cloud Computing", in *Usenix Association. Proceedings of the 2009 Conference on Hot Topics in Cloud Computing*[S.l.], 2009, pp. 5-5.

LI, H. et al. "Identity-based Authentication for Cloud Computing", in *Cloud Computing,* Springer, 2009, pp. 157-66.

MUSTHALER, L. "Cost-effective Data Encryption in the Cloud", 2009. Disponível em: http://www.networkworld.com/newsletters/2009/121409bestpractices.html.

NELSON, S. D.; SIMEK, J. W. "Virtualization and Cloud Computing: Benefits and E-Discovery Implications", julho/2011. Disponível em: http://www.slaw.ca/2011/07/19/virtualization-and-cloud-computing-benefits-and-e-discovery-implications.

PAVOLOTSKY, J. "Top Five Legal Issues For The Cloud", 2010. Disponível em: http://www.forbes.com/2010/04/12/cloud-computing-enterprise-technology-cio-network-legal.html.

RISTENPART, T. et al. "Hey, You, Get off of My Cloud: Exploring Information Leakage in Third-party Compute Clouds", in *ACM. Proceedings of the 16th ACM Conference on Computer and Communications Security* [S.l.], 2009, pp. 199-212.

ROSE, J. "Cloudy with a Chance of 0-day", 2009. Disponível em: https://www.owasp.org/images/1/12/Cloudy_with_a_chance_of_0_day_-_Jon_Rose-Tom_Leavey.pdf

SIMMONDS, P.; REZEK, C.; REED, A. *Security Guidance for Critical Areas of Focus in Cloud Computing* V3.0, dezembro/2011.

TECH, C. "Examining Redundancy in the Data Center Powered by the Cloud and Disaster

Recovery", 2010. Disponível em: http://consonustech.hubpages.com/hub/Examining-Redundancy-in-the-Data-Center.

TOMPKINS, D. "Security for Cloud-based Enterprise Applications". Fevereiro/2009. Disponível em: http://blog.dt.org/index.php/2009/02/security-for-cloud-based-enterprise-applications.

TRENDMICRO. "Making Virtual Machines Cloud-Ready". Maio/2010. Disponível em: http://resources.idgenterprise.com/original/AST-0024016_Making_virtual_machines_cloud_ready.pdf.

VENTERS, W., and WHITLEY, E.A. "A Critical Review of Cloud Computing: Researching Desires and Realities", in *Journal of Information Technology* (JIT), v. 27, n. 3, 2012, pp. 179-7.

YAN, L.; RONG, C.; ZHAO, G. "Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-based Cryptography", in C*loud Computing*, Springer, 2009, pp. 167-77.