REQUISITOS DE SEGURANÇA PARA PROVEDORES DE SERVIÇOS EM NUVEM DE ACORDO COM A NORMA ISO 27017

Safety Requirements for Cloud Service Providers in Accordance with Standard ISO 27017

Gislaine Parra Freund [(1)], Priscila Basto Fagundes [(2)], Douglas Dyllon Jeronimo de Macedo [(2)]

(1) Dígitro Tecnologia S.A, Florianópolis, SC - Brasil,
gislaineparraf@gmail.com
(2) Universidade Federal de Santa Catarina, Florianópolis, SC - Brasil,
priscila.bfagundes@gmail.com, 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 tecnicamente concebidos, utilizados e gerenciados. O presente artigo trata-se de um estudo da norma ISO/IEC 27017:2016 com o objetivo de apresentar de maneira direta e objetiva, os requisitos de segurança referentes aos temas: definição de papéis e responsabilidades, controle de acesso e armazenamento dos dados, destinados aos provedores dos serviços em nuvem, conforme as recomendações desta norma. Trata-se de uma pesquisa bibliográfica, de abordagem qualitativa e de caráter exploratório. Para selecionar os temas da norma a serem abordados neste estudo, estes foram analisados considerando a relevância, independente da situação e do propósito de uso dos serviços em nuvem. Foi possível concluir que o tratamento da ambiguidade das responsabilidades e papéis, e a definição das responsabilidades compartilhadas permeiam outros requisitos apresentados e precisam ser abordados com atenção, e que o quadro apresentado neste estudo possibilita um entendimento rápido para aplicação dos requisitos, porém requer adicionalmente avaliações técnicas para operacionalizá-las.
Palavras-chave: *Big data*; Serviços em nuvem; Segurança da Informação; ISO 27017.

Abstract:
With the occurrence of the big data phenomenon, the need for technology and adequate infrastructure to support this new scenario. In this context, cloud services meet this demand, but require specific security controls because of the way in which computing resources are technically designed, used, and managed. The present article deals with a study of ISO / IEC 27017: 2016 with the objective of presenting in a direct and objective way, the safety requirements related to the themes: definition of roles and responsibilities, access control and data storage, For cloud service providers, in accordance with the recommendations of this standard. This is a bibliographical research, with a qualitative and exploratory approach. In order to select the themes of the standard to be addressed in this study, these were analyzed considering the relevance, regardless of the situation and the purpose of using the cloud services. It was possible to conclude that the treatment of the ambiguity of responsibilities and roles, and the definition of shared responsibilities permeate other requirements presented and need to be approached with attention, and that the table presented in this study allows a fast understanding for application of the requirements, Techniques to operationalize them.
Keywords: Big data; Cloud Services, Information Security; 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 exibido por Taurion (2016), a geração de zetabytes diários, deixa de ser uma escala imaginária e futurista e passa a ser uma escala real.

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 e LIU, 2014). Algumas das características desta tecnologia é a capacidade de processamento e armazenamento, virtualização de recursos, largura de banda disponível, queda nos custos de *hardware,* etc. (SILVA, 2014)

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 infra-estrutura 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 as características técnicas e operacionais oriundas desse tipo de serviço.

O foco deste artigo é elencar e apresentar de maneira direta e objetiva, os requisitos de segurança destinados aos seguintes temas: papéis e responsabilidades pela segurança da informação, acesso e armazenamento dos dados nos serviços em nuvem, conforme as recomendações da norma ISO/IEC 27017:2016. Serão contemplados apenas os itens relacionados aos temas supracitados por serem compreendidos como requisitos essenciais e aqueles que apresentam recomendações específicas para atender as particularidades dos serviços em nuvem destinados ao provedor.

Pretende-se com esse estudo auxiliar profissionais da área da segurança da informação na aplicação destes controles da norma ISO/IEC 27017:2016.

2 Referencial Teórico

O conceito *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, o *big data* 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 acessíveis, convenientes e provisionados com esforço mínimo de gerenciamento ou interação do provedor. Classifica 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). E apresenta 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, segurança da informação é alcançada com a implementação de um conjunto adequado de controles de forma coordenada e coerentes com os riscos associados em uma visão holística da organização.

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 sendo que alguns deles 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 parte de seu conteúdo de forma resumida e objetiva.

3 Procedimentos Metodológicos

Para este estudo foram realizadas pesquisas entre os dias 03 e 10/07/2017, no Google Acadêmico e na base de dados *Web Science* para identificar as publicações acadêmicas que contemplam os temas segurança nos serviços em nuvem, vinculada com a norma ISO/IEC 27017:2016. Observou-se que os trabalhos 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.

Para selecionar os temas a serem abordados neste estudo, os 13 controles da norma foram analisados com a premissa de identificar aqueles que são essenciais, independente do propósito do uso de serviços em nuvem e dos riscos associados a ele. O resultado desta análise apontou que em todas as situações de uso de serviços em nuvem, as responsabilidades e papéis pela segurança precisam ser definidos, assim como requisitos de segurança no armazenamento e no controle de acesso aos dados. Diante disso, foi realizado o estudo da norma e identificados nos controles, os requisitos relacionados com estes temas e foram apresentados em um quadro. Os requisitos abordados, limitou-se aos aplicáveis ao provedor do serviço em nuvem. Sendo assim, 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”.

4 Resultados

A partir do estudo realizado na norma ISO/IEC 27017:2016 foram extraídos os requisitos referentes a organização da segurança quanto aos papéis e responsabilidades, segurança no armazenamento e controle de acesso aos dados, destinados ao provedor do serviço.

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.

Organização da Segurança da Informação

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 as 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 consequências 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. Estas atribuições devem ser identificadas, atribuídas às partes, documentadas, comunicadas e implementadas conforme acordado. E o provedor do serviço em nuvem, no papel de custodiante, deve considerar a criticidade dos dados e aplicações de seus clientes na alocação dos papéis e responsabilidades a seus funcionários, além de comunicar a eles sobre os requisitos de segurança envolvidos 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.

Armazenamento e Controle de Acesso

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 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 na tabela de metadados.

O provedor do serviço deve possibilitar que o cliente gerencie os direitos de acesso aos serviços e de seus usuários, fornecendo funções e especificações para registro, restrição e cancelamento desses acessos. A norma orienta ainda que o provedor apoie 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.

Os direitos de acesso privilegiados, os quais permitem acessos aos recursos administrativos do serviço em nuvem, também devem ser controlados. 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.

Recursos de criptografia podem ser adotados pelos provedores dos serviços em nuvem na proteção dos dados processados e armazenados, cabendo a ele informar o 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.

O Quadro 01 apresenta os requisitos abordados nessa seção de maneira sumarizada.

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

Temas	Requisitos de Segurança conforme ISO/IEC 27017:2016
Referente ao tema: Responsabilidades e Papéis pela Segurança da Informação, é recomendado ao provedor do serviço em nuvem:	- 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; - 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.
Referente ao tema: armazenamento e controle de acesso, é recomendado ao provedor do serviço em nuvem:	- Adotar proteção adicional nos acessos em ambientes virtuais compartilhados. - Implementar segregação lógica dos dados. - 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. - 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.

Fonte: Desenvolvido pelos autores

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

4 Considerações Finais

Observa-se que, no universo dos temas estudados, o tratamento da ambigüidade das responsabilidades e papéis e a definição das responsabilidades compartilhadas permeiam todos os demais temas. Salvo as recomendações que são diretas, ou seja, que indicam a ação exata a ser realizada, como por exemplo, implementar segregação lógica dos dados, na implantação dos demais requisitos é necessário atentar-se para evitar a ambiguidade das responsabilidades e definir com clareza e riqueza de detalhes

todas as atribuições que serão compartilhadas.

Os requisitos identificados na norma foram apresentados em um quadro que sumariza os conteúdos e possibilita um entendimento rápido sobre eles de forma a auxiliar e agilizar sua aplicação, porém requer avaliações técnicas para operacionalizar as recomendações apresentadas. Além disso, o propósito de cada cenário de uso de serviços em nuvem e os riscos de segurança associados a cada um deles deve ser considerado para implementar os requisitos na medida certa.

Para obter uma solução completa de segurança, os outros controles da norma ISO/IEC 27017:2016 devem ser analisados e adotados, pois este trabalho limitou-se a apenas três dos treze controles apresentados na norma. Além disso, a norma ISO/IEC 27002:2013 deve ser consultada assim como materiais adicionais que forem pertinentes ao cenário de aplicação.

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

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.

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 03/07/2017.

CHEN Min, MAO Shiwen, LIU Yunhao. ***Big Data: A Survey***. New York, Springer Science+Business Media, 2014.

Disponível em:

https://link.springer.com/article/10.1007%2Fs11036-013-0489-0. Acesso em 05/07/2017.

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.

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

GERHARDT, Tatiana E.; SILVEIRA, Denise T. **Métodos de pesquisa.** Porto Alegre: Editora da UFRGS, 2009.

GIL, ANTONIO CARLOS. **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: 05/07/2017 .

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 **17/07/2017.**

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 17/07/2017.

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 03/07/2017.