RECIIS – R. Eletr. de Com. Inf. Inov. Saúde. Rio de Janeiro, v.7, n.2, Jun., 2013
[www.reciis.icict.fiocruz.br] e-ISSN 1981-6278

* Artigo Original

A percepção da importância de Controles de segurança da informação em hospitais públicos brasileiros

The perceived importance of information security controls in Brazilian public hospitals

Antonio Eduardo de Albuquerque-Junior

Graduação em Processamento de dados, especialização em Redes de computadores, Mestrado em Administração. Doutorando em Administração pela Universidade Federal da Bahia. É Tecnologista da Fundação Oswaldo Cruz.

aealbuquerque@bahia.fiocruz.br

Ernani Marques dos Santos

Graduação em Administração de Empresas e em Processamento de dados, mestrado e doutorado em Administração e Pós Doutorado em Administração na Universidade de São Paulo. É Professor Adjunto da Escola de Administração da UFBA.

emarques@ufba.br

DOI: 10.3395/reciis.v7i2.688pt

Resumo

A dependência da infraestrutura de Tecnologia da Informação (TI) e a necessidade de proteger as informações, tanto por força de normas legais quanto por sua importância, exigem que hospitais públicos adotem controles de segurança da informação apropriados para as atividades que desenvolvem, pois lidam com informações sensíveis importantes tanto para seu funcionamento quanto para garantia da privacidade dos pacientes. A norma NBR ISO/IEC 27002:2005 propõe 133 controles que visam proteger as informações em diferentes organizações, mas há a necessidade de identificar quais desses controles são realmente importantes para o tipo de atividade e para as informações com que lidam os hospitais públicos. Este trabalho teve o objetivo de identificar a percepção da importância de controles de segurança da informação para gestores e profissionais das áreas de TI e segurança da informação de hospitais públicos tendo em vista as atividades desenvolvidas nessas instituições.

Palavras-chave: Tecnologia da Informação; Informática em Saúde; Segurança da Informação; Gestão hospitalar; Setor público.

Abstract

Public hospitals must adopt information security for their activities because they are dependent on the information technology (IT) infrastructure and must protect information due to legal

regulations and the importance of such information. This is necessary because public hospitals manage sensitive information, which is important for their operation, and patient privacy should be ensured. The NBR ISO/IEC 27002:2005 standard proposes 133 controls to protect information for different organizations; but we must identify the controls that are important for public hospital activities and information. This study was aimed at discerning the perceived importance of information security controls for public hospital managers as well as IT and information security professionals given such institutions' activities.

Key words: Information Technology; Health Informatics; Information Security; Hospital management; Public sector.

Introdução

Sendo a informação insumo importante para a tomada de decisões, o acesso e a divulgação indevidos podem provocar danos graves para a organização. Os avanços nas tecnologias da informação (TI) e nos meios de comunicação aumentam o risco de divulgação e acesso indevidos (FACHINI, 2009) e a relação que a informação tem com diferentes ativos utilizados no seu processamento, armazenamento e transmissão leva à necessidade de controles de segurança da informação para proteger tanto a informação quanto essa infraestrutura (SÊMOLA, 2003; NOBRE; RAMOS; NASCIMENTO, 2010). A crescente dependência que as organizações têm da TI expõem informações, infraestrutura, transações e pessoas a ameaças relacionadas às facilidades de acesso (MARCIANO, 2006). Sendo um ativo essencial, a informação precisa ser protegida de forma adequada e, para isso, a Associação Brasileira de Normas Técnicas -ABNT (2005) apresenta a norma NBR ISO/IEC 27002:2005, um conjunto de controles de segurança da informação que podem ser adotados no todo ou em parte por diferentes organizações.

As instituições de saúde utilizam intensamente informações sensíveis em grande quantidade, pondo os registros dos pacientes – muitas vezes eletrônicos - como a unidade central de informações, levando à utilização massiva de computadores. Isso tem levado a um processo de integração e compartilhamento de informações sobre pacientes, trazendo para essas instituições novas demandas para a segurança da informação (AHLFELDT, 2005). A TI atualmente permeia todas as atividades de um hospital e que isso tem levado à evolução dos registros médicos para registros eletrônicos de saúde (KOBAYASHI; FURUIE, 2007), e com o desenvolvimento da TI, das telecomunicações e da medicina, está havendo uma transformação dos serviços de saúde (JANCZEWSKI; SHI, 2002), um ambiente em que há muita troca de informações, tanto dentro da instituição quanto com outras organizações (KWAK, 2005).

As discussões sobre segurança da informação em instituições de saúde levam a questões éticas sobre proteção à privacidade dos pacientes (RAGHUPATHI; TAN, 2002), em um contexto em que se procura prestar o melhor atendimento, com informações corretas e no momento certo, e diante da possibilidade de divulgação não autorizada de informações (AHLFELDT, 2005). Como agravante, há a possibilidade de uso indevido de sistemas de informação em instituições de saúde, pondo em risco informações de pacientes, desencorajando o uso da TI e prejudicando o compartilhamento de informações nessas instituições, o que pode comprometer o tratamento e a pesquisa médica (KOBAYASHI; FURUIE, 2007).

Ao tratar de instituições públicas de saúde, acrescentam-se às discussões as obrigações criadas por órgãos que regulam as atividades de organizações públicas. Segundo Cepik, Canabarro e Possamai (2010), a segurança da informação em organizações públicas federais

foi objeto de auditoria do Tribunal de Contas da União (TCU) em 2007 e levou o Governo Federal a exigir a adoção de boas práticas de segurança da informação. Para Britto (2011), nas organizações públicas, parte das informações pode estar vulnerável, o que pode provocar a interrupção de serviços e funções essenciais e a perda de dados, além de possibilitar fraudes, o que pode prejudicar a sociedade como um todo. Dessa forma, hospitais públicos são obrigados a proteger as informações com que lidam tanto por serem informações de pacientes quanto por integrarem a administração pública.

Parte das leis e regulamentos que orientam a proteção das informações em hospitais públicos, na realidade, é voltada para organizações públicas em geral ou para toda a sociedade: a Lei nº 8.159/1991 obriga a proteção de documentos de apoio ao desenvolvimento científico e elementos de prova e informação; a Lei nº 9.983/2000 tipifica como crime a violação indevida e proposital da confidencialidade e integridade dos dados armazenados em sistemas computacionais; a Lei de Acesso à Informação (Lei nº 12.527/2011) garante o acesso às informações públicas, mas garante também o respeito à intimidade, à vida privada e a proteção de informações que possam pôr em risco a vida, a segurança ou a saúde da população; e a Constituição Federal do Brasil, de 1988, garante, através do seu Art. 5º, inciso X, o direito à privacidade.

Outros instrumentos legais são aplicáveis diretamente às instituições de saúde: a própria Constituição Federal, no Art. 5º, inciso XIV, garante o sigilo profissional entre médico e paciente; o Código Penal Brasileiro (Decreto-Lei nº 2.848/1940) complementa essa garantia tipificando como crime a violação de informação cujo conhecimento se deu através do exercício profissional; o Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) estabelece que instituições de saúde mantenham por 18 anos a identificação de recém-nascidos e de suas mães; e a Lei nº 9.434/1997 obriga as instituições de saúde a manterem por pelo menos cinco anos os prontuários médicos em algumas situações específicas.

Além dessas leis, algumas normas do Conselho Federal de Medicina regulamentam a segurança das informações em hospitais: o Código de Ética Médica (Resolução CFM nº 1.931/2009) garante que os prontuários dos pacientes sejam manuseados apenas por pessoas sujeitas ao sigilo profissional, põe os prontuários sob responsabilidade do médico ou da instituição de saúde, garante o acesso do paciente ao seu prontuário, obriga que este seja legível e exige autorização por escrito do paciente para realização de cópias. Já a Resolução CFM nº 1.331/89 obriga que os prontuários médicos sejam mantidos permanentemente pelos médicos ou instituições de saúde.

Está clara, portanto, a necessidade de promover segurança da informação nessas instituições, de forma que se faz necessário ampliar os conhecimentos sobre o tema. Assim sendo, este trabalho é resultado de uma pesquisa exploratória que teve como objetivo identificar a percepção funcionários de hospitais públicos brasileiros a respeito da importância dos controles de segurança da informação presentes na norma NBR ISO/IEC 27002:2005, proposta feita por Albuquerque Junior e Santos (2012), que realizaram pesquisa semelhante em hospitais privados.

O trabalho teve também o objetivo de propor uma metodologia que pode ser adaptada para avaliar a implementação de controles de segurança da informação em hospitais públicos, e seus resultados abrem caminho para novas pesquisas sobre segurança da informação em instituições de saúde, como a adoção dos controles e práticas e a efetividade das práticas adotadas, além das implicações dessas práticas nas atividades desenvolvidas.

Fundamentação Teórica

Ao tratar de segurança da informação, é preciso conceituar o termo conforme autores que escrevem sobre o tema. Beal (2005) a define como a proteção da informação contra ameaças à sua integridade, disponibilidade e confidencialidade. Donner e Oliveira (2008) definem como proteção da informação contra ameaças visando assegurar sua integridade, disponibilidade e confidencialidade. Já a ABNT (2005) apresenta dois conceitos: preservação da confidencialidade, da integridade e da disponibilidade da informação; e proteção da informação contra ameaças visando garantir a continuidade do negócio, minimizar o risco e maximizar o retorno sobre os investimentos e as oportunidades de negócio.

Embora pareçam contraditórias, estas duas definições da ABNT (2005) se complementam e, junto com as outras apresentadas, indicam três componentes principais da segurança da informação: a integridade, que visa garantir a exatidão da informação por modificações ou remoções feitas sem autorização; a disponibilidade, que visa garantir o acesso à informação por quem é autorizado a fazê-lo; e a confidencialidade, que procura garantir que apenas pessoas autorizadas tenham acesso (SILVA NETTO; SILVEIRA, 2007). Assim, a finalidade da segurança da informação é a proteção das informações contra acessos não autorizados, alterações indevidas ou indisponibilidade (SÊMOLA, 2003). Essa proteção pode ser obtida pela definição e implementação de controles adequados, que precisam ser monitorados, analisados de forma crítica e melhorados para atender aos objetivos do negócio e de segurança da informação (ASSOCIAÇÃO..., 2005).

Apesar da utilização de computadores para armazenar grande parte dos dados importantes, da dependência que as organizações têm da TI (SILVA NETTO; SILVEIRA, 2007) e da necessidade de proteger os equipamentos que processam as informações – uma decorrência dessa dependência (MARCIANO, 2006) -, a tecnologia por si só não é suficiente para garantir a proteção das informações (MARCIANO, 2006; SILVA; STEIN, 2007). Para isso, os controles devem cobrir segurança física e lógica, orientados por uma Política de Segurança da Informação (MOURA; GASPARY, 2008), documento que pode ser definido dentro de um contexto técnico, como regras de controle aos componentes de um sistema computadorizado, ou dentro de um contexto de gestão, como o compromisso, o apoio e a orientação da gestão para segurança da informação (LOPES, 2012). Dentro do contexto de gestão, a Política deve abranger a infraestrutura utilizada, os processos, os sistemas de informação e os serviços relacionados às informações, e os controles devem estar de acordo com o valor que a informação tem para a organização e os possíveis efeitos da sua perda, acesso indevido ou indisponibilidade (SILVA; STEIN, 2007).

Segundo Marciano (2006), a Política de Segurança da Informação aborda recursos computacionais, recursos humanos e a estrutura organizacional necessária para promover a segurança da informação, o que concorda com Albrechtsen (2008), que afirma que a segurança da informação não é apenas uma questão tecnológica. Silva e Stein (2007) identificam duas faces diferentes e possivelmente conflitantes para a segurança da informação: a tecnologia e os seres humanos, enquanto Sêmola (2003) afirma que a gestão da segurança da informação deve considerar aspectos tecnológicos, físicos e humanos. Já Albuquerque Junior e Santos (2012) dizem que a proteção da informação envolve aspectos físicos, lógicos e humanos, enquanto Silva Netto e Silveira (2007) propõem a organização dos controles de segurança da informação da norma NBR ISO/IEC 27002:2005 nas dimensões física, lógica e humana, conforme Quadro 1.

Por ter o objetivo principal de proteger a informação, a norma NBR ISO/IEC 27002:2005 oferece um conjunto de controles que podem ser utilizados para atender a essa obrigação. Organizada em 11 seções de controles e 39 categorias de controles, a norma contém 133

controles que direcionam e dão os princípios de segurança da informação que podem ser adotados por qualquer organização (FERNANDES; ABREU, 2008). Embora tenha essa quantidade de controles, nem sempre a adoção de todos eles é necessária, sendo possível selecionar parte deles, conforme os requisitos de cada organização.

Para Albuquerque Junior e Santos (2011), antes de adotar os controles da norma, é preciso identificar quais são necessários, considerando a realidade e buscando mitigar os riscos específicos da organização. Segundo Albuquerque Junior e Santos (2012), como a norma tem características mais voltadas para a gestão da segurança da informação, a realização de um diagnóstico sobre segurança da informação não deve envolver apenas profissionais de TI e segurança da informação, mas também os gestores da organização.

A seção seguinte trata da metodologia utilizada, caracterizando a pesquisa, mostrando como foi elaborado e organizado o instrumento de coleta, como os possíveis respondentes foram identificados e convidados a responder os questionários e as quantidades de questionários enviados e respostas recebidas.

Quadro 1: Seções de controle e objetivos de controle da camadas física, lógica e humana.

CAMADA	SEÇÃO	OBJETIVOS DE CONTROLE
Física	Gestão das Operações e Comunicações	Garantir a operação segura e correta dos recursos de processamento da informação.
	Segurança física e do ambiente	Prevenir o acesso físico não-autorizado, danos e interferências nas instalações e informações; impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades.
	Controle de acesso	Controlar acesso à informação; assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação; prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou roubo da informação e dos recursos de processamento da informação; prevenir acesso não autorizado aos serviços da rede.
	Gestão de incidentes de segurança da informação	Assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes da segurança da informação.
Lógica	Aquisição, desenvolvimento e manutenção de Sistemas de Informação	Garantir que segurança é parte integrante de sistemas de informação; prevenir a ocorrência de erros, perdas, modificação não autorizada ou uso indevido de informações em aplicações; proteger a confidencialidade, a autenticidade ou a integridade das informações por criptografia; garantir a segurança de arquivos de sistema; manter a segurança de informações e sistemas aplicativos; reduzir riscos resultantes da exploração de vulnerabilidades técnicas

		conhecidas.
Humana	Organizando a segurança da informação	Gerenciar a segurança de informação dentro da organização; manter a segurança da informação e dos recursos de processamento da informação, que são acessados, processados, comunicados ou gerenciados por partes externas.
	Gestão de Ativos	Alcançar e manter a proteção adequada dos ativos da organização; assegurar que a informação receba um nível adequado de proteção.
	Segurança em recursos humanos	Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com seus papéis, e reduzir o risco de roubos, fraudes ou uso indevido de recursos.
	Gestão da continuidade do negócio	Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil.
	Conformidade	Evitar violação de qualquer lei criminal ou civil, estatutos, regulamentos ou obrigações contratuais e de quaisquer requisitos de segurança da informação.
	Política de segurança da informação	Prover uma orientação e apoio da direção para a segurança da informação, de acordo com os requisitos do negócio e com as leis e regulamentos relevantes.

Fonte: Adaptado de Silva Netto e Silveira (2007, p.381-382).

Metodologia

Esta pesquisa é exploratória e descritiva e teve como objetivo identificar a percepção de funcionários das áreas de TI e segurança da informação e de gestores de hospitais públicos brasileiros sobre a importância dos controles de segurança da informação da norma NBR ISO/IEC 27002:2005 para suas instituições.

Nesta pesquisa, foram elaborados três formulários com perguntas sobre os controles presentes na norma, o que reduziu significativamente a quantidade de perguntas, minimizando uma das limitações apontadas por Albuquerque Junior e Santos (2012) em sua pesquisa com hospitais privados brasileiros.

As perguntas foram agrupadas nos três formulários conforme a classificação proposta por Silva Netto e Silveira (2007) (ver Quadro 1): "Controles da Camada Física", com 75 controles; "Controles da Camada Lógica", com 16 controles; e "Controles da Camada Humana", com 42 controles. Juntos, os três formulários contêm 140 perguntas, sendo sete relacionadas ao respondente e à instituição em que trabalha, e 133 relacionados aos controles de segurança da informação. As afirmativas correspondentes aos controles foram associadas a uma escala

Likert de cinco pontos: 1 – sem importância; 2 – pouco importante; 3 – importante; 4 – muito importante; 5 – extremamente importante. Assim, os respondentes deveriam indicar a importância percebida sobre cada controle para as atividades do hospital em que trabalham.

Os formulários foram inseridos no sistema FormSUS (http://formsus.datasus.gov.br) e os endereços de acesso foram enviados eletronicamente para os respondentes, convidando-os a participar da pesquisa, garantindo o sigilo e orientando sobre o preenchimento. No total, 236 hospitais públicos receberam as mensagens e 26 preencheram os formulários, sendo descartadas respostas incompletas de três hospitais. Foram consideradas na pesquisa, portanto, respostas de 23 hospitais (9,75% dos que receberam o convite). Não houve avaliação dos formulários por parte de especialistas nem teste de validação antes da realização da pesquisa, e devido à sua extensão, não foi possível incluir os questionários neste trabalho.

Os prováveis respondentes foram identificados através de consultas nos *websites* dos hospitais públicos federais, estaduais e municipais, e nas secretarias de saúde dos estados e de grandes municípios brasileiros, bem como em pesquisas em *sites* de busca na Internet.

Os formulários ficaram disponíveis para preenchimento entre junho e novembro de 2012 e, ao final deste período, a importância percebida para cada controle foi calculada somando as notas dadas pelos respondentes, resultando nos respectivos *scores*.

Resultados

Embora os formulários tenham sido enviados para hospitais públicos de todos os estados brasileiros, foram obtidas respostas de apenas 10 estados: Distrito Federal, Rio Grande do Sul, Santa Catarina e Sergipe, cada um com participação de um hospital; Bahia, Ceará e Pernambuco, com participação de dois hospitais; Rio de Janeiro, com respostas de três hospitais; Minas Gerais, com quatro hospitais; e São Paulo, com respostas de seis hospitais. O porte dos 23 hospitais variou, com concentração maior de instituições que têm entre 151 e 500 leitos (43,5%). A Tabela 1 mostra a distribuição dos hospitais pela quantidade de leitos.

A pesquisa mostrou que a maioria dos hospitais (73,9%) é estadual e que estes concentram a maior quantidade de leitos: o único que tem mais de 500 leitos, os dez que têm entre 151 e 500 leitos e seis entre os oito que têm entre 51 e 150 leitos são estaduais. Entre os municipais, dois têm entre 51 e 150 leitos e quatro têm até 50 leitos. Nenhum hospital federal participou da pesquisa.

Os formulários foram respondidos por pessoas que trabalham na área de TI (47,8%), de gestão ou diretoria (39,1%) e de Segurança da Informação (13%). Entre os respondentes do formulário "Controles da Camada Física", 15 se declararam Analistas, três são Administradores, dois são Gestores, um é Diretor, um é Coordenador e um é Gerente. Para o formulário "Controles da Camada Lógica", 13 afirmaram ser Analistas, quatro são Administradores, dois são Gestores, um é Diretor, dois são Coordenadores e um é Gerente. Já entre os respondentes do formulário "Controles da Camada Humana", 13 são Analistas, quatro são Administradores, dois são Gestores, dois são Gerentes, um é Diretor e um é Coordenador.

Cruzando dados sobre as quantidades de leitos e de usuários de TI, identificou-se que o hospital que tem menor número de usuários de TI (164) está entre os hospitais que têm menos leitos (menos de 50), e o que tem mais usuários de TI (750) é o único que tem mais de 500 leitos. Respondentes de três hospitais afirmaram ter 400 usuários de TI, sendo esta a moda, número próximo à média de usuários de TI, que é 399,83.

Tabela 1: Quantidade de hospitais distribuídos pelas quantidades de leitos que dispõem.

QUANTIDADE DE LEITOS	HOSPITAIS	%
Até 50 leitos	4	17,4
De 51 a 150 leitos	8	34,8
De 151 a 500 leitos	10	43,5
Mais de 500 leitos	1	4,3
TOTAL	23	100

Fonte: Elaborada pelos autores.

Quanto à percepção da importância dos indicadores de segurança da informação, identificou-se que o formulário que teve maior *score* médio foi "Controles da Camada Humana", com 89,43 pontos. Este mesmo formulário inclui o controle com menor *score* (75, do controle **Verificações do histórico de candidatos a emprego, fornecedores e terceiros, de acordo com a ética, legislação e outros regulamentos pertinentes, e proporcionalmente aos requisitos do negócio, à classificação das informações e aos riscos percebidos**) e o maior *score* (105, do controle **Documento da política de segurança da informação aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas**) dentre os três formulários. A mediana calculada para este formulário foi 88,50 e a moda foi 87, obtida por seis controles. Este formulário teve também o segundo maior *score* da pesquisa - 102 pontos, do controle **Proteção de registros importantes contra perda, destruição e falsificação, de acordo com requisitos legais, regulamentares, estatutários, contratuais e de negócio**.

O formulário "Controles da Camada Física" teve 89,13 pontos de *score* médio e a mediana calculada foi 90, enquanto a moda foi 95, *score* que apareceu nove vezes neste formulário. O maior *score* foi 99, obtido por dois controles, enquanto o menor *score* foi 78.

Já o formulário "Controles da Camada Lógica" teve *score* médio de 84,81 e a mediana foi 85. Os *scores* 81 e 85 são os que aparecem mais vezes nos controles deste formulário: três vezes cada. O *score* mais alto obtido neste formulário foi 93 e o menor foi 78 pontos.

Considerando todos os controles de segurança da informação dos três formulários, a média calculada foi 88,70. Diante disso, 58,67% dos controles do formulário "Controles da Camada Física" estão acima dessa média. Do formulário "Controles da Camada Lógica", identificou-se que 25% estão acima da média, enquanto o mesmo ocorre com 50% dos controles do formulário "Controles da Camada Humana".

Como o formulário "Controles da Camada Lógica" tem apenas 16 controles, para efeito de comparação entre os três formulários foram considerados apenas os 16 controles que obtiveram maior *score* dos outros dois. Esses controles estão representados na Tabela 2, Tabela 3 e Tabela 4, respectivamente para os formulários "Controles da Camada Física", "Controles da Camada Lógica" e "Controles da Camada Humana".

Como o formulário "Controles da Camada Humana" teve um empate entre três controles com 91 pontos de *score* na 16ª posição, utilizou-se como critério de desempate a quantidade de vezes que os respondentes atribuíram importância 5 (Extremamente importante) para cada controle.

Tabela 2: Os 16 controles mais importantes da Camada Física.

CONTROLE	SCORE	MÉDIA	MEDIANA	DESV. PADR.
Existência de procedimento formal de registro e cancelamento de usuário para que os acessos em todos os sistemas e serviços de informação sejam garantidos ou revogados.	99	4,30	4,00	0,702
Proteção da integridade de informações disponibilizadas em sistemas publicamente acessíveis para prevenir modificação não autorizada.	99	4,30	4,00	0,764
Procedimentos para tratamento e armazenamento de informações contra divulgação não autorizada ou uso indevido.	97	4,21	4,00	0,735
Adoção por parte dos usuários de política de mesa limpa (sem papéis e mídias de armazenamento removíveis) e de tela limpa (sem documentos sensíveis no desktop do sistema operacional do computador).	97	4,21	4,00	0,795
Garantia de que os usuários tem um identificador único (ID de usuário, username, login de acesso, PIN) para uso pessoal e exclusivo e de que existe uma técnica de autenticação adequada para validar a identidade do usuário.	97	4,21	4,00	0,850
Controle de pontos de acesso (áreas de entrega e carregamento, áreas de acesso permitido a pessoas de fora da organização) e, se possível, isolamento entre essas áreas e recursos de processamento de informação.	96	4,17	4,00	0,716
Controle da concessão de senhas por meio de um processo formal de gerenciamento.	96	4,17	4,00	0,777
Utilização de perímetros de segurança (barreiras, paredes, portões controlados) para proteger áreas que contenham informações e recursos de processamento de informação.	95	4,13	4,00	0,694
Proteção de áreas seguras através de controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso.	95	4,13	4,00	0,757
Separação entre recursos de desenvolvimento, teste e produção para reduzir o risco de acessos ou modificações não autorizadas.	95	4,13	4,00	0,757
Realização e teste regular de cópias de segurança das informações e softwares, de acordo com uma política definida e documentada de realização de cópias de segurança.	95	4,13	4,00	0,757

Concessão de direitos de acesso aos usuários somente aos serviços que tenham sido especificamente autorizados a utilizar.	95	4,13	4,00	0,757
Controle do acesso aos sistemas operacionais por meio de procedimento seguro de entrada (log-on) no sistema.	95	4,13	4,00	0,814
Existência de um sistema de gerenciamento de senhas interativo que assegure senhas de qualidade.	95	4,13	4,00	0,814
Restrição do acesso à informação e às funções dos sistemas para usuários e pessoal de suporte, de acordo com o que está definido na política de controle de acesso.	95	4,13	4,00	0,868
Coleta, armazenamento e apresentação de evidências para ações de acompanhamento após a ocorrência de incidentes de segurança da informação que impliquem em ações administrativas e legais cíveis ou criminais.	95	4,13	4,00	0,868

Fonte: Elaborada pelos autores.

Dessa forma, o controle **Apoio da Direção à segurança da informação por meio de um claro direcionamento, demonstrando compromisso, definindo explicitamente atribuições e reconhecendo responsabilidades** figurou na Tabela 4, pois foi avaliado como "Extremamente importante" oito vezes, enquanto os outros dois foram avaliados como extremamente importantes seis e cinco vezes.

Tabela 3: Os 16 controles da Camada Lógica.

CONTROLE	SCORE	MÉDIA	MEDIANA	DESV. PADR.
Implementação de procedimentos para controlar a instalação de software em sistemas operacionais.	93	4,04	4,00	0,824
Prevenção de oportunidades de vazamento de informações em ações de desenvolvimento e suporte.	92	4,00	4,00	0,797
Seleção cuidadosa, proteção e controle de dados de teste.	90	3,91	4,00	0,733
Restrições e controle de mudanças em pacotes de software e limitação às mudanças necessárias.	90	3,91	4,00	0,824
Utilização de procedimentos formais para controlar mudanças em sistemas e informações.	87	3,78	4,00	0,795
Análise crítica e teste de aplicações críticas para o negócio para garantir que não haverá impacto adverso na operação ou na segurança quando	86	3,73	4,00	0,810

houver mudanças de sistemas operacionais.				
Especificação de requisitos para controles de segurança nas especificações de requisitos de negócio para novos sistemas de informação ou para mudanças em sistemas existentes.	85	3,69	4,00	0,634
Incorporação de checagens de validação de dados de entrada com o objetivo de detectar corrupção de informações nas aplicações, por erro ou ações deliberadas.	85	3,69	4,00	0,702
Supervisão e monitoramento de desenvolvimento terceirizado de software.	85	3,69	4,00	0,702
Restrição de acesso a códigos-fonte de programas.	82	3,56	4,00	0,727
Desenvolvimento e implementação de uma política de uso de controles criptográficos.	82	3,56	4,00	1,079
Validação de dados de entrada para garantir que são corretos e apropriados.	81	3,52	4,00	0,845
Implementação de um processo de gerenciamento de chaves criptográficas para apoiar o uso de técnicas de criptografia na organização.	81	3,52	4,00	1,122
Obtenção de informações sobre vulnerabilidades técnicas de sistemas em uso, avaliação da exposição a essas vulnerabilidades e medidas apropriadas para lidar com os riscos associados.	81	3,52	3,00	0,730
Validação de dados de saída das aplicações para assegurar que o processamento das informações armazenadas está correto e é apropriado às circunstâncias.	79	3,43	3,00	0,843
Identificação de requisitos para garantir autenticidade e integridade das mensagens em aplicações e identificação e implementação de controles apropriados.	78	3,39	3,00	0,838

Fonte: Elaborada pelos autores.

Considerando apenas 16 controles considerados mais importantes, o formulário "Controles da Camada Física" teve *score* médio de 96 pontos, e a mediana e a moda foram 95 pontos. Como os *scores* deste formulário variaram de 95 a 99, o range ficou com 4 pontos. O formulário "Controles da Camada Lógica", como já apresentado anteriormente, teve *score* médio 84,81 e a mediana calculada foi 85 pontos.

Os *scores* 81 e 85 aparecem três vezes cada, sendo os que aparecem mais vezes neste formulário. O *score* mínimo é 78 e o máximo é 93, com um range de 15 pontos. Já os 16 controles mais importantes do formulário "Controles da Camada Humana" têm uma média de 96,31 pontos e uma mediana de 95,50 pontos. A confiabilidade dos formulários foi estimada utilizando o alfa de Cronbach utilizando Stata 11, considerando tanto as respostas dadas para

os 16 controles percebidos como mais importantes (alfa de Cronbach), quanto para todos os controles dos formulários (alfa de Cronbach total). Como o menor *score* é 91 e o maior é 105, o range é de 14 pontos. Estes dados estão representados na Tabela 5.

Tabela 4: Os 16 controles mais importantes da Camada Humana.

CONTROLE	SCORE	MÉDIA	MEDIANA	DESV. PADR.
Documento da política de segurança da informação aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas (fornecedores e parceiros).	105	4,56	5,00	0,662
Proteção de registros importantes contra perda, destruição e falsificação, de acordo com requisitos legais, regulamentares, estatutários, contratuais e de negócio.	103	4,47	5,00	0,790
Definição explícita, documentação e atualização dos requisitos estatutários, regulamentares e contratuais para cada sistema de informação.	99	4,30	5,00	1,019
Garantia da conformidade com requisitos legais, regulamentares e contratuais no uso de material que pode ter direitos de propriedade intelectual e no uso de software proprietário.	99	4,30	4,00	0,764
Garantia da privacidade e da proteção de dados pessoais, conforme exigências legais, regulamentares e contratuais.	99	4,30	4,00	0,764
Análise crítica da política de segurança da informação a intervalos planejados ou quando ocorrem mudanças significativas.	97	4,21	4,00	0,671
Classificação da informação em termos de seu valor, por requisitos legais, por sensibilidade e por criticidade para a organização.	96	4,17	4,00	0,716
Existência de processo disciplinar formal para funcionários que tenham cometido violações à política de segurança da informação.	96	4,17	4,00	0,777
Remoção dos direitos de acesso às informações e aos recursos de processamento de informação de funcionários, fornecedores e terceiros após o encerramento de suas atividades e contratos, ou realização de ajustes após mudanças nessas atividades.	95	4,13	4,00	0,814
Identificação clara de todos os ativos e estruturação e manutenção de inventário de todos os ativos importantes.	94	4,08	4,00	0,733
Definição e implementação de procedimentos	94	4,08	4,00	0,733

para rotular e tratar a informação de acordo com o esquema de classificação adotado pela organização.				
Devolução, ao fim do contrato ou ao encerramento das atividades, de ativos da organização que estiverem sob posse de funcionários, fornecedores e terceiros.	94	4,08	4,00	0,792
Desenvolvimento e manutenção de um processo de gestão de continuidade do negócio contemplando os requisitos de segurança da informação.	94	4,08	4,00	0,949
Prevenção do uso de recursos de processamento de informação para propósitos não autorizados.	93	4,04	4,00	0,928
Designação formal de responsáveis pelas informações e ativos associados com recursos de processamento de informações.	92	4,00	4,00	0,674
Apoio da Direção à segurança da informação por meio de um claro direcionamento, demonstrando compromisso, definindo explicitamente atribuições e reconhecendo responsabilidades.	91	3,95	4,00	0,928

Fonte: Elaborada pelos autores.

Assim, mesmo considerando apenas os 16 controles mais importantes, o formulário "Controles da Camada Humana" é o que tem maior *score* médio entre os três, embora o formulário "Controles da Camada Física" tenha a menor variação entre o menor e o maior *score*. Os coeficientes alfa, calculados tanto para os 16 controles percebidos como mais importantes quanto para todos os controles dos três formulários, mostram que a confiabilidade dos formulários é muito alta, segundo a classificação utilizada por Freitas e Rodrigues (2005), a saber: muito baixa para $\alpha \leq 0{,}30$; baixa para $0{,}30 < \alpha \leq 0{,}60$; moderada para $0{,}60 < \alpha \leq 0{,}75$; alta para $0{,}75 < \alpha \leq 0{,}90$; e muito alta para $\alpha > 0{,}90$.

Tabela 5: Média, mediana, máximo, mínimo, alfa de Cronbach e desvio padrão calculados com base nos 16 controles considerados mais importantes de cada formulário, e alfa de Cronbach calculado com base em todos os controles de cada formulário.

FORMULÁRIO	*SCORE* MÍNIMO – 16 CONT.	*SCORE* MÁXIMO – 16 CONT.	*SCORE* MÉDIO – 16 CONT.	MEDIANA – 16 CONT.	*a* DE CRONBACH – 16 CONT.	*a* DE CRONBACH – FORMUL.
Controles da Camada Física	95	99	96,00	95,00	0,961	0,980
Controles da Camada Lógica	78	93	84,81	85,00	0,923	0,923
Controles da Camada	91	105	96,31	95,50	0,908	0,957

Humana						

Fonte: Elaborada pelos autores.

Cruzando dados dos perfis dos respondentes com a importância atribuída aos controles, observa-se que os Analistas de TI e segurança da informação percebem o controle **Procedimentos para tratamento e armazenamento de informações contra divulgação não autorizada ou uso indevido** como mais importante do formulário "Controle da Camada Física", atribuindo uma importância média de 4,53. Para os demais respondentes (Gestores, Administradores e Diretores), o controle mais importante é **Coleta, armazenamento e apresentação de evidências para ações de acompanhamento após a ocorrência de incidentes de segurança da informação que impliquem em ações administrativas e legais cíveis ou criminais**, que teve 4,12 de importância média. Nesta comparação e nas duas que se seguem, optou-se por comparar as importâncias médias dos controles por serem diferentes as quantidades de respondentes dos perfis, o que dificultaria a comparação pelos *scores* dos controles.

Dessa forma, os Analistas percebem como mais importantes do formulário "Controles da Camada Humana" os controles: **Documento da política de segurança da informação aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas (fornecedores e parceiros)**; **Proteção de registros importantes contra perda, destruição e falsificação, de acordo com requisitos legais, regulamentares, estatutários, contratuais e de negócio**; e **Garantia da privacidade e da proteção de dados pessoais, conforme exigências legais, regulamentares e contratuais**. Nesse caso, a importância média atribuída pelos Analistas aos três controles foi 4,69. Os demais perfis de respondentes concordam com os Analistas quanto ao controle **Documento da política de segurança da informação aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas (fornecedores e parceiros)** ser o mais importante, com importância média igual a 4,40. Ainda para eles, o controle **Proteção de registros importantes contra perda, destruição e falsificação, de acordo com requisitos legais, regulamentares, estatutários, contratuais e de negócio** está também entre os mais importantes – a importância média foi 4,20, a segunda mais alta.

Já para o formulário "Controle da Camada Lógica", os Analistas percebem como mais importante o controle **Prevenção de oportunidades de vazamento de informações em ações de desenvolvimento e suporte**, cuja média calculada para sua importância foi 4,38. Os outros perfis percebem como mais importante o controle **Desenvolvimento e implementação de uma política de uso de controles criptográficos**, que teve uma importância média igual a 3,45.

Discussão

Comparando as respostas válidas recebidas com a quantidade de hospitais convidados a participar da pesquisa, percebe-se que 23 respostas válidas representam um número significativamente baixo face os 236 convites enviados – 9,75% dos hospitais responderam à pesquisa. A título de comparação, na pesquisa de Albuquerque Junior e Santos (2012), foram enviados 173 convites, com 48 respostas válidas, o que dá 27,74% de respostas válidas. Isso pode significar um menor interesse das pessoas que trabalham em hospitais públicos para participar da pesquisa.

Os resultados demonstraram também que houve pouca participação de hospitais com mais de 500 leitos, e que a grande maioria (78,3%) tem entre 51 e 500 leitos. No estudo de Albuquerque Junior e Santos (2012), 73% das respostas vieram de hospitais menores, com

até 150 leitos. As respostas da pesquisa de Albuquerque Junior e Santos (2012) vieram de 22 Estados diferentes, enquanto nesta pesquisa as respostas vieram de apenas 10 Estados. Esses fatos relativos à diferença de disposição em participar de pesquisas científicas para profissionais de hospitais públicos e privados merecem ser investigados.

Ressalta-se também nesta pesquisa a grande participação de hospitais estaduais (73,9%) e a ausência de respostas de hospitais federais, o que suscita uma análise sobre as estruturas de TI e segurança da informação de hospitais federais e municipais, que pode ajudar a explicar esses fatos.

Do total de controles do formulário "Controles da Camada Física", 58,67% estão acima da média geral, o que mostra sua importância no contexto em que se realizou a pesquisa e que pode ser explicado pela grande participação de profissionais com perfil mais técnico. Por outro lado, o fato de metade dos controles do formulário "Controles da Camada Humana" ser considerada importante mostra o reconhecimento por parte dos respondentes da importância do fator humano na segurança da informação.

Ao analisar os controles com *scores* mais altos nos três formulários, nota-se que, de maneira geral, há uma preocupação em estabelecer políticas e procedimentos de segurança da informação nos hospitais. O *score* mais alto entre todos foi obtido pelo controle que trata da formalização de uma Política de Segurança da Informação, confirmando a importância deste controle em instituições de saúde, uma vez que na pesquisa realizada por Albuquerque Junior e Santos (2012) a prática considerada mais importante entre todas pelos respondentes de hospitais privados foi também a que trata da existência de uma Política de Segurança da Informação formalizada e aprovada. Este controle é considerado extremamente importante nesta pesquisa por nove respondentes da área de TI e por três da área de segurança da informação, enquanto dois respondentes da área de TI consideram-no muito importante, três da área de gestão ou direção o consideram extremamente importante, quatro consideram muito importante e dois consideram importante. Nota-se com isso uma pequena diferença de percepção para respondentes de perfis diferentes sobre este controle, embora todos o tenham considerado pelo menos importante. Uma possível explicação é o fato de os profissionais de TI e segurança da informação vejam a necessidade de uma Política de Segurança da Informação de forma mais objetiva, como instrumento que autoriza a implementação de regras, restrições e procedimentos, o que não se aplica para diretores e gestores.

É também notável a preocupação dos respondentes com a proteção de informações sensíveis, o que pode refletir tanto compreensão de uma obrigação ética e legal quanto a necessidade de garantir o funcionamento da instituição. O controle **Proteção de registros importantes contra perda, destruição e falsificação, de acordo com requisitos legais, regulamentares, estatutários, contratuais e de negócio** foi o segundo mais importante, e exemplifica isso, reforçado pela importância atribuída pelos respondentes da pesquisa de Albuquerque Junior e Santos (2012).

A importância da existência e da utilização de procedimentos para garantir a proteção das informações também aparece nos controles que tratam de processos, técnicas e procedimentos de controle de acesso, presentes em alguns controles considerados importantes e voltados para a confidencialidade das informações. O mesmo foi observado por Albuquerque Junior e Santos (2012), que teve práticas relacionadas à existência de procedimentos formais incluídas entre as mais importantes.

Também foi possível observar a importância percebida de controles que visam punir o desrespeito às normas de segurança da informação, o que pode ter ocorrido devido ao fato de os respondentes serem servidores públicos e estarem sujeitos a processos administrativos disciplinares e, por se tratar da área de saúde, de haver um grande apelo ao cumprimento de

normas emitidas pelos conselhos profissionais e ao cumprimento dos códigos de ética das categorias profissionais. Isso não foi observado na pesquisa de Albuquerque Junior e Santos (2012), o que reforça a possibilidade de os respondentes desta pesquisa serem servidores públicos e, por isso, perceberem como importantes esses controles.

De maneira geral, os controles considerados mais importantes destacam principalmente uma preocupação com a proteção da privacidade dos pacientes e com o cumprimento dos requisitos legais, que estão muito relacionados às atividades desempenhadas e ao tipo de informações com que lidam os hospitais públicos. O mesmo foi observado na pesquisa de Albuquerque Junior e Santos (2012), segundo os quais a prática que trata diretamente da garantia da privacidade foi a terceira mais importante da camada humana.

Por fim, como o formulário "Controles da Camada Humana" teve maior *score* médio entre os três e por 50% dos seus controles estarem acima da média geral, ressalta-se a importância do componente humano na segurança da informação, o que leva a autores como Silva e Stein (2007) e Albrechtsen (2008) a sugerirem pesquisas sobre o tema utilizando uma abordagem social.

Conclusões

Neste estudo, utilizou-se a norma NBR ISO/IEC 27002:2005 para identificar a percepção da importância dos seus controles em hospitais públicos brasileiros. Respondida por profissionais das áreas de TI, segurança da informação e gestão ou diretoria de 23 hospitais públicos de 10 Estados diferentes, a pesquisa permitiu identificar os controles percebidos como mais importantes para as atividades desenvolvidas em hospitais públicos.

De todos os controles, o mais importante trata da elaboração e manutenção de Políticas de Segurança da Informação – uma formalização das regras de proteção de informações sobre os pacientes, presentes em diversos instrumentos normativos aos quais essas instituições estão submetidas. E o formulário que teve *score* médio mais alto foi "Controles da Camada Humana", o que mostra a importância do componente humano na segurança da informação no contexto em que foi realizada a pesquisa.

A pesquisa destacou também a importância de controles mais diretamente relacionados à proteção das informações dos pacientes, aos processos que controlam o acesso a essas informações e o respeito às leis e regulamentos que tratam da proteção à privacidade, a exemplo do que foi identificado por Albuquerque Junior e Santos (2012) em sua pesquisa com profissionais de hospitais privados.

Em suma, a importância dos controles de segurança da informação segundo os respondentes das áreas de TI, segurança da informação e gestão/diretoria de hospitais públicos brasileiros aponta para uma necessidade de estabelecer políticas, identificar e classificar informações, além de respeitar as normas de garantia do sigilo dos pacientes.

O trabalho tem como limitação a pequena quantidade de hospitais que responderam aos três formulários corretamente. Assim, as conclusões tomadas a partir da pesquisa não podem ser generalizadas. Outra limitação é o fato de o porte dos hospitais não ter sido considerado na pesquisa, embora a pesquisa tenha procurado levantar as quantidades de usuários de TI e de leitos.

Apesar de os formulários terem ficado significativamente menores do que os utilizados por Albuquerque Junior e Santos (2012), considera-se ainda grande a quantidade de perguntas, o que é mais uma limitação deste trabalho, e que pode ter sido um dos fatores que determinaram a baixa participação na pesquisa.

Como sugestões de trabalhos futuros, propõe-se a realização de pesquisas sobre a utilização efetiva dos controles mais importantes de segurança da informação, sobre as implicações desses controles nas atividades desempenhadas pelos profissionais de saúde desses hospitais e sobre os mecanismos de institucionalização de normas de segurança da informação em hospitais públicos.

Referências Bibliográficas

AHLFELDT, Rose-Mharie. Information Security in a Heterogeneous Healthcare Domain. In: INTERNATIONAL CONFERENCE ON INTEROPERABILITY OF ENTERPRISE SOFTWARE AND APPLICATIONS, 1 th, 2005, Genebra. **Proceedings...** Genebra: INTEROP, 2005. p. 103-114.

ALBRECHTSEN, Eirik. **Friend or foe?** Information security management of employees. Trondheim. 2008. Tese (Doutorado em Economia Industrial e Gestão Tecnológica) – Norwegian University of Science and Technology, Trondheim, 2008.

ALBUQUERQUE JUNIOR, Antonio E. ; SANTOS, Ernani M. dos. Controles e Práticas de Segurança da Informação em um Instituto de Pesquisa Federal. In: SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA, 8., 2011, Resende. **Anais...** Resende: AEDB, 2011.

ALBUQUERQUE JUNIOR, Antonio E. ; SANTOS, Ernani M. dos. Segurança da Informação em Hospitais: A Percepção da Importância de Controles para Gestores e Profissionais de TI. **Revista Gestão & Saúde**, Curitiba: Herrero, n.2, v.4, p.1-14, ago. 2012.

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.

BEAL, A. **Segurança da Informação: Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações**. São Paulo: Atlas, 2005.

BRITTO, Thiago D. **Levantamento e Diagnóstico de Maturidade da Governança da Segurança de Informação na Administração Direta Federal Brasileira**. 2011. Dissertação (Mestrado em Gestão do Conhecimento e da Tecnologia da Informação) – Universidade Católica de Brasília, Brasília, 2011.

CEPIK, Marco; CANABARRO, Diego R.; POSSAMAI, Ana J. A Institucionalização do SISP e a Era Digital no Brasil. In: CEPIK, Marco; CANABARRO, Diego R. **Governança de TI**: Transformando a Administração Pública no Brasil. Porto Alegre: WS Editor, 2010. p.3 7-74.

DONNER, M. L.; OLIVEIRA, L. R. Análise de Satisfação com a Segurança no Uso de Internet Banking em Relação aos Atuais Recursos Disponíveis no Canal Eletrônico. In: ENCONTRO DA ANPAD, 32., 2008, Rio de Janeiro. **Anais...** Rio de Janeiro: ANPAD, 2008. CD ROM.

FACHINI, G. J. **Análise do Nível de Formalização da Política de Segurança da Informação à Luz da NBR ISO/IEC 17799:2005 nas Empresas de Tecnologia da Informação de Blumenau, SC**. 2009. Dissertação (Mestrado em Ciências Contábeis) – Universidade Regional de Blumenau, Blumenau, 2009.

FERNANDES, A. A.; ABREU, V. F. **Implantando a Governança de TI**: da estratégia à gestão dos processos e serviços. 2. ed. Rio de Janeiro: Brasport, 2008.

FREITAS, André L. P.; RODRIGUES, Sidilene G. A avaliação da Confiabilidade de Questionários: uma Análise utilizando o coeficiente Alfa de Cronbach. In: SIMPÓSIO DE ENGENHARIA DE PRODUÇÃO, 12., 2005, Bauru. **Anais...** Bauru: UNESP, 2005.

JANCZEWSKI, Lech; SHI, Frank X. Development of Information Security Baselines for Healthcare Information Systems in New Zealand. **Computers & Security**, v. 21, n. 2, p.172-192, 2002.

KOBAYASHI, L. O. M.; FURUIE, S. S. Segurança em Informações Médicas: Visão Introdutória e Panorama Atual. **Revista Brasileira de Engenharia Biomédica**. n.1, v.23, p.53-77, abr. 2007.

KWAK, Y. S. International Standards for Building Electronic Health Record (EHR). In: INTERNATIONAL WORKSHOP ON ENTERPRISE NETWORKING AND COMPUTING IN HEALTHCARE INDUSTRY, 7th, 2005, *Busan***,** South Korea. **Proceedings...** *Busan*, South Korea: Korea Multimedia Society, 2005. p.18-23.

LOPES, Isabel M. **Adopção de Políticas de Segurança de Sistemas de Informação na Administração Pública Local em Portugal**. 2012. Tese (Doutorado em Tecnologias e Sistemas de Informação, Engenharia e Gestão de Sistemas de Informação) – Escola de Engenharia, Universidade do Minho, Braga, 2012.

MARCIANO, J. L. P. **Segurança da Informação** – uma abordagem social. 2006. Tese (Doutorado em Ciência da Informação) – Universidade de Brasília, Brasília, 2006.

MOURA, G. C. M.; GASPARY, L. P. Uma Proposta para Medição de Complexidade de Segurança em Procedimentos de Tecnologia da Informação. In: SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, 8., 2008, Gramado. **Anais...** Gramado: SBC, set. 2008, p.129-142.

NOBRE, A. C. S.; RAMOS, A. S. M.; NASCIMENTO, T. C. Fatores que Influenciam a Aceitação de Práticas Avançadas de Gestão de Segurança da Informação: um estudo com gestores públicos estaduais no Brasil. In: ENCONTRO DA ANPAD – ENANPAD, 34., Rio de Janeiro, 2010. **Anais...** Rio de Janeiro: ANPAD, set.2010, 17 p. CD ROM.

RAGHUPATHI, W.; TAN, J. Strategic IT Applications in Health Care. **Communications of the ACM**. v. 45, n. 12, p.56-61. 2002.

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

SILVA, D. R. P.; STEIN, L. M. Segurança da Informação: uma reflexão sobre o componente humano. **Ciências & Cognição**. v. 10, p.46-53, mar. 2007.

SILVA NETTO, A. S.; SILVEIRA, M. A. P. Gestão da Segurança da Informação: Fatores que Influenciam sua Adoção em Pequenas e Médias Empresas. **JISTEM**. v. 4, n. 3, p.375-397. 2007.

Recebido: 15.11.2012

Aceito: 04.06.2013