Uma contribuição para a segurança da informação: um estudo de casos múltiplos com organizações brasileiras1

Napoleão Verardi Galegale

Professor e Pesquisador da Unidade de Pós-Graduação do Centro Paula Souza.Doutor em Controladoria, Centro Estadual de Educação Tecnológica Paula Souza – CEETEPS, Unidade de Pós-Graduação

Edison Luiz Gonçalves Fontes

Mestre em Tecnologia, Centro Estadual de Educação Tecnológica Paula Souza – CEETEPS, Unidade de Pós-Graduação

Bernardo Perri Galegale

Mestrando em Ciência da Informação. Escola de Comunicação e Artes – ECA. Universidade de São Paulo – USP

http://dx.doi.org/10.1590/1981-5344/2866

A política de segurança da informação figura dentre os fatores críticos para o sucesso da proteção da informação, devendo declarar controles adequados. A literatura acadêmica sobre este tema é reduzida e os gestores se deparam com dificuldades em selecionar controles para a política de uma organização. Este trabalho tem como objetivo compreender os controles citados nas políticas de segurança da informação das organizações visando identificar a existência de controles recorrentes para subsidiar a tomada de decisão pelo gestor da informação, acerca da definição dos controles comuns que devem ser considerados na elaboração da política. Como metodologia, utiliza uma abordagem qualitativa, com objetivo descritivo por meio de pesquisa bibliográfica, estudo de casos múltiplos e análise de documentos primários com análise de conteúdo e síntese de casos cruzados. A coleta de dados foi realizada com base em uma amostragem não probabilística com dez organizações

[1] Artigo elaborado a partir da dissertação de mestrado de Edison Luiz Gonçalves Fontes, intitulada "Política de segurança da informação: uma contribuição para o estabelecimento de um padrão mínimo", Centro Estadual de Educação Tecnológica Paula Souza (CEETEPS), 2011.

brasileiras distintas, com políticas de segurança da informação maduras. Como resultados foram identificados 40 controles citados de forma recorrente em políticas, os quais também foram associados à principal referência da literatura da área, descritos e agrupados em quatro extratos de frequência: 12 controles citados por 100% das políticas, 15 por 90%, 16 por 80% e 40 por 70%.

Palavras-chave: *Políticas de segurança; Segurança da informação; Proteção da Informação.*

A contribution for information security: a multiple case study with brazilian organizations

The information security policy appears among the critical success factors for information protection and it should contain adequate controls. There is rather sparse academic literature about this subject and the managers face difficulties on selecting controls for a organization's policy. The main purpose of this study is to understand the controls that appear on organization information security policies to identify recurring controls that support the decision making by the information owner about the definition of the common controls that should be included in the policy. The methodology uses a qualitative approach with a descriptive objective by means of a bibliographic research, multiple case studies and primary document analysis with content analysis and cross referenced cases. The data collection was done with a non-probabilistic sample of ten distinct brazilian organizations that had mature information security policies. The results show that recurring mention of 40 controls and which in turn were associated to the main literature reference for the area and grouped in four frequency extracts: 12 controls were present on 100% of the policies, 15 were present on 90% and 40 were present on 70% of the evaluated policies.

Keyords: *Security policies; Information security; Information protection.*

Recebido em 06.03.2017Aceito em 12.07.2017

1 Introdução

A informação é um recurso essencial para toda organização, independente do porte e do segmento de atuação. É com a informação que processos organizacionais funcionam, a geração de conhecimento acontece e o compartilhamento desse conhecimento é realizado. Gestores utilizam a informação para tomada de decisão fazendo com que as organizações alcancem seus objetivos e melhorem seu desempenho no mercado. Assim, a informação tem importância estratégica, é impulsionada com a utilização de Tecnologia da Informação (TI) nos processos organizacionais e deve ter proteção adequada.

Falhas na segurança da informação comprometem a informação e podem representar tanto prejuízos financeiros como danos à imagem das organizações (POSTHUMUS; VON SOLMS, 2004), reforçando a necessidade de sua proteção.

A empresa de consultoria e auditoria PriceWaterhouseCoopers (2014) realizou uma pesquisa mundial sobre segurança da informação – *The Global State of Information Security Survey 2014* – entre 01/02 a 01/04/2013 envolvendo 9.600 executivos de organizações de 115 países. A análise das respostas possui margem de erro inferior a 1% e sugere que apesar do investimento em segurança ter aumentado, notou-se que as empresas ainda se perdem na hora de definir as melhores práticas, têm dificuldade de conduzir analises situacional e de identificar e priorizar os dados que precisam ser adequadamente resguardados. Houve um aumento de 25% dos incidentes de segurança em relação ao ano anterior e a perda financeira média associada a tais incidentes também cresceu 18% em relação ao mesmo período (PRICEWATERHOUSECOOPERS, 2014).

Um dos documentos fundamentais para a proteção da informação é a política de segurança da informação. As políticas são diferentes das normas e procedimentos na medida em que as políticas se constituem no alicerce para elaboração dos demais documentos. Para Almeida (2000, p. 6), "as políticas ou diretrizes são planos gerais de ação, guias genéricos que estabelecem guias mestras, orientam a tomada de decisão e dão estabilidade à organização".

A política de segurança da informação deve conter declarações sobre o comprometimento da direção da organização, responsabilidades gerais e específicas, conscientização, gerenciamento de riscos, objetivos de controle e controles, consequências da violação da política, etc. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT, 2005).

Os controles têm um papel relevante na segurança da informação, pois é por meio deles que a segurança é obtida e de alguma forma devem ser referenciados na política. O controle possibilita o gerenciamento dos riscos de proteção da informação por meio de procedimentos, estruturas

organizacionais e práticas de natureza administrativa, técnica ou legal (ABNT, 2005).

Os controles selecionados e declarados na política são derivados dos requisitos de segurança da informação de cada organização. Após ter definido tais requisitos, ao buscar elaborar sua política, a organização se depara com uma grande quantidade de controles na literatura (muitos equivalentes), geralmente focada na descrição dos aspectos técnicos e operacionais da implementação, tratando todos os controles de forma igualitária quanto à sua criticidade. A título de exemplo, a norma ABNT ISO/IEC 27002:2005 tem por objetivo estabelecer diretrizes sobre as metas geralmente aceitas para a gestão da segurança da informação e apresenta 133 controles (ABNT, 2005).

Este cenário – valor da informação para as organizações, a importância de proteger tais informações, os avanços tecnológicos e a exposição a tais ameaças, bem como a multiplicidade de controles disponíveis – justifica a presente pesquisa, que visa bem compreender os controles citados nas políticas de segurança da informação das organizações, com o objetivo de identificar a existência controles recorrentes. Para melhor direcionar o estudo, o problema da pesquisa foi assim enunciado: Há controles citados nas políticas de segurança da informação das organizações de forma recorrente? Quais?

Com esta pesquisa espera-se contribuir para a Ciência da Informação por meio de uma visão geral da literatura sobre o assunto, complementando-a com os resultados empiricamente obtidos da pesquisa e subsidiar a tomada de decisão pelo gestor da informação acerca da definição dos controles comuns que devem ser considerados na elaboração da política de segurança da informação e implementados em uma organização. Também se espera subsidiar a avaliação de uma determinada política em relação às práticas de mercado (*benchemarking*[2]).

A sequência do presente artigo apresenta a fundamentação teórica, os procedimentos metodológicos utilizados, os resultados/discussão e as conclusões alcançadas.

2 Fundamentação teórica

A definição de segurança da informação pode ser resumida como a proteção da informação, de modo a preservar as suas propriedades de confidencialidade, integridade, disponibilidade, autenticidade e não repúdio, evitando que as vulnerabilidades dos ativos a ela relacionados sejam exploradas por ameaças e possam ocasionar perdas para os negócios de uma organização, não estando restrita a sistemas de computação, nem à informação em formato eletrônico. (GORDON; LOEB, 2002; SÊMOLA, 2003; ABNT, 2006).

[2] Processo de pesquisa e comparação de práticas empresariais de diversas organizações como instrumento de gestão de uma determinada empresa.

Considerando-se os objetivos e a cultura de uma organização, a segurança da informação pode ser entendida sob três pontos de vista: (i) técnico, com ênfase na utilização de controles tecnológicos como medida de proteção da informação; (ii) social, com foco na motivação de pessoas e no comportamento coletivo para resolução de problemas de segurança; e (iii) sociotécnico, com a exploração das vantagens e minimização das desvantagens das duas abordagens anteriores, de forma simultânea (SIPONEN, 2001).

Dentre os fatores críticos para o sucesso da cultura de segurança da informação, a política de segurança é considerada uma das melhores práticas (WILLIAMS, 2001). Imoniana (2004) desenvolveu um estudo sobre a validade de modelos de políticas de segurança da informação utilizados na indústria automobilística na região metropolitana do ABC da cidade de São Paulo. Comprovou a existência de uma política de segurança da informação nestas empresas e que as mesmas contemplam o modelo baseado em quatro pilares: segurança administrativa, segurança física, segurança do acesso lógico e segurança legal e ambiental.

A segurança da informação e seus problemas são tratados em diversas dimensões e por diversas iniciativas, tanto na literatura como dentro das organizações. Em se tratando da dimensão dos negócios, para Almeida, Souza e Cardoso (2010, p.156), "Ainda que se perceba a necessidade de implementá-la, em geral não há clareza sobre o que deve ser protegido e sobre como fazê-lo" e para nortear o trabalho de gestores responsáveis por projetos de segurança, defende o uso de uma ontologia para classificar a informação no ambiente corporativo para fins de proteção.

Uma ontologia tem como funcionalidade descrever e representar conceitos e propriedades relevantes de um domínio específico, facilitando o compartilhamento e agregação de conhecimento por meio de um vocabulário baseado em axiomas e regras definidas para a ontologia proposta. A ontologia tem sido tratada tanto em Ciência da Computação (GUARINO, 1998; SOWA, 2000; SMITH, 2003), quanto em Ciência da Informação (VICKERY, 1997; GILCHRIST, 2003; ALMEIDA, 2014).

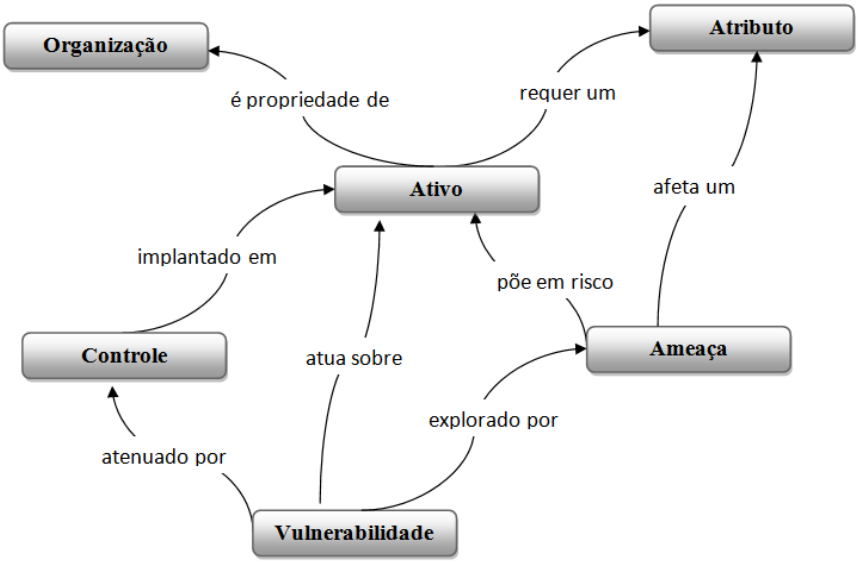
Gualberto *et al.* (2013) propõem uma ontologia para apoio à gestão de riscos de segurança da informação, visando contribuir: (i) com o processo de gerenciamento destes riscos por meio de uma representação formal das informações relacionadas, promovendo a aquisição e o compartilhamento de conhecimento neste domínio; (ii) na implementação de uma gestão de riscos e na tomada de decisões; e (iii) no reuso de conhecimento e informações, treinamento de colaboradores e para o desenvolvimento de novas ontologias.

Schiavone, Garg e Summers (2014) apresentam uma ontologia para um modelo de segurança da informação onde o domínio se estende para fora do ambiente interno de uma organização e considera o ecossistema à qual pertence. Considera, além do modelo de risco de ativos, vulnerabilidades, ameaças e contramedidas, também as capacidades técnica e de negócio, bem como a complexidade dos cenários de falhas.

Almeida *et al.* (2010) apresentam uma proposta para o estágio terminológico de uma ontologia de domínio sobre segurança da informação para o nível organizacional, passível de utilização no contexto de forma geral. A Figura 1 apresenta o esquema preliminar proposto para esta ontologia, com as seguintes definições (ALMEIDA *et al.,* 2010):

> a)organização: entidade social composta por recursos materiais e humanos, a qual possui objetivos comuns, procedimentos sistemáticos para controle de seu desempenho e limites definidos que a separam do ambiente. Pode ser uma instituição pública ou privada;
>
> b)atributo de segurança: propriedade atribuída a um ativo, a qual diz respeito a requisitos de segurança. Pode ser um atributo de confidencialidade, de integridade e de disponibilidade;
>
> c)ativo: bem de propriedade da organização, utilizado para alcançar seus objetivos sociais. Pode ser um equipamento, estoque, imóvel, dentre outros;
>
> d)controle: procedimento padrão sistemático implementado para atenuar vulnerabilidades, bem como para proteger ativos através de medidas preventivas e corretivas;
>
> e)ameaça: possibilidade de dano aos ativos da organização, a qual afeta atributos de segurança específicos e explora vulnerabilidades da organização. Pode ser de origem humana ou natural, e ter como fonte um evento acidental ou uma ação deliberada;
>
> f)vulnerabilidade: situação caracterizada pela falta de medidas de proteção adequadas. Uma vulnerabilidade possui um grau de severidade associado (por exemplo, crítico, moderado ou baixo). Pode ser uma vulnerabilidade de origem administrativa, técnica ou física.

Figura 1 - Esquema preliminar da ontologia de segurança da informação



Fonte: ALMEIDA *et al.* (2010).

Albuquerque Junior e Santos (2014) efetuaram um levantamento da produção científica sobre segurança da informação em anais de eventos científicos brasileiros das áreas de Administração e afins, no período entre 2004 e 2013, envolvendo os eventos: CNEG[3], CONTECSI[4], SEMEAD[5], SEGET[6], ENEGEP[7], SIMPEP[8], SBTI[9] e ENANCIB[10]. Tais eventos foram escolhidos por apresentarem trabalhos sobre sistemas de informações e segurança da informação tanto com enfoque tecnológico quanto utilizando alguma abordagem social, por mais de 10 anos (com exceção do SBTI, que iniciou em 2013). Desta pesquisa foram obtidos, entre outros, os seguintes resultados (ALBUQUERQUE JUNIOR; SANTOS, 2014):

> a)do total de 29.616 artigos publicados nos eventos pesquisados, foram identificados 67 artigos (0,23%) com foco específico na segurança da informação, como tema ou como dimensão de análise;
>
> b)dos 12 textos mais referenciados nos 67 artigos, 4 são normas técnicas e 8 são livros;
>
> c)entre os 3 textos mais referenciados, figura em primeiro lugar (com 31 vezes) a norma técnica ISO/IEC 27002:2005 (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION;

[3] CNEG - Congresso Nacional de Excelência em Gestão.
[4] CONTECSI - *International Conference on Information Systems and Technology Management.*
[5] SEMEAD - Seminários em Administração.
[6] SEGET - Simpósio de Excelência em Gestão e Tecnologia.
[7] ENEGEP - Encontro Nacional de Engenharia de Produção.
[8] SIMPEP - Simpósio de Engenharia de Produção.
[9] SBTI - Simpósio Brasileiro de Tecnologia da Informação.
[10] ENANCIB - Encontro Nacional de Pesquisa em Ciência da Informação.

INTERNATIONAL ELECTROTECHNICAL COMMISSION – ISO/IEC, 2005), consideradas todas as versões em que ela já foi publicada, inclusive a original da *British Standards Institution* (BSI) e a versão em português publicada pela Associação Brasileira de Normas Técnicas (ABNT). Em segundo lugar (com 19 vezes) está o livro "Gestão da Segurança da Informação: Uma Visão Executiva", de Sêmola (2003) e em terceiro lugar (com 11 vezes), a norma técnica ISO/IEC 27001:2006 (ISO/IEC, 2006);

d)entre os três modelos ou abordagens teóricas mais utilizadas pelos autores nas suas pesquisas para análise de fenômenos relacionados à segurança da informação, em primeiro lugar (com 22 vezes) está a norma técnica ISO/IEC 27002:2005 ISO/IEC, 2005); em todas as versões em que já foi publicada. Em segundo lugar (com 5 vezes) estão a norma técnica ISO/IEC 27001:2006 (ISO/IEC, 2006); em todas as versões em que já foi publicada e o COBIT e em terceiro lugar (com 3 vezes) o ITIL;

e)grande parte dos trabalhos que vem sendo realizados tem um foco maior na tecnologia;

f)normas técnicas e livros são os textos mais referenciados, podendo significar uma lacuna de artigos científicos que possam ser citados e uma necessidade a ser suprida;

g)a norma técnica ISO/IEC 27002:2005 (ISO/IEC, 2005) é o modelo de análise mais utilizado e o texto mais referenciado, o que reforça sua importância para pesquisadores que estudam o tema segurança da informação.

Em complemento à pesquisa em eventos científicos, Albuquerque Junior, Santos e Gonzales Junior (2015) efetuaram um levantamento da produção brasileira de artigos sobre segurança da informação publicados em revistas científicas de administração, sistemas de informação e ciência da informação no mesmo período de 10 anos, ou seja, entre 2004 e 2013, que publicam artigos em português, inglês ou espanhol. Para tanto foi utilizado o sistema WebQualis, disponibilizado pela CAPES[11], agência pública brasileira que avalia revistas científicas em uma escala em ordem crescente de qualidade, que consiste em C, B5, B4, B3, B2, B1, A2 e A1. Foram selecionadas 43 revistas classificadas como B3 ou superior. A pesquisa reafirmou que norma técnica ISO/IEC 27002:2005 (ISO/IEC, 2005); é base do modelo ou teoria mais utilizada nas pesquisas.

A ISO/IEC 27002:2005 (ISO/IEC, 2005); teve sua origem como um *British Standard* na forma da norma BS-7799-1:1995 (BRITISH

[11] Coordenação de Aperfeiçoamento de Pessoal de Nível Superior é uma fundação do Ministério da Educação (MEC) e desempenha papel fundamental na expansão e consolidação da pós-graduação *stricto sensu* (mestrado e doutorado) em todos os estados da Federação.

STANDARD INSTITUTION -BSI, 1995) com o título de "*Information security management. Code of practice for information security management systems*", criada em 1995 com o objetivo de fornecer recomendações aos gestores responsáveis pela segurança da informação em suas organizações e prover uma base comum para desenvolver normas e práticas efetivas de gestão da segurança. Em 1999 o referido padrão foi revisado e atualizado para BS-7799-1:1999 (BSI, 1999), com a incorporação de novos controles para atender a evolução tecnológica e as necessidades do mercado. Em 2000 a ISO[12] publicou a norma internacional ISO/IEC 17799:2000 (ISO/IEC, 2000) com o título de "*Information technology - Code of practice for information security management*", inteiramente baseada na BS-7799-1:1999 (BSI, 1999), revisada e atualizada em 2005 para ISO/IEC 17799:2005 e recodificada em 2007 para ISO/IEC 27002:2005 (ISO/IEC, 2005) em função da alteração do sistema de codificação de normas da ISSO.

Em 2001 a ABNT publicou a norma brasileira NBR ISO/IEC 17799:2001 (ABNT, 2001) com o título de "Tecnologia da Informação - Código de prática para a gestão da segurança da informação", totalmente equivalente à ISO/IEC 17799:2000 (ISO/IEC,, 2000) e em 2005 a NBR ISO/IEC 17799:2005, recodificada para NBR ISO/IEC 27002:2005 (ABNT, 2005), assegurando a total compatibilidade com as respectivas normas da ISO.

Tais normas são largamente adotadas por organizações de todo o mundo. É possível uma organização obter uma certificação em segurança da informação e para tanto ela deve se adequar às práticas da norma ISO/IEC 27002:2005 (ou NBR ISO/IEC 27002:2005) e ser auditada conforme padrões estabelecidos na ISO/IEC 27001:2006 - *Information technology - Security techniques - Information security management systems - Requirements* (ou NBR ISO/IEC 27001:2006 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos).

De acordo com a última pesquisa da ISO há um grande número de empresas com certificações nesta norma e este número vem crescendo. Em 2014 existiam 23.972 organizações certificadas no mundo. O Japão aparece em primeiro lugar em quantidade de organizações (7.181), cerca de três vezes a quantidade de organizações nos países que aparecem em segundo, terceiro e quarto lugares, respectivamente, Reino Unido (2.261), China (2.202) e Índia (2.170). No Brasil o número de organizações cerificadas ainda é pequeno (86). Há organizações certificadas dos mais variados segmentos do mercado, entre os quais: telecomunicações, órgãos públicos, prestação de serviços, tecnologia da informação, construção, etc. (ISO, 2014).

[12] *International Organization for Standardization* é uma organização internacional independente, não-governamental com adesão de 162 organismos nacionais de normalização. Atua por meio de seus membros, que reúne especialistas para compartilhar conhecimentos e desenvolver de forma voluntária, baseado no consenso, normas internacionais pertinentes que apoiam a inovação e fornecem soluções para os desafios globais.

A norma NBR ISO/IEC 27002:2005 (ABNT, 2005) está estruturada em 11 seções contendo controles de segurança da informação, estes últimos agrupados em categorias principais de segurança. Por sua vez, cada categoria principal contém: (i) um objetivo de controle que deve ser alcançado, e (ii) um ou mais controles que podem ser aplicados para alcançar o objetivo de controle em questão. As 11 seções e respectivas quantidades de categorias principais com a corresponde quantidade de controles são (ABNT, 2005):

a) Política de Segurança da Informação: 1 categoria e 2 controles;
b) Organizando a Segurança da Informação: 2 categorias e 11 controles;
c) Gestão de Ativos: 2 categorias e 5 controles;
d) Segurança em Recursos Humanos: 3 categorias e 9 controles;
e) Segurança Física e do Ambiente: 2 categorias e 13 controles;
f) Gestão das Operações e Comunicações: 10 categorias e 32 controles;
g) Controle de Acesso: 7 categorias e 25 controles;
h) Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação: 6 categorias e 16 controles;
i) Gestão de Incidentes de Segurança da Informação: 2 categorias e 5 controles;
j) Gestão da Continuidade do Negócio: 1 categoria e 5 controles; e
k) Conformidade: 3 categorias e 10 controles.

Em 2013 a ISO revisou e atualizou a norma para ISO/IEC 27002:2013 (ISO/IEC, 2013). Neste mesmo ano a ABNT publicou a respectiva versão brasileira NBR ISO/IEC 27002:2013 (ABNT, 2013).

3 Procedimentos metodológicos

Para cumprir o objetivo da pesquisa e responder a questão formulada – Há controles citados nas políticas de segurança da informação das organizações de forma recorrente? Quais? – neste trabalho foi utilizada a abordagem de pesquisa qualitativa, com objetivo descritivo e como procedimentos, pesquisa bibliográfica, estudo de casos múltiplos e análise de documentos primários por meio da análise de conteúdo e da síntese de casos cruzados (GIL, 1999; RICHARDSON, 1999; YIN, 2005; BARDIN, 2011).

A abordagem qualitativa se justifica por possibilitar a compreensão dos controles citados nas políticas de segurança da informação das organizações selecionadas com o objetivo de identificar, descrever e classificar tais controles segundo o referencial teórico de suporte apresentado anteriormente, desenvolvido com base na pesquisa bibliográfica realizada, a qual permitiu verificar a amplitude e profundidade do conhecimento existente sobre o tema em questão.

O método de estudo de caso é aplicável, pois possibilita o entendimento do contexto organizacional onde a política de segurança da informação está implantada.

O estudo de caso se caracteriza pela capacidade de lidar com uma completa variedade de evidências, não se restringindo apenas à análise de documentos, mas também entrevistas, observações, etc. e pode ser restrito a uma ou a várias unidades, caracterizando-o como único ou múltiplo. O estudo de casos múltiplos tem provas mais convincentes, sendo visto como mais robusto. No entanto, a lógica de sua utilização diz respeito à replicação e não amostragem, ou seja, não permite generalização dos resultados para a toda a população, mas sim a possibilidade de previsão de resultados similares ou a de produzir resultados contrários por razões previsíveis, de modo semelhante ao método de experimentos (YIN, 2005).

Para Boyd Junior e Westfall (1987), o estudo de casos múltiplos possibilita a identificação de três situações: a existência de fatores comuns a todos os casos analisados, aqueles não comuns a todos, mas apenas a alguns casos e aqueles existentes em apenas um caso.

Neste trabalho foi utilizado o estudo de casos múltiplos com dez organizações brasileiras selecionadas de forma intencional, portanto não probabilística. Procurou-se selecionar organizações representativas de segmentos de negócio variados, com políticas de segurança da informação implantadas. Foram analisadas políticas de organizações representantes de nove segmentos, assim distribuídas: financeiro: 2, ensino: 1, varejo: 1, construção: 1, transporte de passageiros: 1, seguros e finanças: 1, serviços de informação (tv, internet e telefonia): 1, serviços de TI/telecom: 1 e bolsa de valores: 1. Os trabalhos de campo foram desenvolvidos durante o primeiro semestre de 2011.

O convite às organizações para participar da pesquisa foi decorrente da condição de possuírem maturidade na política considerada, de pelo menos três anos de uso. Todas as participantes manifestaram o desejo do compromisso de não divulgação do nome da organização.

Foram realizadas entrevistas com o profissional que tem a responsabilidade pela segurança da informação de cada organização. As informações coletadas nas entrevistas e observações tiveram como finalidade identificar características do ambiente onde a política foi elaborada e publicada e ajudaram a conhecer melhor cada organização por meio de perguntas abertas.

O método de análise de conteúdo (BARDIN, 2011) foi utilizado para inspeção da política de segurança da informação – fonte original de

primeira mão – de cada organização. Além de oferecer uma técnica para análise documental, ou seja, passar de um documento primário (política de segurança da informação) para um documento secundário (indexação de controles chaves citados), esta metodologia também possibilita deduções lógicas e justificadas referentes à mensagem do documento original e seu contexto. A metodologia esta estruturada em três fases e foi aplicada da seguinte forma:

a)Fase 1 - Pré-análise: composta pela escolha dos documentos, formulação dos objetivos e a elaboração de indicadores que fundamentem a interpretação final. Neste trabalho os documentos se constituíram nas políticas de segurança da informação das organizações, com o objetivo de identificar os respectivos controles citados com o apoio do esquema da ontologia de segurança da informação apresentado na Figura 1 e da norma ABNT NBR ISO/IEC 27002:2005 (ABNT, 2005). A referida norma foi considerada como principal fonte de controles de segurança da informação tendo em vista a constatação da revisão teórica apresentada anteriormente, complementada com a abordagem da ontologia para ajudar as interpretações.

b)Fase 2 - Exploração do material: consiste em operações de decodificação, decomposição ou enumeração em função das definições elaboradas na Fase 1. No caso deste trabalho, as políticas de segurança da informação das organizações foram inspecionadas manualmente, sem o auxílio de software, de forma analítica e exaustiva visando identificar a presença dos controles, associando-os aos apresentados na norma ABNT NBR ISO/IEC 27002:2005 (ABNT, 2005), gerando um relatório para cada caso estudado.

c)Fase 3 - Tratamento dos dados obtidos e interpretação: consiste na avaliação dos resultados obtidos na Fase 2 quando confrontando com as definições da Fase 1, de maneira a se tornarem significativos. Neste trabalho procurou-se identificar os controles comuns, ou seja, aqueles presentes na totalidade das políticas de segurança da informação das organizações participantes. A análise final foi realizada por meio da técnica de síntese de casos cruzados (Yin, 2005), onde após a análise individual dos casos, foram relacionadas as evidências das citações encontradas entre eles a fim de verificar a frequência dos controles dos diversos casos.

4 Resultados e discussão

A seguir são analisados e discutidos os dados levantados, tanto do ambiente das organizações com relação à política de segurança da informação como dos controles citados nas mesmas.

4.1 Análise do ambiente das organizações com relação à política de segurança da informação

Os profissionais entrevistados de todas as organizações possuem mais de cinco anos de experiência profissional em atividades de segurança da informação, evidenciando com isto a maturidade profissional das informações coletadas nas entrevistas. Em relação à formação formal de especialização na área de segurança da informação, 50% dos profissionais possuem certificações internacionais.

Todas as organizações pesquisadas possuem políticas há vários anos, sendo que 90% há mais de cinco anos e apenas 10% há menos de cinco anos. Porém se considerarmos o menor tempo, todas as organizações possuem políticas há mais de quatro anos. O fato da existência de políticas há vários anos é importante por indicar que as organizações possuem políticas de segurança da informação maduras e consolidadas, com controles úteis para as mesmas.

Um dado que reforça a maturidade das políticas é o fato de que em todas as organizações as políticas de segurança da informação foram assinadas por um nível hierárquico de diretoria, sendo 30% aprovadas por um comitê executivo e 30% assinadas pelo presidente ou vice-presidente. Este nível de aprovação indica que o assunto segurança da informação, representado pela sua diretriz – a política de segurança da informação – é formalmente tratado em grau estratégico da organização.

Outro fator importante é que 70% das organizações possuem uma área específica para a gestão da segurança da informação. Nesta pesquisa não foi investigado o grau hierárquico desta unidade organizacional, porém a existência de uma área com a responsabilidade explícita de tratar a segurança da informação indica a consciência da criticidade da proteção da informação para que a organização atinja os seus objetivos.

Todas as políticas analisadas indicam, de maneira direta ou indireta, que a proteção da informação deve contemplar a informação tanto dentro como fora do ambiente de tecnologia da informação. Um fato importante identificado em todas as políticas analisadas é o escopo considerado para os tipos de usuários: funcionários, estagiários, fornecedores e prestadores de serviço, denotando a abrangência da responsabilidade para com a informação da organização, envolvendo tanto pessoas internas como externas à mesma.

A quantidade de usuários afetados pela política de segurança da informação de cada organização confirma a sua representatividade:

a)80% das organizações possuem políticas que afetam mais de 1.000 usuários;

b)10% afetam cerca de 24.000 usuários;

c)10% afetam cerca de 35.000 usuários.

A exigência de que os fornecedores de produtos e prestadores de serviços devem possuir uma política de segurança da informação própria para poderem ser contratados foi constatada em apenas 20% das organizações. Outras 20% indicaram que consideram a exigência apenas para fornecedores críticos. Este fato denota que o tema política de segurança da informação ainda não está consolidado como um elemento crítico para que uma organização preste serviço para outra organização.

Uma resposta comum em todas as organizações pesquisadas foi o fato de tomarem como base a norma ABNT NBR ISO/IEC 27002:2005 (ABNT, 2005) para elaboração da sua política, comprovando o referencial teórico pesquisado neste trabalho. Outro ponto comum diz respeito à total compatibilidade do esquema da ontologia de segurança da informação apresentado na Figura 1 à realidade das organizações, facilitando a homogeneidade dos estudos desenvolvidos.

4.2 Análise dos controles citados nas políticas de segurança da informação

O método de análise de conteúdo utilizado na inspeção de cada uma das dez normas avaliadas possibilitou identificar um conjunto de controles citados em cada uma delas. Tais controles foram individualmente associados, sem exceção, com os controles da mesma versão da norma ABNT NBR ISO/IEC 27002:2005 (ABNT, 2005) utilizada pelas organizações para elaboração das políticas. Apesar de ter sido lançada uma nova versão da norma (ABNT, 2013) após o trabalho de campo ter sido concluído, verificou-se que os resultados obtidos não ficaram comprometidos com a nova versão.

Esta associação permitiu a compatibilidade e comparabilidade dos controles para fins de interpretação e avaliação dos resultados.

A frequência da citação de um controle nas normas analisadas foi estruturada em quatro faixas: 100%, 90%, 80% e 70%, sendo desconsideradas as demais faixas inferiores. Assim, foram identificados 40 controles recorrentes, distribuídos como segue:

a)12 controles citados por 100% das políticas;

b)15 controles citados por 90% das políticas;

c)16 controles citados por 80% das políticas;

d)40 controles citados por 70% das políticas.

A associação dos controles citados nas políticas com aqueles da norma, também permitiu a vinculação dos mesmos a uma das 39 categorias principais de segurança da informação com as quais a norma está estruturada. Foram vinculas aos controles recorrentes 19 categorias, distribuídas como segue:

a)6 categorias associadas a 100% das políticas;

b)8 categorias associadas a 90% das políticas;

c)9 categorias associadas a 80% das políticas;

d)19 categorias associadas a 70% das políticas.

Visando tornar concisas as discussões sobre os resultados alcançados com a identificação dos controles recorrentes, optou-se por apresentar os objetivos das categorias de segurança a eles associada, ao invés da descrição analítica de cada um.

Foram citados por 100% das políticas os controles apresentados no Quadro 1, com as respectivas categorias.

Quadro 1 - Controles e respectivas categorias citados em 100% das políticas

Controle	Categoria
Política de controle de acesso	Requisitos de negócio para controle de acesso
Registro de usuário	Gerenciamento de acesso do usuário
Gerenciamento de privilégios	
Gerenciamento de senha do usuário	
Uso de senhas	Responsabilidades dos usuários
Autenticação para conexão externa do usuário	Controle de acesso à rede
Procedimentos seguros de entrada nos sistema (*log on*)	Controle de acesso ao sistema operacional
Identificação e autenticação do usuário	
Sistema de gerenciamento de senha	
Limite de tempo de sessão	
Restrição de acesso à informação	
Uso aceitável dos ativos	Responsabilidade pelos ativos

Fonte: Elaborado pelos autores (2011).

Os controles integrantes das categorias: Requisitos de negócio para controle de acesso, Gerenciamento de acesso do usuário, Responsabilidades dos usuários, Controle de acesso à rede e Controle de acesso ao sistema operacional estão diretamente associados com o conceito de identidade do usuário. A gestão de identidade pode ser definida como a combinação de sistemas técnicos, regras e procedimentos que definem a posse, utilização, e segurança de uma identidade. Seu objetivo primário é estabelecer a confiança na associação de atributos a uma identidade digital e conectar esta identidade com uma entidade individual (NATIONAL SCIENCE AND TECHNOLOGY COUNCIL – NSTC, 2008).

A gestão de identidade é complementada pela gestão de acesso que tem como propósito assegurar que a verificação da identidade seja realizada quando um indivíduo tenta acessar os dados, sistemas de informação ou instalações físicas. Está estruturada em três áreas principais: (a) Gestão de recursos: envolve estabelecer e manter os dados (regras de acesso, requisitos de credenciais) para uma determinada informação ou recurso que possa ser acessado; (b) Gestão de privilégios: envolve a gestão de políticas e processos que definem como são fornecidos os direitos de acesso das entidades aos sistemas de informação, engloba a gestão de todos os dados que constituem os privilégios de acesso e atributos, armazenamento, organização e acesso a informação nos diretórios; e (c) Gestão de políticas: envolve os processos que estabelecem e mantêm as políticas de controle de acesso que são incorporadas nas lógicas e regras de negócio e gerencia o que é permitido ou não de ser acessado em uma determinada transação (FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT - FICAM, 2011).

Os controles da categoria **Responsabilidade pelos ativos** tem por objetivo alcançar e manter a proteção adequada dos ativos da organização. Ainda com relação à responsabilidade pelos ativos, em determinadas políticas foram detalhados o tipo, modelo e até o fabricante do ativo (tecnologia), particularizando a política o que poderá exigir sua constante atualização na medida em que novas tecnologias vierem a ser utilizadas.

Foram citados por 90% das políticas todos os controles apresentados no Quadro 1 e, adicionalmente, os controles apresentados no Quadro 2, com as respectivas categorias.

Quadro 2 - Controles e respectivas categorias adicionalmente citados em 90% das políticas

Controle	Categoria
Recomendações para classificação	Classificação da informação
Tratamento da informação	
Cópias de segurança da informação	Cópias de segurança

Fonte: Elaborado pelos autores (2011).

Historicamente, a **Classificação da Informação** foi a principal preocupação da segurança da informação a ser tratada, muito antes do advento do primeiro computador. A informação a ser classificada pode se encontrar em diferentes tipos de mídia, tais como: bases de dados, documentos eletrônicos, cartões de memória, e-mail, documentos em papel, etc.

A norma ABNT NBR ISO/IEC 27001:2006 (ABNT, 2006) não prescreve os níveis de classificação, ficando esta responsabilidade para a organização, em função do tipo de legislação existente em cada país e do tipo de indústria à qual a organização pertence. Normalmente, o "proprietário" da informação tem a incumbência de classifica-la levando em consideração os resultados de uma análise de riscos: quanto maior o risco, maior deve ser o nível da classificação de confidencialidade. De uma forma geral, nas políticas analisadas, foram identificados

os seguintes níveis de classificação da informação quanto à confidencialidade: Confidencial (mais alto nível), Restrita (nível médio), Uso interno (mais baixo nível) e Pública (nenhum nível associado).

Os controles da categoria **Cópias de segurança** visam manter a integridade e disponibilidade da informação. Normalmente a cópia de segurança (também conhecida como *backup* ou cópia de reserva) é uma tarefa de responsabilidade do administrador do sistema. Simplificadamente, trata-se de uma cópia da informação contida em um banco de dados local ou remoto, sendo, na prática, uma réplica dos dados originais atuais, guardados em um outro local seguro. No caso de falha séria no sistema, somente estas podem restaurar os arquivos de volta. Há na literatura vários tipos de *backup*: normal, diferencial, incremental, etc., cada qual com determinada característica para atender determinada necessidade. Vale salientar que o controle de continuidade de negócio, que necessita de cópias de segurança, foi citado por apenas 50% das políticas.

Foram citados por 80% das políticas todos os controles apresentados nos Quadros 1, 2 e, adicionalmente, o controle apresentado no Quadro 3, com a respectiva categoria.

Quadro 3 - Controle e respectiva categoria adicionalmente citado em 80% das políticas

Controle	Categoria
Monitoramento de uso do sistema	Monitoramento

Fonte: Elaborado pelos autores (2011).

Os controles da categoria de **Monitoramento** visam detectar atividades não autorizadas de processamento da informação. No Brasil não existe legislação sobre o assunto, porém a jurisprudência possibilita que a organização monitore os acessos de seus usuários no seu ambiente, desde que exista uma formalização indicando este fato (política de segurança da informação, por exemplo) e que o usuário tenha conhecimento explícito desta regra.

Foram citados por 70% das políticas todos os controles apresentados nos Quadros 1, 2, 3 e, adicionalmente, os controles apresentados no Quadro 4, os quais foram associados às respectivas categorias.

Quadro 4 - Controles e respectivas categorias adicionalmente citados em 70% das políticas

Controle	Categoria
Documento da política de segurança da informação	Política de segurança da informação
Análise crítica da política de segurança da informação	
Conscientização, educação e treinamento em segurança da informação	Durante a contratação (Segurança em recursos humanos)

Controle	Categoria
Processo disciplinar	
Encerramento de atividades	Encerramento ou mudança da contratação (Segurança em recursos humanos)
Devolução de ativos	
Retirada de direitos de acesso	
Trabalho remoto	Computação móvel e trabalho remoto
Análise e especificação dos requisitos de segurança	Requisitos de segurança de sistemas de informação
Validação dos dados de entrada	Processamento correto nas aplicações
Controle do processamento interno	
Integridade de mensagens	
Validação de dados de saída	
Política para o uso de controles criptográficos	Controles criptográficos
Gerenciamento de chaves	
Controle de software operacional	Segurança dos arquivos do sistema
Proteção dos dados para teste de sistema	
Controle de acesso ao código-fonte de programa	
Procedimentos para controle de mudanças	Segurança em processos de desenvolvimento e de suporte
Análise crítica técnica das aplicações após mudanças no sistema operacional	
Restrições sobre mudanças em pacotes de software	
Vazamento de informações	
Desenvolvimento terceirizado de software	
Controle de vulnerabilidades técnicas	Gestão de vulnerabilidades técnicas

Fonte: Elaborado pelos autores (2011).

Os controles da categoria de **Política de segurança da informação** visam promover uma orientação e apoio da direção da organização para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes. Os controles de segurança em recursos humanos, das categorias **Durante a contratação** e **Encerramento ou mudança da contratação** asseguram que os funcionários, fornecedores e terceiros estão conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, e estão preparados para apoiar a política de segurança da informação durante os seus trabalhos normais, ou quando deixarem a organização ou mudarem de trabalho, visando reduzir o risco de erro/comportamento humano. Algumas políticas analisadas deixaram explicito que o não cumprimento das regras definidas é passível de punição administrativa, contratual, civil e até penal. Os controles da categoria **Computação móvel e trabalho remoto** possibilitam o adequado nível de segurança da informação quando se utilizam a computação móvel e recursos de trabalho remoto. Estes controles devem ser cada vez mais referenciados na medida em que as organizações precisam que seus usuários acessem remotamente as suas informações. Os controles da categoria **Requisitos de segurança de sistemas de informação** visam assegurar que as necessidades de segurança foram devidamente consideradas e são parte integrante dos sistemas. Os

controles da categoria **Processamento correto nas aplicações** previnem a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações durante o ciclo operacional do sistema. Os controles da categoria **Controles criptográficos** protegem a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos. Os controles da categoria **Segurança dos arquivos do sistema** visam proteger os arquivos que podem, involuntariamente, dar permissões excessivas a usuários ou fornecer acesso a invasores. Os controles da categoria **Segurança em processos de desenvolvimento e de suporte** tratam do gerenciamento proativo de mudanças tanto durante o desenvolvimento como na operação do sistema e visam assegurar que tais mudanças sejam consistentes e que os envolvidos sejam informados. Os controles da categoria **Gestão de vulnerabilidades técnicas** visam prevenir e tratar as falhas em um sistema que permitem utilizá-lo de forma indevida, tais como: configurações inseguras, quebra de autenticidade, *SQL Injection*, etc.

5 Conclusões

Ao final dos trabalhos pode-se considerar que os objetivos da pesquisa foram satisfatoriamente alcançados. Os levantamentos de campo por meio do estudo de casos, apoiado pela pesquisa bibliográfica, possibilitaram uma coleta de informações detalhada e aprofundada, permitindo a compilação dos controles das políticas de segurança da informação de modo sistematizado. Os resultados obtidos contribuem de modo prático para o mercado e para a produção acadêmica, uma vez que tratou de um assunto pouco explorado.

Foram identificados 40 controles citados de forma recorrente em políticas, os quais também foram associados à principal referência da literatura da área, descritos e agrupados em quatro extratos de frequência: 12 controles citados por 100% das políticas, 15 por 90%, 16 por 80% e 40 por 70%. Sem dispensar a análise de riscos e os requisitos de segurança da informação próprios de cada organização, tais controles podem desempenhar o papel de subsidiar e nortear o gestor da informação acerca da definição de um conjunto de controles comuns que devem ser considerados, além de facilitar a avaliação de uma determinada política em relação às práticas de mercado.

Entretanto, não há dúvida de que o resultado alcançado não conta com base empírica suficiente para ser representativo e definitivo para a definição dos controles que, minimamente, devem ser considerados em uma política de segurança da informação. Para tanto, ainda serão necessários numerosos estudos de casos semelhantes e até mesmo comprovações estatísticas.

Como reflexão final, pode-se citar como oportunidades de trabalhos futuros: (i) análise aprofundada deste tema em busca de comprovações estatísticas; e (ii) análise das políticas de segurança de informação das

organizações de segmentos de mercado distintos em busca de conhecer se há ou não controles comuns, particulares de organizações que atuam em cada tipo de segmento.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. NBR ISO/IEC 17799:2001: Tecnologia da Informação – *Código de prática para gestão da segurança da informação*. Ri de Janeiro, 2001.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS*. NBR ISO/IEC 27001: 2006 Tecnologia da informação - Técnicas de segurança - Sistema de Gestão de segurança da informação - Requisitos*. Rio de Janeiro, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27002:2005: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação*. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27002:2013: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação.* Rio de Janeiro, 2013.

ALBUQUERQUE JUNIOR, A. E.; SANTOS, E. M. Produção científica sobre segurança da informação em eventos científicos brasileiros. *In:* INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS AND TECHNOLOGY MANAGEMENT, 2014, São Paulo. *Proceedings of…* São Paulo: CONTECSI, 2014. p. 2085-2103. CD-Rom.

ALBUQUERQUE JUNIOR, A. E.; SANTOS, E. M; GONZALEZ JUNIOR, I. P. Scientific production on information security from the social perspective on portuguese speaking scientific journals between 2004 and 2013. *Business and Management Review*, v. 4, n. 7, p. 54-66, 2015.

ALMEIDA, M. C. B. *Planejamento de bibliotecas e serviços de informação*. Brasília: Briquet de Lemos, 2000.

ALMEIDA, M. B. Uma abordagem integrada sobre ontologias: Ciência da Informação, Ciência da Computação e Filosofia. *Perspectivas em Ciência da Informação*, v. 19, n. 3, p. 242-258, 2014.

ALMEIDA, M. B.; SOUZA, R. R.; CARDOSO, K. Uma proposta de ontologia de domínio para segurança da informação em organizações*. Informação e Sociedade: Estudos*, v. 20, n. 1, p. 155-168, 2010.

BARDIN, L. *Análise de conteúdo*. São Paulo: Edições 70, 2011.

BOYD JUNIOR, H.W.; WESTFALL, R. *Pesquisa mercadológica:* textos e casos. 7. ed. Rio de Janeiro: Fundação Getúlio Vargas, 1987.

BRITISH STANDARD INSTITUTION – BSI. *BS 7799-1:1995 - Information security management*. Code of practice for information security management systems. Inglaterra: British Standards Institution, 1995.

~~BSI~~ BRITISH STANDARD INSTITUTION – BSI. *BS 7799-1:1999 - Information security management. Code of practice for information security management systems*. Inglaterra: British Standards Institution, 1999.

FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (FICAM). *Roadmap and Implementation Guidance*. Version 2.0. USA, 2011.

GIL, A. C. *Métodos e técnicas em pesquisa social*. 5. ed. São Paulo: Atlas, 1999.

GILCHRIST, A. Thesauri, taxonomies and ontologies: an etymological note. *Journal of Documentation,* v. 59, n.1, p. 7-18, 2003.

GORDON, L. A.; LOEB, M. P. The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, v. 5, n, 4, p. 438-457, 2002.

GUALBERTO, E. S. *et al.* Proposição de uma ontologia de apoio à gestão de riscos de segurança da informação. *Revista Brasileira de Sistemas de Informação*, v. 6, n. 1, p. 30-43, 2013.

GUARINO, N. Formal ontology and information systems. *In:* FORMAL ONTOLOGY IN INFORMATION SYSTEMS, 1998, Italy. *Proceedings…* Italy, 1998. p. 3-15.

IMONIANA, J.O. Validity of information security policy models. *Transinformação*, v. 16, n. 3, p. 263-274, 2004.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. *ISO/IEC 17799:2000 Information technology* - Code of practice for information security management. Geneva: ISO/IEC, 2000.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. *ISO/IEC 27001:2006 Information technology - Security techniques - Information security management systems – Requirements*. Geneva: ISO/IEC, 2006.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. *ISO/IEC 27002:2005 Information technology* - Code of practice for information security management. Geneva: ISO/IEC, 2005.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. *ISO/IEC 27002:2013 Information technology* - Code of practice for information security management. Geneva: ISO/IEC, 2013.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO Survey 2014.* 2014. Disponível em: <http://www.iso.org/iso/iso-survey>. Acesso em: 2 fev. 2016.

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL. Subcommittee on Biometrics and Identity Management. *Identity Management Task Force Report*. USA, 2008.

POSTHUMUS, S.; VON SOLMS, R. A framework for the Governance of Information Security. *Computers & Security*, v. 23, issue 8, p. 638-646, 2004.

PRICEWATERHOUSECOOPERS. *Pesquisa global de segurança da informação 2014*. Disponível em: <https://www.pwc.com.br/pt/publicacoes/servicos/assets/consultoria-negocios/pesq-seg-info-2014.pdf>. Acesso em: 2 fev. 2016.

RICHARDSON, R. J. *Pesquisa social:* métodos e técnicas. 3. ed. São Paulo: Atlas, 1999.

SCHIAVONE, S.; GARG, L.; SUMMERS, K. Ontology of information security in enterprises. *The Electronic Journal Information Systems Evaluation*, v. 17, n. 1, p. 71-87, 2014.

SÊMOLA, M. *Gestão da Segurança da Informação:* uma visão executiva. Rio de Janeiro: Campus, 2003.

SIPONEN, M. T. A paradigmatic analysis of conventional approaches for developing and managing secure IS. *In:* INTERNATIONAL CONFERENCE ON INFORMATION SECURITY, 16., 2001, MA, USA. *Proceedings of…* Trusted information: The new decade challenge. MA: Kluwer Academic Publishers Norwell, 2001. p. 437-452

SMITH, B. *Ontology and Informations Systems*. 2003. Disponível em: <http://www.ontology.buffalo.edu/ontology>. Acesso em: 2 fev. 2016.

SOWA, J. F. *Ontology, metadata, and semiotics*. 2000. Disponível em: <http://users.bestweb.net/~sowa/peirce/ontometa.htm>. Acesso em: 2 fev. 2016.

VICKERY, B.C. Ontologies. *Journal of Information Science*, London, v. 23, n. 4, p. 227-286, 1997.

YIN, R.K. *Estudo de caso:* planejamento e métodos. 3. ed. Porto Alegre: Bookman, 2005.

WILLIAMS, P. Information security governance. *Information Security Technical Report*, v. 6, n. 3, p. 60-70, 2001.