FORENSE COMPUTACIONAL E A GARANTIA DAS EVIDÊNCIAS NO USO DA COMPUTAÇÃO EM NUVEM NUMA ORGANIZAÇÃO.[1]

VANDERLEI ROMANOSKI

Resumo: Nos dias atuais, a Tecnologia da Informação está cada vez mais presente nas organizações, facilitando a capacidade de comunicação em rede e o armazenamento das informações na nuvem. Assim, a Segurança da Informação torna-se um desafio porque através dela buscam-se soluções de como tratar as ameaças e os ataques aos sistemas, que vão desde as simples invasões e até mesmo ao roubo e sequestro de dados. Para a realização de uma Perícia Forense Computacional dentro de uma organização cujos dados estejam disponíveis na nuvem, será necessário a criação de procedimentos e medidas de segurança proativa e uma constante campanha de conscientização de seus colaboradores quanto ao trato da informação e as consequências que poderão vir a sofrer quanto ao não cumprimento de normas estabelecidas na Política de Segurança da Informação da empresa.

Palavras-chave: Computação em Nuvem, Forense Computacional, Segurança da Informação.

1 INTRODUÇÃO

No campo da Computação em Nuvem observa-se que existem vários desafios para a realização da perícia forense numa organização em que os dados estejam armazenados na nuvem, principalmente no que se refere à coleta das evidências onde os dados originais deverão ser mantidos intactos.

Diversos autores têm se dedicado à modelagem ou frameworks de Forense Computacional em Cloud Computing, um assunto que está em plena expansão, muito embora exista pouca informação sobre como garantir a qualidade e a disponibilidade das evidências para uma perícia forense dentro de uma organização quando seus dados estão sob a responsabilidade de terceiros.

Segundo Didoné (2011), não há indícios de como se garantir a qualidade nem a disponibilidade de evidências na nuvem, uma vez que uma instância virtual pode ser facilmente iniciada e/ou finalizada. Etapas importantes como a maximização das evidências e avaliação dos riscos de destruição e/ou ocultação são dificultados, tornando-se o primeiro desafio ao perito.

[1]Artigo apresentado como Trabalho de Conclusão do Curso de Especialização em Gestão da Segurança da Informação, da Universidade do Sul de Santa Catarina, como requisito parcial para a obtenção do título de Especialista em Gestão da Segurança da Informação. Orientador: Prof. Luiz Otavio Botelho Lento, MSC, 2019.

As metodologias da computação forense empregadas pelos analistas e investigadores na análise de dados em redes de computadores já estão bem documentadas e validadas. No entanto, em uma arquitetura de Computação em Nuvem onde os dados são persistidos em um ambiente distribuído, surgem muitos desafios relacionados com o local da persistência dos dados, registros de logs, sincronização de arquivos e compartilhamento de diretórios. (DAMACENA, 2014).

Conforme Sousa (2016) a computação forense é a fonte para encontrar a evidência da cena do crime através das evidências digitais. Segundo a pesquisa de diversos autores, a computação forense é a busca da verdade nos vestígios computacionais. A equipe forense também tem muitas ferramentas diferentes disponíveis para trabalhar em vários tipos de crimes. A equipe forense computacional trabalha em processo básico que inclui a identificação, coleta, preservação, análise e relatório.

Por meio do portal do Instituto Nacional de Padrões e Tecnologia (NIST, na sigla em inglês) dos Estados Unidos, podemos encontrar uma classificação clara que permite pesquisar as diferentes ferramentas forenses filtradas de acordo com a funcionalidade. O catálogo permite pesquisar parâmetros técnicos com base em funções forenses digitais específicas, como imagens de disco ou recuperação de arquivos excluídos. (PAUS, 2018).

Este trabalho classifica-se quanto ao seu enquadramento metodológico como um estudo de natureza aplicada, que procurou entender uma demanda de Segurança da Informação e propor possíveis melhorias a serem aplicadas nas organizações que utilizam a Computação em Nuvem. Conforme Gerhardt e Silveira (2009, p.35), a pesquisa de natureza aplicada tem como objetivo gerar conhecimentos para aplicação prática, dirigidos à solução de problemas específicos.

Referente ao aprofundamento do estudo considera-se de origem exploratória, pois tem como objetivo proporcionar uma maior familiaridade com o objeto de estudo. Segundo Cavalcanti e Moreira (2010, p. 22 apud Jung, 2003) a pesquisa exploratória tem como finalidade a descoberta de práticas ou diretrizes que precisam ser modificadas e a obtenção de alternativas ao conhecimento científico existente.

O campo da pesquisa foi as fontes de diferentes contribuições científicas, com o objetivo de analisar as informações e conhecimentos prévios sobre o tema apresentado.

Com a finalidade de sustentar os objetivos propostos na pesquisa de como garantir a qualidade e a disponibilidade das evidências para uma perícia forense na Computação em Nuvem dentro de uma organização, as técnicas e os instrumentos de coleta de dados

escolhidos foram desenvolvidos através de uma consulta a documentos e bibliografias e também a observação realizada no próprio campo objeto do estudo.

Os resultados da presente pesquisa serão apresentados através dos seguintes itens visando esclarecer o problema pesquisado. No item dois, será feito uma breve Fundamentação Teórica, no item três será feita a apresentação dos resultados da pesquisa, que será dividido nos seguintes subitens: Aspectos Jurídicos, Terceirização dos Serviços, Segurança da Informação, Avaliação do Risco, Auditoria e Garantia das evidências e da disponibilidade dos dados. No item quatro, será feita uma conclusão.

2 COMPUTAÇÃO EM NUVEM

Fruto da evolução de uma tecnologia aliada à necessidade de diminuição de gastos com equipamentos e softwares surgiu a Computação em Nuvem, que tem como principal característica a transformação dos modos tradicionais de como as empresas utilizam e adquirem os recursos da Tecnologia da Informação (TI).

A ideia principal de sua abordagem parte do princípio de que toda a infraestrutura de TI (hardware, software e gestão de dados e informação), até então tratada como um ativo das empresas passará a ser acessada e administrada por estas remotamente através da rede mundial de computadores.

O uso da Computação em Nuvem vem se consolidando no cotidiano da população, empresas e governos, tornando-se necessário que sejam moldados padrões de utilização, bem como o grau de confiabilidade, privacidade e demais questões de Segurança da Informação.

Dentre as vantagens que a Computação em Nuvem nos proporciona está o fato de que todas as tarefas são realizadas em servidores remotos, o que possibilita a agilidade e a praticidade de acessar dados, arquivos e aplicativos a partir de qualquer lugar do mundo, permitindo o compartilhamento de recursos por um grande número de usuários.

A perícia forense computacional tem por finalidade investigar um incidente apresentado em computadores e em mídias de armazenamento digital, seguindo uma metodologia de aquisição, preservação, recuperação e análise de dados, investigando suas causas e os responsáveis pelas mesmas.

Na realização da perícia forense na nuvem, o perito não terá o acesso físico aos dispositivos envolvidos no incidente, a destruição ou a ocultação das evidências poderão ser causadas pelos colaboradores da organização ou até mesmo pelo próprio provedor do serviço.

Conforme Didioné (2011) as questões técnicas, legais e organizacionais são alguns dos desafios para se realizar uma perícia na nuvem.

Diversas características da nuvem geram a impossibilidade de se criar linhas do tempo (timelines) precisas para recriar os eventos acontecidos no passado através da auditoria de logs.

A falta de ferramentas que auxiliem os peritos a lidar com a nuvem acaba por inviabilizar as perícias. Além disso, as tarefas que ocorrem na etapa de levantamento de informações sobre tecnologias, aplicativos, sistemas, e servidores utilizados de forma a definir os procedimentos e ferramentas mais adequados ainda carecem de procedimentos específicos para a computação em nuvem. (DIDONÉ, 2011 apud REILLY, 2010, p. 60).

A investigação forense em nuvem necessita de metodologias, procedimentos e ferramentas para a obtenção de resultados concretos com valor probatório. Alguns procedimentos são necessários para realizar uma investigação forense em nuvem tais como: identificar o provedor de nuvem que precisa ser investigado; utilizar um computador conectado à internet; acessar a conta de armazenamento em nuvem utilizando login e senhas fornecidas pelo suspeito ou encontradas em arquivos pessoais ou outros meios; utilizar softwares para capturar telas do processo e tráfegos de rede; verificar todos os arquivos disponíveis, datas e horários de acessos, computadores, usuários e IP's associados; realizar uma cópia dos arquivos verificados; analisar os arquivos e dados salvos e produzir o laudo pericial com base na análise feita anteriormente. (IPOG, 2017).

Conforme Damacena (2014, p. 14), o modelo de Computação em Nuvem apresenta uma arquitetura distribuída e dispersa, o que traz como consequência uma maior dificuldade na coleta de evidências por peritos forenses.

Nos casos de investigações criminais em ambientes tradicionais, é prática comum que a perícia computacional desligue o equipamento e realize uma cópia dos discos que será analisada posteriormente em laboratório. Isso é inviável num ambiente de computação em nuvem, tendo em vista a grande capacidade de armazenamento, questões jurídicas, distribuição geográfica e controle dos dados, que podem variar conforme o modelo de serviço contratado. Além disso, a falta de acesso físico para a coleta dos dados e a falta de controle sobre o sistema tornam a aquisição das informações uma tarefa desafiadora para a perícia em nuvem. (SOUZA, 2018).

Em sistemas de computação em nuvem o perito normalmente não possui acesso físico às máquinas envolvidas no incidente, nem à cena do crime, e por isso não há busca e

apreensão de dispositivos. Além disso, buscar e apreender dispositivos poderia causar transtornos ao fornecedor da nuvem e a outros usuários do serviço que não sejam alvos da investigação. (DIDONÉ, 2011, p. 61).

Na Computação em Nuvem os serviços 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. (DAMACENA, 2014, p. 14).

A computação forense vem se reestruturando, trazendo novas técnicas, soluções e métodos investigativos, dando origem à "cloud forensics" ou perícia na nuvem. Assim, a chamada Computação Forense como um Serviço (Forensic as a Service - FaaS) dedica-se a solucionar os desafios de segurança inerentes ao ambiente de nuvem, disponibilizando ferramentas e recursos que organizam, filtram e integram as informações com outros sistemas, procurando assegurar que os dados obtidos sejam armazenados de forma segura, tornando-os acessíveis aos técnicos e profissionais legais, atendendo ainda às legislações do país onde o serviço foi contratado para a realização da perícia na nuvem. (SOUZA, 2018).

Muitos gestores de empresas se esquecem que a Segurança da Informação é um dos pilares que sustentam a sua organização, principalmente nos dias atuais em que a TI muda constantemente com o advento de novos softwares e hardwares, fato este que era impossível em outras épocas da história da humanidade.

3 APRESENTAÇÃO DOS RESULTADOS DA PESQUISA

Através do levantamento realizado em fontes de diferentes contribuições científicas foram coletados e analisados 35 (trinta e cinco) trabalhos que tratam sobre os temas de Perícia Forense Computacional, desafios, garantia das evidências e da disponibilidade dos dados, e também, a Segurança da Informação na Computação em Nuvem, os quais serão apresentados através dos seguintes subitens visando esclarecer o problema da pesquisa.

3.1 ASPECTOS JURÍDICOS

Em casos de mandados judiciais de busca e apreensão, a coleta de dados depende muito da lei do país do servidor em nuvem. Questões jurídicas, distribuição geográfica e controle dos dados podem variar conforme o modelo de serviço contratado. Além disso, a

falta de acesso físico para a coleta dos dados e a falta de controle sobre o sistema tornam a aquisição das informações uma tarefa desafiadora para a perícia em nuvem.

Damacena (2014, p. 46) destaca que esbarrando na ausência de leis específicas, inúmeros crimes ficaram sem punição por absoluto desconhecimento de muitos magistrados quanto à possibilidade de se rastrear o que foi feito em um computador, e como foi feito.

Com a aprovação da Lei Geral de Proteção de Dados (LGPD), Lei n° 13.709, de 14 de agosto de 2018, que entrará em vigor a partir do ano de 2020, que trata sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), todos os negócios realizados no Brasil deverão ter sua política de tratamento de dados regularizados e em conformidade da lei, evitando-se algum tipo de prejuízo que poderá surgir caso a mesma não seja observada.

Um provedor de serviços poderá receber de terceiros a solicitação de informações na forma de intimações ou mandados de busca nos quais acessos aos dados de clientes são solicitados. Para isso, acordos e contratos devem possuir cláusulas requerendo que o provedor notifique o cliente do recebimento de tais solicitações judiciais dando-lhe tempo para resposta. (CSA, 2017, p. 47).

Além das questões técnicas da Computação em Nuvem, tais como, criptografia, formatos de dados desconhecidos e descentralização do armazenamento, é preciso lidar com as questões jurídicas. A localização precisa dos dados na nuvem é incerta, podem estar distribuídos em diversos centros computacionais, em diferentes países e sob diferentes jurisdições, tornando-se necessário que os peritos atuem de forma cordial com a justiça, selando acordos nacionais e internacionais, para que se respeitem tanto as jurisdições de cada Estado, quanto às questões de privacidade dos usuários. (GONZALEZ, et al, 2013; JESUS e COUTO, 2017).

Apesar dos provedores de serviço em nuvem garantirem a confiabilidade e a segurança, os ataques realizados nestes ambientes são difíceis de serem investigados, trazendo grandes desafios aos peritos forenses digitais. As dificuldades são apresentadas ao perito na forma de coletar os dados, que muitas vezes se encontram distribuídos geograficamente e o acesso às informações que podem estar sob a responsabilidade do provedor ou questões legais. (SOUZA, 2017).

Antes de se contratar um serviço em nuvem torna-se necessário uma avaliação profunda das cláusulas contratuais com relação ao tratamento da Segurança da Informação.

A organização deverá avaliar suas próprias práticas, necessidades e restrições, para identificar as barreiras legais e aderências aos requisitos associados com a proposta de transição para a nuvem. Além disso, deverá realizar verificações proativas nos provedores de serviços, para verificar se a oferta irá permitir que a empresa cumpra com as obrigações de proteção de seus ativos. (SANTOS e MACHADO, 2010; CSA, 2017).

Todos os processos de Investigação Forense Computacional deverão ocorrer sobre segredo absoluto, sendo essa capacidade de dissimulação e sigilo um dos principais atributos do Investigador. Também é obvio que o profissional que conduz a investigação detenha conhecimentos teóricos e práticos sobre como realizar esse importante trabalho. (PERES e LEIMAN, 2017).

Conforme Mesquita (2017), o perito também deve preocupar-se em adquirir as informações, garantindo que todas suas ações não causarão nenhum efeito de perda, modificação ou dano sobre as evidências nas situações mais adversas, respeitando a legalidade das operações.

Para que a organização não venha a ter problemas com um contrato que contenha margens para questionamento de cláusulas quanto ao risco oferecido e a demanda de serviços prestados pelo provedor na nuvem, os responsáveis pela área jurídica da empresa deverão também dominar a área de Segurança da Informação, principalmente aos aspectos relativos para uma possível Perícia Forense Computacional.

3.2 TERCEIRIZAÇÃO DOS SERVIÇOS

A confiabilidade no serviço prestado se dá através do Acordo em Nível de Serviço (SLA), que é uma política que rege sua utilização nos termos do contrato estabelecido entre o usuário e a empresa prestadora do serviço na nuvem.

Ressalta-se ainda, que no SLA esteja previsto a colaboração entre o Provedor de Serviço na Nuvem (CSP) e a organização com finalidade de uma investigação forense, para que se tenha o conhecimento de quem tem acesso aos dados armazenados pela empresa contratada e que os mesmos tenham tomado ciência do termo de manutenção do sigilo.

Conforme Didoné (2011, p. 89), quanto mais questões a respeito de segurança forem satisfeitas pelo SLA na relação entre CSP e cliente, menores serão as chances de expor seus dados a riscos desnecessários.

Uma vez que a organização já sabe o que necessita contratar como serviço, ela deve organizar um documento chamado de Requisição de Serviços, conhecido pela sigla Request for Proposal (RFP). Nesta requisição, torna-se necessário esclarecer tudo o que se espera alcançar, com definição de prioridades e diversos atributos que caracterizam o serviço esperado. Essa requisição é entregue a provedores candidatos, como estímulo para que eles façam uma proposta comercial de prestação do serviço. (MÜLBERT, 2009, p. 146).

É muito importante o detalhamento do SLA para que o mesmo contenha cláusulas sobre questões de privacidade e disponibilidade dos dados. Utilizar a nuvem pública significa depender de terceiros, o que pode limitar a flexibilidade de acesso. (DAMACENA, 2014).

O Guia de Segurança para Áreas Críticas Focado em Computação em Nuvem, CSA (2017), apresenta algumas práticas a serem adotadas quanto aos serviços a serem contratados:

- Departamentos de segurança devem ser envolvidos durante o estabelecimento de um SLA e de obrigações contratuais para assegurarem que os requisitos de segurança sejam aplicáveis contratualmente.

- As organizações devem, no mínimo, compreender e documentar as métricas atuais e como elas mudarão quando as operações forem movidas para um serviço de Computação em Nuvem, que pode ser um provedor onde as métricas usadas sejam diferentes.

- Se os serviços prestados na nuvem são essenciais para as operações empresariais, uma abordagem de gestão de risco deve incluir a identificação e a avaliação de ativos, a identificação e a análise de ameaças e SLA de vulnerabilidades e, o potencial impacto das mesmas sobre os ativos, a análise das probabilidades de eventos/cenários, os níveis e critérios de aceitação de riscos aprováveis pela gerência, bem como o desenvolvimento de planos de tratamento de riscos com múltiplas opções (controle, prevenção, transferência, aceitação).

- Caso o prestador de serviços não demonstre processos abrangentes e eficazes de gestão risco, deve-se avaliar cuidadosamente o uso desse fornecedor, bem como as próprias habilidades do usuário para compensar as potenciais lacunas de gestão de risco.

- O SLA que é utilizado por cada provedor de nuvem deve garantir o suporte ao tratamento de incidentes requerido para a execução eficaz do plano de resposta a incidentes da empresa para cada etapa do processo de tratamento de incidentes (detecção, análise, contenção, erradicação e recuperação).

Quanto ao aspecto da segurança na contratação de serviços, as empresas que prestam o serviço na nuvem deverão ter processos claros, com um bom nível de conformidade quanto às políticas adotadas, bem como, a importância de incluir no contrato de prestação de serviço

alguns requisitos de notificação, identificação, preservação e acesso às fontes de evidências necessárias durante a perícia. (SOUZA, 2017, 2018).

Muitos gestores de organizações ainda possuem dúvidas quanto aos seus dados estarem fora de seus limites físicos, pois a dificuldade na adoção de serviços na nuvem se tornará um desafio porque a tomada de decisão poderá colocar em risco os ativos da empresa quando os mesmos forem transferidos ao controle de terceiros. A interoperabilidade entre provedor e consumidor deve ser cuidadosamente avaliada para que a migração de dados não se torne um problema. (MARCON JR, et al, 2010; SANTOS e MACHADO, 2010).

Ao se contratar um serviço na nuvem é importante que seja bem definido no SLA a importância de como o CSP irá apresentar as informações relevantes referente aos dados armazenados para uma possível perícia forense.

3.3 SEGURANÇA DA INFORMAÇÃO

Ao se adotar serviços na Computação em Nuvem as empresas encontram desafios quanto à Segurança da Informação porque uma falha que venha a ocorrem em qualquer um de seus componentes poderá impactar nos demais, ocasionando prejuízos e muitas das vezes vazamento de dados sigilosos.

Vasconcelos (2017 apud REESE, 2009, p. 121) destaca alguns pontos que estão relacionados à Segurança da Informação na Computação em Nuvem:

1) Recuperação de desastres: capacidade de retomar os sistemas quando o mesmo enfrenta um cenário de desastre;

2) Segurança dos dados: define como o usuário controlará o acesso físico aos servidores;

3) Controle dos dados: O consumidor não tem conhecimento de onde os dados estão armazenados.

4) Segurança da Rede: tem relação com as regras de firewall e detecção de entradas não desejadas na rede, que servirá para monitorar o tráfico local para eventuais irregularidades;

5) Segurança do Servidor: o servidor deve estar organizado em relação às tarefas de prevenção de ataques;

6) Segmentação dos dados: ao presumir que os servidores possuem falhas de segurança, deve-se estar ciente que eventualmente uma delas será comprometida.

7) Integridade dos dados: para manter a integridade dos dados, as transações entre muitas fontes de dados devem ser realizadas de maneira segura;

8) Segregação dos dados: em Sistemas de Computação em Nuvem deverá ser garantido uma limitação para os dados de cada usuário.

9) Acesso aos dados: primordialmente relacionada às políticas de segurança oferecidas pelos usuários enquanto acessam os dados;

10) Autenticação e autorização: quando as credenciais dos usuários são guardadas nas bases de dados dos provedores, deve-se remover contas quando funcionários deixam a organização;

11) Confidencialidade dos dados: todo o conteúdo dos usuários deve ser guardado em um único provedor ou vários provedores, e os fornecedores devem assegurar que os dados não serão acessados por outros clientes;

12) Backup: o fornecedor deve garantir que os dados dos clientes serão regularmente copiados em diferentes fontes.

À medida que as organizações migram para a Computação em Nuvem, a segurança dos dados, as preocupações de privacidade e a confidencialidade aumentam cada vez mais. A gestão da informação é um grande desafio que afeta todas as organizações. A perspectiva de existência de potenciais falhas de segurança e violação da privacidade faz com que as empresas se questionem sobre a adoção desses ambientes. Assim, as empresas prestadoras de serviço na nuvem devem proporcionar aos usuários mecanismos ou ferramentas de segurança virtual eficazes contra possíveis violações. (CSA, 2017; VASCONCELOS, 2017).

Dentre os desafios para a Segurança da Informação de uma organização na Computação na Nuvem destacam-se as preocupações relacionadas à privacidade, ameaças externas e a falta de controle sobre os recursos e dados de TI, mesmo que os provedores de serviço na nuvem tenham garantido no acordo de nível de serviços. Os serviços estão sujeitos a vários incidentes intencionais ou não que ameaçam a segurança, incluindo ameaça à integridade, confidencialidade e disponibilidade dos recursos. Se o meio tecnológico da empresa estiver com uma segurança precária ou até desatualizada isso acarretará em vários problemas no futuro, como prejuízo de produção e financeiros. (VAIDOTAS, 2011; SOUZA, 2017; NDG, 2019).

A Segurança da Informação na Computação em Nuvem apresenta alguns desafios, pois se buscam soluções de como tratar as ameaças e ataques ao sistema computacional, devendo ser analisados e endereçados por todos os envolvidos no modelo. Neste sentido, a

forense computacional tem como objetivo investigar esses crimes cibernéticos, coletando vestígios, examinando-os e analisando-os com o intuito de buscar evidências do crime cometido, e se possível, montar o cenário criminoso. Tais problemas, porém, não são provas de que o modelo de Computação em Nuvem seja inseguro. (GONZALEZ, et al, 2013; MESQUITA, 2017).

Ao fazer a migração dos dados para a nuvem, a organização não poderá deixar de realizar uma profunda análise dos seus procedimentos de segurança, bem como, quais alterações e controles precisarão ser colocados em prática para que a empresa venha a operar de modo seguro.

3.4 AVALIAÇÃO DO RISCO

Apesar dos benefícios que a Computação em Nuvem pode trazer, os consumidores estão preocupados com os riscos que a utilização de um ambiente novo pode representar para os ativos da organização. Esse ambiente está sendo utilizado para hospedar vários tipos de serviços, e todos exigem garantias de segurança dos dados sendo processados e armazenados. Para o máximo proveito de todo o poder oferecido, as diferentes entidades, provedores e consumidores de serviços necessitam de abordagens de segurança abrangentes e confiáveis. (VASCONCELOS, 2017).

Antes de transferir seus dados, sistemas e aplicativos para o ambiente da Computação em Nuvem, as organizações deverão realizar uma profunda avaliação do risco dos principais ativos suportados por este ambiente (dados, aplicações, processos e serviços). É importante que esses ativos sejam analisados para determinar a importância para o negócio da organização. Neste processo de análise busca-se avaliar os impactos gerados caso algum requisito de segurança (confidencialidade, integridade ou disponibilidade) seja comprometido. (VAIDOTAS, 2011; VASCONCELOS, 2017).

O Guia de Segurança para Áreas Críticas Focado em Computação em Nuvem, CSA (2017) recomenda que para a avaliação do risco seja determinado exatamente quais dados ou função estão sendo considerados:

1) Deverá ser feito um questionamento para cada ativo procurando levantar como poderíamos ser prejudicados se o ativo se tornasse amplamente público, se um empregado do provedor acessasse o ativo, se o processo ou função fossem manipulados por um estranho, se

o processo ou função falhasse ao apresentar os resultados esperados, se as informações/dados fossem inesperadamente alteradas, se o ativo estivesse indisponível por um período de tempo.

2) Antes de iniciar a busca por fornecedores, precisamos saber se podemos aceitar os riscos implícitos para os diversos modelos de implantação e os cenários de hospedagem.

3) Avaliar os Modelos de Serviços em Nuvem e os Provedores, deve-se focar no grau de controle que terá em cada camada para implantar qualquer gestão de riscos necessária.

4) Realizar análises de risco das aplicações de segurança e privacidade, construir e manter os modelos de ameaças.

A decisão em se adotar a Computação em Nuvem, independente da sua aplicação, é baseada em riscos, não em tecnologia, uma vez que assume vários níveis de segurança. As organizações devem avaliar o risco e as opções de segurança antes de mover seus sistemas e aplicativos para o ambiente de computação em nuvem. É necessário avaliar quais dados e serviços que podem ser transferidos para o ambiente externo. (MARCON JR, et al, 2010; DIDONÉ e QUEIROZ, 2011).

Para mitigar os novos riscos gerados com a adoção de um serviço na nuvem, a empresa terá que contratar ou implantar um sistema de gestão do processo de autenticação e identificação, o qual será responsável por gerir os acessos aos dados e gerar o token de segurança através do controle de acesso baseado em funções. (VARELA, 2017).

No que se refere a questões legais e de segurança na avaliação do risco, antes de se adotar a Computação em Nuvem devemos observar alguns requisitos, dentre eles, como e onde estarão armazenados os dados, quem poderá ter acesso aos mesmos, existirá proteção aos dados, as instalações de armazenamento são seguras e que com frequência são realizados auditorias e rotinas de teste na plataforma.

3.5 AUDITORIA

Uma auditoria em sistemas de Computação em Nuvem consiste em um processo de verificação de toda a estrutura computacional da empresa, feito por profissionais específicos e capacitados para tal que avaliarão o sistema como um todo e farão um relatório completo sobre a eficácia e o desempenho, considerando o que a empresa busca e necessita nessa área.

Entre os principais objetivos dessa inspeção estão a análise da eficiência dos processos, garantir a segurança dos dados e assegurar o cumprimento das leis e demais normas que permeiam as ações.

Alguns provedores, por exemplo, podem restringir as avaliações de vulnerabilidade e os testes de invasão, enquanto outros podem limitar a disponibilidade de logs de auditoria e de monitoramento de atividades. Se as políticas internas exigirem esses requisitos, será preciso procurar opções de avaliação, exceções contratuais específicas ou um fornecedor alternativo melhor alinhado com as necessidades de gestão de risco. (CSA, 2017, p. 36).

É difícil falar em possibilidade de auditoria quando o assunto é Computação em Nuvem. Assim, o desenvolvedor ou fornecedor do serviço deve adotar mecanismos transparentes e de fácil detecção da qualidade dos recursos contratados pelo usuário. Um dos aspectos mais relevantes inerente à avaliação dos serviços na nuvem é a segurança dos serviços de dados. (VASCONCELOS, 2017).

O Guia de Segurança para Áreas Críticas Focado em Computação em Nuvem, CSA (2017, p. 49) recomenda que os clientes em nuvem devam considerar e compreender o seguinte:

- As implicações regulatórias para utilizar um determinado serviço em nuvem ou provedores, dando especial atenção a eventuais problemas fronteiriços ou de múltiplas jurisdições, quando aplicável.

- Os recursos do provedor para demonstrar em tempo hábil a conformidade, incluindo a geração de documentos, produção de comprovantes e conformidade dos processos.

- As relações entre os clientes, os prestadores e os auditores para garantir o necessário acesso e o alinhamento com os requisitos de governança.

Com as atuais implantações em nuvem, os clientes corporativos têm uma visibilidade muito limitada dentro dos provedores de serviços de nuvem para uma auditoria dos dados. Uma empresa precisa ter acesso a esses dados, não só para atender a conformidade direcionada dos negócios, mas também para atender as regulamentações do setor e também lidar com litígios de fraude. (CSA, 2017, p. 126).

Para que uma perícia seja bem-sucedida, é necessário que existam registros de auditoria, ou logs, íntegros e confiáveis. Assim, a maneira como os logs são armazenados torna-se um fator de extrema relevância e os mesmos necessitam conter informações suficientes para identificação do usuário. (SANTOS e MACHADO, 2010).

Alguns prestadores de serviço não veem razões para armazenar seus logs fora da nuvem, mas os riscos deste ato devem ser levados em consideração. Numa invasão, dependendo do nível e controle que o invasor tiver sobre os dados, poderá facilmente apagar os logs e eliminar possíveis provas e encobrir seus rastros. (SANTOS e MACHADO, 2010).

As trilhas de auditoria deixadas pelos processos podem ser utilizadas para rastrear a execução de um serviço desde sua fonte de dados. Essa informação é vital para o entendimento, a descoberta, a validação de dados e processos. Requisitos devem ser fornecidos para que dados corporativos possam ser movidos para nuvens computacionais, permitindo que o acesso aos mesmos possa ser rastreado. (MARCON JR, et al, 2010).

A auditoria nos serviços prestados na nuvem tem por finalidade determinar se os objetivos dos controles, processos e procedimentos do sistema estão sendo executados, conforme determinados pela organização. O programa da auditoria deverá ser planejado, levando-se em consideração o estado e a importância dos processos e áreas a serem auditadas, bem como os resultados das auditorias realizadas anteriormente.

3.6 GARANTIA DAS EVIDÊNCIAS E DA DISPONIBILIDADE DOS DADOS

As organizações devem estar constantemente revendo sua Política de Segurança da Informação, garantindo que seja possível a realização de uma perícia forense na nuvem através de medidas proativas, como por exemplo, o armazenamento de logs, a redundância e criptografia dos dados e o controle de acesso.

A obrigatoriedade e o armazenamento dos logs de dados é um dos principais fatores a serem considerados na hora de regulamentar o modelo de Computação em Nuvem. O log é princípio básico, pois nele estarão armazenados os dados para recuperação do sistema em caso de falhas, a origem do erro ou problema, os usuários que estavam utilizando, e assim, identificar autores de crimes cibernéticos. (SANTOS e MACHADO, 2010).

Quando existir a replicação do serviço oferecido na nuvem, as evidências nesse ambiente dificilmente serão destruídas ou mesmo perdidas, servindo de alerta para que a organização esteja ciente que ao contratar um provedor de serviço na nuvem o mesmo venha a dar garantias quando for necessária uma perícia forense.

Os métodos utilizados para coletar as evidências numa investigação em nuvem dependerão da natureza do caso. A recuperação de dados excluídos na nuvem poderá estar limitada ao tipo de sistema de arquivo que o provedor utiliza em seu ambiente. Com sistemas e infraestrutura em nuvem, os snapshots são grandes aliados dos peritos nas investigações e podem fornecer informações importantes antes, durante e depois de um incidente, possibilitando recriar o ambiente analisado para cada momento que foi realizado o snapshot, calculando o hash de todos os arquivos gerado. (SOUZA, 2017).

Toda a informação que a organização venha a transferir para o provedor na nuvem deverá estar protegida, sendo recomendável o uso de uma Rede Privada Virtual (Virtual Private Network - VPN) e também o uso da criptografia, que torna o armazenamento e o tráfego de dados mais seguro de possíveis ataques e crimes cibernéticos na Nuvem.

A técnica de criptografar os dados possibilita a integridade e a confiabilidade do mesmo, sendo um mecanismo de segurança indispensável no uso da Computação em Nuvem, assegurando a privacidade da informação e impossibilitando o acesso de terceiros. (VAIDOTAS, 2011; VARELA, 2017).

Com a crescente evolução do uso da Computação em Nuvem torna-se necessário para as organizações a adoção de medidas de controle de acesso aos usuários, principalmente no que se refere a uma necessidade de perícia forense. A cada acesso, deve ser gerado um log informando quem é o usuário, a data e horário, de qual dispositivo está sendo realizado o acesso e também qual dado foi inserido, modificado ou apagado. Recomenda-se a utilização de acesso em duas etapas, tornado mais difícil a quebra de segurança.

Cada organização consumidora de serviços fornecidos pela nuvem precisa definir os perfis e as políticas de controle de acesso que poderá ser descrito como um conjunto de atributos utilizados pela nuvem para customizar o serviço e possivelmente restringir o acesso a outros serviços. Também é importante ressaltar que os fornecedores devem apresentar garantias sistêmicas de segurança e de privacidade dos dados dos usuários, promovendo a separação de dados confidenciais dos dados não confidenciais, seguido da criptografia de elementos confidenciais. (VASCONCELOS, 2017).

Embora exista divergência entre autores em trabalhos apresentados sobre como garantir as evidências e a disponibilidade dos dados para uma perícia forense computacional, ambos concordam que deverão existir medidas que possibilitem as melhores práticas para a preservação das evidências e também um cuidado especial para que as provas não venham a ser contaminadas ou mesmo alteradas enquanto estiverem sob custódia do perito.

Não há indícios de como se garantir a qualidade nem a disponibilidade de evidências na nuvem, uma vez que uma instância virtual pode ser facilmente iniciada e/ou finalizada. Etapas importantes como a maximização das evidências e avaliação dos riscos de destruição e/ou ocultação são dificultados, tornando-se o primeiro desafio ao perito. (DIDONÉ, 2011).

Para assegurar a autenticidade e integridade dos dados obtidos em um processo de análise forense, devem existir procedimentos bem definidos, claros e documentados, garantindo que as provas não foram comprometidas ou alteradas durante o processo de coleta

e enquanto estiveram sob custódia dos peritos envolvidos na investigação. (DAMACENA, 2014, p. 25).

Um trabalho de conscientização dos colaboradores, que são o ativo mais fraco da Segurança da Informação dentro de uma organização, ainda é a melhor prática para se preservar a informação. Não basta o investimento em tecnologia para o controle de acesso e proteção dos dados, o colaborador deverá ter a consciência de que não poderá negligenciar a Política de Segurança adotada na empresa.

À medida que os especialistas contribuem para o desenvolvimento contínuo de melhores tecnologias de segurança, tornando ainda mais difícil a exploração de vulnerabilidades técnicas, os atacantes se voltarão cada vez mais para a exploração do elemento humano. Quebrar a "**firewall humana**" quase sempre é fácil, não exige nenhum investimento além do custo de uma ligação telefônica e envolve um risco mínimo. (MITNICK, 2003, p. 04, grifo nosso).

4 CONCLUSÕES

No decorrer da realização deste trabalho, buscou-se por elementos que possam auxiliar o gestor de Tecnologia da Informação de uma organização de como garantir a qualidade e a disponibilidade das evidências para uma perícia forense na Computação em Nuvem.

Através dos resultados obtidos no campo Aspectos Jurídicos podemos observar que há um consenso entre os autores citados, quanto à necessidade de saber a localização geográfica onde os dados estão armazenados, de serem incluídas cláusulas nos contratos que venham a garantir a confidencialidade, integridade e a disponibilidade dos dados, principalmente no que se refere a uma eventual necessidade de Perícia Forense Computacional. Assim, a organização deverá contar com profissionais capacitados e sempre atentos às mudanças de legislação, sem deixar margens para questionamentos jurídicos.

Nos resultados apresentados no campo Terceirização dos Serviços podemos observar que ao se realizar um Acordo em Nível de Serviço (SLA) com um Provedor de Serviços na Nuvem (CSP) o mesmo deverá ser inteligível para a organização, devendo apontar quais os requisitos dos serviços desejados, sendo necessário o envolvimento de técnicos e usuários envolvidos com o serviço e principalmente, da alta administração na tomada de decisão, a qual estará ciente dos benefícios e também os riscos associados à terceirização.

No item apresentado que trata sobre a Segurança da Informação observamos que existe uma preocupação maior por parte dos gestores de TI com a privacidade e a confidencialidade dos dados armazenados na nuvem, onde, há o aumento de potenciais falhas de segurança devendo ser criadas barreiras com o objetivo de restringir os riscos, através de uma análise profunda dos procedimentos de segurança com uma Política de Segurança mais consistente e a utilização da estratégia de segurança com privilégio mínimo, dificultando o acesso do usuário e criando barreiras de proteção mais consistentes.

Sob a óptica da segurança, é importante que as organizações que prestam serviços em nuvem tenham um processo claro, com bom nível de conformidade com as políticas e a prática real e que, sobretudo, permita um correto diagnóstico dos incidentes ocorridos, com retroalimentação de suas práticas e até com adequada previsão para casos futuros.

Através dos resultados obtidos no campo Avaliação do Risco observa-se que é necessário a implantação de um processo de gestão de risco que tem por finalidade relacionar todos os riscos que a organização terá ao disponibilizar seus dados na nuvem, tendo como destaque o que poderá ocorrer caso algum dos requisitos de segurança (confidencialidade, integridade ou disponibilidade) venham a ser comprometidos. Destaca-se ainda, que na avaliação do risco a empresa saiba a real localização onde os dados estão armazenados e sob a responsabilidade de quem, e também se o prestador de serviço realiza com frequência testes de segurança e auditorias para a validação de seus serviços.

Torna-se de suma importância para uma organização que o plano de tratamento de incidentes seja estruturado observando-se a cultura empresarial e que sejam destacados membros para comporem a equipe de respostas a incidentes, atribuindo qual será o serviço que a mesma deverá buscar uma resposta, ou seja, através de políticas específicas para a recuperação de desastres.

Os resultados obtidos no campo Auditoria alertam que antes da migração dos dados da organização para a nuvem deverá ser realizada uma auditoria muito bem planejada, com a finalidade de verificar se todos os controles de Segurança da Informação necessários estão implantados e sendo executados de forma correta, minimizando assim, as falhas e impactos negativos no negócio da empresa. Destaca-se também, a necessidade de estar previsto no contrato de prestação de serviço a garantia de que será possível se ter acesso aos registros de auditoria, ou logs, íntegros e confiáveis e que os mesmos estejam guardados em local seguro e de preferência fora da nuvem para uma futura perícia forense computacional.

A garantia das evidências e da disponibilidade dos dados é uma preocupação constante das organizações que utilizam a Computação em Nuvem, principalmente quando ocorrer um vazamento de uma informação e existir a necessidade de realização de uma perícia forense. Assim, os acordos de nível de segurança deverão ser constantemente revistos e atualizados conforme a tecnologia avança.

Durante a realização deste trabalho foi possível verificar a importância de uma análise mais profunda das cláusulas contratuais e os riscos que poderão surgir com o envolvimento entre o ativo ser humano, o elo mais fraco da segurança, dentro de uma organização e os sistemas que estarão disponíveis na nuvem.

Espera-se que este trabalho venha a contribuir para que os gestores da Tecnologia da Informação e os tomadores de decisão na organização tenham um melhor entendimento sobre como garantir as evidências na Computação em Nuvem, ou seja, devemos estar sempre em constante revisão da Política de Segurança e que a mesma seja difundida em todos os níveis de colaboradores, inclusive com os prestadores de serviço que terão contato com a informação que estará circulando nos servidores.

Como trabalho futuro pretende-se realizar um estudo para a criação de uma metodologia de como assegurar que todos os dados disponíveis da nuvem possam ser auditados e serem disponíveis para uma possível perícia forense computacional a qualquer momento.

COMPUTATIONAL FORENSE AND GUARANTEE OF EVIDENCE IN THE USE OF CLOUD COMPUTING IN AN ORGANIZATION.

Abstract: Nowadays, Information Technology is increasingly presents in many organizations, facilitating the networking communication and the storage of information into the cloud. Thus, Information Security becomes a challenge because it seeks solution to how to treat threats and attacks on systems, ranging from simple invasions and even data theft and data hijacking. In order to perform a Computational Forensic Expertise within an organization whose data is available in the cloud, it will be necessary to create procedures and proactive security measures, as well as a constant campaign of awareness of its collaborators in relation to the handling of information and the consequences that may arise from non observance of the rules established in the Company´s Information Security Policy.

Keywords: Cloud Computing, Computational Forensics, Information Security.

REFERÊNCIAS

CAVALCANTI, Marcelo José e MOREIRA, Enzo de Oliveira. **Metodologia para o estudo de caso**. Livro Didático. 5. Ed. Palhoça: Unisul Virtual, 2010, p. 22.

CSA, Cloud Security Alliance. **GUIA DE SEGURANÇA PARA ÁREAS CRÍTICAS FOCADO EM COMPUTAÇÃO EM NUVEM V3.0**.2017. Disponível em:<https://chapters.cloudsecurityalliance.org/brazil/files/2017/02/Guia-CSA-v-3.0.1-PT-BR-Final.pdf>. Acesso em: 18 Mai. 2019.

DAMACENA, Barbara Larissa Candido. **DESAFIOS DA PERÍCIA FORENSE EM UM AMBIENTE DE COMPUTAÇÃO NAS NUVENS.** UNIPLAC. LAGES/SC. 2014. Disponível em:<http://revista.uniplac.net/ojs/index.php/tc_si/article/view/1911/988>. Acesso em: 17 Mai. 2019.

DIDONÉ, Dener. **COMPUTAÇÃO EM NUVEM: Desafios e oportunidades para a Forense Computacional**. Tese de Mestrado. UFPE. Recife/PE. 2011. Disponível em:<https://repositorio.ufpe.br/bitstream/123456789/2745/1/arquivo6996_1.pdf>. Acesso em: 16 Mai. 2019.

DIDONÉ, Dener. QUEIRÓZ, Ruy de. **COMPUTAÇÃO FORENSE E AS OPORTUNIDADES OFERECIDAS PELA COMPUTAÇÃO EM NUVEM**. UFPE. 2011. Disponível em:<https://docplayer.com.br/3499083-Computacao-forense-e-as-oportunidades-oferecidas-pela-computacao-em-nuvem.html>. Acesso em: 20 Mai. 2019.

GERHARDT, Tatiana Engel e SILVEIRA, Denise Tolfo. **Métodos de Pesquisa**. Porto Alegre: Editora da UFRGS, 2009. Disponível em: <http://www.ufrgs.br/cursopgdr/downloadsSerie/derad005.pdf>. Acesso em: 17 Mar. 2019.

GONZALEZ, Nelson Mimura.et al. **SEGURANÇA DAS NUVENS COMPUTACIONAIS:** Uma visão dos principais problemas e soluções. REVISTA USP. São Paulo/SP. n. 97. p. 27-42. 2013. Disponível em:<http://twixar.me/wK2n>. Acesso em: 20 Mai. 2019.

IPOG, Blog. **Computação Forense: como investigar em nuvem?** 2017. Disponível em:<https://blog.ipog.edu.br/tecnologia/computao-forense-como-investigar-em-nuvem/>. Acesso em: 22 Jul. 2019.

JESUS, Cátia Oliveira de. COUTO, Mailson Sousa. **FORENSICWORK: Desenvolvimento de um Framework para Perícia Forense em Computação na Nuvem**. IFBA, Vitória da Conquista/BA. 2017. Disponível em:<http://twixar.me/zn2n>. Acesso em: 18 Mai. 2019.

MARCON JR, et al. **ASPECTOS DE SEGURANÇA E PRIVACIDADE EM AMBIENTES DE COMPUTAÇÃO EM NUVEM**. Instituto Federal de Educação, Ciência e Tecnologia do Paraná (IFPR). 2010. Disponível em:<https://www.researchgate.net/publication/262567797_Aspectos_de_Seguranca_e_Privacidade_em_Ambientes_de_Computacao_em_Nuvem>. Acesso em: 19 Mai. 2019.

MESQUITA, Pablo Lopes. **DESAFIOS DA FORENSE EM DISPOSITIVOS MÓVEIS.** Universidade do Sul de Santa Catarina (UNISUL). 2017. Disponível em:<http://twixar.me/ln2n>. Acesso em: 25 Mai. 2019.

MITNICK, Kevin D. **A ARTE DE ENGANAR**. Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. In: SIMON, William L. Tradução: ROQUE, Kátia Aparecida. Título original: The art of deception: controlling the human element of security. Pearson Education. São Paulo, 2003, p. 04.

MÜLBERT, Ana Luisa. **Gestão de Serviços em Tecnologia da Informação**. Livro didático. 2. ed. rev. e atual. Palhoça/SC. Unisul Virtual, 2009. p. 146.

NDG, Linux Essentials. **WORKING IN LINUX - CLOUD COMPUTING.** Chapter 3. 2019. Disponível em:<https://content.netdevgroup.com/contents/linux-essentials/GV3sPWsQ7r/>. Acesso em: 17 Mai. 2019.

PAUS, Lucas. **Ferramentas para Análise Forense Computacional**. 2018. Disponível em:<https://www.welivesecurity.com/br/2018/09/06/ferramentas-para-analise-forense-computacional-como-encontrar-o-caminho-certo-para-cada-incidente/>. Acesso em: 17 Set. 2019.

PERES, João Roberto. LEIMAN, Cristina Moraes. **IoT - Investigação Forense Digital:** Fundamentos e Guia de Referências. São Paulo/SP. 2017. Disponível em:<http://www.komp.com.br/gallery/iot-investigacao-forense-digital-e-book-p.pdf>. Acesso em 23 Mai. 2019.

SANTOS, Ana P. V. e MACHADO, Marcos. **CLOUD COMPUTING: IMPASSES LEGAIS E NORMATIVOS.** Revista Científica Intra Ciência**.** Ano 2, nº 1, p.16-105, 2010. Disponível em:<http://uniesp.edu.br/sites/_biblioteca/revistas/20170531153544.pdf>. Acesso em: 18 Mai. 2019.

SOUSA, Adriano Gomes. **ETAPAS DO PROCESSO DE COMPUTAÇÃO FORENSE: UMA REVISÃO**. Acta de Ciências e Saúde. Número 05, Volume 02. 2016. Disponível em:<http://twixar.me/PsV1>. Acesso em 17 Set. 19.

SOUZA, Ieda Maria de. **OS DESAFIOS DA FORENSE COMPUTACIONAL NA COMPUTAÇÃO EM NUVEM.** 2017. Universidade do Sul de Santa Catarina. Disponível em:<https://riuni.unisul.br/bitstream/handle/12345/2085/OsDesafios_da_Forense_Computacional_Computacao_Nuvem.pdf?sequence=1&isAllowed=y>. Acesso em: 19 Mai. 2019.

SOUZA, Ieda Maria De. **EVIDÊNCIAS NAS NUVENS.** Cloud Computing traz novos desafios para a investigação forense. 2018. Disponível em:<http://www.serpro.gov.br/menu/noticias/noticias-2018/evidencias-nas-nuvens>. Acesso em: 17 Mai. 2019.

VAIDOTAS, Guilherme. **TÉCNICAS DE SEGURANÇA NA COMPUTAÇÃO EM NUVENS.** Faculdade de Tecnologia de Lins. LINS/SP. 2011. Disponível em:<http://www.fateclins.edu.br/v4.0/trabalhoGraduacao/UoPcDsU5y21t85FDz0H5O3CGKsZaAnwpcwayfQ9GPu.pdf>. Acesso em: 18 Mai. 2019.

VASCONCELOS, Francisco Victor. **A SEGURANÇA JURÍDICA DA COMPUTAÇÃO EM NUVEM:** Responsabilidade Jurídica na Proteção de Dados Digitais por parte dos

Provedores de Aplicação de Internet. UNISUL. 2017. Disponível em:<https://repositorio.ufsc.br/handle/123456789/186195>. Acesso em: 14 Mai. 2019.

VARELA, Patrick de Macedo. **UMA VISÃO DA GESTÃO DO PROCESSO DE IDENTIFICAÇÃO E AUTENTICAÇÃO ENTRE DOMÍNIOS DE SEGURANÇA NA COMPUTAÇÃO EM NUVEM**. Universidade do Sul de Santa Catarina (UNISUL). Florianópolis/SC. 2017. Disponível em:<http://twixar.me/8K2n>. Acesso em: 25 Mai. 2019.