DOI: 10.5748/9788599693148-15CONTECSI/PS-5823

Information Security and Healthcare: a systematic review of the literature
Segurança da Informação e a Área da Saúde: revisão sistemática da literatura

Cristiana Fernandes De Muÿlder, 0000-0002-0813-0999, (Universidade FUMEC, MG, Brasil) - cristiana.muylder@fumec.br
Jeferson Gonçalves de Oliveira, 0000-0003-4936-5820, (Universidade FUMEC, MG, Brasil) – jeferson.oliveirabh@gmail.com
Cássio Luís Batista, 0000-0002-0278-2232, (Universidade FUMEC, MG, Brasil) – batista@fumec.br
Rodrigo Moreno Marques, 000-0002-6320-4874, (Universidade FUMEC, MG, Brasil) – rodrigo.marques@fumec.edu.br

Abstract
It is understood that information security is a critical problem in recent years regardless of area or business. Regarding the health area, it is related to the greater use of information systems containing patient data and treatments. In this context, we tried to answer the following problem: What are the main information security frameworks used in the health area? The objective of this article is to systematically review articles that address studies on health information security and to identify the main frameworks and focus of information security discussion cited in the literature. We selected articles in English, indexed as of year 2008, from the Web of Science, Scopus and Ebsco bases where some studies on the subject were found. More generic frameworks, such as the ISO / IEC 27001 family, were the most cited and the lowest occurrence of those specific to the health area, such as ISO / IEC 27779 and HIPAA. Thus, there is a possible gap in the discussion of the relevance of information security in the area of health that instigates new studies.

Keywords: Information, Security, Frameworks, Healthcare, Privacy

Resumo
Entende-se que a segurança da informação é um problema crítico nos últimos anos independente da área ou negócio. Com relação à área da saúde, a está relacionada a maior utilização de sistemas de informação contendo dados de pacientes e tratamentos. Neste contexto, buscou-se responder ao seguinte problema: Quais são os principais frameworks de segurança da informação utilizados na área de saúde? O objetivo deste artigo consiste em revisar sistematicamente artigos que abordam estudos sobre a segurança da informação na saúde e identificar os principais frameworks e focos de discussão de segurança da informação citados na literatura. Foram selecionados artigos em inglês, indexados a partir do ano de 2008, das bases Web of Science, Scopus e Ebsco onde alguns estudos sobre o tema foram encontrados. Frameworks mais genéricos, como a família ISO/IEC 27001, foram os mais citados e menor ocorrência daqueles específicos para a área de saúde, como o ISO/IEC 27779 e o HIPAA. Observa-se, assim, uma possível lacuna na discussão da relevância da segurança da informação na área da saúde que instiga novos estudos.

Palavras-Chave: Informação, Segurança, Frameworks, Saúde, Privacidade

Agradecimento a agências de fomento CAPES, CNPq e FAPEMIG e centro de pesquisa GEICE e Nupad.

1. Introdução

Com o desenvolvimento tecnológico e melhoria na utilização dos recursos da Internet, comunicação móvel, computação em nuvem, percebe-se que ocorre uma verdadeira explosão de informação em todas as áreas de conhecimento.

Na área da saúde estes avanços permitiram gerar novas tecnologias e aplicações inovadoras. Entretanto, a informática em saúde apresenta algumas barreiras que dificultam sua adoção em larga escala. Destacam-se as questões associadas à privacidade e segurança da informação.

A segurança da informação pode ser considerada um desafio para instituições de saúde que devem garantir a privacidade e confidencialidade dos dados do paciente e, ao mesmo tempo, proporcionar o registro, acesso e compartilhamento de informações entre profissionais, equipes e serviços de saúde. Um primeiro passo fundamental nesse sentido é definir uma Política de Segurança da Informação, descrevendo, por exemplo: os deveres dos usuários, como evitar infrações éticas e como as informações disponíveis podem ser utilizadas.

Desde a edição de 2014, a pesquisa TIC Saúde (Comitê Gestor da Internet No Brasil, 2015) vem investigando nos estabelecimentos de saúde brasileiros a adoção de ferramentas e processos voltados à segurança da informação, importantes para a garantia da integridade e sigilo dos dados tanto dos próprios estabelecimentos quanto dos pacientes atendidos. Dentre os estabelecimentos que usaram a Internet, 24% disseram possuir algum documento que define uma política de segurança da informação, sendo que esse tipo de documento foi mais encontrado entre os estabelecimentos privados (30%), os localizados em capitais (41%) e aqueles com mais de 50 leitos de internação (48%). Além disso, a proporção dos estabelecimentos com uma área de tecnologia da informação (TI) que disseram contar com um documento que define uma política de segurança da informação (45%) foi maior do que a daqueles que não possuem uma área ou departamento específico de TI (18%).

Diante desse cenário, este trabalho objetiva apresentar uma revisão sistemática da literatura que permita responder à pergunta: quais são os principais frameworks de segurança da informação citados nos trabalhos para a área de saúde? A partir da análise dos trabalhos indexados sobre segurança da informação na saúde buscou-se: i) identificar os principais frameworks de segurança da informação que estão sendo utilizadas na área da saúde; ii) identificar o principal foco dos estudos em relação à segurança da informação.

Como resultado, observa-se que a maioria dos estudos analisados citam frameworks mais genéricos, como a família ISO/IEC 27000, ao passo que normas específicas como a HIPAA e ISO/IEC 27779 são menos abordadas. Além disso, a "governança da segurança" e o fator "pessoas" revelam-se os principais focos dos estudos que compõem o corpus eleito pela presente pesquisa. Na sequência, apresentam-se as seções de referencial teórico, metodologia, resultados, trabalhos relacionados e as considerações finais.

2. Referencial teórico

A seção de referencial teórico aborda as legislações e frameworks de segurança da informação na saúde, os objetivos fundamentais da segurança da informação, a segurança

cibernética na saúde e a segurança da informação em soluções de nuvem e cliente-servidor.

2.1. Legislação e Frameworks de Segurança de informação na Saúde

Atualmente, há varias padronizações, ferramentas, frameworks e recomendações de melhores práticas para gerência e manutenção de serviços de Tecnologia da Informação que são aplicados a vários segmentos de negócio. As padronizações mais aplicadas são ISO/IEC 27002 em segurança da informação, COBIT, ISO 20000 e ITIL (Sahibudin, Sharifi, & Ayat, 2008).

Conforme apresentado por Sahibudin et al. (2008), a norma ISO/IEC 27002 é caracterizada pela preservação da Confidencialidade, Integridade e Disponibilidade. No ITIL, a disponibilidade é relacionada a aspectos de qualidade tais como confiabilidade, manutenção, capacidade de manutenção e resiliência. Quando a ITIL é comparada ao COBIT, observa-se que eles possuem um alto grau de correspondência, especialmente quando os processos do COBIT são baseados no ITIL.

De acordo com Orel e Bernik (2013), existe uma opinião geral que havia uma necessidade de mais especificidade na área de segurança da informação de saúde do que para outros domínios de informação. Posteriormente, a ISO 27799: 2008 (Informática em saúde - Gestão da segurança da informação na saúde usando ISO/IEC 27002) foi desenvolvida especificamente para ajudar as organizações de saúde a interpretar a padrão original ISO/IEC 27002: 2005.

Em 2009, foi promulgado nos Estados Unidos o American Recovery and Reinvestment Act -ARRA (EEUU, 2009), que impactou significativamente o desenvolvimento das tecnologias de informação em saúde, particularmente os Sistemas de Registros Eletrônicos de Saúde. O ARRA apresenta cinco objetivos: melhorar a qualidade médica, a segurança do paciente, a eficiência do tratamento de saúde e a redução das disparidades na saúde; engajar os pacientes e familiares; melhorar a coordenação do tratamento; assegurar a adequada privacidade e segurança da informação de saúde pessoal; beneficiar a população e a saúde pública (Hoyt & Yoshihashi, 2014).

Dentre as iniciativas importantes do ARRA, destacam-se as mudanças na privacidade e no ato da Portabilidade do Seguro de Saúde e Prestação de Contas (Health Insurance Portability & Accountability Act – HIPAA) criado em 1996. O HIPAA (EEUU, 1996) foi criado inicialmente para a portabilidade, privacidade e segurança da informação de saúde pessoal (Protect Health Information - PHI) que até então era principalmente registrada em fichas de papel. Em 2009 e 2013, a regulamentação passou por atualizações para cobrir melhor a transmissão eletrônica do PHI ou (ePHI). Este ato fez com que as organizações de saúde reavaliassem as questões que envolvem a privacidade e a segurança da informação em saúde.

Nos últimos anos, têm surgido uma série de brechas e identidades roubadas em organizações de saúde, aumentando as preocupações em relação à segurança e privacidade de informação. Segundo (Drevin, Kruger, Bell, & Steyn, 2017), o HIPAA é a legislação mais conhecida sobre a segurança e privacidade da informação. Nota-se que o HIPAA inclui cláusulas de proteção de direitos do usuário dos serviços de saúde como, por exemplo: ter acesso e obter cópia dos seus registros em saúde; corrigir ou complementar

suas informações; receber uma notificação que apresenta como a informação em saúde pode ser usada e compartilhada; ser consultado sobre a possibilidade de que suas informações sejam usadas ou compartilhadas para certos propósitos, tais como marketing; obter relatórios que informem quando e porque a informação em saúde foi compartilhada para certos propósitos; registrar uma reclamação com o provedor do serviço de saúde, seguradora de saúde e/ou Governo dos EEUU se os direitos são negados ou a informação em saúde não foi protegida.

A regra de segurança da HIPAA (EEUU, 1996) e a Health Information Technology for Economic and Clinical Health, conhecido como HITECH (EEUU, 2009), são um passo em direção a padrões que assegurem a segurança e a integridade das informações dos pacientes armazenadas ou transmitidas eletronicamente. Da mesma forma, a Lei de Proteção de Informações Pessoais e Documentos Eletrônicos (PIPEDA) também recebeu Assentimento Real no Canadá em 13 de abril de 2000 (Canada, 2000).

Já o padrão ISO 15026 introduz o conceito de um caso de garantia de segurança (He & Johnson, 2017). Pode ser definido como "um corpo de evidências documentado que fornece um argumento convincente e válido de que uma o sistema é adequadamente seguro para uma determinada aplicação em um dado meio ambiente".

He e Johnson (2017) usaram as recomendações em duas falhas de segurança ocorridas no Departamento de Assuntos de Veteranos nos Estado Unidos e na China, onde as recomendações do VA estão ligadas aos controles de segurança do Federal Information Security Management Act – FISMA (EEUU, 2002) e as relacionadas à China estão ligadas ao controle de segurança do GB/T22239-2008 (China, 2008).

O FISMA foi promulgado em lei em dezembro 17, 2002, como Título III do E-Government Act de 2002 e definiu os três objetivos fundamentais de segurança, apresentados neste trabalho, mais à frente, para os sistemas de informação do governo federal americano: (1) Confidencialidade; (2) Integridade e (3) Disponibilidade.

O GB/T22239-2008 (Information security technology - Baseline for classified protection of information system security) é uma padronização adotada na China a partir de 1/11/2008, na qual se classificam cinco níveis de segurança para a garantia de segurança da informação.
No Brasil, o acesso à informação pública é um direito fundamental do cidadão previsto na Constituição Federal e regulamentado pela Lei de Acesso à Informação (Lei 12.527, de 18 de novembro de 2011). Segundo a lei brasileira, a todo cidadão deve ser franqueado o acesso a informações produzidas ou custodiadas pelo Estado. A lei admite apenas restrições ao acesso às informações classificadas como sigilosas (por razões de segurança, saúde pública e privacidade das pessoas). Esse aparato legislativo regulamenta o amplo direito ao acesso à informação pública e determina o dever de o Estado gerir de forma eficiente a documentação governamental ou sob sua guarda, e viabilizar a possibilidade de acesso a todos. A Lei no 12.527/2011 trata de forma especial as informações pessoais e estabelece uma cláusula segundo a qual somente quando houver "evidente interesse público ou geral" ou nos casos "previstos em lei" o acesso aos dados pessoais poderá ser autorizado sem o consentimento da pessoa (Ventura, 2013).

O uso de dados pessoais em pesquisas em saúde tem regulamentação nacional, do Conselho Nacional de Saúde, e internacional, como a da Associação Médica Internacional, que reafirmam a confidencialidade dos dados pessoais, e excepcionalmente autorizam o acesso sem o consentimento dos indivíduos, após análise por um comitê de ética em pesquisa (Ventura, 2013).

A comissão especial de estudos em informática em saúde (ABNT/CEE-78IS, 2015), por ser um espelho do comitê ISO TC 215 – Health informatics, adota o mesmo escopo: "Padronização na área de informática em saúde para facilitar a troca e o uso consistente e coerente de dados, informação e conhecimento relacionados à saúde, para apoiar todos os aspectos de sistemas de saúde".
Da mesma forma, o GT4 dessa comissão – segurança da informação e do paciente - tem seu trabalho alinhado com o do WG4 – security, safety and privacy do comitê ISO TC 215 – Health Informatics e possuem o mesmo escopo:

> "Padronização de métodos e sistemas para proteger e aumentar a confidencialidade, integridade e disponibilidade da informação em saúde, evitar que sistemas de informação afetem adversamente a segurança do paciente, resguardar a privacidade das informações pessoais e relativas aos cuidados com a saúde, e assegurar a responsabilização dos usuários dos sistemas de informação de saúde" (ABNT/CEE-78IS, 2015).

A Sociedade Brasileira de Informática em Saúde (SBIS) define que o Sistema de Registros eletrônicos de Saúde (S-RES) é qualquer sistema que capture, armazene, apresente, transmita ou imprima informação identificada em saúde. Informação identificada em saúde é aquela atinente à atenção e gestão da saúde, que pode levar à identificação do cidadão. Segundo a Resolução 1821 do Conselho Federal de Medicina (CFM), toda informação em saúde identificada individualmente necessita de proteção em sua confidencialidade, por ser princípio basilar do exercício da medicina; ainda, os dados do prontuário pertencem ao paciente e só podem ser divulgados com sua autorização ou a de seu responsável, ou por dever legal ou justa causa (de Sá Leitão-Júnior, de Lucena, Braga, & Neira, 2016). Além dos documentos regulamentadores citados, os autores criaram uma tabela com outros documentos regulares, conforme encontrados em sua pesquisa, que são listados abaixo.

- Código de Processo Civil (autenticidade de documentos), Lei 11419/2006 (informatização de processo judicial);
- Resoluções CFM (genericamente, legitimidade de RES), Constituição brasileira, Código penal brasileiro e Código de ética médica (confidencialidade);
- ISO/IEC 27000 (sistemas de gestão de segurança da informação);
- Constituição brasileira, Código penal brasileiro, Código de processo penal, Código civil brasileiro, Código de processo civil (confidencialidade), Código de ética médica (confidencialidade), Resolução CFM 1639/2002 (Revogada por CFM 1821/2007), Manual de Certificação para SRES, ISO/IEC 17799/2005 (Código de prática para a gestão da segurança da informação), Resolução CREMESP 097/2001 (Uso da Internet), Resolução CMF 1643/2002 (Telemedicina), Resoluções CFP 002/1995, 003/2000, 006/2000 (Exercício da psicologia a distância);
- Lei 6065/1981 (Confidencialidade), Resolução CFFa 427/2013 (Teles saúde em fonoaudiologia);

- Lei 8069/1990 (impressões planares e digitais);
- Lei 12527/2011 (Acesso à informação), Lei 8080/1990 (Direito à saúde), Lei 12527/2011(Acesso sem consentimento);
- Medida provisória/2200-2/2001 (certificação digital).

Apesar da regulamentação de segurança, o profissional da saúde é identificado como o elemento que traz mais vulnerabilidade para a segurança da informação de uma organização. A cultura de segurança de informação é reconhecida como a forma de influenciar o usuário a adotar os controles e políticas de segurança da informação nas organizações (Hassan & Ismail, 2016).

Ghazvini e Shukur (2017) propõem um Framework para treinamento na difusão de cultura de segurança da informação – o Training Method Selection (TMS), baseado na avaliação de especialistas e profissionais. O TMS guia as organizações para a seleção do método de treinamento que preenchem as necessidades da organização, visando promover o engajamento dos empregados e aumentar seu interesse pelo tema.
Atualmente, há uma proliferação de equipamentos de saúde baseados em computação ubíqua que requerem um framework de segurança para equipamentos de saúde. Son, Kim, Park, Cha, & Park (2013) apresentam requisitos de segurança para informação médica usada em equipamentos u-healthcare, baseado no j de padronização IEC 60601.

2.2. Os Objetivos Fundamentais da Segurança da Informação

A implementação da segurança da informação requer que três objetivos fundamentais sejam atendidos: confidencialidade, disponibilidade e integridade. A definição desses foi apresentada no guia oficial de certificação do (ISC)2 (Tipton, 2007). Outros artigos também apresentam estas definições (de Sá Leitão-Júnior et al., 2016) e (Haas et al., 2011) dentre outros.

A Confidencialidade refere-se à prevenção de perda de dados é a categoria mais facilmente identificada com a privacidade e segurança no HIPAA dentro do ambiente de assistência em saúde. A adoção de nome de usuário e senha, além de criptografia, são medidas comumente implementadas para assegurar a confidencialidade e garantir que apenas remetente e destinatário pretendidos devem ter acesso ao conteúdo da mensagem.

A disponibilidade refere-se à disponibilidade do sistema e à acessibilidade à rede. A perda de disponibilidade pode ser causada por: desastres naturais ou acidentais tais como tornados, terremotos e furacões ou fogo; cenários produzidos por ação humana, tais como ataques Denial of Service (DoS) ou uma infecção maliciosa que compromete a rede e evita o uso do sistema. Para reação a tais questões, geradores de backup, planejamento de continuidade de operação e equipamentos periféricos de segurança são usados para manutenção da disponibilidade dos sistemas e da infraestrutura de TI.

A Integridade descreve a confiabilidade e consistência dos dados. No caso da saúde, se trata de uma garantia que os resultados de laboratório ou histórico médico de um paciente não sejam modificáveis por entidades não autorizadas ou corrompidas por processos pobremente projetados.

Melhores práticas de base de dados, soluções contra perda de dados, realização periódica

de backup de dados, e uso de ferramentas de arquivamento devem ser práticas correntes. Adicionalmente, visando evitar manipulação indevida de informações, todas as alterações realizadas nas bases de dados devem ser detectáveis.

2.3. Segurança Cibernética (Cyber Security) na Saúde

Langer (2017) define os atores relacionados à segurança de computadores e, de forma mais genérica da Internet (incluindo a Internet de Todas as Coisas[1]), os quais denomina como Cast ou, elenco, incluindo o Black Hat (agentes humanos que procuram obter controle sobre computadores ou dispositivos de outras pessoas para usuários com fins nefastos) e os sumarizam em grupos, os quais são aplicados no campo da segurança cibernética na saúde:

- Ataques criptográficos: seu propósito é revelar o conteúdo de transações criptografadas ou password de uma vítima. De forma alternativa, também se aplica aos crypto-attacker, os quais criptografam os arquivos do usuário, tornando-os incessíveis – os ataques ransomware.
- Crime cibernético: é o termo usado para todos os crimes cometidos em computadores, mas inclui um significado mais específico: remover qualquer tipo de vestígio de um crime cometido.
- Ataques de impedimento de serviço (denial-of-service – DOS): impedem o acesso a um determinado serviço ou máquina. No caso da saúde, este ataque é extremamente grave, pois compromete o suporte à manutenção de vidas. O ataque ransomware é um exemplo de ataque do tipo DOS.
- Injection Exploits: usam intencionalmente dados falsos ou entrada de códigos em um serviço para subverte-lo. Geralmente, esta vulnerabilidade é resultado de validação insuficiente de um dado ou entrada; são mais utilizados contra servidores Web e bases de dados.
- Malware, qualquer software instalado, sem a concessão do usuário, que altera o comportamento normal do computador, que o usuário não permitiria se soubesse. Normalmente, os usuários se infectam desapercebidamente através de e-mails maliciosos ou websites maliciosos.
- Escalação de privilégios: o objetivo é converter uma conta de usuário normal em uma conta que possua direitos administrativos – geralmente, como um precursor da instalação do Malware.
- Exploração da segurança web: normalmente, quando um usuário direciona seu navegador para um website, mais coisas são feitas, sem ciência do usuário. O servidor web pode obter informações do computador do usuário explorando brechas de segurança no navegador. O black hat pode até executar software arbitrário no computador do usuário.

Para assegurar o armazenamento e a gerência de acesso aos S-RES, vários requisitos de segurança da informação devem ser levados em consideração (Chiuchisan, Balan, Geman, Chiuchisan, & Gordin, 2017):

- Armazenagem dos registros eletrônicos de saúde (RES), onde o desafio está no

[1] Internet de Todas as Coisas é o termo utilizado para a rede de objetos físicos ou “coisas” incorporadas em produtos eletrônicos, softwares, sensores e conectividade para habilitar objetos a trocar dados com o fabricante, o operador e/ou outros dispositivos conectados.

compromisso entre a velocidade e a segurança no acesso aos recursos;
- Código Malicioso: proteção a ataques intrusivos, aplicações de antivírus, firewalls e atualizações de software são alguns dos requisitos para a proteção do sistema de informação;
- Proteção ao acesso, onde a informação somente deve ser acessível ao usuário autorizado;
- Dispositivos móveis devem habilitar acesso seguro e eficiente à infraestrutura de saúde;
- Sistemas de proteção online, onde recursos humanos e de equipamento de segurança (firewalls, antivírus e dispositivos de filtragem de conteúdo) devem ser agregados na proteção de informação de saúde e atividades criminais na Internet.
- Segurança física, humana e de TI, porque qualquer falha de segurança é uma porta para o vazamento de informação.

Relatórios da indústria indicam que o número de incidentes de segurança em organização de saúde tem aumentado. Os relatórios da Symantec mostram que a indústria da saúde contabiliza 36% do total de incidentes de segurança no Reino Unido. Em 44%, a indústria da saúde continuava a ser o setor responsável pela maior porcentagem de divulgação indevida de dados (He & Johnson, 2017).

Em 13 de maio de 2017, hackers começaram a espalhar um ransomware (um programa que bloqueia todos os arquivos em um sistema infectado) nos computadores de todo o mundo. De acordo com a Europol, mais de 200.000 computadores em 150 países foram vítimas do ataque cibernético que envolvia a requisição de resgate de 300 dólares para devolver o controle sobre os arquivos criptografados. No Reino Unido, o ataque cibernético afetou os sistemas de tecnologia de informação dos hospitais do Serviço Nacional de Saúde, resultando em operações canceladas, hospitais sendo colocados no status de transferência e os documentos como os registros de pacientes ficando indisponíveis na Inglaterra e na Escócia (Mattei, 2017).

2.4. Segurança em Nuvem x Soluções Cliente-Servidor

Tradicionalmente, hospitais e clínicas mantidos por um sistema de TI e equipamento local, trabalham com fornecedores para manutenção e aprimoramento dos softwares usados.

Cloud Computing é um novo paradigma para computação distribuída que provê armazenagem, recursos de computação e software ou plataformas para desenvolvimento de software sob demanda ou, de outra forma, reservando recursos na nuvem. Cloud Computing preenche algumas das necessidades mais prementes da indústria da saúde: provê uma conveniência de armazenagem em grande escala, o que em geral não é viável nos softwares de tratamento de saúde legados (Fatima & Auti, 2017). As principais restrições em relação à nuvem estão associadas à integridade e privacidade da informação dos pacientes. No entanto, alegam os autores, o controle da informação pelos próprios pacientes traria os seguintes benefícios:

- Compartilhamento dos RES entre médicos e centros de pesquisa em várias áreas distribuídas;
- Provisão de acesso a clínicos para segunda opinião e referência;
- Provê os direitos de autorização nas mãos dos pacientes melhoram a confiabilidade

na passagem de informação nos RES (com a própria governança da informação).

Abbas, Maennel e Assar (2017) organizaram uma publicação que reuniu os resultados recentes de pesquisas sobre a computação em nuvem. Estes artigos incluem alguns conceitos importantes associados à segurança da informação em nuvem e propostas de frameworks para segurança na nuvem.

O ataque DDoS (Distributed Denial of Service) é um dos mais notórios ataques na lista dos principais ataques recentes. Há um grande número de incidentes que fizeram os negócios baseados na internet indisponíveis ou em alto risco. Serviços e infraestrutura baseados em nuvem estão entre os alvos favoritos dos ataques DDoS (Somani, Gaur, Sanghi, Conti, & Buyya, 2017).

Gbadeyan, Butakov e Aghili (2017) focou nas questões de computação na nuvem no Canadá. A pesquisa apresentou uma detalhada governança de TI e em uma abordagem de mitigação de risco para implementação em tecnologias de computação na nuvem. Áreas específicas para avaliação de risco em modelos de avaliação de implantação de computação na nuvem foram delineadas e mapeadas para componentes na arquitetura em nuvem. O COBIT 5 foi usado como a principal ferramenta para propor mitigação de risco e governança de IT e níveis de manutenção.

Os serviços disponibilizados na nuvem ou software as a servisse (SaaS) têm crescido significativamente. Entretanto, segundo o (ISC)2 ((ISC)2, 2017), 36 por cento das aplicações críticas para o negócio estão alojadas na nuvem, mas os departamentos de TI não conseguem acompanhar todos eles.

Além disso, 72 por cento dos profissionais de saúde consultados em uma pesquisa (Ponemon, 2014) acreditavam que seu provedor de serviços em nuvem (Cloud Service Provider – CSP) não os notificaria imediatamente se houvesse uma brecha de segurança envolvendo perda ou roubo de informação confidencial do negócio ou propriedade intelectual.

3. Metodologia

O presente estudo baseia-se no modelo de revisão sistemática da literatura (RSL) proposto por Kitchenham (2004) que basicamente divide-se em três etapas: o planejamento da revisão, a condução da revisão e a análise dos resultados.

3.1. Planejamento da revisão sistemática

Na fase de planejamento foi estabelecido o protocolo para a execução da RSL que seguiu as seguintes etapas:

a. Descrição dos objetivos: tem como objetivo primário identificar os principais frameworks de segurança da informação apontados nos estudos e a distribuição dos mesmos pelas seguintes categorias: confidencialidade, integridade e disponibilidade.
b. Elaboração da questão de pesquisa: o presente estudo considerou as seguintes questões para subsidiar o processo de busca:
    i) Questão de pesquisa 01: Quais são os principais frameworks de segurança

da informação utilizados na área de saúde descritos na literatura?

ii) Questão de pesquisa 02: Quais são os principais focos dos estudos em relação à segurança da informação?

c. Com relação à estratégia de busca, o presente estudo baseia-se nos seguintes critérios:

i) Seleção das bases para a pesquisa: as bases de dados utilizadas no trabalho foram: Web of Science, Scopus e Ebsco.

ii) Elaboração da string de pesquisa: foi elaborada uma string que continha as palavras "informação", "segurança" e "saúde". Esses termos foram traduzidos para a língua inglesa e resultou no seguinte: ("information" and "security" and ("healthcare" or "health care")).

d. Adoção de critérios para inclusão e exclusão de trabalhos:

i) Para inclusão dos estudos: as publicações devem estar disponíveis na Web, especificamente nas bases selecionadas, na língua inglesa, abordando estudos sobre segurança da informação na área de saúde e respondendo a qualquer uma das questões de pesquisa. Além disso, os artigos devem ter a sua data de publicação a partir de 2008.

ii) Para exclusão dos estudos: trabalhos duplicados, que não abordam o tema necessário, não respondam a nenhuma das questões de pesquisa ou possuem o ano de publicação anterior ao ano de 2008.

3.2. Condução da revisão sistemática

Na fase de condução da RSL foram executados os seguintes passos: a string de busca foi executada nas bases selecionadas; os estudos primários foram identificados e selecionados de acordo com os critérios de inclusão e exclusão; os trabalhos foram avaliados seguindo os critérios de qualidade estabelecidos durante o planejamento da revisão.

3.2.1. Processo para recuperação dos estudos primários

Após a recuperação dos estudos primários por meio da string de busca, os trabalhos foram organizados na ferramenta ENDNOTE X7 para facilitar a separação e o rastreamento de cada uma das fases e critérios de inclusão/exclusão (Figura 01).

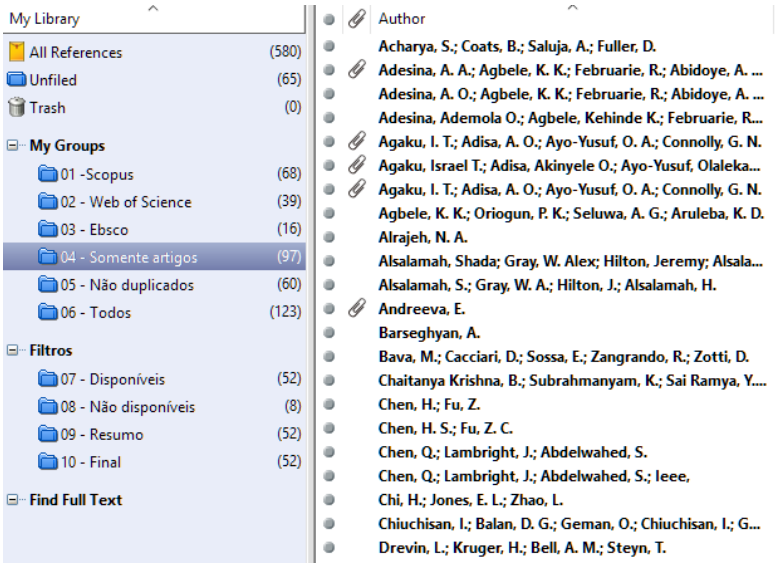

Figura 01 – Utilização da ferramenta ENDNOTE X7
Fonte: Dados da pesquisa

Sendo assim, foram encontrados 123 estudos após a busca inicial nas bases. Com a remoção dos trabalhos que não eram artigos científicos (capítulos de livros, textos técnicos e etc.), restaram 97 estudos. Após a remoção dos duplicados, obteve-se um total de 60 trabalhos. Destes, 8 não estavam disponíveis gratuitamente na Web e não puderam ser recuperados. Dos 52 artigos restantes, todos foram selecionados após a leitura dos resumos. Sendo assim, essa fase terminou com a seleção de 52 trabalhos conforme mostrado na Figura 02.

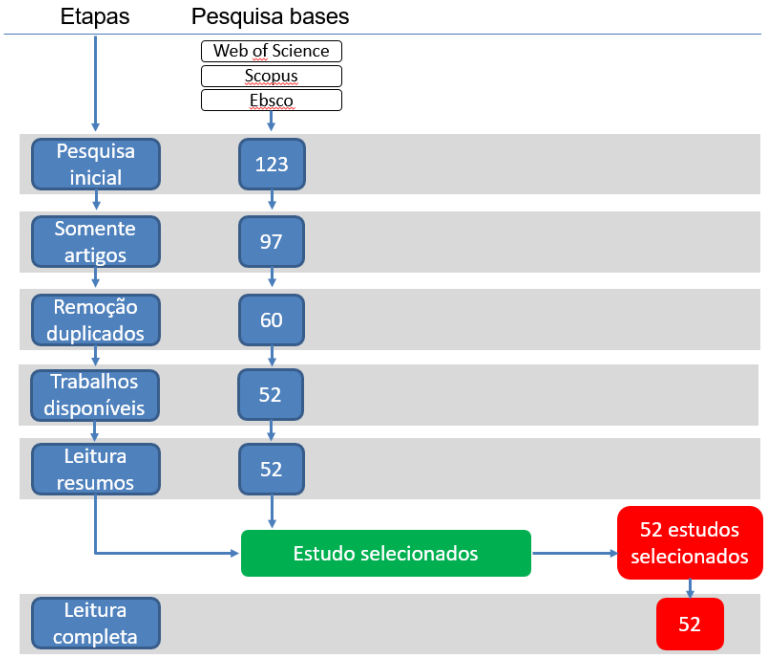

Figura 02 – Processo de recuperação e pré-seleção
Fonte**:** Elaborado pelos autores

3.2.2 Processo de seleção dos estudos

Após as fases de recuperação e pré-seleção, os artigos foram analisados por meio de uma leitura completa do seu conteúdo. Marconi e Lakatos (2003) citam que uma avaliação mais detalhada se faz necessária para garantir a qualidade dos estudos selecionados. Assim, os 52 trabalhos selecionados na fase anterior foram analisados e todos foram mantidos.

4. Resultados e Discussões

O presente estudo elaborou uma revisão sistemática da literatura baseada no protocolo proposto por Kitchenham (2004) e após o processo de seleção final dos estudos chegou a um total de 52 trabalhos. Nestes, observa-se uma concentração de estudos nos anos de 2012, 2013 e 2017 conforme a Figura 03.

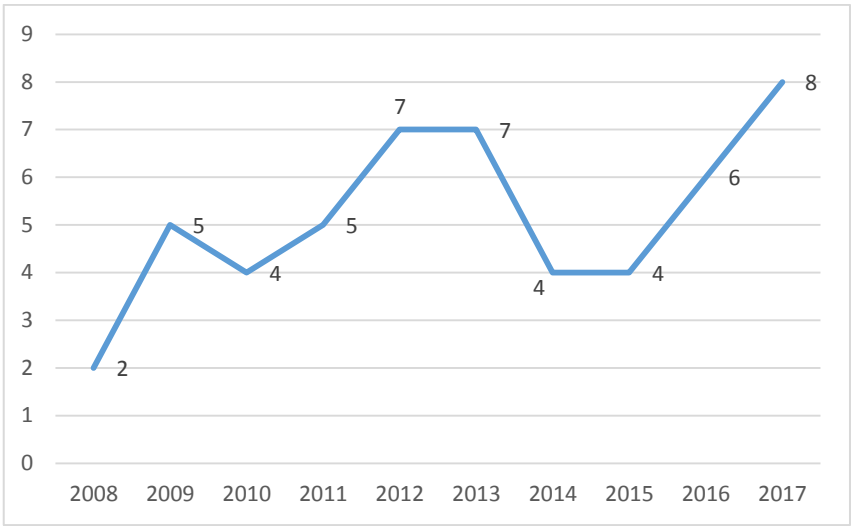

Figura 03 – Distribuição dos 52 estudos por ano de publicação
Fonte**:** Dados da pesquisa

A distribuição dos artigos pelas bases pesquisadas mostra que, dos 52 estudos selecionados, 48 deles foram encontrados na base Scopus (Figura 4). A base Web of Science totalizou 31 artigos e a base Ebsco somente 14 trabalhos. A soma total resulta em mais de 52 artigos porque muitos deles foram encontrados em mais de uma base e foram removidos posteriormente.

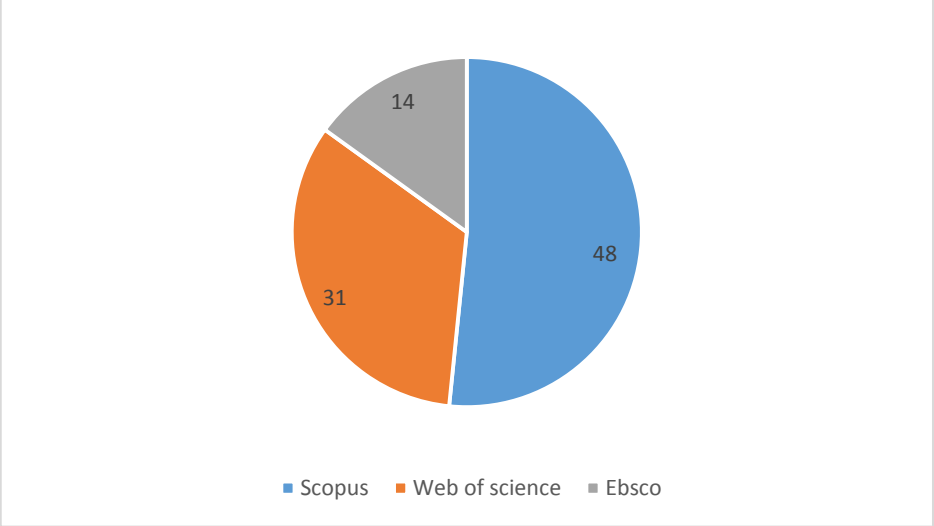

Figura 04 – Distribuição dos 52 estudos por base de pesquisa
Fonte**:** Dados da pesquisa

Os 52 artigos selecionados são descritos e categorizados, no Quadro 01, em ordem cronológica:

Nº	REFERÊNCIA	FOCO DO ESTUDO
1	Chi, H., et al. (2008)	Controle de acesso
2	Gottberg, H. and I. T. Pisa (2008)	Governança da segurança
3	Bava, M., et al. (2009)	Governança da segurança
4	Gleni, S., et al. (2009)	Criptografia de dados
5	Nemati, H. R. and M. Church (2009)	Profissional de saúde

6	Stockdale, R., et al. (2009)	Governança da segurança
7	Sumner, J., et al. (2009)	Profissional de saúde
8	Ferreira, A., et al. (2010)	Controle de acesso
9	Narayana Samy, G., et al. (2010)	Governança da segurança
10	Tyali, S. and D. Pottas (2010)	Governança da segurança
11	Williams, J. (2010)	Redes sociais
12	Adesina, A. A., et al. (2011)	Criptografia de dados
13	Kimura, E., et al. (2011)	Controle de acesso
14	Krens, R., et al. (2011)	Profissional de saúde
15	Ribas, C. E., et al. (2011)	Governança da segurança
16	Zineddine, M. (2011)	Governança da segurança
17	He, Y. and C. W. Johnson (2012)	Notações
18	Khansa, L., et al. (2012)	Investimento em segurança
19	Liu, C. H., et al. (2012)	Infraestrutura de rede
20	Ribas, C. E., et al. (2012)	Governança da segurança
21	Stahl, B. C., et al. (2012)	Política de segurança
22	Wang, J., et al. (2012)	Ferramenta de buscas
23	Zafar, H. and S. Sneha (2012)	Sistemas de informação
24	Alsalamah, S., et al. (2013)	Controle de acesso
25	Andreeva, E. (2013)	Dispositivos de acesso
26	Hameed, S. A. and H. Yuchoh (2013)	Criptografia de dados
27	Hassan, N. H., et al. (2013)	Profissional de saúde
28	Orel, A. and I. Bernik (2013)	Governança da segurança
29	Son, J., et al. (2013)	Dispositivos médicos
30	Van Deursen, N., et al. (2013)	Profissional de saúde
31	Agaku, I. T., et al. (2014)	Percepção do paciente
32	Huang, C. D., et al. (2014)	Investimento em segurança
33	Mahncke, R. J. and P. A. H. Williams (2014)	Governança da segurança
34	Vorakulpipat, C., et al. (2014)	Segurança como serviço
35	Chaitanya Krishna, B., et al. (2015)	Gerenciamento de riscos
36	Chen, H. and Z. Fu (2015)	Dispositivos wireless
37	Papoutsi, C., et al. (2015)	Percepção do paciente
38	Patel, V., et al. (2015)	Infraestrutura de rede
39	Chen, Q., et al. (2016)	Infraestrutura de rede
40	Agbele, K. K., et al. (2016)	Infraestrutura de rede
41	Ghazvini, A. and Z. Shukur (2016)	Profissional de saúde
42	Hassan, N. H. and Z. Ismail (2016)	Profissional de saúde
43	Sedlack, D. J. (2016)	Profissional de saúde
44	Uwizeyemungu, S. and P. Poba-Nzaou (2016)	Governança da segurança
45	Chiuchisan, I., et al. (2017)	Infraestrutura de rede
46	Drevin, L., et al. (2017)	Vocabulário
47	Ghazvini, A. and Z. Shukur (2017)	Profissional de saúde
48	Ghazvini, A. and Z. Shukur (2017b)	Profissional de saúde
49	He, Y. and C. Johnson (2017)	Profissional de TI
50	Langer, S. G. (2017)	Governança da segurança
51	Mattei, T. A. (2017)	Lições aprendidas
52	Naik, B. B., et al. (2017)	Infraestrutura de rede

Quadro 01: O principal foco dos 52 estudos selecionados
Fonte**:** Dados da Pesquisa

Com relação ao enfoque dos trabalhos selecionados, nota-se que 12 artigos estão voltados para um aspecto mais completo de segurança na Governança de Tecnologia da Informação. A maioria desses estudos abordam frameworks (ou normas) mais abrangentes sobre segurança da informação. Já o enfoque no "profissional de saúde", discutido em 10 trabalhos, mostra como os estudos na área de segurança da informação em saúde têm sido

direcionados para disseminação da cultura de segurança para os profissionais da área, sendo que os mesmos são considerados uma parte crítica do processo. A segurança da infraestrutura de redes foi discutida em 6 trabalhos e controle de acesso em 4. Apenas 3 trabalhos abordaram o uso de recursos de criptografia de dados e outros 2 trabalhos sobre investimentos em segurança também foram encontrados e devem ser mencionados.
Em relação aos trabalhos que citam normas ou frameworks, observa-se abaixo a classificação, no Quadro 02.

FRAMEWORK CITADO	**ENFOQUE**	**ABRANGÊNCIA**	**REFERÊNCIAS**
ISO/IEC 27001	Segurança da informação	Internacional	Bava et al. (2009); He e Johnson (2012); Narayana, Ahmad e Ismail (2010); Orel e Bernik (2013); Ribas et al. (2011); Ribas et al. (2012); Son et al. (2013); Tyali e Pottas (2010); Vorakulpipat, Siwamogsatham e Kawtrakul (2014); Zineddine (2011)
ISO/IEC 27002	Segurança da informação	Internacional	Gottberg e Pisa (2008); He e Johnson (2012); Orel e Bernik (2013); Ribas et al. (2011); Ribas et al. (2012); Stockdale et al. (2009); Zineddine (2011)
ISO/IEC 27799	Segurança da informação na saúde	Internacional	Bava et al. (2009); Gottberg e Pisa (2008); Narayana, Ahmad e Ismail (2010); Orel e Bernik (2013); Tyali e Pottas (2010)
ISO/IEC 15026	Engenharia de sistemas e software	Internacional	He e Johnson (2012)
Health Insurance Portability and Accountability (HIPAA)	Segurança da informação na saúde	Estados Unidos da América	He e Johnson (2012); Khansa et al. (2012); Langer (2017); Nemati e Church (2009); Orel e Bernik (2013); Sedlack (2016); Son et al. (2013); Zineddine (2011)
Promotion of Access to Information Act (PAIA)	Direito de acesso à informação	África do Sul	Drevin et al. (2017)
Protection of Personal Information (POPI)	Segurança da informação pessoal	África do Sul	Drevin et al. (2017)
GB/T22239	Segurança da informação	China	He e Johnson (2017)
IEC 60601	Certificação de dispositivos eletromédicos	Internacional	Son et al. (2013)

Software Development Life Cicle (SDLC)	Ciclo de vida de desenvolvimento de sistemas de informação	Internacional	Zafar e Sneha (2012)
Personal Information Protection and Electronic Documents (PIPEDA)	Segurança de informação pessoal	Canadá	Zineddine (2011)

Quadro 02: Os principais frameworks identificados nos 52 estudos selecionados
Fonte**:** Dados da Pesquisa

Nota-se que as normas da família ISO/IEC 27000 são citadas em 18 estudos. É importante salientar que essas normas são de aplicação geral e não possuem especificidades para a área de saúde. As normas HIPAA (com 8 citações) e ISO/IEC 27799 (com 5 citações) aparecem na terceira e quarta colocação em relação ao número de artigos. Essas duas normas são específicas para tratar da segurança da informação na área de saúde.

Outros frameworks de alguns países como África do Sul, China e Canadá aparecem em artigos isolados. Observa-se, também, que normas criadas para o desenvolvimento de sistemas de informação, como o ISO/IEC 15026 e o SDLC são citadas em dois trabalhos onde são abordados aspectos de segurança para esse fim.

5. Considerações finais

Os estudos sobre a segurança da informação na área de saúde abordam um tema extremamente crítico para a sociedade atual. Alguns episódios como os problemas causados pelo *ransomware WannaCry* instiga a necessidade de novos estudos acerca da governança de segurança da informação na área da saúde, em especial.

A partir desta afirmativa buscou-se com esta pesquisa, apresentar o cenário de artigos publicados nos últimos 10 anos em relação ao tema, permitindo uma análise do cenário mundial tratado pelos meios acadêmicos. Por meio de uma revisão sistemática da literatura, observou-se que existe uma preocupação com a governança da segurança, sob um aspecto mais abrangente de gestão. Outro ponto importante é o número de trabalhos que focam na capacitação dos profissionais de saúde, mostrando, assim, que existe um cuidado com a capacitação de fator “pessoas”, ativo importante da segurança da informação. Com isso, observa-se um cenário onde existe um enfoque mais distribuído, englobando a cultura e o treinamento dos profissionais que utilizam a infraestrutura de TI.

A presente investigação mostra que os frameworks da família ISO 27000 são os mais abordados nos estudos selecionados. Essas normas preconizam diretrizes mais genéricas e não possuem especificidades para a área de saúde. A HIPAA e ISO/IEC 27799, específicas para a saúde, ficaram na terceira e quarta colocação no número de citações. Isso pode indicar um possível cenário de fragilidade na segurança da informação, visto que as normas como a ISO 27001 e ISO 27799 deveriam se complementar, pois a primeira estabelece requisitos de segurança para um sistema de gestão de segurança da informação e a segunda prevê a implementação de controles de segurança específicos para a área de saúde - a ISO 27002 o faz de forma genérica e não focada na saúde.

Dessa forma, conclui-se que, nos últimos 10 anos, foram feitos alguns estudos sobre a segurança da informação na saúde (60 trabalhos encontrados), sendo que destes, notou-se

que frameworks específicos para a área de saúde são menos abordados que as normas mais genéricas de segurança da informação, podendo assim, não descrever ameaças específicas.

O presente trabalho não buscou esgotar a discussão e contou ainda, como limitação, a possível subjetividade presente em uma das fases de seleção a RSL (inerente ao método) referente a escolha das bases de artigos acessadas.

Como trabalho futuro, pretende-se descrever os frameworks aplicados a partir de survey em hospitais ou centros de saúde brasileiros.

Referências

ADESINA, Ademola O. et al. Ensuring the security and privacy of information in mobile health-care communication systems. **South African Journal of Science**, v. 107, n. 9-10, p. 27-33, 2011.

ABBAS, Haider; MAENNEL, Olaf; ASSAR, Saïd. Security and privacy issues in cloud computing. 2017.

ABNT/CEE-78IS. SOBRE O GT4 – SEGURANÇA DA INFORMAÇÃO E DO PACIENTE. Disponível em: http://www.cee78is.org.br/?page_id=35. Acessado em: 03 de outubro de 2017.

AGAKU, Israel T. et al. Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. **Journal of the American Medical Informatics Association**, p. 374-378, 2014.

AGBELE, Kehinde K. et al. Towards a model for enhancing ICT4 development and information security in healthcare system. In: **Technology and Society (ISTAS), 2015 IEEE International Symposium on**. IEEE, 2015. p. 1-6.

ALSALAMAH, Shada et al. Information security requirements in patient-centred healthcare supporting systems. 2013.

ANDREEVA, E. Information security of healthcare systems: using a biometric approach. **Modelling in Medicine and Biology X**, v. 17, p. 109, 2013.

BAVA, Michele et al. Information security risk assessment in healthcare: the experience of an Italian Paediatric Hospital. In: **Computational Intelligence, Communication Systems and Networks, 2009. CICSYN'09. First International Conference on**. IEEE, 2009. p. 321-326.

CANADÁ. The Personal Information Protection and Electronic Documents Act (PIPEDA) 2000. Disponível em: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/ Acessado em: 03 de outubro de 2017.

CHAITANYA KRISHNA, B., et al. A novel approach for information security and risk management in distributed health care systems. **International Journal of Applied Engineering Research 10**(4): 10119-10126.

CHEN, Hongsong; FU, Zhongchuan. Hadoop-based healthcare information system design and wireless security communication implementation. **Mobile Information Systems**, v. 2015, 2015.

CHEN, Qian; LAMBRIGHT, Jonathan; ABDELWAHED, Sherif. Towards Autonomic Security Management of Healthcare Information Systems. In: **Connected Health: Applications, Systems and Engineering Technologies (CHASE), 2016 IEEE First International Conference on**. IEEE, 2016. p. 113-118.

CHI, Hongmei; JONES, Edward L.; ZHAO, Lang. Implementation of a security access control model for inter-organizational healthcare information systems. In: **Asia-Pacific Services Computing Conference, 2008. APSCC'08. IEEE**. IEEE, 2008. p. 692-696.

CHINA. Chinese national standard, information security technology-basic requirements of GRADE protection of information system security. **GB/T22239-2008**; 2008.

CHIUCHISAN, Iuliana et al. A security approach for health care information systems. In: **E-Health and Bioengineering Conference (EHB), 2017**. IEEE, 2017. p. 721-724.

Comitê Gestor da Internet no Brasil. PESQUISA SOBRE O USO DAS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO NOS ESTABELECIMENTOS DE SAÚDE BRASILEIROS. 2015. Disponível em: http://cetic.br/media/docs/publicacoes/2/tic_saude_2015_livro_eletronico.pdf no dia 03/10/2017 Acessado em: 03 de outubro de 2017.

DE SÁ LEITÃO-JÚNIOR, Plinio et al. Regulação de segurança da informação eletrônica em saúde: visão geral. **Journal of Health Informatics**, v. 8, n. 4, 2016.

DREVIN, Lynette et al. A Linguistic Approach to Information Security Awareness Education in a Healthcare Environment. In: **IFIP World Conference on Information Security Education**. Springer, Cham, 2017. p. 87-97.

EEUU. Health Insurance Portability and Accountability Act of 1996. Disponível em: https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf . Acessado em: 03 de outubro de 2017.

EEUU. Federal Information Security Management Act 2002 – FISMA. Disponível em: https://www.gpo.gov/fdsys/pkg/STATUTE-116/pdf/STATUTE-116-Pg2899.pdf . Acessado em: 03 de outubro de 2017.

EEUU. American Recovery and Reinvestment Act. 2009. Disponível em: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1enr.pdf. Acessado em: 03 de outubro de 2017.

EEUU. DEPARTMENT OF HEALTH AND HUMAN SERVICES et al. HITECH Act enforcement interim final rule. **US Department of**, 2009. Disponível em: https://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html . Acessado em: 03 de outubro de 2017.

FATIMA, Syed Imrana; AUTI, R. A. Multi-Level Privacy-Preserving Patient Self-Controllable algorithm Healthcare in Cloud. **INTERNATIONAL JOURNAL**, v. 2, n. 9, 2017.

FERREIRA, Ana et al. Grounding information security in healthcare. **International Journal of Medical Informatics**, v. 79, n. 4, p. 268-283, 2010.

GBADEYAN, Ayo; BUTAKOV, Sergey; AGHILI, Shaun. IT governance and risk mitigation approach for private cloud adoption: case study of provincial healthcare provider. **Annals of Telecommunications**, v. 72, n. 5-6, p. 347-357, 2017.

GHAZVINI, Arash; SHUKUR, Zarina. Awareness Training Transfer and Information Security Content Development for Healthcare Industry. **INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS**, v. 7, n. 5, p. 361-370, 2016.

GHAZVINI, Arash; SHUKUR, Zarina. Information Security Content Development for Awareness Training Programs in Healthcare. **INTERNATIONAL JOURNAL OF SECURITY AND ITS APPLICATIONS**, v. 11, n. 7, p. 87-96, 2017.

GHAZVINI, Arash; SHUKUR, Zarina. A Framework for an Effective Information Security Awareness Program in Healthcare.

GLENI, Sofia; MAPLE, Carsten; YUE, Yong. Security issues of a biometrics health care information system: the case of the NHS. In: **Computing, Engineering and Information, 2009. ICC'09. International Conference on**. IEEE, 2009. p. 279-284.

GOTTBERG, Heitor; PISA, Ivan Torres; LEÃO, B. Dealing with the Complexities when Implementing Information Security Practices in Healthcare Organizations. In: **HEALTHINF (1)**. 2008. p. 205-208.

HAAS, Sebastian et al. Aspects of privacy for electronic health records. **International journal of medical informatics**, v. 80, n. 2, p. e26-e31, 2011.

HAMEED, Shihab A.; YUCHOH, Habib. Toward Managing Security Cost for Healthcare Information. In: **Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference on**. IEEE, 2012. p. 414-418.

HASSAN, Noor Hafizah; ISMAIL, Zuraini. INFORMATION SECURITY CULTURE IN HEALTHCARE INFORMATICS: A PRELIMINARY INVESTIGATION. **Journal of Theoretical and Applied Information Technology**, v. 88, n. 2, p. 202, 2016.

HASSAN, Noor Hafizah; ISMAIL, Zuraini; MAAROP, Norazean. A conceptual model for knowledge sharing towards information security culture in healthcare organization. In: **Research and Innovation in Information Systems (ICRIIS), 2013 International Conference on**. IEEE, 2013. p. 516-520.

HE, Ying; JOHNSON, Chris. Challenges of information security incident learning: an industrial case study in a Chinese healthcare organization. **Informatics for Health and Social Care**, p. 1-16, 2017.

HE, Ying; JOHNSON, C. W. Generic security cases for information system security in healthcare systems. 2012.

HOYT, Robert E.; YOSHIHASHI, Ann K. **Health informatics: practical guide for healthcare and information technology professionals**. Lulu.com, 2014.

HUANG, C. Derrick; BEHARA, Ravi S.; GOO, Jahyun. Optimal information security investment in a Healthcare Information Exchange: An economic analysis. **Decision Support Systems**, v. 61, p. 1-11, 2014.

ISO/TC 215 Health informatics. Disponível em: https://www.iso.org/committee/54960.html. Acessado em: 03 de outubro de 2017.

$(ISC)^2$. Crisis Preparedness: A Full-Time Exercise The Cloud Security Specialist as Crisis Manager. 2017. Disponível em: https://education.isc2.org/css-as-crisis-manager-whitepaper/?utm_campaign=csswhitepaper&utm_source=isc2&utm_medium=bannerad-training-mega . Acessado em: 06 de outubro de 2017

KHANSA, Lara et al. Impact of HIPAA provisions on the stock market value of healthcare institutions, and information security and other information technology firms. **computers & security**, v. 31, n. 6, p. 750-770, 2012.

KIMURA, Eizen et al. A framework for an authorization system with spatial reasoning capacity to improve risk management and information security in healthcare. In: **Applications and the Internet (SAINT), 2011 IEEE/IPSJ 11th International Symposium on**. IEEE, 2011. p. 587-591.

KITCHENHAM, B. **Procedures for Performing Systematic Reviews**, 2004. Joint Technical Report Software Engineering Group, Keele University, United Kingdom and Empirical Software Engineering, National ICT Australia Ltd, Australia, 2004.

KRENS, Robin; SPRUIT, Marco R.; URBANUS-VAN LAAR, Nathalie. Information Security in Health Care-Evaluation with Health Professionals. In: **HEALTHINF**. 2011. p. 61-69.

LANGER, Steve G. Cyber-Security Issues in Healthcare Information Technology. **Journal of digital imaging**, v. 30, n. 1, p. 117-125, 2017.

LIU, Chia-Hui et al. The enhancement of security in healthcare information systems. **Journal of medical systems**, v. 36, n. 3, p. 1673-1688, 2012.

MAHNCKE, Rachel J.; WILLIAMS, Patricia A. Developing and Validating a Healthcare Information Security Governance Framework. 2014.

MASETI, Ophola S. A model for role-based security education, training and awareness in the South African healthcare environment. 2008.

MATTEI, Tobias A. Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack. **World Neurosurgery**, v. 104, p. 972-974, 2017.

NAIK, B. Balaji et al. Security attacks on information centric networking for healthcare system. In: **Advanced Communication Technology (ICACT), 2017 19th International Conference on**. IEEE, 2017. p. 436-441.

NARAYANA SAMY, Ganthan; AHMAD, Rabiah; ISMAIL, Zuraini. Security threats categories in healthcare information systems. **Health informatics journal**, v. 16, n. 3, p. 201-209, 2010.

NEMATI, Hamid R.; CHURCH, Mitchell. A human centered framework for information security management: a healthcare perspective. **AMCIS 2009 Proceedings**, p. 591, 2009.

OREL, Andrej; BERNIK, Igor. Implementing Healthcare Information Security: Standards Can Help. **Data and Knowledge for Medical Decision Support. B. Blobel, A. Hasman and J. Zvarova. Amsterdam, European Federation for Medical Informatics**, p. 195-199, 2013.

PAPOUTSI, Chrysanthi et al. Patient and public views about the security and privacy of Electronic Health Records (EHRs) in the UK: results from a mixed methods study. **BMC medical informatics and decision making**, v. 15, n. 1, p. 86, 2015.

PATEL, Vaishali et al. The role of health care experience and consumer information efficacy in shaping privacy and security perceptions of medical records: national consumer survey results. **JMIR medical informatics**, v. 3, n. 2, 2015.

PONEMON INSTITUTE. Data Breach: The Cloud Multiplier Effect. 2014. Disponível em: http://go.netskope.com/rs/665-KFP-612/images/Ponemon-DataBreach-CloudMultiplierEffect-June2014.pdf. Acessado em: 04 de outubro de 2017

RIBAS, Carlos Eduardo et al. Information Security Management System-A Case Study in a Brazilian Healthcare Organization. In: **HEALTHINF**. 2012. p. 147-151.

RIBAS, Carlos Eduardo et al. A New Approach to Information Security Assessment: a case study in a Brazilian healthcare organization.

SAHIBUDIN, Shamsul; SHARIFI, Mohammad; AYAT, Masarat. Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. In: **Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on**. IEEE, 2008. p. 749-753.

SEDLACK, Derek. Understanding Cyber Security Perceptions Related to Information Risk in a Healthcare Setting. 2016.

SOMANI, Gaurav et al. Service resizing for quick DDoS mitigation in cloud computing environment. **Annals of Telecommunications**, v. 72, n. 5-6, p. 237-252, 2017.

SON, Jaebum et al. Security requirements for the medical information used by U-Healthcare medical equipment. **International Journal of Security and Its Applications**, v. 7, n. 1, p. 169-180, 2013.

STOCKDALE, R. et al. Standards for information security and processes in healthcare. **Journal of Systems and Information Technology**, v. 11, n. 3, p. 295-308, 2009.

STAHL, Bernd Carsten; DOHERTY, Neil F.; SHAW, Mark. Information security policies in the UK healthcare sector: a critical evaluation. **Information Systems Journal**, v. 22, n. 1, p. 77-94, 2012.

SUMNER, Jennifer et al. Health Care Communication Networks: Disseminating Employee Information for Hospital Security. **The health care manager**, v. 28, n. 4, p. 287-298, 2009.

TIPTON, Harold F. **Official (ISC) 2 guide to the ISSMP CBK**. CRC Press, 2007.

TYALI, S.; POTTAS, D. Information Security Management Systems in the Healthcare Context. In: **Proceedings of the South African Information Security Multi-Conference: Port Elizabeth, South Africa, 17-18 May 2010**. Lulu. com, 2011. p. 177.

UWIZEYEMUNGU, Sylvestre; POBA-NZAOU, Placide. Security and Privacy Practices in Healthcare Information Systems: A Cluster Analysis of European Hospitals. In: **ICISSP**. 2016. p. 37-45.

VAN DEURSEN, Nicole; BUCHANAN, William J.; DUFF, Alistair. Monitoring information security risks within health care. **computers & security**, v. 37, p. 31-45, 2013.

VENTURA, Miriam. Lei de acesso à informação, privacidade e a pesquisa em saúde. **Cad. saúde pública**, v. 29, n. 4, p. 636-638, 2013.

VORAKULPIPAT, Chalee; SIWAMOGSATHAM, Siwaruk; KAWTRAKUL, Asanee. An investigation of information security as a service practice: case study in healthcare. **International Journal of Computer Applications in Technology**, v. 49, n. 3-4, p. 365-371, 2014.

WANG, Jingguo; XIAO, Nan; RAO, H. Raghav. An exploration of risk information search via a search engine: Queries and clicks in healthcare and information security. **Decision Support Systems**, v. 52, n. 2, p. 395-405, 2012.

WILLIAMS, James. Social networking applications in health care: threats to the privacy and security of health information. In: **Proceedings of the 2010 ICSE workshop on software engineering in health care**. ACM, 2010. p. 39-49.

ZAFAR, Humayun; SNEHA, Sweta. Ubiquitous Healthcare Information System: Toward Crossing the Security Chasm. **Communications of the Association for Information Systems**, v. 31, 2012.

ZINEDDINE, Mhamed. Automated healthcare information privacy and security: UAE case. In: **Internet Technology and Secured Transactions (ICITST), 2011 International Conference for**. IEEE, 2011. p. 592-595.