Requisitos para análise de segurança da informação em provedores de serviços em nuvem

Gislaine Parra Freund
Universidade Federal de Santa Catarina – UFSC, E-mail: gislaineparraf@gmail.com

Priscila Basto Fagundes
Universidade Federal de Santa Catarina – UFSC, E-mail: priscila.bfagundes@gmail.com

Douglas Dyllon Jeronimo de Macedo
Universidade Federal de Santa Catarina – UFSC, E-mail: douglas.macedo@ufsc.br

RESUMO

Com a ocorrência do fenômeno *big data*, surge a necessidade de tecnologia e infraestrutura adequada para suportar esse novo cenário. Neste contexto, os serviços em nuvem atendem essa demanda, porém requerem controles de segurança específicos devido a forma em que os recursos computacionais são concebidos, utilizados e gerenciados. O presente artigo apresenta um estudo da norma ISO/IEC 27017:2016 com o objetivo de avaliar os requisitos de segurança destinados aos provedores dos serviços em nuvem, classificados conforme sua aplicação aos aspectos organizacional, físico e técnico. Com este estudo foi possível observar que tanto para o aspecto organizacional quanto para o técnico, a norma apresenta diversos controles específicos para os serviços em nuvem. Já quanto ao aspecto físico, as recomendações são muito similares aos de um ambiente tradicional. O tema que trata sobre as responsabilidades e papéis de segurança permeiam os demais controles e precisam ser definidos detalhadamente entre as partes envolvidas. O trabalho apresenta um quadro com os controles abordados pela norma para agilizar o entendimento e sua aplicação, porém requer avaliações técnicas adicionais para operacionalizá-las. Observa-se também que para obter uma solução completa de segurança, os controles da norma ISO/IEC 27002:2013 devem ser adotados. Além disso, o propósito dos cenários de uso dos serviços em nuvem, o modelo de serviço adquirido e os riscos de segurança associados a cada um deles são determinantes para implementar os requisitos de forma adequada.

Palavras-chave: *Big data.* Serviços em nuvem. Segurança da Informação. ISO 27017.

---

1 INTRODUÇÃO

Com a ascensão da tecnologia, dados e informações se tornaram ativos de alto valor para as organizações. De acordo com Mayer e Cukier (2013), o uso massivo de dispositivos tecnológicos contribui para a geração desenfreada de dados, fenômeno referido por ele como a “avalanche de informação".

O volume de dados é de fato um fator relevante e cresce exponencialmente de forma que, o que era visto como futuro muito distante há uma década, já é uma realidade. Conforme Taurion

(2016), a geração de zetabytes diários, deixa de ser uma escala imaginária e futurista e passa a ser uma escala real. Porém, um fator relevante neste contexto são os sistemas, a infraestrutura e os requisitos de segurança que são necessários e precisam ser ajustados para atender a demanda do *big data*.

Mayer e Cukier (2013) relacionam o termo *big data* com a necessidade de aprimoramento da tecnologia para atender a demanda de processamento, armazenamento e análise desse grande volume de dados e informações.

Davenport (2014) também defende que os ambientes precisam estar adequados para as soluções *big data*, de maneira a armazenar os grandes volumes de dados sendo estes estruturados ou não estruturados, de diferentes tipos e formatos gerados a partir de fluxos intensos e contínuos. Com o intuito de fornecer, dentre outros recursos, soluções para o armazenamento e processamento de grandes volumes de dados, surge a computação em nuvem (CHEN; MAO; LIU, 2014). A computação em nuvem possui características específicas que para Silva (2014) são: a capacidade de processamento e armazenamento, o uso de virtualização de recursos, a largura de banda disponível para uso atualmente, a queda nos custos de *hardware*, etc.

Observa-se que soluções *big data* necessitam de alta capacidade de processamento e armazenamento para que seja possível a transformação de grandes volumes de dados em resultados que agreguem valor, e os ambientes em nuvem podem oferecer a infraestrutura necessária para isso. Porém, os serviços em nuvem demandam um conjunto de requisitos de segurança que precisam ser observados e tratados para não comprometer dados de usuários e de provedores deste tipo serviço.

Para atender essa necessidade, as diretrizes apresentadas na norma ISO/IEC 27002:2013 foram complementadas e em 2016 foi disponibilizada pela ABNT a ISO/IEC 27017 – Código de práticas para controles de segurança da informação para serviços em nuvem. A ISO/IEC 27002:2013 – Código de prática para controles de segurança da informação, fornece diretrizes para práticas de gestão e normas gerais de segurança da informação para organizações de qualquer natureza, tipo e tamanho. Já a ISO/IEC 27017:2016 fornece diretrizes que apóiam a implementação de controles de segurança para clientes e provedores de serviços em nuvem. Seu objetivo é fornecer controles específicos para serviços em nuvem para mitigar riscos inerentes aos requisitos técnicos, organizacionais e físicos oriundos desse tipo de serviço.

Desta forma, o foco deste artigo é apresentar o conjunto de requisitos de segurança da informação prescritos na norma ISO 27017:2016, para atender as demandas de segurança específicas oriundas da utilização de serviços em nuvem, destinados aos provedores dos serviços. Os controles são apresentados em grupos categorizados conforme os aspectos organizacionais, físicos ou técnicos e pretende-se com esse estudo auxiliar profissionais da área da segurança da informação na aplicação dos controles da norma ISO/IEC 27017:2016.

2 REFERENCIAL TEÓRICO

O conceito de *big data*, assim como os cenários e projetos a ele relacionados, tornou as informações ainda mais importantes para as organizações por assumirem um papel estratégico de apoio na tomada de decisão. Erl, Khattak e Buhler, (2016) consideram que *big data* tem a capacidade de mudar a natureza de uma empresa e que em algumas delas, a base de suas atividades são os insights que somente *big data* pode entregar.

Vianna, Dutra e Frazzon, (2016) resumem *big data* como a explosão de dados de forma incontrolável e a necessidade de transformar esses dados em informações relevantes para direcionar os negócios. Contudo, este tipo de ambiente requer infraestrutura e tecnologias apropriadas para processar e armazenar essa grande massa de dados. Neste contexto, os serviços oferecidos em nuvem atendem essa demanda e possibilitam o armazenamento e processamento de grandes volumes de dados com algumas facilidades de uso.

O *National Institute of Standards and Technology* (NIST) [Mell; Grace, 2011], definiu a computação em nuvem como um modelo de serviço que possibilita o uso de recursos computacionais compartilhados de forma acessível, conveniente e provisionado com esforço mínimo de gerenciamento ou interação do provedor, e classificam os serviços em nuvem em três modelos, são eles: Software as a Service (SaaS), Plataform as a Service (PaaS) e Infraestructure as a Service (IaaS), apresentando quatro padrões de implantação para esses serviços:

- Nuvem privada: provisionada para uso exclusivo de uma organização.
- Nuvem comunitária: provisionada para uso exclusivo de uma comunidade específica que compartilham as mesmas preocupações.
- Nuvem publica: provisionada para uso aberto pelo publico em geral.

- Nuvem híbrida: composta por duas ou mais infraestruturas de nuvens distintas.

Dentre as possibilidades e facilidades oferecidas pelos serviços em nuvem existe a preocupação com aspectos relacionados com a segurança. A segurança da informação é um tema importante que vem sendo discutido pela maioria das empresas de diferentes segmentos com o intuito de reduzir riscos. Segundo a norma ISO/IEC 27002:2013, a segurança da informação é alcançada com a implementação de um conjunto adequado de controles, de forma coordenada e coerente com os riscos associados em uma visão holística da organização.

Segundo o NIST [Badge *et al*, 2012], uma organização que possui e executa suas operações de Tecnologia da Informação (TI), normalmente implanta controles de segurança de seus dados conforme os seguintes aspectos:

- Requisitos organizacionais que especificam as operações relacionadas às pessoas e entidades e os dados, como por exemplo diretrizes para criação, acesso, divulgação, transporte e destruição dos mesmos.
- Requisitos físicos que estão relacionados ao perímetro físico de segurança os quais protegem as mídias de armazenamento e às instalações que mantem os dados armazenados.
- Requisitos Técnicos que definem os recursos e mecanismos tecnológicos para a proteção dos dados, tais como: gerenciamento de identidade e acesso, criptografia de dados armazenados e em trânsito e outros requisitos de gerenciamento de auditoria de dados para cumprir requisitos regulamentares aplicáveis.

O NIST aponta que com o uso de serviços em nuvem, muitas vezes os dados são gerados, processados e armazenados no ambiente físico do provedor do serviço e que neste contexto é fundamental ter a garantia que o fornecedor implante controles de segurança equivalentes aos adotados na computação tradicional contemplando requisitos organizacionais, físicos e técnicos.

A computação em nuvem possui fontes de riscos de segurança próprios, derivadas de suas características, que diferem da computação tradicional, tais como: escalabilidade e elasticidade dos sistemas, compartilhamento de recursos, provisionamento de serviços sob diversas jurisdições e visibilidade limitada sobre a implementação de controles de segurança, entre outros (ISO/IEC 27017, 2016).

O *Gartner Group* [Brodkin, 2008], destaca sete quesitos de segurança que precisam ser observados na utilização de serviços em nuvem, são eles: acesso privilegiado do provedor aos dados do cliente, cumprimento das regulamentações de segurança por parte dos provedores do serviço, jurisdições específicas quanto aos locais em que os dados serão armazenados, segurança no processo de segregação dos dados e uso de criptografia, recuperação dos dados em caso de incidente em tempo hábil, investigação das ações realizadas durante a prestação dos serviços em nuvem e disponibilidade dos dados mesmo na ocorrência de alterações na estrutura organizacional e estatutária do provedor.

No sentido de apoiar clientes e provedores de serviços em nuvem na implantação de controles de segurança, uma extensão da norma ISO/IEC 27002:2013 denominada de ISO/IEC 27017:2016 foi disponibilizada pela ABNT em meados de 2016. A ISO/IEC 27002:2013 é uma referência que apresenta os controles para a implementação de segurança da informação comumente aceitos, aplicáveis em organizações de qualquer porte e segmento (ISO/IEC 27002, 2013). Já a ISO/IEC 27017:2016 foi projetada utilizando a mesma estrutura de tópicos existentes na ISO/IEC 27002:2013, alguns deles quando pertinente, foram complementados com orientações de segurança específicas para a utilização e o provimento de serviços em nuvem e alguns permaneceram iguais por aplicarem as mesmas orientações gerais de segurança apresentadas na ISO/IEC 27002:2013.

Para facilitar o entendimento da norma ISO/IEC 27017:2016 à interessados pela segurança em serviços em nuvem, esse artigo apresenta de forma objetiva, os requisitos destinados à provedores desses serviços.

3 PROCEDIMENTOS METODOLOGICOS

Conforme Gerhardt e Silveira (2009), este estudo tem a abordagem qualitativa, visto que não se preocupa com representatividade numérica e trata-se de uma pesquisa básica, pois seu objetivo é gerar conhecimentos novos, úteis para o avanço da ciência, sem aplicação prática prevista. Do ponto de vista dos objetivos, é de caráter exploratório, visto que tem o propósito de promover maior familiaridade com os temas, para torná-los mais explícito ou construir hipóteses (GIL, 1991). Quanto aos procedimentos, é uma pesquisa bibliográfica, que na definição de Fonseca (2002) “é feita a partir do levantamento de referências teóricas já analisadas, e

publicadas por meios escritos e eletrônicos, como livros, artigos científicos, páginas de web sites".

Para este estudo foram realizadas pesquisas entre os dias 03/07/2017 e 03/12/2017, no Google Acadêmico e na base de dados Web of Science para identificar as publicações acadêmicas que contemplam o tema: segurança nos serviços em nuvem vinculada com a norma ISO/IEC 27017:2016. Observou-se que os trabalhos relacionados que versam sobre a norma, a referenciam como o padrão que apresenta controles adicionais aos recomendados na ISO/IEC 27002, específicos para a segurança dos serviços em nuvem, porém, não foram identificados trabalhos que abordam seus requisitos, conforme a proposta deste artigo.

4 TRABALHOS RELACIONADOS

Dentre os trabalhos relacionados, estão o de Ferreira (2017) que propõe um modelo de instalação de infraestrutura confiável para *cloud* baseada em *OpenStack*. O autor propõe um modelo de instalação de alta disponibilidade para o Departamento de Ciência da Computação da Faculdade de Ciências da Universidade do Porto. A ISO 27017 é abordada pelo autor como uma das certificações obtidas pelo Google.

Rodrigues (2016) descreve as melhores técnicas de segurança das informações utilizadas por grandes empresas com base em uma revisão na literatura. Faz uma análise histórica sobre o desenvolvimento das normas de segurança da informação e menciona a ISO 27017 como parte das normas da família ISO 27000, destinada para a segurança dos serviços em nuvem.

Já Silva (2015) discorre sobre recomendações de segurança em SaaS. O autor compila as recomendações propostas por autores e grupos especializados em segurança na computação em nuvem e apresenta um conjunto de recomendações gerais de segurança. Apresenta também que a autenticação de dois fatores e a criptografia fim-a-fim são soluções que podem ser implementadas tanto por administradores de ambientes em SaaS e de computação em nuvem em geral, como podem formar a base para a criação de políticas de segurança para autenticação forte. E Silva (2013) apresenta, com base em uma pesquisa bibliográfica exploratória, as motivações e características da computação em nuvem, os principais riscos envolvidos e um compilado de recomendações de segurança para reduzi-los. Ambos autores Silva (2015) e Silva (2013)

referenciam a norma ISO 27017 como um dos padrões de conformidade para a computação em nuvem em fase de desenvolvimento.

Ferreira (2013) apresenta um sistema de monitoramento de acordos de níveis de serviço de segurança para infraestrutura de serviços em nuvem. O autor desenvolve também mecanismos para detecção de anomalias de segurança com base em técnicas de aprendizado de máquina utilizando os dados de desempenho coletados durante a execução das máquinas virtuais em monitoramento. Ao mencionar a ISO 27017 descreve que ela “definirá um código de práticas de controle de segurança da informação em nuvens baseado nos controles já existentes no padrão ISO 27002 e em novos controles, específicos para nuvens que serão voltados tanto para uso de provedores de serviço quanto para usuários”, considerando que a norma ainda estava em fase de desenvolvimento.

Para este estudo são abordados os controles da ISO 27017:2016 que são complementares aos apresentados na ISO 27002:2013, os quais foram adicionados para atender as necessidades específicas dos serviços em nuvem. Os controles foram analisados e classificados quanto à sua natureza em relação aos aspectos organizacional, físico e técnico. E os requisitos abordados, limitaram-se aos aplicáveis a provedores do serviço em nuvem.

5 RESULTADOS

A partir do estudo realizado na norma ISO/IEC 27017:2016 foram extraídos os requisitos destinados ao provedor do serviço e estes avaliados quanto a sua aplicação nos aspectos organizacional, físico e técnico. Vale ressaltar que a adoção dos requisitos de segurança apresentados na norma ISO/IEC 27017:2016 não elimina a necessidade de adotar os controles preconizados pela ISO /IEC 27002:2013, os quais não foram abordados neste artigo. É recomendada pela própria norma, que ambas sejam consultadas, pois muitos controles, diretrizes e requisitos se aplicam tanto para computação geral quanto em nuvem.

5.1 REQUISITOS ORGANIZACIONAIS

O provimento de serviços em nuvem requer diferentes ações no âmbito organizacional para especificar as operações e gerenciar os recursos de TI com segurança. Diante disso, políticas de segurança devem ser definidas pelos provedores de serviços em nuvem para atender as

especificidades de segurança necessárias para essa modalidade de serviço. A ISO 27017:2016 recomenda que para isso, os provedores estendam sua política para que sejam aplicáveis à concepção e implementação do serviço em nuvem oferecido incluindo requisitos básicos de segurança da informação, tais como: isolamento dos multilocatários e dos clientes do serviço em nuvem; proteção quanto aos acessos de seus funcionários aos ativos e informações dos clientes assim como aos acessos administrativos aos serviços; segurança da virtualização (gerenciamento do ciclo e vida das instâncias virtuais, controle de acesso ao armazenamento das imagens virtuais, proteção de *hipervisores*, etc); proteção dos dados dos clientes, gestão do ciclo de vida das contas dos clientes, entre outros.

É recomendado pela norma que o cliente do serviço em nuvem considere suas políticas e defina o que é necessário para atender as suas necessidades de segurança, conforme o serviço em nuvem contratado. Já o provedor do serviço em nuvem, no papel de custodiante, deve treinar e conscientizar seus funcionários para que estejam preparados para lidar com as solicitações de segurança requisitadas pelos clientes. Além disso, deve considerar a criticidade dos dados e aplicações de seus clientes na alocação dos papéis e responsabilidades a seus funcionários e comunicar a eles sobre os requisitos de segurança envolvidos e acordados entre as partes para que sejam cumpridos e gerenciados como parte do serviço provido em nuvem.

Cabe ao provedor do serviço de nuvem, ainda como custodiante dos dados, informar a seus clientes sobre os países e as localizações geográficas que os mesmos podem ser armazenados para que as entidades regulatórias e as jurisdições possam ser mapeadas pelo cliente.

A norma recomenda que todos os recursos de segurança da informação adotados e oferecidos pelo provedor do serviço em nuvem sejam disponibilizados ao cliente para que o mesmo avalie se atendem ou não os requisitos desejados. Recomenda também ao provedor, que os recursos de segurança da informação sejam informados a seus clientes ou potenciais clientes dos serviços em nuvem que possuem acordos de sigilo, para evitar a exposição de informações detalhadas sobre os controles de segurança que possam ser úteis a pessoal mal-intencionadas. Dentre os recursos a serem adotados pelo provedor, a norma menciona os procedimentos e as práticas utilizadas para o desenvolvimento seguro. Ressalta que este quesito é crítico para o modelo de serviço SaaS, porém recomenda que o provedor forneça ao cliente informações sobre

as práticas de desenvolvimento seguro que utiliza de forma compatível com a sua política de divulgação.

Definir papéis e responsabilidades para garantir a segurança de dados é primordial em qualquer cenário e mais fácil de ser praticado quando estas atribuições estão concentradas em uma única instituição. Na utilização de serviços em nuvem, os quais envolvem outras partes no processo, de diferentes instituições, essa tarefa se torna mais complexa e precisa ser avaliada com atenção.

A ambigüidade dos papéis e das responsabilidades pela segurança dos dados nestes ambientes é um fator preocupante tanto do ponto de vista do provedor quanto do cliente desses serviços. A recomendação da norma ISO/IEC 27017:2016, é que os provedores de serviços em nuvem acordem e documentem os papéis e responsabilidades pela segurança da informação com seus clientes, prestadores de serviços e fornecedores para evitar a ambiguidade nessas definições e conseqüências drásticas para ambas as partes. Recomenda definir com detalhes, dentre outros itens, de quem é a responsabilidade pela propriedade dos dados, controle de acesso e manutenção da infraestrutura. Complementa com a orientação de definir e documentar as responsabilidades também pela manutenção e pelas operações desses dados, evitando assim, que práticas vitais tais como backup, recuperação, entre outras, deixem de ser realizadas pela falta de definição sobre a quem compete estas atribuições.

No uso de serviços em nuvem alguns papéis e responsabilidades de segurança são compartilhados, ou seja, são divididos entre os funcionários do cliente e do provedor e podem variar conforme o modelo de serviço. Ao tratar sobre a responsabilidade de registros de eventos (logs) em serviços IaaS por exemplo, essa responsabilidade é compartilhada, o provedor limita-se a responsabilidade de registrar os eventos dos componentes da infraestrutura e o cliente é responsável por registrar os eventos de suas máquinas virtuais e aplicações. Da mesma forma, também em serviços IaaS geralmente a responsabilidade pelas cópias de segurança é do cliente, já nas demais modalidades, é relevante definir e documentar.

Estas atribuições devem ser identificadas, atribuídas às partes, documentadas, comunicadas e implementadas conforme acordado. A norma recomenda que o provedor especifique as medidas de segurança que foram acordadas com o cliente assim como as

responsabilidades definidas entre as partes em acordos de níveis de serviço, para evitar mal-entendido entre eles.

A ISO 27017:2016 contempla também os casos em que os provedores oferecem seus serviços apoiados por uma cadeia de suprimentos, ou seja, depende de outros fornecedores para prover seus serviços. Para estes casos, a norma aponta que o provedor deve garantir que o nível de segurança praticado pelos seus fornecedores será o mesmo ou até superior ao que ele adota com seus clientes. Recomenda ainda que os objetivos de segurança sejam fornecidos pelo provedor a seus fornecedores e que seja exigido gerenciamento de riscos para que os objetivos sejam atendidos.

Os ativos envolvidos nos serviços em nuvem devem ser gerenciados e para isso é importante que o inventário destes seja mantido tanto pelo cliente, quanto pelo provedor. A norma ISO 27017:2016 recomenda que o cliente mantenha em seu inventário as informações, os ativos associados a elas e o local (identificação do serviço) que o ativo é mantido. E para o fornecedor a recomendação é que identifique e mantenha em seu inventário, os dados que são originais do cliente e os que foram gerados pelo serviço, ou seja, aqueles que foram produzidos pelas aplicações de gerenciamento das informações do serviço em nuvem.

A norma complementa com a recomendação que os ativos de informação mantidos em inventário tenham um proprietário, ou seja, que sejam nomeadas pessoas ou entidades que sejam responsáveis por qualificar o ciclo de vida dos ativos, assegurando que os mesmos estejam inventariados, devidamente classificados e protegidos, se estão sendo acessados de forma apropriada e se estão sendo excluídos ou destruídos de forma adequada. Esta atribuição varia de acordo com o modelo do serviço em nuvem utilizado. Em um serviço de SaaS por exemplo, a responsabilidade pelos softwares aplicativos pertence ao provedor, enquanto nos modelos de PaaS e IaaS esta responsabilidade pertencerá ao cliente.

Para que as informações recebam o tratamento adequado quanto segurança, é importante que estejam classificadas, rotuladas quando ao nível de sigilo aplicável, para que assim sejam tratadas conforme as regras definidas em políticas de classificação e tratamento da informação definidas pelas empresas. No contexto de serviços em nuvem, a ISO 27017:2016 recomenda que as informações e os ativos associados a elas, mantidos em um ambiente de computação em nuvem, sejam classificados e rotulados de acordo com as políticas já adotadas pelo cliente.

Cabendo ao provedor, documentar e divulgar as funcionalidades que o serviço oferece que permitem aos clientes classificar e rotular as informações e ativos.

Para os casos de mudanças a serem executadas nos serviços oferecidos pelo provedor, estas devem ser comunicadas ao cliente antecipadamente para que o mesmo avalie o impacto que podem causar em sua operação. Logo, é uma recomendação da norma que o fornecedor agende as denominadas “janelas de manutenção” informando ao cliente a categoria, data e hora programada para a realização da mudança e notifique o início e o término das atividades.

Alguns aspectos específicos da operação dos serviços em nuvem devem ser monitorados pelos clientes, aponta a ISO 27017:2016. A norma recomenda que os provedores disponibilizem a seus clientes recursos que possibilitem a eles realizarem alguns monitoramentos como por exemplo, sobre o vazamento de dados sensíveis ou se o serviço não está sendo utilizado para atacar outros. Além disso, complementa que o acesso a esses monitoramentos seja protegido adequadamente permitindo ao cliente, acesso apenas a instância de monitoramento que pertence a ele.

Todos os controles de segurança adotados, tanto no aspecto organizacional, físico ou técnico, minimizam os riscos de ocorrência de incidentes, mas não os eliminam, tornando essencial estar preparado e assegurar um enfoque efetivo para gerenciar os incidentes, caso eles ocorram. Desta forma, os procedimentos adotados nas operações críticas dos serviços em nuvem, tais como: instalação, mudanças e remoção de dispositivos virtualizados, procedimentos no término dos contratos de uso dos serviços em nuvem, cópias de segurança e recuperação, devem adotar mecanismos de proteção considerando os sérios incidentes de segurança que podem ser causados por uma falha nos mesmos. E estes procedimentos devem ser fornecidos aos clientes para que possam definir e documentar os procedimentos que irão adotar se houver uma falha que possa causar danos irrecuperáveis aos ativos envolvidos no serviço contratado. Além disso, para este quesito a norma considera que o provedor deve fornecer ao cliente as especificações documentadas quanto às responsabilidades na gestão de incidentes que contemple: o escopo dos incidentes que serão notificados ao cliente, o procedimento para as notificações (telefones de contato e e-mail), o tempo em que as notificações devem ocorrer, informações de contato para tratar sobre incidentes, entre outras. Além disso, considerando que um evento pode ser identificado tanto pelo cliente quanto pelo provedor e que em ambos os casos, deve-se ter o

procedimento definido para notificar imediatamente a outra parte, a norma indica que o provedor forneça também, mecanismos ao cliente para notificar um evento de segurança que venha a ser identificado por ele.

No contexto de utilização de serviços em nuvem, a remoção e o retorno dos ativos do cliente, no encerramento do acordo de prestação do serviço em nuvem trata-se de um tópico relevante que deve ser previsto e documentado para que ocorra em tempo hábil e não acarrete danos ao cliente. Desta forma, é recomendado pela ISO 27017:2016 que o provedor do serviço em nuvem documente este processo de encerramento incluindo a lista dos ativos, as providências a serem adotadas para a remoção e retorno dos mesmos, assim como o tempo que as ações previstas serão executadas.

A norma contempla também recomendações relacionadas a conformidade com requisitos legais e contratuais. Recomenda que o provedor identifique seus requisitos legais pertinentes, aplicáveis aos tipos de serviços oferecidos, informe ao cliente e forneça evidencias de sua conformidade com os mesmos. Além disso, recomenda que o provedor tenha um processo definido para responder a notificações referentes a propriedade intelectual, visto que, dependendo do tipo de serviço utilizado, o cliente tem autonomia de instalar softwares nos ambientes em nuvem, fato que se não observados os termos de licença para o uso do software nesses ambientes, podem quebrar os requisitos dos termos.

O uso da criptografia também requer atenção quanto a legislação aplicável do local onde os dados são armazenados. A norma recomenda que o provedor do serviço em nuvem forneça ao cliente as especificações da criptografia utilizada para que possam ser realizadas análises críticas da conformidade com as regulamentações, legislações e acordos aplicáveis.

Ainda no tópico de conformidade, a norma contempla que o provedor deve evidenciar para o cliente que todos os controles de segurança acordados estão implantados e sendo praticados adequadamente. Para isso, podem ser utilizadas auditorias individuais dos clientes, auditorias realizadas por terceira parte, certificações em normas pertinentes ou até mesmo auto avaliações conduzidas pelo próprio provedor, quando as auditorias são impraticáveis ou representem riscos a segurança da informação.

5.2 REQUISITOS FÍSICOS

Referente aos requisitos físicos, a ISO 27017:2016 apresenta apenas uma diretriz adicional aos controles apresentados na ISO 27002:2013. A norma apresenta que o fornecedor do serviço em nuvem deve possuir políticas e procedimentos para o descarte e reuso seguro de equipamentos e mídias de armazenamento de dados. O fornecedor deve assegurar que as definições estabelecidas para este fim sejam realizadas de forma precisa e garanta ao cliente que seus dados não serão acessados após o descarte ou reuso dos ativos.

5.3 REQUISITOS TÉCNICOS

Para proteger os dados no provimento de serviços em nuvem é necessário definir recursos e mecanismos tecnológicos aplicáveis a este modelo de serviço. A elasticidade e escalabilidade são características inerentes aos serviços em nuvem assim como a contratação dos recursos sob demanda. No entanto, as restrições de capacidade desses recursos existem em algumas situações e podem variar conforme o tipo de serviço adquirido e a oferta contratada. A norma ISO 27017:2016 apresenta que estas restrições devem ser de conhecimento do cliente para que o mesmo possa monitorar esses recursos, avaliar se os mesmos continuam atendendo sua necessidade e a conveniência de alterar o serviço ou o pacote contratado. No entanto, aborda também que a provisão e o controle da capacidade dos recursos oferecidos nos pacotes tais como conectividade, software, ativos de processamento e armazenamento de dados, ficam sob a responsabilidade e controle do provedor do serviço cabendo a ele monitorá-los para evitar incidentes de segurança da informação causados por escassez de recursos dentro do escopo contratado.

A norma apresenta que também cabe ao provedor, nos casos em que o serviço contratado contemplar cópias de segurança, disponibilizar ao cliente as informações sobre o procedimento do backup, tais como: escopo e cronograma, métodos e o formato dos dados, período de retenção, procedimentos de verificação da integridade dos dados das cópias, procedimentos para a restauração dos dados e o tempo necessário para isso, local de armazenamento das cópias. Complementa que, caso o serviço em nuvem contratado não ofereça capacidade para as cópias de segurança, o cliente deve implementá-las.

Serviços em nuvem utilizam ambientes virtuais compartilhados para acesso e armazenamento de dados e necessitam de proteção adicional para evitar acessos não autorizados aos dados pelos outros clientes do serviço em nuvem que compartilham o mesmo ambiente. Para isso, a norma recomenda que o provedor do serviço em nuvem implemente segregação lógica dos dados do cliente. Ressaltando que, no caso dos serviços que envolvem multilocatários, o provedor deve garantir a segregação e isolamento apropriado para cada locatário. A ISO 27017:2016 apresenta que o requisito para segregação de rede para o isolamento das instâncias seja definido pelo cliente e que o mesmo verifique se o provedor atende os requisitos desejados. Já para o provedor, a norma recomenda que a segregação de rede seja estabelecida ao menos na segregação entre as instâncias nos ambientes multilocatários e na segregação entre o ambiente de administração interna e o ambiente de computação em nuvem do cliente.

A norma complementa que ao armazenar dados de clientes em áreas de armazenamento compartilhado fisicamente com a tabela de metadados, a segregação dos dados de outros clientes pode ser implementada com a adoção de controle de acesso a este recurso.

Os ambientes em nuvem que são constituídos com a tecnologia de virtualização, a rede virtual é configurada em uma rede física existente e as políticas, tanto para a rede virtual quanto para a rede física, devem ser consistentes para evitar problemas no controle de acesso ou até mesmo interrupções no sistema. Referente a este item, a norma recomenda também que o provedor do serviço em nuvem considere a política de segurança definida para a rede física ao estabelecer a política de segurança para a configuração da rede virtual. As máquinas virtuais também devem ter os controles de segurança reforçados em sua configuração para garantir que somente as portas, protocolos e serviços necessários estejam habilitados e que as medidas relevantes de segurança estejam configuradas para cada máquina virtual.

Conforme citado anteriormente, os ambientes de computação em nuvem contemplam funções adicionais, tais como gerenciamento de *hipervisores* e demais controles administrativos decorrentes das características deste modelo de serviço e que precisam ter o acesso controlado. O provedor do serviço deve possibilitar que o cliente gerencie os direitos de acesso aos serviços, às funcionalidades e aos dados mantidos nos serviços, fornecendo funções e especificações para registro, restrição e cancelamento desses acessos. A norma orienta ainda que o provedor apóie o uso de ferramentas para gestão de identidade e gestão de acesso, mesmo que fornecida por

terceiros, para facilitar o uso de múltiplos serviços de nuvem com login único e para possibilitar a integração e administração de identidade do cliente com o serviço em nuvem.

Já quanto aos direitos de acesso privilegiados, os quais permitem acessos aos recursos administrativos do serviço em nuvem, o provedor deve fornecer técnicas adequadas para autenticação dos administradores do serviço em nuvem, tanto para seus funcionários como para os funcionários do cliente, coerentes com os riscos associados a esses acessos. Além disso, o provedor deve disponibilizar ao cliente, informações sobre os procedimentos adotados para gerenciar e armazenar os dados referentes as autenticações realizadas no serviço, tais como: login, senhas, dados biométricos, etc.

A norma ISO 27017:2016 também recomenda que o provedor de serviços em nuvem forneça a seus clientes o registro de logs de eventos em seus serviços e que os clientes avaliem se o recurso oferecido atende aos requisitos desejados, bem como que os computadores utilizados pelos clientes e pelos provedores dos serviços em nuvem devem ter seus relógios sincronizados para garantir a exatidão dos registros de eventos (logs). Para isso, recomenda que o provedor forneça as informações sobre o relógio utilizado em seus sistemas e como o cliente pode proceder para sincronizar os relógios locais com o relógio do serviço em nuvem.

Recursos de criptografia podem ser adotados pelos provedores dos serviços em nuvem na proteção dos dados processados e armazenados, cabendo a ele informar ao cliente em quais circunstâncias a criptografia é utilizada e sobre quaisquer recursos que possa ser oferecido por ele para auxiliar o cliente na aplicação de proteções criptográficas próprias. Para este item vale uma ressalva referente a existência de algumas jurisdições que requerem a utilização de criptografia para determinados tipos de dados.

Os provedores de serviços em nuvem devem ter planos para a gestão de vulnerabilidades técnicas de forma que sejam tomadas ações apropriadas em no tempo devido para prevenir a exposição dos serviços. Neste quesito a ISO 27017:2016 recomenda que o provedor do serviço disponibilize aos clientes, informações sobre a gestão de vulnerabilidades técnicas que podem afetar os serviços oferecidos cabendo aos clientes identificar quais dessas vulnerabilidades podem ser administradas por ele e definam claramente quais os processos para gerenciamento. O Quadro 01 apresenta os requisitos abordados nessa seção de maneira sumarizada.

Quadro 01 - Resumo dos Requisitos de Segurança conforme ISO/IEC 27017:2016

Aspecto	Requisitos de Segurança conforme ISO/IEC 27017:2016 Cabe ao provedor do serviço em nuvem:
Organizacional	- Informar aos clientes os recursos de segurança adotados para prover o serviço. - Definir as políticas de segurança da informação incluindo requisitos aplicáveis à concepção e implementação do serviço em nuvem oferecido. - Evitar ambigüidade – acordar e documentar responsabilidade e papéis com seus clientes, prestadores de serviços e fornecedores. - Definir responsabilidade e papéis quanto a: propriedade dos dados; controle de acesso; manutenção da infraestrutura; manutenção e operações vitais dos dados (backup, recuperação, etc). - Identificar, documentar, implementar, atribuir e comunicar as responsabilidades que são compartilhadas. n acordos de níveis de serviço as medidas de segurança acordadas e as responsabilidades definidas - Garantir que o nível de segurança será mantido pela cadeia de suprimentos. - Treinar, educar, conscientizar e preparar os funcionários para lidar com as solicitações de segurança requisitadas pelos clientes. - Comunicar a seus funcionários os requisitos de segurança acordados com os clientes para que sejam cumpridos e gerenciados. - Informar os países e as localizações geográficas de armazenamento dos dados. - Manter inventário dos ativos dos clientes contendo os dados que são originais do cliente e os que foram gerados pelo serviço. - Documentar e divulgar as funcionalidades que o serviço oferece que permitem aos clientes classificar e rotular as informações e ativo. - Agendar e informar o cliente com antecedências sobre a execução de mudanças. - Disponibilizar aos clientes recursos de monitoramento a aspectos específicos da operação. - Adotar e fornecer ao cliente os mecanismos de proteção adotados para as operações críticas dos serviços em nuvem. - Fornecer aos clientes as especificações documentadas quanto as responsabilidade na gestão de incidentes. - Definir e documentar o procedimento para a remoção e o retorno dos ativos do cliente, no encerramento do acordo de prestação do serviço. - Identificar requisitos legais e contratuais aplicáveis aos tipos de serviços oferecidos e fornecer evidências de conformidade com os mesmos. - Definir processo para responder a notificações referentes a propriedade intelectual e informar ao cliente as especificação da criptografia utilizada. - Evidenciar aos clientes o cumprimento de todos os controles de segurança acordados.
Físico	- Possuir políticas e procedimentos para o descarte e reuso seguro de equipamentos e mídias de armazenamento de dados.
Técnico	- Informar o cliente sobre as restrições de capacidade dos recursos existentes no serviço em

	nuvem contratado. - Monitorar a capacidade dos recursos dos serviços contratados. - Disponibilizar para o cliente informações sobre o procedimento de backup. - Adotar proteção adicional nos acessos em ambientes virtuais compartilhados. - Implementar segregação lógica dos dados. - Estabelecer a política de segurança para a configuração da rede virtual considerando a política de segurança definida para a rede física. - Reforçar os controles de segurança na configuração das máquinas virtuais. - Possibilitar ao cliente gerenciar os direitos de acesso aos serviços e dados. - Apoiar o uso de ferramentas de gestão de identidade. - Fornecer técnicas adequadas para controle dos acessos privilegiados. - Disponibilizar informações sobre os procedimentos adotados para armazenamento e gerência dos dados de autenticação. - Fornecer aos clientes o registro de logs de eventos. - Adotar criptografia e informar ao cliente em quais circunstâncias o recurso é utilizado. - Informar sobre os recursos oferecidos que auxilie o cliente a utilizar proteção criptográfica própria. - Fornecer informações aos clientes sobre o relógio utilizado em seus sistemas para sincronização. - Disponibilizar aos clientes, informações sobre a gestão de vulnerabilidades técnicas

Fonte: Elaborado pelos autores (2017).

Todos os requisitos abordados são recomendação sobre “o que” deve ser tratado pelo provedor de serviços em nuvem. Não apresenta as recomendações tecnológicas e operacionais de “como fazer” as implementações. Essas definições devem ser tratadas conforme cada situação e considerar a intenção de uso e o tipo dos serviços em nuvem.

6 CONSIDERAÇÕES FINAIS

No universo dos temas estudados sobre segurança da informação aplicáveis aos provedores de serviços em nuvem recomendados pela ISO 27017:2016, observa-se que os temas tratamento da ambiguidade das responsabilidades e papéis e a definição das responsabilidades compartilhadas permeiam a maioria das vertentes. Devido às características inerentes a computação em nuvem, tanto no aspecto organizacional, físico e técnico, salvo as recomendações que são diretas, ou seja, que indicam a ação exata a ser realizada, fica evidente a importância de atentar-se para evitar a ambiguidade das responsabilidades e definir com clareza e riqueza de

detalhes todas as atribuições que serão compartilhadas e a quem compete tais responsabilidades. Outra recomendação recorrente da norma é a transparência do provedor do serviço com os clientes referente aos controles de segurança adotados e praticados. Estas recomendações possibilitam que o cliente avalie se o nível de segurança oferecido pelo provedor é satisfatório e opte pelo uso do serviço ou não de forma consciente.

Foi possível observar também que a maioria dos controles de segurança física recomendados para ambiente computacionais tradicionais são os mesmos para os ambientes de computação em nuvem. O aspecto físico é o que contemplou menos controles adicionais de segurança para a computação em nuvem em relação aos controles apresentados na ISO 27002:2013. Para esta vertente a norma ISO 27017:2016 apresenta apenas um controle de segurança complementar referente ao descarte ou reuso de ativos que armazenam informações.

Os controles de segurança preconizados pela norma ISO 27017:2016, aplicáveis aos provedores de serviços em nuvem foram apresentados em um quadro que sumariza seus conteúdos para possibilitar o entendimento rápido sobre eles e agilizar sua aplicação, porém, requerem avaliações técnicas para operacionalizar as recomendações apresentadas. Além disso, observa-se que o propósito de cada cenário de uso de serviços em nuvem, o modelo de serviço adquirido e os riscos de segurança associados a cada um deles são fatores primordiais a serem considerados para implementar os requisitos de segurança adequados e na medida certa.

Para obter uma solução completa de segurança em cenários de computação em nuvem, a ISO 27017:2016 deve ser adotada de forma complementar aos controles da norma ISO/IEC 27002:2013, pois esta apresenta requisitos de segurança primordiais e fundamentais para um ambiente computacional independente da forma em que os recursos de tecnologia da informação são administrados. Materiais e normativas adicionais também podem ser utilizados quando forem pertinentes ao cenário de aplicação.

Como sugestão de trabalhos futuros indica-se que o estudo seja complementado com os requisitos da norma ISO/IEC 27017:2016 destinados aos clientes e os temas da ISO/IEC 27002:2013 interpretados e adaptados para os cenários de computação em nuvem. Opções técnicas para a implementação das recomendações também podem ser apresentadas para enriquecer o estudo.

Requirements for safety analysis of information in cloud service providers

ABSTRACT
With the occurrence of the big data phenomenon, the need for technology and adequate infrastructure to support this new scenario arises. In this context, cloud services meet this demand, but require specific security controls because of the way in which computing resources are designed, used, and managed. This paper presents an evaluation of the ISO / IEC 27017: 2016 standard with the objective of reporting security requirements for cloud service providers, classified according to their application to the organizational, physical and technical aspects. With the study it was possible to observe that for the organizational as well as the technical aspect, the standard presents several specific controls for the cloud services. Regarding the physical aspect, the recommendations are very similar to those of a traditional environment. The issue of security responsibilities and roles permeates the other controls and needs to be defined in detail among the parties involved. The work presents a framework with the controls addressed by the standard to streamline the understanding and its application, but requires additional technical evaluations to operationalize them. It is also noted that to achieve a complete safety solution, the controls of ISO / IEC 27002: 2013 should be adopted. In addition, the purpose of the cloud service usage scenarios, the service model purchased, and the security risks associated with each are decisive for properly implementing the requirements.

Keywords: Big data. Cloud Services. Information Security. ISO 27017.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 2002:2013: **Tecnologia da Informação – Técnicas de segurança – Código de prática para controle de segurança da informação**. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 2017:2016: **Tecnologia da Informação – Técnicas de segurança – Código de prática para controle de segurança da informação com base na ABNT NBR ISO/IEC 27002 para serviços em nuvem**. Rio de Janeiro, 2016.

BADGER, Lee; GRANCE, Tim; PATT-CORNER, Robert; VOAS Jeff. **Cloud Computing Synopsis and Recommendations.** NIST Special Publication 800-146, 2012. Disponível em: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf>. Acesso em: 07 dez. 2017.

BRODKIN, Jon. **Gartner**: Seven cloud-computing security risks Cloud computing is picking up traction with businesses, but before you jump into the cloud, you should know the unique security risks it entails. 2008. Disponível em: <http://www.infoworld.com/article/2652198/security/gartner--seven-cloud-computing-security-risks.html>. Acesso em: 10 nov. 2017.

CHEN Min; MAO Shiwen; LIU Yunhao. **Big Data**: a Survey. New York, Springer Science+Business Media, 2014. Disponível em: <https://link.springer.com/content/pdf/10.1007%2Fs11036-013-0489-0.pdf>. Acesso em: 05 nov. 2017.

DEVENPORT, Thomas H. ***Big Data* @ Work: Dispelling the Mhyts, Uncovering the Opportunities**. Boston, Massachusetts: Harvard Business School Publishing Corporation, 2014.

ERL, Thomas; KHATTAK, Wajid; BUHLER, Paul. ***Big Data* Fundamentals Concepts, Drivers & Techniques**. U.S: Arcitura Education Inc, 2016.

FERREIRA, Anderson Soares. **Uma arquitetura para monitoramento de segurança baseada em acordos de níveis de serviço para nuvens de infraestrutura**. 2013. Dissertação (Mestrado em Ciência da Computação) - Universidade Estadual de Campinas, Campinas, 2013. Disponível em: < http://repositorio.unicamp.br/jspui/handle/REPOSIP/275624>. Acesso em: 06 jun. 2018.

FERREIRA, Duarte Miguel Petiz. **Infraestrutura Confiável para Cloud baseada em OpenStack**. 2017. Dissertação (Mestrado em Engenharia de Redes e Sistemas Informáticos) - Faculdade de Ciências da Universidade do Porto, Portugal 2017. Disponível em <https://repositorio-aberto.up.pt/bitstream/10216/106587/2/206203.pdf >. Acesso em: 06 jun. 2018.

FONSECA, J. J. S. **Metodologia da pesquisa científica**. Fortaleza: UEC, 2002. Apostila.

GERHARDT, Tatiana; SILVEIRA, Denise. **Métodos de pesquisa.** Porto Alegre: Ed. UFRGS, 2009.

GIL, Antonio C. **Como elaborar projetos de pesquisa**. 3. ed. São Paulo: Atlas, c1991.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. ***Big data***: como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. Rio de Janeiro: Elsevier, 2013.

MELL, Peter; GRACE, Timothy. **The NIST Definition of Cloud Computing.** NIST Special Publication 800-145, 2011. Disponível em: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>. Acesso em: 05 set. 2017.

RODRIGUES, Marcio Affonso. **Segurança da informação em empresas**. 2016. Trabalho de Conclusão de Curso de Tecnologia em Sistemas de Computação – Universidade Federal Fluminense, Niterói, 2016. Disponível em: < https://app.uff.br/riuff/handle/1/5692>. Acesso em: 06 jun. 2018.

SILVA, Paulo Matheus Nicolau. **Recomendações de segurança da informação para soluções de tecnologia da informação e comunicação baseadas em computação em nuvem**. 2013. Monografia de Graduação em Engenharia de Redes de Comunicação - Universidade de Brasília,

Faculdade de Tecnologia, 2013. Disponível em: <http://bdm.unb.br/handle/10483/14032>. Acesso em: 06 jun. 2018.

SILVA, Roberto Carlos Gomes da. **Migração e segurança em plataformas cloud computing**. Dissertação de Mestrado. 2014. Disponível em: <https://repositorio.ucp.pt/bitstream/10400.14/16110/1/Disserta%C3%A7%C3%A3o-Migra%C3%A7%C3%A3o%20e%20seguran%C3%A7a%20em%20plataformas%20cloud%20computing%20-%20Roberto%20Silva.pdf>. Acesso em: 17 jul. 2017**.**

SILVA, Thiago Barros Zanette da. Estudo dos Aspectos de Autenticação para SaaS. 2015. Trabalho de Graduação em Engenharia de Redes de Computadores, Universidade de Brasília, Brasília, 2015. Disponível em <http://bdm.unb.br/handle/10483/15242>. Acesso em: 06 jun. 2018.

TAURION, Cezar. 2016. **Volume, variedade, velocidade, veracidade e valor**: os cinco Vs do *Big Data*. Disponível em: <http://computerworld.com.br/volume-variedade-velocidade-veracidade-e-valor-os-cinco-vs-do-big-data>. Acesso em: 17 out. 2017.

VIANNA, Willian Barbosa; DUTRA Moisés Lima; FRAZZON, Enzo Morosini. ***Big Data*** **e a Gestão da Informação**: modelagem do contexto decicional apoiado pela sistemografia**,** 2016. Disponível em:<http://www.uel.br/revistas/uel/index.php/informacao/article/view/23327/18993>. Acesso em: 03 jul. 2017.