REVISTA GESTÃO & SAÚDE (ISSN 1984-8153)

SEGURANÇA DA INFORMAÇÃO EM HOSPITAIS: A PERCEPÇÃO DA IMPORTÂNCIA DE CONTROLES PARA GESTORES E PROFISSIONAIS DE TI

INFORMATION SECURITY IN HOSPITALS: THE PERCEPTION OF IMPORTANCE OF CONTROLS FOR MANAGERS AND IT PROFESSIONALS

Antonio Eduardo de Albuquerque JUNIOR [1]
Ernani Marques dos SANTOS[2]

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 adotem controles de segurança da informação apropriados para as atividades que desenvolvem, e a norma NBR ISO/IEC 27002:2005 propõe diversos controles e práticas de segurança da informação que visam a segurança das informações. Este trabalho exploratório teve o objetivo de identificar a percepção de gestores e funcionários das áreas de TI e segurança da informação de hospitais privados sobre a importância das práticas de segurança da informação para as atividades desenvolvidas nos hospitais.

Palavras-chave: segurança, informação, hospitais.

Abstract: The hospitals dependence about Information Technology (IT) infrastructure and the need to protect information about the patients requires the adoption of information security controls by hospitals, which should be appropriate to its activities. The ISO/IEC 27002:2005 standard suggests various information security controls and practices that can be used by hospitals to protect information. This study aimed to identify the perception of managers, IT professionals and information security professionals of Brazilian private hospitals about the importance of information security practices.
Keywords: information, security, hospitals.

1 Mestre em Administração pela Universidade Federal da Bahia (UFBA), Especialista em Redes de Computadores pela Faculdade Ruy Barbosa (FRB) e Graduado em Processamento de Dados pela FRB. Tecnologista em Saúde Pública da FIOCRUZ. Centro de Pesquisa Gonçalo Moniz, FIOCRUZ, Rua Waldemar Falcão, 121, Salvador – Bahia, CEP. 40.296-710. Tel.: (71) 3176-2451. E-mail: aealbuquerque@bahia.fiocruz.br

2 Doutor em Administração pela Universidade de São Paulo (USP), Mestre em Administração pela UFBA, Graduado em Administração de Empresas pela Universidade Católica do Salvador (UCSAL) e em Processamento de Dados pela Universidade Salvador (UNIFACS). Professor Adjunto da Escola de Administração da UFBA. Escola de Administração da UFBA, Av. Reitor Miguel Calmon, s/n, Vale do Canela, Salvador – Bahia, CEP. 40.110-903. Tel.: (71) 3283-7678. E-mail: emarques@ufba.br

INTRODUÇÃO

As informações estiveram presentes em todas as fases do processo de evolução das organizações (Donner; Oliveira, 2008). Isso fez com que a informação ganhasse importância e passasse a ser disseminada e disponibilizada entre diferentes organizações através das facilidades trazidas pelos meios de comunicação e pela tecnologia (Sêmola, 2003). A informação tem também servido como base para um novo modelo de economia e para uma forma diferente de gestão organizacional (Mello et al., 2010).

Embora seja um ativo intangível, pode estar também entre os bens mais valiosos de uma organização (Nobre; Ramos; Nascimento, 2010), compondo, juntamente com ativos tangíveis, seu valor econômico (Kayo et al., 2006). São considerados pela Associação Brasileira de Normas Técnicas (ABNT) (2005) ativos organizacionais as informações digitais ou não, os computadores, os serviços de computação, os meios de armazenamento de informações (discos rígidos e óticos, fitas magnéticas), os meios de impressão e transmissão de informações (as impressoras, as copiadoras e os aparelhos de fax) e qualquer outro equipamento ou objeto que processe, contenha, armazene, receba, envie ou imprima informações sensíveis, bem como a comunicação, a reputação, a imagem, o nome e a marca da organização, entre outros exemplos. Em sua norma NBR ISO/IEC 27002:2005 voltada para a segurança da informação e baseada em normas internacionais, a ABNT (2005) classifica os ativos associados às informações como: ativos de informação; ativos de software; ativos físicos; serviços; pessoas e suas qualificações, habilidades e experiências; e intangíveis. A norma traz também uma série de controles e objetivos de controles a serem adotados e seguidos visando a proteção da informação e a continuidade das operações da organização.

Além de ser um ativo organizacional e estar envolvida com tantos outros ativos, a informação tem importância destacada na tomada de decisões e isso aumenta o impacto provocado pela sua divulgação por meios não autorizados. O risco de divulgação não autorizada aumenta com as facilidades trazidas pela interconexão de dispositivos em redes e pela portabilidade dos equipamentos usados para acessar e transmitir informações (Fachini, 2009). Aliado à importância da informação está a dependência que as organizações tem de sua infraestrutura de Tecnologia da Informação (TI), que vem se tornando cada vez mais complexa. Esses fatores tem deixado a TI sujeita a ameaças que podem comprometer a segurança das próprias informações, das transações organizacionais e das pessoas (Marciano, 2006). Assim, há a necessidade de proteger as informações e os equipamentos que as processam, armazenam e transmitem, fazendo com que a administração de pessoas, as políticas e os programas que visam assegurar a continuidade das operações nas organizações venham sendo tratados com prioridade cada vez maior (Herath; Herath; Bremser, 2010). Para a ABNT (2005), a informação é essencial para uma organização e, por isso, necessita ser adequadamente protegida, como acontece com qualquer outro ativo importante.

Por existirem diferentes mecanismos de proteção para as informações e por estarem as informações relacionadas a tantos outros ativos, é importante o entendimento do ambiente onde elas são transmitidas, processadas, armazenadas ou utilizadas (Silva, 2009). Falhas na estrutura de transmissão, processamento, armazenamento ou utilização podem tornar as informações indisponíveis ou expô-las a acessos não autorizados e a alterações indevidas. A segurança da informação inclui, portanto, a integridade dos equipamentos que compõem essa estrutura (Sêmola, 2003; Nobre; Ramos; Nascimento, 2010).

Este artigo é resultado de uma pesquisa quantitativa, exploratória e descritiva, que teve como objetivo identificar a percepção de gestores e funcionários das áreas de TI e segurança da informação de hospitais privados brasileiros a respeito da importância das práticas de segurança da informação propostas pela norma NBR ISO/IEC 27002:2005. Os resultados obtidos com a pesquisa ajudarão na realização de pesquisas futuras sobre a adoção de práticas de segurança da informação em hospitais, sua efetividade e as implicações dessas práticas nas atividades dos profissionais de saúde, bem como na comparação com resultados obtidos em pesquisas semelhantes realizadas em hospitais da rede pública.

Para realizar a pesquisa, as práticas presentes na norma foram divididas e organizadas em três formulários eletrônicos, sendo um para as práticas relacionadas à camada física, um para as práticas da camada lógica e um para a camada humana, conforme proposto por Silva Netto e Silveira (2007). As práticas, que correspondem aos itens retirados do questionário utilizado por Karabacak e Sogukpinar (2006), foram associadas a uma escala Likert de cinco pontos correspondendo à importância percebida para cada respondente.

Os endereços eletrônicos de acesso aos três formulários foram enviados através de mensagens de correio eletrônico para ouvidorias, diretorias, departamentos de TI e assessorias de comunicação de 173 hospitais privados localizados em todos os estados brasileiros, juntamente com os convites para participar da pesquisa e orientando

para que cada formulário fosse preenchido apenas uma vez em cada hospital e por pessoas capazes de avaliar a importância das práticas apresentadas. Do total, 48 hospitais responderam aos três formulários enviados.

O artigo está dividido em cinco seções principais, além desta introdução e das referências bibliográficas: a seção seguinte apresenta a teoria sobre segurança da informação utilizada neste trabalho e trata da norma NBR ISO/IEC 27002:2005; a seção 3 trata de segurança da informação em serviços de saúde e da legislação relacionada ao tema; a seção 4 trata da metodologia utilizada na pesquisa; a seção 5 traz a apresentação e a análise dos resultados obtidos na pesquisa; a seção 6 traz as considerações finais do trabalho.

SEGURANÇA DA INFORMAÇÃO

Segurança da Informação é conceituada por Donner e Oliveira (2008) como o processo de proteção da informação contra ameaças visando assegurar sua integridade, disponibilidade e confidencialidade. De forma bem próxima, Beal (2005) define segurança da informação como a proteção da informação contra ameaças à sua integridade, disponibilidade e confidencialidade. Na NBR ISO/IEC 27002:2005, a ABNT (2005) conceitua segurança da informação de duas formas: como a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio; e como a preservação da confidencialidade, da integridade e da disponibilidade da informação. A norma diz que essa proteção pode ser obtida a partir da definição e implementação de controles adequados, que precisam ser também monitorados, analisados criticamente e melhorados para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Ainda segundo a norma, esses controles incluem políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware.

Diante de uma das definições da ABNT (2005) e da definição apresentada por Beal (2005), observa-se que a segurança da informação tem três componentes principais: integridade, disponibilidade e confidencialidade. Silva Netto e Silveira (2007) apresentam os objetivos de cada um desses componentes: integridade, que visa garantir a exatidão da informação contra modificações ou remoções não autorizadas; disponibilidade, que visa garantir que a informação esteja acessível pelas pessoas que estão autorizadas a fazer esse acesso quando ela for necessária; e confidencialidade, que visa garantir que somente pessoas autorizadas tenham acesso à informação. Em suma, segurança da informação é a garantia de que as informações serão protegidas de três maneiras: serão acessadas apenas pelas pessoas que devem ter acesso a elas, estarão corretas e completas e estarão disponíveis sempre que seus usuários precisarem. Sua finalidade é a proteção de ativos de informação contra acessos não autorizados, alterações indevidas ou indisponibilidade (Sêmola, 2003), ou a proteção das informações contra ameaças para garantir a continuidade do negócio, a minimização das perdas e a maximização do retorno sobre os investimentos (Mandarini, 2004), embora não seja possível erradicar completamente o risco de uso indevido da informação (Silva; Stein, 2007).

O fato de computadores armazenarem grande parte dos dados importantes de uma organização faz com que haja grande dependência destas para com a TI (Silva Netto; Silveira, 2007). A dependência das organizações com relação à TI tornou-se aguda e há uma necessidade de proteger os recursos de processamento de informações contra perda, indisponibilidade ou violação (Caruso; Steffen, 1999). Embora o uso da TI seja motivo de dependência e alvo de ataques, Marciano (2006) diz que seu uso para proteger a informação não é suficiente para garantir que a informação seja protegida. Para este autor, a TI pode ajudar na proteção, mas também traz riscos relacionados à segurança da informação. Silva e Stein (2007) concordam ao afirmarem que a segurança da informação não deve ficar restrita à tecnologia. A informação deve ser protegida em todas as formas em que são encontradas e essa proteção deve cobrir a infraestrutura para seu uso, os processos, sistemas e serviços relacionados. As autoras dizem que a proteção deve ser correspondente ao valor que a informação tem e deve considerar também o que representam a perda ou acesso indevido dessa informação para a organização.

Para que se tenha a proteção da informação, as organizações precisam aplicar controles de segurança física e lógica em suas operações, orientadas por uma Política de Segurança da Informação, conforme Moura e Gaspary (2008). Segundo Marciano (2006), as Políticas de Segurança da Informação abrangem recursos computacionais, recursos humanos, infraestrutura e logística. Segundo a ABNT (2005), a Política de Segurança da Informação serve como orientação e apoio da direção da organização para as iniciativas de segurança da informação, e deve expressar as intenções e diretrizes globais para preservação da confidencialidade, da integridade e da disponibilidade da informação. Fernandes e Abreu (2008) afirmam que a Política de Segurança da Informação determina formalmente as diretrizes e ações referentes não só à segurança dos aplicativos, da infra-

estrutura e dos dados, mas também das pessoas e de outras organizações, como fornecedores e parceiros. A necessidade de proteger a informação está ligada, portanto, à sua importância para continuidade das operações da organização e ao nome e imagem da organização, e essa necessidade envolve a proteção de aspectos físicos, lógicos e humanos relacionados às informações.

Silva e Stein (2007) afirmam que a segurança da informação tem duas faces com características diferentes e, por vezes, conflitantes: a tecnologia e os seres humanos. Já Sêmola (2003) apresenta três aspectos para classificar a gestão da segurança da informação: tecnológicos, físicos e humanos.

Para as organizações que tem a obrigação legal de proteger informações suas ou de terceiros, sejam elas armazenadas de forma temporária ou definitiva, como organizações que prestam serviços de saúde, a necessidade de proteger essas informações é ainda mais evidente. Nesse contexto, as normas de segurança da informação são importantes balizadores, servindo como orientação para a adoção de controles que visam proteger as informações em uma diversidade de organizações e sobre diferentes aspectos, com destaque para a norma NBR ISO/IEC 27002:2005, um dos modelos mais destacados (Moraes; Mariano, 2008).

A NORMA ABNT NBR ISO/IEC 27002:2005

Os modelos, padrões e normas de segurança da informação representam um papel importante na elaboração de um roteiro de segurança da informação (Karabacak; Sogukpinar, 2006), e praticamente todas as normas sobre segurança da informação tem origem no Governo Britânico (Fernandes; Abreu, 2008), que, através do British Standards Institute (BSI), criou em 1995 e revisou em 1999 a British Standard 7799 (BS 7799). Esta norma foi adotada pela International Organization for Standardization (IOS) em 2000 com o nome ISO/IEC 17799:2000, como ficou mais conhecida, sendo adotada por organizações de todo o mundo, inclusive pela ABNT, com o nome NBR ISO/IEC 17799. Em 2005, a norma foi revisada e passou a se chamar ISO/IEC 27002:2005, o que fez com que a ABNT alterasse o nome da versão brasileira para NBR ISO/IEC 27002:2005, como é atualmente conhecida e como será tratada neste trabalho.

Para Martins e Santos (2005), a norma surgiu quando organizações de todo o mundo passaram aumentar seus investimentos em segurança da informação, mas esse investimento muitas vezes era feito sem orientação. Ainda para os autores, após sua publicação, a norma passou a ser referenciada como sinônimo de segurança da informação. A NBR ISO/IEC 27002:2005 está organizada em 11 seções de controles, que podem ser compostos de uma ou mais categorias de controles, formando um total de 39 categorias de controles, que, por sua vez, contêm um ou mais controles de segurança da informação, num total de 133 controles de segurança da informação, estabelecendo, assim, uma diretriz e os princípios de gestão da segurança da informação (Fernandes; Abreu, 2008). Antes de uma organização adotar controles de segurança da informação conforme a NBR ISO/IEC 27002:2005, é preciso diagnosticar a lacuna entre o que está previsto na norma e o que efetivamente é adotado ou utilizado. Existem diversas ferramentas que permitem avaliar a aderência à norma, tanto visado certificação da organização quanto servir como guia para estabelecer um sistema de gestão de segurança da informação, segundo Karabacak e Sogukpinar (2006). Estes autores utilizaram o Information Security Risk Analysis Method (ISRAM) para realizar uma pesquisa visando expressar os riscos de segurança da informação de forma quantitativa.

A norma não trata de questões técnicas, mas dos riscos para o negócio e das informações propriamente ditas (Karabacak; Sogukpinar, 2006). Dessa forma, a avaliação da conformidade de uma organização à norma não deve ser restrita aos profissionais da área técnica de TI ou aos que trabalham diretamente com segurança da informação, mas deve se estender também aos gestores e pessoas que trabalham na área administrativa e demais áreas de apoio ou mesmo na área fim da organização, o que pode permitir um diagnóstico mais completo.

Apesar de a norma propor uma série de controles e de haver diversas ferramentas e metodologias para análise de riscos e implementação de controles de segurança da informação (Cavalli et al., 2004), é preciso identificar quais controles são necessários para mitigar os riscos associados antes de fazer a avaliação e de acordo com a realidade e necessidades das organizações (Albuquerque Junior; Santos, 2011). Martins e Santos (2005) afirmam que nem sempre a adoção de todos os mecanismos existentes na norma é necessária e a ABNT (2005) diz que parte dos controles da NBR ISO/IEC 27002:2005 pode ser selecionada, de acordo com os requisitos e necessidades de segurança da informação de cada organização, e que convém que a seleção considere as leis e regulamentos relevantes para a organização.

SEGURANÇA DA INFORMAÇÃO EM SERVIÇOS DE SAÚDE

Para Kobayashi e Furuie (2007), a TI permeia todas as atividades de um hospital, incluindo a admissão e o tratamento dos pacientes, o acompanhamento do almoxarifado de medicamentos e outros suprimentos, além da disponibilidade de leitos. Os autores dizem também que a utilização de TI nesse contexto tem levado à evolução dos registros médicos, que tem gradualmente deixado de ser feitos em papel para serem feitos em sistemas informatizados, ou Registros Eletrônicos de Saúde (RES).

Da mesma forma que acontece com organizações que atuam em outras áreas, a quantidade e diversidade de informações que precisam ser armazenadas, processadas e gerenciadas pelos hospitais levam à necessidade de estabelecer controles de segurança, mas com a preocupação adicional com a ética no tratamento dos dados dos pacientes, que está regulada em diferentes normas legais, como será apresentado adiante.

A utilização de TI nos hospitais para armazenamento e processamento de informações de pacientes se dá em um ambiente onde há interação, comunicação e troca de informações eletrônicas, tanto entre diferentes setores internos (Ruotsalainen, 2004) quanto por diferentes entidades que interagem com o hospital (Kwak, 2005), e que precisam dessas informações para diferentes finalidades (Kobayashi; Furuie, 2007). Em muitos casos, ocorrem acessos externos por empresas de seguro de vida e operadores de planos de saúde, organismos de saúde pública e programas sociais, entre outras organizações, e os acessos de dentro da própria organização podem ser feitos por médicos diferentes, por áreas de apoio responsáveis por controle de qualidade e gerenciamento de suprimentos, por exemplo. Dessa forma, é necessário discutir padrões, questões éticas, privacidade, confidencialidade e segurança das informações dos pacientes (Raghupathi; Tan, 2002).

A falta de controles, procedimentos e políticas de segurança da informação pode levar ao uso indevido dos sistemas de informação dos serviços de saúde, o que pode desencorajar o uso de TI pelos hospitais e o compartilhamento de informações pelos pacientes, comprometendo o tratamento e a pesquisa médica (Kobayashi; Furuie, 2007).

Como reflexo dessas questões éticas e tecnológicas e com o desenvolvimento e crescimento da utilização da TI, que inclui os acessos remotos a sistemas e bancos de dados o crescimento da utilização de dispositivos móveis de acesso à Internet e a redes de computadores, o Conselho Federal de Medicina (CFM) tem emitido diversos pareceres em resposta a consultas sobre captura, armazenamento e transmissão de dados em serviços de saúde (Salvador; Almeida Filho, 2005), o que leva à necessidade de conhecer a legislação que trata do tema.

NORMAS LEGAIS SOBRE SEGURANÇA DA INFORMAÇÃO VOLTADAS PARA HOSPITAIS

A preocupação com segurança da informação em hospitais está regulada por uma série de leis e resoluções, que fazem diversas exigências para garantir a proteção de informações sobre os pacientes, que podem estar em bancos de dados de prontuários médicos ou de informações financeiras. A Constituição Federal de 1988 assegura o direito à privacidade no seu Artigo 5º, inciso X. Este mesmo artigo traz no seu inciso XIV a garantia do sigilo profissional onde houver necessidade de ampla confidência entre duas partes, contexto em que está inserida a relação entre médico e paciente. Complementando esta garantia constitucional, o Código Penal Brasileiro (Decreto-Lei Nº 2.848/1940) estabelece no Artigo 154 a pena por violação de informação de que se tenha ciência em razão de exercício de profissão.

Outras normas infraconstitucionais também tratam de assuntos relacionados à segurança das informações sobre pacientes. A Lei Nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), diz no Artigo 10 que os hospitais e outros estabelecimentos de atenção à saúde de gestantes, sejam eles públicos ou privados, são obrigados a manter registro das atividades desenvolvidas em prontuários individuais, pelo prazo de dezoito anos e identificar os recém-nascidos mediante o registro de sua impressão plantar e impressão digital e da impressão digital da mãe. A Lei 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), garante ao consumidor o direito de acesso a informações pessoais arquivadas nos bancos de dados de hospitais. Já a Lei Nº 9.434/1997 diz, no seu Artigo 3º, que os prontuários médicos contendo resultados ou laudos de exames referentes a diagnóstico de morte encefálica e detalhando atos cirúrgicos de transplantes e enxertos, além de outros documentos, devem ser mantidos pelas instituições por pelo menos cinco anos.

O CFM vem reforçando a necessidade de garantir segurança das informações dos pacientes. A Resolução CFM Nº 1.931/2009 (Código de Ética Médica, de 17 de setembro de 2009) proíbe que o médico permita o manuseio dos prontuários dos pacientes por pessoas não sujeitas ao sigilo profissional, diz que o prontuário deve ser legível e ficar sob guarda do médico ou da instituição que presta assistência ao paciente e que o médico não pode negar ao

paciente acesso ao seu prontuário nem permitir que eles sejam copiados sem autorização escrita dos pacientes. De forma adicional, a Resolução CFM Nº 1.331/89 diz que o prontuário médico deve ser mantido permanentemente pelos estabelecimentos de saúde.

Essas normas visam proteger os pacientes com relação às suas informações, que são processadas e armazenadas nos hospitais. Para Salvador e Almeida Filho (2005), embora os códigos de ética dos profissionais de saúde exijam o sigilo e a privacidade das informações sobre os pacientes, o mau uso da TI vem facilitando o extravio, o acesso e a alteração indevidos. Há, portanto, uma necessidade clara de proteger os sistemas e bancos de dados utilizados nos hospitais, onde são armazenadas informações cujo sigilo é obrigatório. Muitos desses sistemas e bancos de dados estão acessíveis e disponibilizadas nas redes de computadores dos hospitais, que facilitam o acesso para quem analisa e alimenta esses dados, mas aumentam a possibilidade de acesso por pessoas não autorizadas, seja intencional ou não.

METODOLOGIA

Esta pesquisa é de caráter exploratório e descritivo, de metodologia dedutiva, que teve o objetivo de identificar a percepção de funcionários das áreas de TI, segurança da informação ou gestão de hospitais privados brasileiros a respeito da importância das práticas de segurança da informação propostas pela norma NBR ISO/IEC 27002:2005 no desempenho de suas atividades, e envolveu três etapas principais: pesquisa bibliográfica sobre segurança da informação de maneira geral e aplicada a serviços de saúde; coleta de dados, em que foram identificados os possíveis respondentes juntamente com seus respectivos endereços eletrônicos, e onde foram enviadas as mensagens convidando para participar da pesquisa e contendo os endereços para os formulários; e análise dos dados, em que os dados coletados foram analisados à luz da teoria sobre o tema.

A pesquisa foi realizada entre os meses de janeiro e junho de 2012, quando foram preenchidos os formulários eletrônicos disponibilizados na Internet através do serviço FormSus do Ministério da Saúde (http://formsus.datasus.gov.br), cujos endereços de acesso foram enviados para os endereços de correio eletrônicos das diretorias, áreas de TI, ouvidorias e áreas de comunicação identificados em pesquisas na Internet de 173 hospitais particulares localizados em todos os estados brasileiros e no Distrito Federal. Cada formulário solicitava informações sobre o respondente (cargo ou função, área em que trabalha), informações sobre o hospital (quantidade de leitos, estado em que está localizado e regime de funcionamento) e continha 235 afirmativas, adaptadas dos 210 itens de auditoria presentes no formulário ISRAM, utilizado por Karabacak e Sogukpinar (2006) para avaliar a aderência aos 133 controles da norma ISO/IEC 27002:2005. As 235 afirmativas dos três formulários correspondem às práticas de segurança da informação pesquisadas neste estudo e foram associados a uma escala Likert de cinco pontos (1 – sem importância; 2 – pouco importante; 3 – importante; 4 – muito importante; 5 – extremamente importante) onde os respondentes deveriam indicar a importância percebida de cada prática nas atividades desenvolvidas pelo hospital.

Para reduzir o tamanho do instrumento de coleta e para permitir que as respostas fossem dadas por pessoas com conhecimentos específicos sobre os assuntos tratados nas afirmativas, decidiu-se por agrupar as perguntas em três formulários, conforme classificação proposta por Silva Netto e Silveira (2007) para os controles da norma: Práticas de Segurança da Informação para a Camada Lógica, com 35 itens; Práticas de Segurança da Informação para a Camada Física, com 150 itens; e Práticas de Segurança da Informação para a Camada Humana, com 68 itens. As importâncias percebidas das práticas foram calculadas somando as notas dadas pelos respondentes para cada prática, resultando nos respectivos scores. Os resultados da análise dos dados estão na seção seguinte.

APRESENTAÇÃO E ANÁLISE DOS DADOS

Os formulários foram enviados para 173 hospitais de todo o Brasil, mas cinco estados não tiveram formulários respondidos: Piauí, Rondônia, Roraima, Sergipe e Tocantins. A Tabela 1 mostra as quantidades de hospitais que responderam aos três formulários nos outros 22 estados. Embora os formulários tivessem um campo para os respondentes informarem o porte do hospital segundo a classificação da Portaria nº 2.224/2002 do Ministério da Saúde, apenas dois formulários foram respondidos com essa informação (ambos indicando serem de porte IV). Apesar disso, todos os respondentes informaram a quantidade de leitos dos hospitais. Os resultados mostram que as quantidades de leitos são variadas. Dos 48 hospitais, 15 tem até 15 leitos (31,3%), 20 tem entre 51

e 150 leitos (41,7%), 10 tem entre 151 e 500 leitos (20,8%) e três tem mais de 500 leitos (6,3%), conforma pode ser visto na Tabela 2.

Na maioria dos hospitais, os três formulários foram respondidos pela mesma pessoa ou por pessoas que ocupam o mesmo cargo e trabalham na mesma área, mas, em alguns casos, os três formulários foram respondidos por pessoas diferentes, que trabalham em áreas diferentes e ocupam cargos diferentes nos hospitais. A Tabela 3 mostra as quantidades e percentuais de respondentes para cada cargo ocupado no hospital, segundo as respostas obtidas nos formulários Práticas de Segurança da Informação para a Camada Física, Humana e Lógica. Analisando a tabela, é possível perceber que a quantidade de Administradores foi menor nas respostas dos formulários para camada física (16 respondentes), talvez por ser este o formulário que tem questões mais técnicas. Outro indício disso é o fato de 50% das respostas deste formulário terem sido dadas por Analistas. Já a Tabela 4 mostra as áreas em que trabalham os respondentes dos três formulários nos 48 hospitais. Nesta tabela, é possível observar que a maioria dos respondentes dos três formulários trabalha na área de gestão ou na diretoria dos seus hospitais: 31 (64,6%) dos respondentes do formulário Práticas de Segurança da Informação para a Camada Lógica; 24 (50,0%) dos respondentes do formulário Práticas de Segurança da Informação para a Camada Física; e 23 (47,9%) dos respondentes do formulário Práticas de Segurança da Informação para a Camada Humana.

Do formulário Práticas de Segurança da Informação para a Camada Física, foi possível identificar que o score máximo foi 218, correspondente à prática Existência de procedimentos formais de registro e cancelamento de registro de usuários para concessão de acesso a todos os serviços e sistemas de informação, sendo esta a prática considerada mais importante, enquanto o score mínimo foi 144, correspondente à prática Cobertura dos equipamentos por seguros e cumprimento dos requisitos das seguradoras, sendo esta a prática considerada menos importante. A média calculada para este formulário foi 188,43, e a mediana calculada foi 187. O desvio padrão calculado foi 16,166 e a moda foi 175, score obtido por oito práticas. A variância calculada foi 261,324.

Entre as práticas do formulário Práticas de Segurança da Informação para a Camada Lógica, a que teve maior score foi Existência de procedimentos para controlar a instalação de software visando minimizar o risco de danos em sistemas operacionais, com 214 pontos, e a que teve menor score foi Utilização de acordos de licença, acordos judiciais e exigências contratuais para garantia da qualidade, e realização de testes antes da utilização dos softwares para detectar códigos maliciosos, com 165 pontos. A média foi 185,21, a mediana foi 180, o desvio padrão foi 14,559. A variância calculada foi 211,956. Sete valores de scores tiveram frequência igual a dois, sendo que dois foi a maior frequência de score para este formulário entre os 29 scores calculados.

Para o formulário Práticas de Segurança da Informação para a Camada Humana, que tinha 62 práticas, os cálculos mostram que o score máximo foi 227, obtido pela prática Existência de uma Política de Segurança da Informação aprovada pela gerência, publicada e comunicada apropriadamente para todos os funcionários, e o score mínimo foi 156, obtido pela prática Existência de um processo disciplinar formal para funcionários que tenham cometido violação de segurança. A média dos scores deste formulário foi 191,82, a mediana foi 191,5, o desvio padrão foi 13,838 e os scores 192 e 205 foram os que tiveram maior freqüência – cinco vezes cada. A variância calculada para as práticas deste formulário foi 191,493.

Considerando como mais importantes as práticas que ficaram acima da média calculada para cada formulário, observa-se que, das 29 práticas da camada lógica, 12, ou 41,38%, obtiveram scores acima da média, e estão representadas na Tabela 5. Para a camada física, observa-se que 69 práticas obtiveram scores acima da média, o que corresponde a 47,91% do total de 144 práticas. Diante da grande quantidade de práticas que obtiveram score acima da média e para fins de comparação com as práticas da camada lógica, a Tabela 6 apresenta apenas as 12 práticas que obtiveram score mais alto para esta camada. Já para as 62 práticas da camada humana, 36 tiveram score acima da média, que correspondem a 58,06% do total. Da mesma forma que foi feito com as práticas da camada física, a Tabela 7 apresenta apenas as 12 práticas que obtiveram score mais elevado.

Analisando os scores mais altos das práticas dos três formulários, percebe-se uma preocupação geral dos respondentes o estabelecimento de procedimentos e políticas relacionadas à segurança da informação, além de práticas de controle de acesso físico e lógico. É possível identificar também uma preocupação com a garantia da disponibilidade dos recursos em caso de incidentes que comprometam as informações ou os meios de armazenamento ou processamento, bem como a possibilidade de recuperação das operações em caso de incidentes. O controle direto sobre os ativos de informação, como inventários e medidas para devolução de ativos ao final de contratos, é uma preocupação constante também. Destaca-se a importância de se estabelecer uma Política de Segurança da Informação nos hospitais, visto que a prática Existência de uma Política de Segurança da

Informação aprovada pela gerência, publicada e comunicada apropriadamente para todos os funcionários, da camada humana, foi a que obteve score mais alto entre todas as práticas dos três formulários – 227 pontos. Esta prática foi considerada extremamente importante por 35 respondentes (72,9%) e muito importante por 13 respondentes (27,1%).

As respostas destacam também a importância de práticas visando a proteção de dados sensíveis ou cuja proteção é exigida por normas legais: a prática Existência de procedimentos de teste que não utilizam informações pessoais ou sensíveis armazenadas em bancos de dados, que teve 207 pontos de score, foi a segunda prática mais importante para os respondentes do formulário Práticas de Segurança da Informação para a Camada Lógica. A prática Garantia de que os dados e a privacidade são protegidos de acordo com a legislação, com os regulamentos e, se for o caso, com as cláusulas contratuais pertinentes, que foi a terceira mais importante do formulário Práticas de Segurança da Informação para a Camada Humana, com 212 pontos. Já a prática Classificação das informações pelo seu valor, por requisitos legais, sensibilidade e criticidade para a organização, que foi a quinta mais importante do formulário que trata da camada humana, teve 211 pontos de score. E a prática Proteção de registros importantes para a organização contra perda por destruição e falsificação, conforme as exigências estatutárias, regulamentares, contratuais e de negócio, também do formulário contendo práticas da camada humana, teve 204 pontos de score. A importância percebida a respeito de cada uma dessas quatro práticas demonstra que os respondentes tem uma preocupação com o estabelecimento de boas práticas de segurança da informação que são diretamente relacionadas ao processamento e armazenamento de informações sobre os pacientes, o que pode ser motivado pelo fato de os respondentes terem consciência dos requisitos legais que envolvem a questão.

Analisando a prática que obteve score mais alto – Existência de uma Política de Segurança da Informação aprovada pela gerência, publicada e comunicada apropriadamente para todos os funcionários –, sua importância fica ainda mais clara ao se observar que a média calculada exclusivamente para ela foi 4,73, muito próxima da avaliação mais alta possível (5 – Extremamente importante). Isso demonstra a percepção da importância de estabelecer uma política para a proteção das informações tratadas nos hospitais, que, via de regra, envolvem dados de pacientes, cujo sigilo é regulado por uma série de normas legais.

CONSIDERAÇÕES FINAIS

Este trabalho teve o objetivo de identificar as práticas de segurança da informação mais importantes segundo a percepção de funcionários das áreas de gestão, segurança da informação e TI de hospitais particulares de diferentes estados brasileiros, a partir de um modelo adaptado da metodologia proposta por Karabacak e Sogukpinar (2006) e utilizando como instrumentos de coleta três formulários disponibilizados na Internet e enviados por correio eletrônico para os contatos dos hospitais.

A prática mais importante identificada na pesquisa foi Existência de uma Política de Segurança da Informação aprovada pela gerência, publicada e comunicada apropriadamente para todos os funcionários, do formulário Práticas de Segurança da Informação para a Camada Humana. Destaca-se também as práticas Existência de procedimentos de teste que não utilizam informações pessoais ou sensíveis armazenadas em bancos de dados, segunda prática mais importante para os respondentes do formulário Práticas de Segurança da Informação para a Camada Lógica, Garantia de que os dados e a privacidade são protegidos de acordo com a legislação, com os regulamentos e, se for o caso, com as cláusulas contratuais pertinentes, a terceira mais importante do formulário Práticas de Segurança da Informação para a Camada Humana, Classificação das informações pelo seu valor, por requisitos legais, sensibilidade e criticidade para a organização, a quinta prática mais importante do formulário que trata da camada humana, e a prática Proteção de registros importantes para a organização contra perda por destruição e falsificação, conforme as exigências estatutárias, regulamentares, contratuais e de negócio, também do formulário relacionado à camada humana, todas elas relacionadas diretamente com a obrigação de proteger os dados dos pacientes.

Assim, a importância das práticas de segurança da informação segundo a percepção dos respondentes aponta para uma necessidade de estabelecer políticas, normas e procedimentos relativos à segurança da informação nos hospitais, além de uma preocupação com o sigilo dos dados utilizados e armazenados nos hospitais, o que remete à obrigação legal das instituições de saúde de proteger dados dos seus pacientes.

O trabalho tem como limitações a pequena quantidade de respondentes (48) diante da quantidade de hospitais que receberam os formulários da pesquisa (173) – 27,74% do total; não foi feita uma análise baseada no porte dos hospitais, o que fica como sugestão para trabalho futuro; embora as perguntas tenham sido divididas em

três formulários, um dos formulários ficou muito extenso, o que pode ter dificultado a participação dos gestores e funcionários. Como estudos futuros, sugere-se: pesquisa semelhante com hospitais públicos; pesquisa sobre adoção das práticas de segurança da informação consideradas mais importantes e sobre a efetividade dessas práticas; e sobre as implicações dessas práticas nas atividades desempenhadas pelos profissionais de saúde.

REFERÊNCIAS

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. 120p.

ALBUQUERQUE JUNIOR, A. E. de; SANTOS, E. M. dos. Controles e Práticas de Segurança da Informação em um Instituto de Pesquisa Federal. In: VIII Simpósio de Excelência em Gestão e Tecnologia – SEGeT, Resende, 2011. Anais... Resende: AEDB, out. 2011, 17 p.

BEAL, A. Segurança da Informação: Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações. São Paulo: Atlas, 2005. 180p.

CARUSO, C. A. A.; STEFFEN, F. D. Segurança em Informática e de Informações. São Paulo: SENAC, 2 ed. 1999. 368p.

CAVALLI, E., MATTASOGLIO, A., PINCIROLI, F., SPAGGIARI, P. Information Security Concepts and Practices: The Case of a Provincial Multi-Specialty Hospital. International Journal of Medical Informatics. v.73, n.3, p.297-303. 2004.

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: XXXII Encontro da ANPAD – EnANPAD. Rio de Janeiro, 2008. Anais... Rio de Janeiro: ANPAD, set.2008, 16 p. 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. 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. 2ª. ed., Rio de Janeiro, Brasport, 2008. 444p.

HERATH, T.; HERATH, H.; BREMSER, W. G. Balanced Scorecard Implementation of Security Strategies: A Framework for IT Security Performance Management. Information Systems Management. Londres: Taylor & Francis, n.1, v.27, p.72-81, jan.2010.

KARABACAK, B.; SOGUKPINAR, I. A Quantitative Method for ISO 17799 Gap Analysis. Computers & Security. n.25, p.413-419, 2006.

KAYO, E. K.; KIMURA, H.; MARTIN, D. M. L.; NAKAMURA, W. T. Ativos Intangíveis, Ciclo de Vida e Criação de Valor. RAC. n.3, v.10, p.73-90, jul.2006.

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: 7th International Workshop on Enterprise Networking and Computing in Healthcare Industry – HEALTHCOM 2005. Proceedings... Busan, jun. 2005. p.18-23.

MANDARINI, M. Segurança Corporativa Estratégica. São Paulo: Usina do Livro, 2004. 350p.

MARCIANO, J. L. P. Segurança da Informação – uma abordagem social. Brasília, 2006. 211f. Tese (Doutorado em Ciência da Informação) – Universidade de Brasília, Brasília, 2006.

MARTINS, A. B.; SANTOS, C. A. S. Uma Metodologia para Implantação de um Sistema de Gestão de Segurança da Informação. JISTEM. v.2, n.2, p.121-136. 2005.

MELLO, L. B. B.; VASCONCELLOS, L. A.; BRAGANÇA, L. R.; MOTTA, O. M. Contribuição para Gestão de Ativos Intangíveis Organizacionais: Proposição de Um Modelo Baseado no Balenced Scorecard. VI Congresso Nacional de Excelência em Gestão – CNEG, 2010, Niterói. Anais... Niterói: CNEG, ago.2010. 24p.

MORAES, E. A. P.; MARIANO, S. R. H. Uma Revisão dos Modelos de Gestão em TI. IV Congresso Nacional de Excelência em Gestão – CNEG, 2008, Niterói. Anais... Niterói: CNEG, jul.2008. 19p.

MOURA, G. C. M.; GASPARY, L. P. Uma Proposta para Medição de Complexidade de Segurança em Procedimentos de Tecnologia da Informação. In: VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais – SBSEG, 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: XXXIV Encontro da ANPAD – EnANPAD. 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.

RUOTSALAINEN, P. A. A Cross-platform Model for Secure Electronic Health Record Communication. International Journal of Medical Informatics. v.73, n.3, p.291-295. 2004.

SALVADOR, V. F. M.; ALMEIDA FILHO, F. G. V. Aspectos Éticos e de Segurança do Prontuário Eletrônico do Paciente. In: II Jornada do Conhecimento e da Tecnologia, 2005, Marília. Anais... Marília: UNIVEM, ago. 2005, 8p.

SÊMOLA, M. Gestão da Segurança da Informação: uma visão executiva. Rio de Janeiro: Campus, 2003. 184p.

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, R. D. Análise de Requisitos de Segurança no Atendimento às Premissas de Contra-Inteligência. Brasília, 2009. 88f. Dissertação (Mestrado em Gestão do Conhecimento e Tecnologia da Informação) – Universidade Católica de Brasília, Brasília, 2009.

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.

Tabela 1: Quantidades de formulários preenchidos por estado do Brasil

ESTADO	QUANTIDADE DE RESPOSTAS
Acre	1
Alagoas	1
Amapá	1
Amazonas	2
Bahia	5
Ceará	2
Distrito Federal	1
Espírito Santo	2
Goiás	3
Maranhão	1
Mato Grosso	2
Mato Grosso do Sul	1
Minas Gerais	4
Pará	1
Paraíba	2
Paraná	2
Pernambuco	1
Rio de Janeiro	5
Rio Grande do Norte	1
Rio Grande do Sul	2
Santa Catarina	1
São Paulo	7
TOTAL	48

Tabela 2: Quantidades hospitais para as faixas de quantidades de leitos

FAIXA DE QUANTIDADE DE LEITOS	QUANTIDADE DE HOSPITAIS	%
Até 50 leitos	15	31,3
De 51 a 150 leitos	20	41,7
De 151 a 500 leitos	10	20,8
Mais de 500 leitos	3	6,3
TOTAL	48	100

Tabela 3: Cargos ou funções ocupadas pelos respondentes dos três formulários

CARGO OU FUNÇÃO	RESPOSTAS PARA CAMADA FÍSICA		RESPOSTAS PARA CAMADA HUMANA		RESPOSTAS PARA CAMADA LÓGICA	
	QTDE.	%	QTDE.	%	QTDE.	%
Administrador	16	33,3	17	35,4	19	39,6
Analista	24	50,0	24	50,0	22	45,8
Gerente de TI	5	10,4	5	10,4	4	8,3
Gerente (outras áreas)	2	4,2	1	2,1	2	4,2
Diretor (outras áreas)	1	2,1	1	2,1	1	2,1
TOTAIS	48	100	48	100	48	100

Tabela 4: Áreas em que trabalham os respondentes dos três formulários

ÁREA DE TRABALHO	RESPOSTAS PARA CAMADA FÍSICA		RESPOSTAS PARA CAMADA HUMANA		RESPOSTAS PARA CAMADA LÓGICA	
	QTDE.	%	QTDE.	%	QTDE.	%
Gestão/Diretoria	24	50,0	23	47,9	31	64,6
Tecnologia da Informação	17	35,4	19	39,6	12	25,0
Segurança da Informação	6	12,5	6	12,5	4	8,3
Outras	1	2,1	-	-	1	2,1
TOTAIS	48	100	48	100	48	100

Tabela 5: As 12 práticas consideradas mais importantes para a camada lógica

PRÁTICA	SCORE
Existência de procedimentos para controlar a instalação de *software* visando minimizar o risco de danos em sistemas operacionais	214
Existência de procedimentos de teste que não utilizam informações pessoais ou sensíveis armazenadas em bancos de dados	207
Proteção de chaves secretas e privadas contra divulgação não autorizada	206
Supervisão e controle do desenvolvimento de software realizado por terceiros	206
Existência de processo ou procedimento para revisão e teste de aplicações críticas para o negócio para impactos adversos nas operações e na segurança após mudanças nos sistemas operacionais	205
Atualização periódica de sistemas operacionais com *service packs*, *patches*, *hot fixes*, etc	205
Proteção física dos equipamentos utilizados para gerar e armazenar chaves de criptografia	202
Controle sobre todas as alterações em sistemas e aplicações	195
Proteção contra modificações, perda e destruição das chaves de criptografia	193
Restrição de acesso a códigos fonte de programas para evitar mudanças não autorizadas e não intencionais	191
Existência de um processo rigoroso de controle sobre a implementação de mudanças em sistemas de informação para evitar que esses sistemas sejam corrompidos	191
Realização das modificações em pacotes de software apenas quando há necessidade	189

Tabela 6: As 12 práticas consideradas mais importantes para a camada física

PRÁTICA	SCORE
Existência de procedimentos formais de registro e cancelamento de registro de usuários para concessão de acesso a todos os serviços e sistemas de informação	218
Implementação de uma barreira de segurança física para proteger o serviço de processamento de informações	216
Disponibilização de sistemas sensíveis em ambiente computacional dedicado (isolado)	216
Existência de controles eficazes de entrada para permitir que somente pessoas autorizadas acessem diferentes áreas dentro da organização	215
Desenvolvimento e revisão de uma política de controle de acesso com base nos requisitos de negócio e de segurança	215
Utilização de mecanismos de segurança de perímetro, como *firewalls*, para separação entre a rede utilizada por parceiros de negócio ou terceirizados e a rede da organização	215
Existência de proteções físicas contra danos provocados por incêndios, inundações, explosões, distúrbios civis e outras formas de desastres naturais ou provocados pelo homem	214
Controle de alocação e realocação de senhas através de processo formal de gestão	212
Existência de uma política sobre redes e serviços de rede	212
Controle de acesso ao sistema operacional por procedimento de log-on seguro	212
Execução e testes regulares de backups de informações e de software de acordo com a política de *backup*	211
Limitação do acesso dos usuários apenas aos serviços que eles foram especificamente autorizados a usar	211

Tabela 7: As 12 práticas consideradas mais importantes para a camada humana

PRÁTICA	SCORE
Existência de uma Política de Segurança da Informação aprovada pela gerência, publicada e comunicada apropriadamente para todos os funcionários	227
Identificação de todos os ativos e manutenção de inventário ou registro com todos os ativos importantes	213
Garantia de que os dados e a privacidade são protegidos de acordo com a legislação, com os regulamentos e, se for o caso, com as cláusulas contratuais pertinentes	212
Aprovação da revisão da Política de Segurança da Informação	211
Classificação das informações pelo seu valor, por requisitos legais, sensibilidade e criticidade para a organização	211
Existência de um processo para garantir que todos os funcionários, contratados e terceiros entreguem todos os ativos da organização em seu poder ao término de seu acordo, contrato ou contrato de trabalho	209
Identificação, documentação e implementação de regulamentos para o uso aceitável de informações e ativos associados a instalações de processamento de informações	206
Definição de um conjunto apropriado de procedimentos para rotulagem e manuseio de informações, conforme o esquema de classificação adotado pela organização	206
Identificação dos eventos que causam interrupção dos processos de negócio juntamente com a probabilidade de ocorrência e o impacto dessas interrupções e suas consequências para a segurança da informação	205
Remoção ou alteração dos direitos de acesso de todos os funcionários, fornecedores e terceiros a informações e instalações de processamento de informação ao fim ou em caso de alteração de seus contratos, acordos ou contratos de trabalho	204
Proteção de registros importantes para a organização contra perda por destruição e falsificação, conforme as exigências estatutárias, regulamentares, contratuais e de negócio	204
Estabelecimento do compromisso dos gestores e definição da abordagem organizacional para gerenciamento da segurança da informação na Política de Segurança da Informação	203