Maj Inf Wellington Ferreira Cipriano

A SEGURANÇA DA INFORMAÇÃO COM O ADVENTO DA INTERNET DAS COISAS EM AMBIENTES HOSPITALARES: uma abordagem bibliográfica

Salvador
2020

Maj Inf Wellington Ferreira Cipriano

A SEGURANÇA DA INFORMAÇÃO COM O ADVENTO DA INTERNET DAS COISAS EM AMBIENTES HOSPITALARES: uma abordagem bibliográfica

Trabalho de Conclusão de Curso apresentado à Escola de Formação Complementar do Exército / Centro Universitário do Sul de Minas – UNIS-MG como requisito parcial para a obtenção do Grau Especialização de Gestão em Administração Pública.

.

Orientador: Prof. Viviel Rodrigo José de Carvalho

Salvador
2020

Maj Inf Wellington Ferreira Cipriano

A SEGURANÇA DA INFORMAÇÃO COM O ADVENTO DA INTERNET DAS COISAS EM AMBIENTES HOSPITALARES: uma abordagem bibliográfica

Trabalho de Conclusão de Curso apresentado à Escola de Formação Complementar do Exército / Centro Universitário do Sul de Minas – UNIS-MG como requisito parcial para a obtenção do Grau Especialização de Gestão em Administração Pública.

.

Aprovado em 5 de agosto de 2020.

COMISSÃO DE AVALIAÇÃO

_____

Prof. Dr. Alessandro Messias Moreira - Presidente
UNIS

_____

Prof. Me. Renato Rezende Neto – Membro 1
UNIS

_____

Prof. Esp. Gustavo Andrade Abreu – Membro 2
UNIS

A SEGURANÇA DA INFORMAÇÃO COM O ADVENTO DA INTERNET DAS COISAS EM AMBIENTES HOSPITALARES: uma abordagem bibliográfica

INFORMATION SECURITY WITH INTERNET OF THIGS' ARRIVAL IN HOSPITAL ENVIRONMENT: a bibliographic approach

Wellington Ferreira Cipriano[1]
Viviel Rodrigo José de Carvalho[2]

RESUMO

Esta pesquisa aborda a segurança da informação com o advento da internet das coisas em ambientes hospitalares. Tal abordagem se faz necessária pelos frequentes casos de falhas na proteção da informação hospitalar. Este trabalho tem como objetivo realizar uma revisão bibliográfica, para atualizar as informações atinentes à compreensão dos mecanismos que podem contribuir para a segurança da informação no ambiente hospitalar, tudo com a finalidade de aprimorar os procedimentos de segurança, contribuindo para o desenvolvimento de uma cultura de segurança hospitalar. Este intento será conseguido a partir da revisão bibliográfica qualitativa, desenvolvida a partir de material já elaborado, constituído de livros e artigos científicos. O estudo evidenciou que, em se tratando de segurança da informação na gestão hospitalar, só há sucesso concreto quando todos os envolvidos se conscientizam da importância de adotar as medidas de segurança capazes de proteger a informação de suas reais ameaças, além da necessidade de se ter investimento na área de tecnologia da informação, profissionais capacitados e constantemente treinados.
Palavras-chave: Segurança da Informação. Internet das Coisas. Segurança Hospitalar.

ABSTRACT

This research approaches information security taking under consideration the internet of things' arrival in hospital environments. Such approach is required due to the frequent cases of breaches in protection of hospital information. This study has the purpose to accomplish a bibliographic research, with the purpose of updating the information concerning the mechanisms that can contribute to information security in hospital environments, all of this has the goal to improve security procedures, contributing with the development of a hospital safety culture. This attempt will be achieved from a qualitative bibliographic research, developed from material already elaborated, consisting on books and scientific articles. The study showed that, in what concerns information security in hospital management, there's only real success when everyone involved realize the importance of taking the security measures that are able to protect the

[1] Graduado em Ciências Militares pela Academia Militar da Agulhas Negras. E-mail:ciprijones@hotmail.com, Pós Graduado em Administração Hospitalar pelo Centro Universitário do Sul de Minas.
[2] Graduado em Enfermagem pelo Centro Universitário do Sul de Minas, Pós Graduado em Enfermagem do Trabalho pelo Centro Universitário do Sul de Minas e Mestre em Ciências da Saúde pela Universidade São Francisco. E-mail: viviel@unis.edu.br.

information against real threats, besides the need of investment in information technology area and capable professionals with constant training.
Keywords: Information Security. Internet of Things. Hospital Safety.

1 INTRODUÇÃO

Com a grande quantidade de informações que circulam nas redes das organizações, os incidentes de segurança da informação tiveram um aumento significativo nos últimos anos, assumindo as mais variadas formas, como por exemplo, roubos e acessos não autorizados às informações, ataques via redes sem fio desprotegidas, a fraca proteção implementada nos sistemas, ataques de negação de serviço, infecção por vírus e malwares, entre outros milhares de motivos. Um dos fatores que impulsionam este cenário é a difusão da internet e a facilidade da realização de ataques através dela. Ao mesmo tempo em que ela ajudou com a democratização da informação e tornou-se essencial para impulsionar os negócios, a internet também viabilizou a atuação de ladrões do mundo digital e a propagação de ameaças que colocam em risco a segurança de uma organização (ZAPATER E SUZUKI, 2005).

Na mesma medida em que cresce o número de dispositivos conectados que coletam informações pessoais, cresce de importância na mesma proporção a necessidade de se preocupar com a segurança da informação na internet das coisas.

Segurança da informação é um tema atual em constante discussão nas mais diversas organizações, seja governo, educação, indústria, comércio ou serviços; visto que as organizações utilizam-se da Tecnologia da Informação (TI) para apoiar e gerar negócios, aliados aos benefícios da Internet. Desse modo, independentemente do segmento de mercado, todas as organizações sempre usufruirão da informação, objetivando melhor produtividade, redução de custos, ganho na participação de mercado, aumento de agilidade, competitividade e apoio à tomada de decisão. (SÊMOLA, 2003, p. 1).

O advento da internet das coisas possibilita o acesso e gerenciamento de componentes físicos de um dispositivo, como uma câmera de segurança, o celular, as informações confidenciais na nuvem, a localização física de uma pessoa, representa um grande risco para a privacidade dos dados e até mesmo para a segurança do usuário.

Percebe-se um grande desafio para a segurança, já que muitos dos dispositivos de acesso possuem recursos limitados de segurança, uma vez que foram idealizados para apenas agregar funcionalidade com um baixo custo.

Este trabalho descreve aspectos relacionados à segurança da informação nos ambientes hospitalares, pois com o aumento no número de episódios recentes de falhas na segurança da informação sigilosa de pacientes, passou-se a ter a percepção de que há aspectos a serem melhorados na gestão hospitalar, a exemplo da restrição ao acesso do banco de dados, da utilização de criptografia de palavras nos meios de tecnologia da informação, da utilização de backups automáticos e da construção de uma escala de permissões, onde cada usuário tem um limite distinto de acesso às informações.

Tal abordagem se faz necessária já que a partir do momento em que são criados mecanismos de segurança, outros mecanismos invasivos também são criados. Trata-se de um desafio para os gestores de hospitais e para os responsáveis pela cultura de segurança hospitalar, pois é necessário realizar ações que mapeiem e identifiquem a situação do hospital, suas ameaças, vulnerabilidades e riscos, para permitir um diagnóstico e a futura solução.

É importante ressaltar também a importância do trabalho para os gestores hospitalares, pois ajuda a compreender os mecanismos que podem contribuir para a segurança da informação no ambiente hospitalar

O propósito desta pesquisa é realizar uma revisão bibliográfica, para atualizar as informações atinentes à compreensão dos mecanismos que podem contribuir para a segurança da informação no ambiente hospitalar, tudo com a finalidade de aprimorar os procedimentos de segurança, contribuindo para o desenvolvimento de uma cultura de segurança hospitalar, mostrando conceitos da segurança da informação e da internet das coisas e levando em consideração a constante busca para garantir que as informações geradas em ambientes hospitalares estejam protegidas de acessos indevidos ou de perdas. Neste sentido, a pesquisa irá identificar os conceitos relacionados à segurança da informação, conhecer os riscos atuais que envolvem as informações geradas em ambientes hospitalares, conhecer conceitos sobre a internet da coisas e estabelecer políticas que desenvolvam a cultura da segurança da informação nos hospitais.

Este propósito será atingido através da pesquisa bibliográfica descritiva, exploratória e qualitativa, pois o objetivo é descrever o processo de segurança da informação com o advento da

internet das coisas em ambientes hospitalares. A fonte de consulta será, fundamentalmente, bibliográfica, além de bases de dados de conteúdo acadêmico e de artigos publicados, de forma mais específica, livros de leitura corrente e publicações periódicas.

2 A SEGURANÇA DA INFORMAÇÃO NA GESTÃO HOSPITALAR

Os primeiros relatos sobre a necessidade de sigilo das informações de pacientes são atribuídos à Hipócrates, quatro séculos antes da era cristã. Considerando que o sigilo médico é um atributo moral obrigatório da medicina e um dos pilares básicos da relação médico-paciente, é obrigação do gestor hospitalar assegurar sua fiel observância.

A despeito de se tratar de preceito tão antigo na área de saúde, o dever de sigilo é, ainda hoje, um dos compromissos éticos mais desrespeitados no dia a dia das unidades hospitalares e sanitárias. Veja-se, por exemplo, quão comuns são as conversas de corredores e elevadores sobre as enfermidades dos pacientes atendidos, ou, ainda, a frequência com que se encontram prontuários sobre balcões com os nomes e diagnósticos à mostra, ou mesmo a disposição física das macas e leitos, permitindo a exposição desnecessária do paciente. De certo modo, a informatização reduziu tal risco, mas ainda é difícil determinar a quem se deve conferir acesso a tais dados, protegendo-os, também, de interferências externas (VILLAS BOAS, 2015).

A segurança da informação é essencial na gestão hospitalar de qualidade, onde a tecnologia desempenha um papel cada vez mais importante, já que os dados gerados por meio de registros eletrônicos, dispositivos médicos conectados à rede, sistemas de gestão e acompanhamento de pacientes são utilizados em grande escala.

Com o avanço constante das tecnologias, a importância da segurança da informação aumenta significativamente. Está cada vez mais difícil manter em segurança as informações referentes às empresas ou pessoas. Um descuido nessa área pode trazer prejuízos significativos, o desafio está em obter o equilíbrio (PWC, 2013).

Segurança da informação é um jogo de técnicas e estratégias avançadas que se transforma com rapidez. Como consequência, os modelos da década passada, não são mais adequados. Os líderes reconhecem que, para ter uma segurança eficaz é preciso se transformar e adotar uma nova maneira de pensar. Eles estão cientes de que a própria sobrevivência do negócio exige a

compreensão das ameaças de segurança, o preparo para enfrentá-las e respostas rápidas. (PWC, 2013).

Segurança da informação, conforme Beal (2005), é o processo de proteção da informação das ameaças à sua integridade, disponibilidade e confidencialidade. Sêmola (2003) define segurança da informação como "uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade".

O Decreto Nr 3.505 de 13 de junho de 2000, que instituiu a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, define Segurança da Informação como *"proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento".*

De acordo com a (ABNT NBR ISO/IEC:27002, 2013), uma segurança da informação eficaz reduz riscos, protegendo a organização das ameaças e vulnerabilidades e, assim, reduzindo o impacto aos seus ativos.

Araújo, Bezerra e Coelho (2014) definem a segurança da informação como um fator determinante para condução de negócios bem sucedidos, tanto no setor público quanto no privado, além disso é um componente que viabiliza negócios, tais como eGov (governo eletrônico) ou e-commerce (comércio eletrônico).

Araújo, Bezerra e Coelho (2014), ainda, completa que a segurança da informação abrange todos os ativos de informação, preservando-os contra desastres e erros (intencionais ou não), tentando reduzir a probabilidade ou os impactos causados por incidentes de segurança.

Para a construção de um conhecimento mais apurado sobre o assunto é interessante conhecermos os princípios básicos do assunto.

2.1 PRINCÍPIOS BÁSICOS DA SEGURANÇA DA INFORMAÇÃO

O conceito de "informação" é utilizado em quase todos os campos dos saberes científicos, consequentemente apresenta uma variedade de definições, a depender do enfoque (olhar do

observador) que se queira lhe atribuir. Possui diferentes dimensões explicativas e conceituais. Isso se justifica, principalmente, por causa do uso da palavra “informação” em diferentes áreas do conhecimento. Mesmo em áreas próximas, a palavra remete a conceitos com algumas variações. Podemos dizer que a “informação” na atualidade tem um conceito interdisciplinar (MARTINS, 2009).

Nas últimas décadas a informação vem cada vez mais assumindo um papel importante tornando-se senso comum na sociedade contemporânea, principalmente alavancadas pelas novas “Tecnologias de Informação e Comunicação” (MARTINS, 2009).

Com o constante avanço da TI (Tecnologia da Informação), as empresas passaram a depender cada vez mais da informação e de sistemas computacionais. Mais do que nunca, informação significa poder e seu uso apropriado pode estabelecer o diferencial competitivo e um melhor atendimento a clientes, otimizando a cadeia de serviços, produtos e pesquisas (PEREIRA, 2012).

No contexto atual de desenvolvimento, em que inovações tecnológicas e produção de conhecimento são características marcantes, a informação assume papel de grande importância, sendo vital para a empresa que deseja obter sucesso no mercado atual na formatação de um sistema de informação que atenda às necessidades da organização no desenvolvimento de suas atividades (CONCEIÇÃO, 2012).

Os princípios básicos que regem a segurança da informação são vistos pela triângulo CIA, composto por confidencialidade, integridade e disponibilidade, conforme vemos na figura a seguir (Fig. 1):

Figura 1 – Triângulo CIA

Fonte: (BROOK,2010)

Estes conceitos de segurança da informação orientam a análise, o planejamento e a implementação da segurança para as informações que se deseja proteger, e são definidos assim:

- A confidencialidade dos dados significa que estes estão disponíveis apenas para as partes apropriadas, que podem ser partes que requerem acesso a dados ou partes que são confiáveis. Os dados que têm sido mantidos confidenciais são aqueles que não foram comprometidos por outras partes; dados confidenciais não são divulgados a pessoas que não necessitam ou que não deveriam ter acesso a eles. Garantir a confidencialidade significa que a informação é organizada em termos de quem deveria ter acesso, bem como a sua sensibilidade. Entretanto, a quebra de sigilo pode ocorrer através de diferentes meios, como por exemplo, a engenharia social. (BROOK, 2010)
- A integridade dos dados refere-se à certeza de que os dados não são adulterados, destruídos ou corrompidos. É a certeza de que os dados não serão modificados por pessoas não autorizadas. Existem basicamente dois pontos durante o processo de transmissão no qual a integridade pode ser comprometida: durante o carregamento de dados e/ou durante o armazenamento ou coleta do banco de dados. (BROOK, 2010)
- A disponibilidade dos dados e da informação significa que esta está disponível quando for necessária. Para que um sistema demonstre disponibilidade, deve dispor um sistema computacional, de controles de segurança e canais de comunicação de bom funcionamento. A maioria dos sistemas disponíveis são acessíveis em todos os momentos e tem garantias contra falhas de energia, desastres naturais, falhas de hardware e atualizações de sistemas. A disponibilidade é um grande desafio em ambientes colaborativos como tais ambientes devem ser estáveis e continuamente mantido. Tais sistemas também devem permitir que os usuários acessem as informações necessárias com o tempo de espera pequeno. Sistemas redundantes pode ser posto em prática para oferecer um alto nível de fail-over. O conceito de disponibilidade pode também referir-se a usabilidade de um sistema. Segurança da informação refere-se à preservação da integridade e do sigilo, quando a informação é armazenada ou transmitida. Violações de segurança da informação ocorrem quando as informações são acessadas por pessoas não autorizadas ou festas. Violações podem ser o resultado de ações de hackers, as agências de inteligência, os criminosos, concorrentes, funcionários ou outros. Além disso, pessoas que valorizam e desejam preservar a sua privacidade está interessado em segurança da informação. (BROOK, 2010)

Segundo Campos:

> Conhecer os conceitos sobre segurança da informação não significa necessariamente saber garantir essa segurança. Muitos têm experimentado esta sensação quando elaboram seus planos de segurança e acabam não atingindo os resultados desejados. (CAMPOS, 2007, p. 29)

Segurança da informação refere-se à preservação da integridade e do sigilo, quando a informação é armazenada ou transmitida. Violações de segurança da informação ocorrem quando as informações são acessadas por pessoas não autorizadas ou festas. Violações podem ser o resultado de ações de hackers, as agências de inteligência, os criminosos, concorrentes, funcionários ou outros. Além disso, pessoas que valorizam e desejam preservar a sua privacidade está interessado em segurança da informação (BROOK, 2010).

Segundo a Pesquisa Global de Segurança da Informação (PWC, 2013), houve uma queda no uso de ferramentas de segurança sendo observado um relaxamento das políticas que estabelecem padrões nas organizações.

As organizações precisam adotar controles de segurança – medidas de proteção que abranjam uma grande diversidade de iniciativas – que sejam capazes de proteger adequadamente dados, informações e conhecimentos, escolhidos levando-se em conta os riscos reais a que estão sujeitos esses ativos (BEAL, 2005).

2.2 MECANISMOS DE SEGURANÇA E CONTROLE

Um meio de se aplicar e suportar os princípios básicos de segurança da informação é o de estabelecer mecanismos de segurança e controle, que podem ser físicos ou lógicos.

Aplicar controles é um dos aspectos para se atingir a segurança da informação, assim diz a ABNT (2013): “ a segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, cultura organizacional e funções de software e hardware”. A norma também destaca nesse mesmo item a importância de manter, monitorar e melhorar controles. “Estes controles precisam ser estabelecidos, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação sejam atendidos” (ABNT NBR ISO/IEC:27002, 2013, item 0.1).

Segundo Abreu (2015), controles físicos são as barreiras que dificultam o contato ou acesso direto à informação ou infra-estrutura a qual garante a sua existência, a exemplo das portas, trancas, paredes e blindagens.

Controles lógicos podem ser definidos como barreiras que impedem ou limitam acesso à informação em meio eletrônico, a exemplo da criptografia, assinatura digital e autenticação.

Controladores lógicos são apoiados por mecanismos de segurança tais como a criptografia e a assinatura digital, porém é mais comum encontrar na Internet, limitadores e controladores de acesso para autenticação de usuários, por meio de um sistema de senhas (ABREU, 2015).

Da Silva e Stein (2007) discutem, contudo, que os requisitos para a elaboração de uma senha segura esbarram na capacidade cognitiva de seus usuários, dando origem a inúmeros problemas.

2.2.1 Senhas

Uma senha é um mecanismo de autenticação, usada no processo de verificação da identidade, assegurando que a pessoa que acessa a informação é quem realmente diz ser.

Uma senha fácil de ser decifrada pode ser obtida por pessoas mal intencionadas e uma vez autenticado como outra pessoa, passa obter informações e desferir ataques sem ser identificada.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.b (2006), aconselha que nomes, sobrenomes, números de documentos, placas de carros e números de telefones estejam fora das senhas, além de apontar regras para a elaboração de seguras.

Segundo ANAHP (2015), as boas práticas recomendadas para política de senhas são:

1) Definir prazos de expiração, que obrigue o usuário a trocar a senha periodicamente.

2) Impedir que a nova senha seja repetida.

3) Obrigar a conciliação de números, letras e até caracteres especiais para que a complexidade seja maior e assim a senha seja menos suscetível a ataques baseados em dicionários de senhas.

4) Obrigar uso de caracteres em maiúsculo e minúsculo.

5) Estabelecer um tamanho mínimo de senha, de pelo menos 8 caracteres.

6) Em casos de segurança avançada, utilização de sistemas de autenticação complementares, a exemplo da biometria.

Os hospitais que disponibilizam serviços e informações pela internet, referentes a dados pessoais de pacientes ou profissionais de saúde, devem requisitar o fornecimento destes dados por meio de consentimento livre e expresso do usuário, principalmente antes de disponibilizar quaisquer dados pessoais colhidos a terceiros.

2.2.2 Gerenciamento de identidade e perfis de acesso

O Gerenciamento de Identidade surgiu como um fundamento essencial para redução de custos, controle de gestão, eficiência operacional e o crescimento dos negócios. Os hospitais precisam gerenciar o acesso às informações e aplicativos espalhados por diversos locais. Além disso, devem fornecer acesso para um número crescente de identidades, sem comprometer a segurança ou exposição de informações sigilosas. Gerenciamento de Identidade é definido como "processos de negócios e TI das organizações, aplicadas para garantir a integridade e a privacidade de identidade, permitindo o acesso, sendo crucial para a segurança da informação.

O controle de acesso é a forma com que uma instituição vai controlar o uso de recursos de uma forma geral. Os modelos de controle de acesso estão divididos em três tipos básicos:

1) O tipo MAC (*Mandatory Access Control*) ou Controle de Acesso Mandatório é um modelo em que o administrador do sistema é responsável por atribuir as devidas permissões para os usuários. Este modelo utiliza o conceito de "Label" para identificar o nível de sensibilidade a um determinado objeto. (ANAHP, 2015)

2) O modelo DAC (*Discretionary Access Control*) ou Controle de Acesso Discricionário é um modelo mais flexível do ponto de vista do usuário que deseja compartilhar recursos para outros usuários. Neste modelo, o usuário tem o controle de garantir privilégios de acesso aos recursos que estão sob a sua responsabilidade. O administrador do sistema precisa ter um cuidado adicional quando adota esse modelo é empregado pois os usuários podem dar mais permissões do que deveriam e com isso abrir uma brecha que pode ser explorada. (ANAHP, 2015)

3) No controle baseado em cargo (RBAC – *Role -Based Access Control*), o administrador do sistema garante privilégios de acordo com a função exercida pelo usuário. Este modelo é

totalmente voltado para a função que o usuário desempenha dentro da instituição. (ANAHP, 2015)

Segundo ANAHP (2015), as melhores práticas para o controle de acesso administrativo são:

1) A Política de Menor Privilégio, onde o acesso negado para todos. O usuário que não tem permissão para acessar determinada informação deve requerer o acesso. A solicitação será avaliada e, caso o acesso seja permitido, caberá ainda definir até que ponto o usuário poderá ter acesso à informação em questão.

2) A política de separação de tarefas é baseada na premissa de que um único usuário não pode ser responsável por tarefas que se intercalam, por exemplo, o usuário que emite uma nota fiscal não pode ser o mesmo que faz a aprovação da compra de um bem material.

Essas boas práticas de segurança da informação também ajudam a evitar fraudes em um ambiente de trabalho ou até mesmo uma conspiração onde mais de um usuário no ambiente tenta fraudar dados para fins de benefícios pessoal ou de terceiros.

2.2.3 Criptografia

Com o avanço da tecnologia da informação, a questão da privacidade, do anonimato e da segurança de transmissões de dados aumentou a importância da criptografia.

A criptografia é essencial para que se possa garantir a segurança em todo o ambiente computacional que necessite de sigilo em relação às informações. Pessoas mal intencionadas contam com sofisticados mecanismos que burlam sistemas de segurança e são capazes de interceptar a comunicação de uma rede. Caso não haja um bom sistema de criptografia implementado nos envios e recebimentos de informações desta rede, os dados estarão vulneráveis.

Com um sistema de criptografia implementado, a informação armazenada ou enviada de um sistema é codificada. Ao chegar em seu ponto de destino, ela é decodificada com o uso de uma chave de criptografia. Somente o destinatário real terá posse desta chave, de forma que, caso a mensagem seja interceptada, ela não poderá ser lida corretamente. (ANAHP, 2015)

Existem dois tipos principais de criptografia: a simétrica e a assimétrica. Na criptografia simétrica, o algoritmo e a chave são iguais. Isso significa que o remetente e o destinatário usam a

mesma chave. A criptografia assimétrica utiliza uma chave (pública) para criptografar e outra (privada) para descriptografar. Podemos dizer que, ao invés de compartilhar uma chave secreta, utiliza-se duas chaves matematicamente relacionadas. Uma das chaves é aberta para que todos possam ver (chave pública) e a outra é mantida em sigilo (chave privada). Dessa forma, uma mensagem criptografada com uma chave pública, somente poderá ser descriptografada com a chave privada correspondente do destinatário. (ANAHP, 2015)

A criptografia assimétrica é usado com maior frequência na Internet, pois é mais viável tecnicamente, uma vez que não se sabe previamente para onde serão enviados os dados. Se fosse usada a criptografia simétrica, poderíamos ter grandes problemas, pois para distribuir a chave para todos os usuários autorizados, teríamos um problema de atraso de tempo, e possibilitar também que a chave chegue a pessoas não autorizadas. (ANAHP, 2015)

3 A INTERNET DAS COISAS (IoT)

A Internet das Coisas pode ser definida como um novo mundo em que os objetos estarão conectados e passarão a realizar tarefas sem a interferência humana (ASHTON, 2015).

A IOT pode ser contemplada como uma estrutura de rede abrangente, consistindo de vários tipos de objetos, que dependem de tecnologias de sensores, de comunicação, de rede e de processamento de informações. A tecnologia base para IOT é identificadores de rádio frequência (RFID, em inglês), que permite que os microchips transfiram dados de identificação para o leitor por meio sem fio. Através dessa tecnologia, pode-se analisar, rastrear e monitorar os objetos conectados com suas *tags*. Outra tecnologia fundamental é a *Wireless Sensor Networks* (WSNs), que funciona principalmente em sensores inteligentes para detecção e monitoramento. A RFID encontra sua aplicação no transporte de mercadorias aos consumidores, produção de produtos farmacêuticos e varejo desde o ano 1980 e a WSN se aplica ao tráfego, saúde e monitoramento. O avanço em ambas as tecnologias acelera o crescimento da IoT. Muitas outras tecnologias e dispositivos, incluindo códigos de barras, serviços baseados em localização, comunicação de campo próximo e computação em nuvem já estão começando a fazer uma rede abrangente para fortalecer a IoT (MEHTA, 2018).

De acordo com Peter Waher (2015) a Internet das Coisas é algo que obtemos quando conectamos as coisas, não operadas por seres humanos, à Internet. Atualmente a principal forma

de comunicação da Internet é humana e segundo o autor a IoT pode ser considerada como a futura avaliação da Internet que realiza aprendizagem máquina a máquina (M2M, do inglês Machine to Machine) fornecendo conectividade para todos e tudo. (PETER WAHER, 2015).

A ideia básica do IoT será permitir uma conexão autônoma e segura e troca de dados entre dispositivos e aplicações do mundo real (FAN e CHEN, 2010).

Imaginemos um hospital capaz de manter a atenção contínua em cada sinal vital de pacientes internados em enfermarias e ajustar automaticamente os parâmetros, sem a intervenção humana. Ou um idoso que tenha sensores que alertam equipes de emergências sobre um potencial ataque cardíaco. Com dispositivos habilitados para IoT, os hospitais estarão capazes de monitorar pacientes de forma mais eficiente, independente de onde estejam, e ter a informação coletada, armazenada e enviada em qualquer lugar e para qualquer lugar.

3.1 O SURGIMENTO DA IoT

Conforme Ashton (2015), o termo IoT foi originado em 1999, quando ele escreveu um artigo chamado “As coisas da Internet das Coisas”. Segundo ele, a falta de tempo das pessoas abre portas para que ferramentas sejam criadas para fazer coisas que, de fato, não necessitam ser feitas por pessoas. Podem ser substituídas por dispositivos. Dispositivos esses, que conversando por diferentes protocolos dentro da mesma rede, conseguem acompanhar as pessoas, ler suas atividades, gerar informações e a partir daí auxiliá-las no dia a dia.

Os dispositivos universais de acesso digital também são uma poderosa tendência, de grande influência para o futuro da informática em saúde. Esse termo significa que diversos dispositivos digitais que antes tinham funções específicas e separadas, como acesso e navegação na Internet, telefonia fixa e celular, TV, rádio, videogames, máquinas fotográficas e de vídeo, etc., rapidamente estão adicionando funções que os tornam máquinas universais. Por exemplo, tocadores de MP3 podem navegar na Internet e mandar e-mails, além de tocar músicas. Aparelhos de TV navegam na Internet e podem fazer videoconferência, telefones celulares permitem comunicação por voz e vídeo, e também acessam e-mail e a Web, fornecem mapas e orientações de caminho por GPS e tocam vídeos e áudios, alguns aparelhos de videogame já são computadores poderosos, capazes de muitas funções que só se encontram em desktops mais complexos, e assim progressivamente. Os *smartphones*, especialmente, estão tendo um grande

impacto nos EUA e Europa quanto ao desenvolvimento de uma área inteiramente nova e de acelerado crescimento, denominada de mHealth (e-saúde móvel, ver Anta *et al*. 2009, e o extenso artigo na Wikipedia, 2010a). Nos EUA, cerca de 94% dos médicos já utilizam *smartphones* na sua profissão, sendo que 75% deles são os iPhones da Apple, um grande divisor de águas na mHealth (SPYGLASS, 2010).

3.2 APLICAÇÕES DA IoT

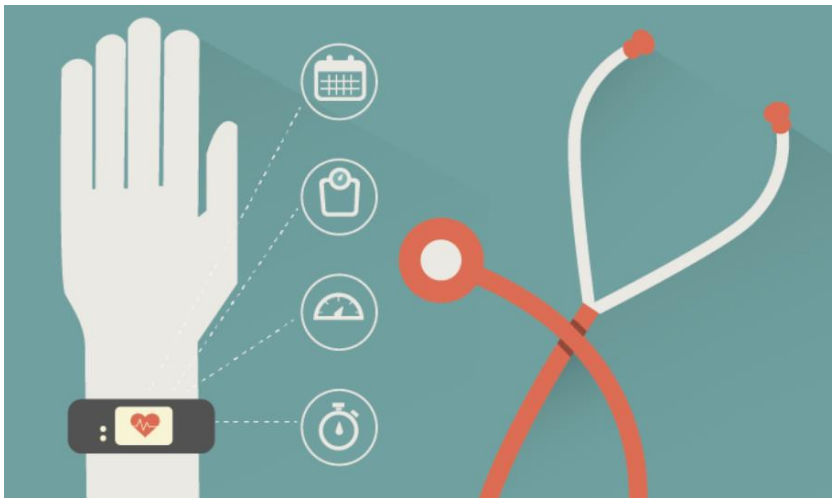
São muitos os domínios de aplicações que serão impactados pela IoT. Podem ser classificadas com base no tipo de disponibilidade de rede, de cobertura, heterogeneidade, escala e envolvimento do usuário. Não há quase nenhuma área de aplicação onde o IoT não consiga encontrar uma função e principalmente não há área de aplicação onde a IoT não traga alguma vantagem econômica ao longo do tempo (SILVA, 2017).

A IoT é a base do processo de digitalização da economia, que tem transformado os métodos tradicionais de produção, no uso das tecnologias de informação e comunicação e na interconexão de dispositivos. A conexão entre sistemas de TI, subsistemas, processos, objetos e aplicativos, que se comunicam entre si e com humanos, é o vetor chave dessa transformação, e é esperado que as aplicações de IoT e as tecnologias digitais promovam ganhos de produtividade e competitividade das nações. Isso ganha ainda maior importância para o Brasil, dado que nas últimas décadas vem perdendo sua capacidade de agregação de valor da produção industrial em comparação às demais economias em desenvolvimento e também perdeu posições no ranking de competitividade industrial para países emergentes, mostrando o quão iminente é que o País tome ações para estimular o desenvolvimento de tecnologias que garantam maior produtividade e competitividade nos setores básicos da economia. É importante também destacar a relevância do envolvimento de setores de governo, empresarial e comunidade científica em iniciativas voltadas à adoção e ao desenvolvimento da Internet das Coisas e das novas tecnologias digitais; à padronização de aplicações digitais; à segurança digital; à modernização do marco legal; à formação e à capacitação profissional; e à melhoria do ambiente de negócios e da infraestrutura. Face a esse 131 reconhecimento, esforços têm sido destinados à expansão do uso de IoT e das tecnologias digitais no Brasil. O Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), juntamente com a iniciativa privada, academia e órgãos de governo num esforço de

construção de uma política pública para o tema, conseguiu a criação do Plano Nacional de Internet das Coisas, cujo objetivo é “acelerar a implantação da Internet das Coisas como instrumento de desenvolvimento sustentável da sociedade brasileira, capaz de aumentar a competitividade da economia, fortalecer as cadeias produtivas nacionais e promover a melhoria da qualidade de vida”. Todos os agentes envolvidos na criação do Plano compartilham da aspiração de que a Internet das Coisas tenha um impacto positivo, relevante e rápido na economia e na vida das pessoas. Para atingir esse objetivo, o Plano Nacional de IoT atuará em diversas dimensões, estabelecendo diretrizes gerais e propondo iniciativas concretas (BRASIL, 2018).

No domínio da saúde humana estão concentradas as aplicações de IoT que tem por principal objetivo melhorar a saúde e o bem-estar através de dispositivos que estão dentro do contexto do corpo humano, não necessariamente relacionados com dispositivos conectados em hospitais ou outras instalações médicas. Diferente de outras aplicações de IoT, onde uma leitura de um sensor pode iniciar uma ação específica como desligar uma chave, os dados de sensores voltados ao corpo humano fornecem informações (Fig. 2) que as pessoas utilizarão em suas ações e decisões, seja para convencê-las a migrarem para hábitos de vida mais saudáveis, para ajudá-las a seguir corretamente prescrições médicas ou manter um médico informado com acesso a dados em tempo real de seus pacientes. (Technology Advice Company, 2017).

Figura 2 - IoT na Saúde



Fonte: TechnologyAdvice - healthcare, 2017.

Três tecnologias dividem os dispositivos utilizados na saúde humana, a tecnologia portátil encontrada sob o termo “Wearables”, do inglês “vestir” que em sua tradução literal significa

"vestível", a tecnologia não portátil encontrada sob o termo "Non-Wearable" e a tecnologia injetável encontrada sob o termo "Implantables" (McKinsey & Company, 2015).

3.2.1 IoT e o monitoramento remoto

O surgimento da Internet das Coisas possibilitou uma série de avanços tecnológicos na saúde. Por meio de dispositivos conectados remotamente é possível reunir automaticamente uma série de informações sobre o estado da saúde do paciente, que ajudam no trabalho de diagnóstico e posterior tratamento ou prevenção (MASSOLA e PINTO, 2018).

Conforme a empresa de consultoria Tractica (2016), com a ajuda da IoT é possível medir indicadores como a pressão arterial, batimentos cardíacos e temperatura corporal à distância. Esses dados são enviados para aplicativos e analisados pelos profissionais da saúde. Com isso, é possível evitar uma série de complicações decorrentes da falta de atendimento, tomando as medidas necessárias o mais rapidamente possível e diminuindo consideravelmente os índices de hospitalização desnecessárias.

Também há os chamados wearables, que são dispositivos usados como peças de vestuário, conectados à internet, que transmitem em tempo real atualizações sobre o estado de saúde do paciente. Hoje existem pulseiras, colares ou relógios que enviam automaticamente um sinal para a equipe de saúde caso algum indicador fuja dos parâmetros de controle. De acordo com um relatório da consultoria Tractica (2016), as remessas mundiais de produtos de saúde aumentarão de 2,5 milhões em 2016 para 97,6 milhões de unidades anualmente até 2021. No final desse período, a firma de inteligência de mercado prevê que o mercado global de produtos de saúde será responsável por US $ 17,8. bilhões em receita anual.

As possibilidades são verdadeiramente ilimitadas e IoT tem o potencial de afetar a área de saúde em diversas vertentes.

3.2.2 Uso da IoT no acompanhamento de recém-nascidos

Em um hospital de Boston, sensores são utilizados para fins de segurança. Bebês recém-nascidos recebem pulseiras, permitindo que uma rede sem fio os localize a qualquer momento. Se um recém-nascido for levado muito perto de uma porta de saída sem ser desconectado, os

elevadores irão parar e as portas de saída serão travadas. E na unidade de terapia intensiva neonatal, os enfermeiros recebem alertas em telefones celulares hospitalares sobre as condições médicas de seus pacientes, incluindo a frequência cardíaca e as mudanças de oxigênio que os sensores detectaram, permitindo que eles cheguem ao leito dos pacientes mais rapidamente. Além disso, o uso da IoT nos serviços de saúde permitiu que o hospital atualizasse prontuários eletrônicos mais rapidamente. O hospital também instalou sensores sem fio em geladeiras, freezers e laboratórios para garantir que amostras de sangue, medicamentos e outros materiais sejam mantidos nas temperaturas adequadas (GUIA ESSENCIAL TECHTARGET, 2016).

Segundo Jim Piepenbrink, diretor de engenharia clínica do hospital de Boston, as temperaturas eram registradas e documentadas manualmente. Mas agora, com a instalação de sensores sem fio, gerou uma grande economia de tempo para a equipe de saúde do local.

3.2.3 IoT no gerenciamento de estoque em hospital

Conforme Ganguly (2016), os hospitais não estão usando a IoT para rastrear estoque da maneira mais ampla que seria desejável. Ele acrescentou que a saúde poderia aprender algumas lições do varejo.

Para os hospitais, a grande vantagem que eles podem obter do gerenciamento de estoques com a IoT será em áreas como farmácia e controle geral de estoque em depósitos.

3.2.4 A IoT no monitoramento de paciente com doenças crônicas

O maior benefício e impacto econômico das aplicações nesta área concentra-se no uso de dispositivos de IoT para monitorar o tratamento de pacientes com doenças crônicas, diminuindo a incidência de crises graves geradas por doenças como a diabetes por exemplo. A falta de um tratamento correto, a não adesão à mudança hábito saudáveis e o descuidado em tomar a medicação adequadamente podem triplicar os custos de um tratamento do paciente que possua uma doença crônica, principalmente quando este tem seu quadro clinico piorado onde acaba o paciente debilitado e com baixa imunidade tendo que voltar a salas de emergências ficando sujeito a novas complicações e até mesmo vulnerável a outras doenças (Maribel Salas, 2009).

Os benefícios incluem uma melhor aceitação do paciente, detecção precoce na alterações de suas condições e um gerenciamento do tratamento em tempo real, alertando os pacientes para que verifiquem com os médicos se as leituras indicarem algum perigo potencial. Nas economias em desenvolvimento, os monitores de saúde em casa podem ser proibitivamente caros, mas esses dispositivos podem ser usados para avaliar pacientes remotamente em clínicas rurais de saúde o que acaba agregando um valor potencial em locais remotos (McKinsey & Company, 2015).

Sem acesso a séries temporais contínuas de dados, os médicos muitas vezes não conseguem detectar mudanças críticas nas condições do paciente com antecedência suficiente para prevenir emergências. Por exemplo, atualmente um paciente que mora no Reino Unido, de meia-idade e um pouco acima do peso, sofre de insuficiência cardíaca crônica, hipertensão arterial e diabetes tipo 2. Ele está sendo tratado com um diurético, seguindo as recomendações de dieta e exercícios de seu médico. Durante as férias, acaba relaxando com suas restrições e sente-se um pouco mais inchado, mas não se preocupando com isso. Algumas semanas antes de seu próximo check-up, ele entra em colapso com insuficiência cardíaca crônica, é hospitalizado por 12 dias a um custo de US $ 4.500, pago pelo SUS, e em seguida, passa por uma estadia de reabilitação. Futuramente, com o uso da IoT, seria possível que o paciente, com quatro dispositivos conectados, sendo: uma balança de peso, um medidor de pressão arterial, uma caixa de comprimidos inteligente e uma pulseira que rastreie sua frequência cardíaca e nível de oxigênio no sangue (custando menos de US $ 300) , pudessem detectar rapidamente uma mudança em sua condição, percebendo que ele está ficando cansado mais rapidamente durante as caminhadas e que não está tomando corretamente seus medicamentos durante as férias. É importante ressaltar que a balança também captou um aumento de 2 kg em seu peso, em apenas alguns dias - um sinal de aumento da retenção de líquidos. Tudo indica então, que deve ser solicitado uma consulta imediata ao seu médico e talvez um aumento na dosagem de seu diurético. Seu médico recebe um alerta com todas essas informações e lhe agenda uma consulta rapidamente, lembrando o paciente como é importante não faltar ao diurético. Em uma visita na semana seguinte, o médico vê que o peso do paciente caiu e ele é capaz de respirar facilmente durante as atividades normais, recomendando que ele siga a uma dieta rigorosa e tome seus medicamentos fielmente, mesmo durante feriados. Estimativas do Mckinsey Global Institute (2015), mostram que os aplicativos de IoT podem reduzir o custo dos cuidados com doenças crônicas a pacientes em 10 a 15%, baseados em experiência de dados clínicos recentes. Alguns

testes de monitoramento remoto indicaram potenciais reduções de custos superior a 50% no tratamento de populações agudas, mas espera-se que essa grande redução de custos não seja sustentável em populações maiores de pacientes. No entanto, se a tecnologia de saúde é capaz de atingir todo o seu potencial para melhorar a adesão a terapias prescritas, a IoT poderia reduzir o custo do tratamento de um paciente com doenças em 50 %. Benefícios adicionais podem ser obtidos se os sistemas baseados em IoT puderem gerar mudanças substanciais em dieta e exercício. Atualmente, a capacidade de incentivar essas mudanças no estilo de vida é limitada. Com dados de monitoramento baseados em IoT, há mais oportunidades de feedback e reforço de prestadores de cuidados de saúde, de outros pacientes e familiares (MCKINSEY Global Institute, 2015).

4 MATERIAL E MÉTODO

O trabalho desenvolvido seguiu os preceitos do estudo exploratório, por intermédio de uma pesquisa bibliográfica qualitativa, que, segundo GIL (2017) "é desenvolvida a partir de material já elaborado, constituído de livros e artigos científicos".

A pesquisa bibliográfica procura explicar e discutir um tema com base em referências teóricas publicadas em livros, revistas, periódicos e outros. Busca também, conhecer e analisar conteúdos científicos sobre determinado tema (MARTINS, 2001).

A coleta de dados seguiu a seguinte premissa:

a) Leitura Exploratória de todo o material selecionado (leitura rápida para verificar se a obra interessa ao trabalho);

b) Leitura Seletiva aprofundando o conhecimento nos quesitos mais importantes; e

c) Registro das informações extraídas das fontes em instrumento específico (autores, ano de publicação, método utilizado e conclusões).

Foi realizada, também, uma leitura analítica a fim de ordenar a sequência das informações obtidas, de forma a viabilizar a resposta ao problema da pesquisa.

5 POLÍTICAS PARA DESENVOLVER A CULTURA DE SEGURANÇA DA INFORMAÇÃO COM O ADVENTO DA INTERNET DAS COISAS

Um dos maiores inimigos da segurança é o excesso de confiança, com isso, os dispositivos de IoT são um alvo atraente para os criminosos, já que coletam informações privadas sobre o comportamento do usuário em diversas áreas, dentre elas a de saúde.

Proteger a Internet das Coisas será uma tarefa complexa e difícil, sua população estimada em bilhões de objetos, que irão interagir uns com os outros e com outras entidades, como seres humanos ou entidades virtuais, criam muitas possibilidades de ataques disponíveis à pessoas mal-intencionadas ataque a vários canais de comunicações, ameaças físicas, negação de serviço, fabricação de identidade entre outras (Babar e Mahalle, 2010).

Existem muitas brechas de segurança envolvendo a IoT, entre os exemplos dessas possíveis brechas estão a marcação de consultas pelo celular. Se o celular é capaz de realizar a marcação de uma consulta, nele podem estar disponíveis dados pessoais de acesso restrito, ou até mesmo informações bancárias. Este aspecto se agrava ainda mais quando os dados de um sistema hospitalar estão salvos em uma nuvem.

A norma ABNT NBR ISO/IEC 27002, que dispões dos controles para implementação de um sistema de gestão da segurança da informação baseado na ABNT NBR ISO/IEC 27001, recomenda a existência de políticas de segurança da informação, pois "convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas interessadas" (ABNT NBR ISO/IEC 27002, 2013, item 5.1.1).

A Política de Segurança atribui direito e responsabilidades às pessoas que lidam com os recursos computacionais de uma instituição e com as informações nelas armazenadas. Ela também define as atribuições de cada um em relação à segurança dos recursos com os quais trabalham. Uma Política de Segurança também deve prever o que pode ser feito na rede da instituição e o que será considerado inaceitável. Tudo o que descumprir a Política de Segurança pode ser considerado um incidente de segurança. Na Política de Segurança também são definidas as penalidades as quais estão sujeitos àqueles que não cumprirem a política (CERT.BR, 2005).

Segundo Monteiro (2009), para que uma política de segurança da informação seja eficiente, deve-se garantir a disponibilidade, integridade, confidencialidade, legalidade e autenticidade das informações, deixando explícito o comprometimento da alta direção. Ainda de acordo com Monteiro (2009, p. 21) "É recomendado para sua elaboração, ter profissionais de

diversos departamentos ou setores da organização, formando um Comitê de Segurança da Informação [...] com a finalidade de compor o documento da política".

A política de segurança da informação pode ser composta por um ou por vários documentos, não existe uma definição de quantidade ou estrutura do conjunto desses documentos, o importante é que eles estejam atrelados, assim diz o Manual de Boas Práticas em Segurança da Informação do Tribunal de Contas da União, que se expressa da seguinte forma: “A Política de Segurança da Informação pode ser composta por várias políticas inter-relacionadas. Ademais, quando a instituição achar conveniente e necessário, sugere-se a criação de outros documentos que especifiquem práticas e procedimentos e que descrevam com mais detalhes as regras de uso da tecnologia da informação" (TCU, 2012, p. 12).

Para Ferreira e Araújo (2008, p. 36), a Política de Segurança define o conjunto de normas, métodos e procedimentos utilizados para a manutenção da segurança da informação, devendo ser formalizada e divulgada a todos os usuários que fazem uso dos ativos de informação.

A análise da bibliografia e as normas anteriormente citadas permitiram elencar ações visando a segurança da informação como se segue:

1. Analisar os riscos;
2. Definir os controles;
3. Criar o Plano de Segurança da Informação;
4. Aplicar o Plano de Segurança da Informação; e
5. Treinar dos usuários.

5 CONSIDERAÇÕES FINAIS

É oportuno afirmar que a informação circula nos ambientes hospitalares por vezes sem a segurança adequada. Como foi visto no trabalho, a segurança da informação carece de tecnologia, mas também de pessoal capacitado. Necessita de planejamento, mas também de ações efetivas. Exige que se conheça as ameaças e os riscos, mas também o próprio hospital. Se tais medidas forem ignoradas, poderão haver sérias consequências e, por isso, investimentos nessa área são imprescindíveis. A conclusão é que só há sucesso concreto quando todos os envolvidos, desde o próprio usuário até o diretor do hospital, se conscientizam da importância de adotar algumas medidas de segurança (uso de senhas para acesso, gerenciamento de identidades e perfis de acesso, sistema de criptografias) capazes de proteger a informação de suas reais ameaças. As

informações aqui contidas são suficientes para que, no mínimo, se tenha uma visão geral sobre as ameaças e soluções associadas à segurança da informação, permitindo até mesmo a elaboração de uma política de segurança da informação ou a melhoria dessa, caso já exista.

É evidente que neste novo cenário, com o advento da IoT, o profissional de tecnologia da informação de um hospital deve possuir um novo perfil, voltado para a preocupação constante com a atualização tecnológica e a busca do autoaperfeiçoamento. O que se vê na prática é que o profissional de TI deve ser um agente multidisciplinar, capaz de transportar uma bagagem de todos os conhecimentos desejáveis, como por exemplo habilidades em auditoria e forense computacional.

Em que pese ser muito importante investir em tecnologia, atualmente, não basta investir apenas em conhecimentos técnicos. É preciso desenvolver as capacidades humanas. Uma das grandes tendências em segurança da informação está no desenvolvimento de pessoal. É necessário investir em programas de conscientização, pois na maioria das vezes o elo mais fraco na corrente da segurança é o ser humano.

Para trabalhos futuros, julgo ser interessante uma análise sobre o novo perfil do profissional de tecnologia da informação e o aperfeiçoamento dos mecanismos de proteção frente às novas ameaças.

REFERÊNCIAS

ABREU, LEANDRO FARIAS DOS SANTOS. **A Segurança da Informação nas Redes Sociais.** São Paulo, 2011.

ANAHP. **Segurança da Informação para Hospitais. Recomendações e melhores práticas para proteger a privacidade do paciente e confidencialidade das informações do hospital**. 2015. Online. Disponível em: <http://anahp.com.br>. Acesso em 20 maio. 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002: **Tecnologia da Informação: Técnicasde Segurança: Código de prática para controles de segurança de informação**. 2013.

ARAÚJO, L. G. S; BEZERRA, E. K; COELHO, F. E. S. **Gestão da Segurança da Informação**. Rio de Janeiro: RNP/ESR, 2014.

BEAL, Adriana. **Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações** – São Paulo: Atlas, 2005.

BRASIL. Decreto Nr 3.505. **Política de Segurança da Informação**. Brasília, 2000.

BRASIL. **Estratégia brasileira para a transformação digital. Brasília, 2018.** Disponível em: http://www.mctic.gov.br/mctic/opencms/publicacao/publicacoes.html-estrategia_digital.pdf.

BRASIL. TCU. **Manual de Boas Práticas em Segurança da Informação**. 4. ed. Brasília. 2012.

BROOK, Jon-Michael C. CIA Triad. **CIPP Guide**, Estados Unidos da América, ago. 2010.

CAMPOS, André. **Sistema de Segurança da Informação**. 2. ed. Florianópolis: Visual Books, 2007.

CERT.br. **Cartilha de Segurança para Internet**. Comitê Gestor da Internet no Brasil, São Paulo, 2006. Disponível em: <https://cartilha.cert.br>. Acesso em 20 maio. 2018.

CONCEIÇÃO, V.M.. **A gestão da qualidade e a sistematização da assistência de enfermagem: uma revisão sobre sistemas de informações**. Revista de Enfermagem do Centro Oeste Mineiro, 2012.

FAN, T CHEN, Y A SCHEME. **Of Data Management in the Internet of Things 2nd IEEE International Conference on Network Infrastructure and Digital Content.** 2010.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Marcio Tadeu. **Política de Segurança da Informação: guia prático para embalagem e implementação**. Rio de Janeiro: Ciência Moderna, 2008.

FINEP. **Entrevista exclusiva com o criador do termo "Internet das Coisas". 2015.** Disponível em: http://finep.gov.br/noticias/todas-noticias/4446-kevin-ashton-entrevistaexclusiva-com-o-criador-do-termo-internet-das-coisas.

GIL, Antonio Carlos, **Como Elaborar Projetos de Pesquisa**, São Paulo, Atlas (2017).

MARIBEL SALAS. **Costs of medication nonadherence in patients with diabetes mellitus: A systematic review and critical analysis of the literature. Value in Health. volume 12.** 2009.
MARTINS, A. P. **Saúde em rede**. Rev. Saúde Business. Ano 2, n.8.2009.

MARTINS, G. A. & PINTO, R. L. **Manual para elaboração de Trabalhos Acadêmicos**. São Paulo: Atlas. 2001.

MCKINSEY & COMPANY. **Industry 4.0 how to navigate digitization of the manufacturing sector.** 2015.

MEHTAA RIDHIKA, SAHNIB JYOTI, KHANNAC KAVITA. **International Conference on Computational Intelligence and Data Science.Internet of Things: Vision, Applications and Challenges.** 2018.

MONTEIRO, I. L. C. O. (2009). **Proposta de um Guia para elaboração de políticas de segurança da informação e comunicação em órgãos da APF**. (Dissertação de mestrado em Ciência da Computação. Universidade de Brasília, Brasília, DF, Brasil).

PEREIRA, S.R. et al. **Sistemas de Informação para Gestão Hospitalar**. J. Health Inform, 2012.

PWC. **Pesquisa Global de Segurança da Informação 2013**. Disponível em: <httt://www.pwc.com.br>. Acesso em 20 maio. 2018.

SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva**. Rio de Janeiro: Elsevier/Campus, 2003.

S. BABAR, P. MAHALLE, A. STANGO, N. PRASAD, R. PRASAD. **Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT).** 3rd International Conference on Recent Trends in Network Security and Applications, Chennai, India, 2010.

SILVA, Denise R. P.; STEIN, Lilian M. **Segurança da informação: uma reflexão sobre o componente humano.** Ciências & Cognição, Porto Alegre, 2007.

SILVA, LEANDRO JAMIR. **Monografia de Trabalho de Conclusão de Curso. Internet Das Coisas.** 2017.

SILZE CRISTINAMASSOLA, GIULIANO SCOMBATTI PINTO. **O uso da internet das coisas (IoT) a favor da saúde.** 2018.

SPYGLASS CONSULTING GROUP. **Healthcare Without Bounds: Point of Care Communication for Physicians. Market Analysis Report.** 2010. Disponível na Internet. URL: http://www.spyglassconsulting. com/Abstracts/Spyglass_PCOM_Physician_abstract.pdf

TECHNOLOGY ADVICE COMPANY. **http://technologyadvice.com/blog/healthcare/study-wearabletechnology-preventative-healthcare/**. 2017.

TECHTARGET. **Essential Guide. IOT for healthcare: Three use cases.** 2016. Disponível em: https://internetofthingsagenda.techtarget.com/feature/IoT-for-healthcare-Three-use-cases.

VILLAS BOAS, Maria Elisa. **O direito-dever de sigilo na proteção ao paciente**. Revista Bioética. 2015.

WAHER, PETER. **Learning Internet of Things Paperback.** Packt Publishing Ltd. Birmingham Mumbai, 2015.

ZAPATER, M.; SUZUKI, R. **Segurança da Informação: um diferencial determinante na competitividade das organizações**. Rio de Janeiro: Promon, 2005.