Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

Milenna Azevedo Pertile

A importância da segurança da informação nos hospitais

Americana, SP

2022

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

Milenna Azevedo Pertile

A importância da segurança da informação nos hospitais

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Esp. Bruno Henrique de Paula Ferreira

Área de concentração: Segurança da informação

Americana, SP.

2022

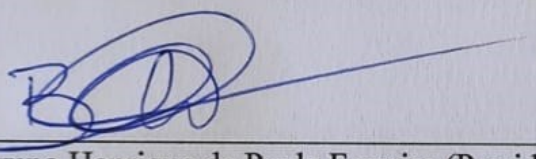
Milenna Azevedo Pertile

A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO NOS HOSPITAIS

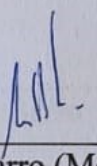
Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana – Ralph Biasi.
Área de concentração: Segurança da Informação.

Americana, 25 de junho de 2022

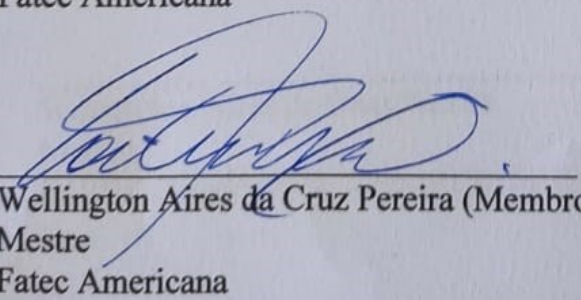
Banca Examinadora:



Bruno Henrique de Paula Ferreira (Presidente)
Especialista
Fatec Americana



Carlos Henrique Rodrigues Sarro (Membro)
Mestre
Fatec Americana



Wellington Aires da Cruz Pereira (Membro)
Mestre
Fatec Americana

A importância da segurança da informação nos hospitais.

Milenna Azevedo Pertile

Curso Superior de Tecnologia em Segurança da Informação – Faculdade de Tecnologia de Americana (FATEC Americana)
Americana – SP - Brasil

Milenna.pertile@outlook.com

Abstract.

The information is increasing even more in people's daily lives, and in the hospital environment it is no different. As the health-care organizations has a great demand of information about their patients, there is a huge risk of being hacked, that is why hospital adopt information security measures, policies and standards to protect them. The main objective of this work is to provide a new view on the topic, the importance of information security in hospitals, as well as to present problems and solutions for the use of IoT equipment in hospitals, besides of showing the opinions of some students and professionals of the area about de subject.

Keywords: Information Security, LGPD, Internet of Things.

RESUMO.

A informação está cada vez mais presente no cotidiano das pessoas, e no ambiente hospitalar não é diferente. Como as organizações da saúde possuem uma grande demanda de informações sobre seus pacientes, há um grande risco de as mesmas serem hackeadas, por isso os hospitais adotam medidas, políticas e normas de segurança da informação para protege-las. O objetivo central desse trabalho é proporcionar uma nova visão sobre o tema a importância da segurança da informação nos hospitais, como também apresentar problemas e soluções para o uso de equipamentos IoT nos hospitais, além de evidenciar as opiniões de alguns estudantes e profissionais da área sobre o assunto.

Palavras-chave: Segurança da informação, LGPD, Internet das coisas.

1. Introdução

Com o grande avanço tecnológico que vem ocorrendo nas últimas décadas, os hospitais, assim como outras áreas da saúde, tiveram que se adaptar a essa nova realidade. Exemplos dessas adaptações são impressora 3D (1984); robôs-cirurgiões (1998); nano robôs, um dos avanços tecnológicos mais recentes; *Software* médico como prontuários, tele consulta, agenda médica *online*, etc.; *wearables*.

Segundo Fontes (2006), a informação é um recurso que move o mundo. Por isso a informação possui um valor significativo para a organização e deve ser gerenciado e

utilizado da forma correta, garantindo que ela seja disponibilizada apenas para as pessoas que precisam dela para o desempenho de suas atividades profissionais.

Para Alves (2006) a segurança da informação busca proteger a informação garantindo a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócios. Sêmola (2003) define Segurança da Informação como a área de conhecimento que é dedicada à proteção dos ativos de uma organização.

A segurança da informação é muito importante para um hospital, uma vez que há a necessidade de preservar as informações e os equipamentos que as processam (HERATH; HERATH; BREMSER, 2010). Por existirem vários mecanismos de proteção para as informações e por estarem as informações relacionadas a outros ativos, é importante entender o ambiente no qual elas são transmitidas, processadas, armazenadas ou utilizadas (SILVA, 2009). Falhas no meio de transmissão, armazenamento, processamento ou utilização das informações podem torná-las indisponíveis ou expô-las a acessos não autorizados e alterações indevidas. (SÊMOLA, 2003; NOBRE; RAMOS; NASCIMENTO, 2010).

2. Segurança da Informação

A informação esteve presente em todas as fases do processo de evolução das organizações. Isso fez com que a informação se tornasse um ativo com grande importância passando a ser disseminada e disponibilizada entre diferentes organizações pelos meios de comunicação e tecnologia, que sofreram grandes avanços (SÊMOLA, 2003).

Segundo Junior e Santos (2012), a informação, além de ser um ativo organizacional e estar envolvida com tantos outros ativos, se destacada na tomada de decisões, com isso aumenta o impacto provocado pela sua divulgação por meios não autorizados. Para a ABNT (2005), a informação é o ativo mais precioso de uma organização e por isso, deve ser adequadamente protegida.

É necessário entender o ambiente onde as informações ficam armazenadas, processadas ou utilizadas, já que existem vários mecanismos para proteção das informações e os mesmos estão relacionados a vários outros ativos. Segundo Junior e

Santos (2012), o risco da divulgação não autorizada dos ativos aumentou devido à conexão dos dispositivos de redes e de equipamentos usados para acessar e transmitir informações. Com isso a necessidade de proteger as informações e os equipamentos aumentou, fazendo com que a administração de pessoas, políticas e programas, sejam tratados com uma prioridade cada vez maior (HERATH; HERATH, BREMSER, 2010).

Segundo Junior e Santos (2012), as falhas nas estruturas de transmissão, processamento, armazenamento ou utilização podem tornar as informações indisponíveis ou expô-las a acessos não autorizados e a alterações indevidas. A segurança da informação inclui a integridade dos equipamentos que compõem essas estruturas.

2.1. Políticas de segurança da informação

A Política de Segurança da Informação (PSI) é um documento que reúne regras, boas práticas, diretrizes e procedimentos a respeito da segurança da informação. Tem o objetivo de minimizar riscos de perdas ou violação de qualquer ativo de TI, além de assegurar que esses ativos, físicos ou lógicos estejam protegidos contra ameaças e riscos. Essa política protege as informações da sua empresa do que poderia causar algum dano intencionalmente ou não.

2.2. Normas de segurança da informação

As normas de segurança da informação foram criadas para fornecer as melhores práticas, diretrizes e princípios gerais para a implementação de sua gestão para qualquer organização (DONDA, 2016). Também servem para elaborar um Sistema de Gestão de Segurança da Informação (SGSI), com o objetivo de garantir a integridade, disponibilidade e a confidencialidade da informação, fatores essenciais no meio corporativo.

Existem várias instituições padronizadoras reconhecidas nacionais e internacionais, as mais evidenciadas para uma boa implementação da gestão da segurança da informação numa organização são (DONDA, 2016):

- ISO – *International Standardization Organization*.
- IEC – *International Electrotechnical Comission*.
- ABNT – Associação Brasileira de Normas Técnicas.

Algumas normas importantes:

- ISO:
    - ISO 27002:2005 –Padrão internacional para a gestão de segurança da informação
    - ISO 27004:2009 – Padrão referente aos mecanismos de mediação e relatórios para um sistema de gestão de segurança da informação (SGSI).
    - ISO 31000 – Norma que foi criada para tratar de assuntos relacionados a gestão de riscos.

- NBR´s (Brasil):
    - NBR 1333, de 12/1990 – Controle de acesso físico a CPDs (Centro de Processamento de Dados).
    - NBR 1334, de 12/1990 – Critérios de segurança física para armazenamento de dados.
    - NBR 1335, de 07/1991 – Segurança física de microcomputadores e terminais em estações de trabalho.
    - NBR 10842 – Equipamentos para Tecnologia da Informação requisitos de Segurança.
- Outras normas importantes:
    - O ITIL (*Information Technology Infrastructure Library*) é o modelo de referência para gerenciamento de processos de TI mais aceito mundialmente.
    - O COBIT (*Control Objectives for Information and Related Technology*) guia de boas práticas apresentado como *framework* e mapas de auditoria, conjunto de ferramentas de implementação e guia com técnicas de gerenciamento.

2.2.1 NBR ISO/IEC 27002:2013

A ISO 27002 é uma norma de segurança da informação que estabelece diretrizes e princípios gerais para iniciar, implementar manter e melhorar a gestão de segurança da informação em uma organização, além disso descreve as melhores

práticas para a implementação do SGSI. Essa norma contém um total de 14 seções de controle de segurança da informação, são eles (GASETA, 2022):

1. Políticas de segurança da informação;
2. Organização da segurança da informação;
3. Segurança em recursos humanos;
4. Gestão de ativos;
5. Controle de acesso;
6. Criptografia;
7. Segurança física e do ambiente;
8. Segurança nas operações;
9. Segurança nas comunicações;
10. Aquisição, desenvolvimento e manutenção de sistemas;
11. Relacionamento na cadeia de suprimento;
12. Gestão de incidentes de segurança da informação;
13. Aspectos de segurança da informação na gestão da continuidade do negócio;
14. Conformidade;

A norma recomenda que: "A política da segurança da informação deve ser analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia".

2.3. Lei Geral de Proteção de Dados (LGPD)

Primeiramente para definir o que é LGPD, é necessário saber a definição de dados e informações. Dado é um fato que está registrado, o mesmo, sozinho, não agrega nenhum valor ou traz conhecimento. Os dados pessoais são considerados, em sentido amplo, como todas as informações que estejam identificadas ou permitam identificar os indivíduos, tais como: nome, CPF, telefone endereço, data de nascimento, e-mail.

Já informação, por sua vez, é considerada o conjunto de dados moldados em um formato determinado dotado de significado e utilidade para o ser humano. Entende-se também como um dado processado de forma significativa para o usuário e que possui valor real ou percebido para decisões correntes e posteriores. Isto é, informação são os

dados que foram organizados e interpretados e possivelmente formatados, filtrados, analisados e resumidos (GORDON; GORDON, 2006).

> A Lei Geral de Proteção de Dados Pessoais (LGPD), dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Conforme o art. 5º da LGPD, dado pessoal é toda informação relacionada a pessoa natural identificada ou identificável. (Brasil, 2020).

2.3.1. LGPD nos hospitais

As organizações de saúde, tais como hospitais, consultórios, clínicas e etc., possuem uma grande demanda de dados de seus pacientes, uma vez que ao fazer o cadastro em um hospital, o paciente já fornece várias informações importantes, como, nome, endereço, histórico médico, documentos, nome de seus pais e entre outros. Além disso, junto com o cadastro fica armazenado os dados de todas as consultas, agendamentos, prontuários, exames, remédios, diagnósticos, atestados e outras informações relevantes.

Com o aumento da quantidade de pacientes que uma organização possui, há também o aumento da quantidade de dados que a organização arquiva. Segundo Brasil (2020), a Lei nº 13.787/2018, dispõe sobre os dados dos pacientes, que devem ser armazenados de acordo com os artigos:

> Art. 1º A digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente são regidas por esta Lei e pela Lei nº 13.709, de 14 de agosto de 2018.
>
> Art. 2º O processo de digitalização de prontuário de paciente será realizado de forma a assegurar a integridade, a autenticidade e a confidencialidade do documento digital.
>
> A organização hospitalar é encarregada de fornecer uma interface para que o indivíduo possa autorizar, bloquear ou revogar o consentimento para o tratamento de dados pessoais a qualquer momento. No mais, é obrigatório que haja, à disposição dos pacientes, uma maneira fácil de revogar o seu consentimento e, ainda, que a instituição tenha um controle e um armazenamento de documentos relativos a ele (digitais ou físicos). (Federação Brasileira de Hospitais, 2020).

Para um hospital ter a adequação correta da LGPD, é essencial que o agente de tratamento, o controlador ou operador, estruture um comitê responsável pelo projeto.

Neste comitê é essencial que estejam presentes pessoas da Alta Diretoria do hospital, pessoas de setores que tratam dados pessoais em seu dia a dia, funcionários dos Recursos Humanos, do Marketing, do Jurídico e do *Compliance*. Além disso, a instituição deve instruir os colaboradores a modo de assinarem um termo de responsabilidade para que, caso haja algum incidente, não seja possível uma futura alegação do desconhecimento das normas e dos procedimentos de segurança da informação presentes no ambiente hospitalar.

2.4. Segurança da Informação nos hospitais

O crescente avanço na tecnologia da informação modificou os métodos tradicionais de armazenamento de dados dos pacientes, tanto nas áreas administrativa como nas informações sobre a saúde dos pacientes, do papel para a tecnologia, como os *softwares* médicos (prontuário), por isso os hospitais devem ter ótimos profissionais de segurança da informação, para prevenirem e impedirem qualquer tipo de ataque e estarem por dentro da LGPD.

Helms, Moore e Ahmadi (2008) apresentam que o uso de sistemas de informações na saúde oferece importantes potenciais como, incremento da segurança do paciente, maior eficiência operacional e infraestrutura de TI já existente na maioria das organizações. Mas o uso também é permeado de fraquezas relevantes: falta de integração de sistemas, lenta adoção da tecnologia de informação e resistência ao uso de novas tecnologias e redesenho de processos.

A Organização Mundial de Saúde (OMS) define Sistema de Informação em Saúde - SIS como um conjunto de componentes que atuam de forma integrada, por meio de mecanismos de coleta, processamento, análise e transmissão da informação necessária e oportuna para implementar processos de decisões no Sistema de Saúde. Define, também, Sistema de Informação de Serviços de Saúde como aquele cujo propósito é selecionar os dados pertinentes a esses serviços, transformando-os em informação para aqueles que planejam, financiam, provêm e avaliam os serviços de saúde.

Segundo a ABNT (2005), a Política de Segurança da Informação serve como orientação e apoio da direção da organização para as iniciativas de segurança da informação, e deve expressar as intenções e diretrizes globais para preservação da confidencialidade, da integridade e da disponibilidade da informação.

Para as organizações que tem a obrigação legal de cuidar de suas informações ou de terceiros, sejam elas armazenadas de forma temporária ou definitiva, como organizações que prestam serviços de saúde, a necessidade de preservar essas informações é ainda mais evidente. Nesse contexto, as normas de segurança da informação são importantes balizadores, servindo como orientação para a adoção de controles que visam proteger as informações em uma diversidade de organizações e sobre diferentes aspectos, com destaque para a norma NBR ISO/IEC 27002:2013, um dos modelos mais destacados (Moraes; Mariano, 2008).

2.5. Cadastros e prontuários médicos

Os cadastros e prontuários médicos possuem informações extremamente valiosas para o hospital, já que são neles que são depositados os dados de todos os pacientes, desde sua data de nascimento até o último exame feito.

> O prontuário médico é um documento elaborado pelo profissional e é uma ferramenta fundamental para seu trabalho. Nele constam, de forma organizada e concisa, todos os dados relativos ao paciente, como seu histórico familiar, anamnese, descrição e evolução de sintomas e exames, além das indicações de tratamentos e prescrições. Feito no consultório ou hospital, o prontuário é composto de informações valiosas tanto para o paciente como para o próprio médico. Seu principal objetivo é facilitar assistência ao paciente. (CFM - Conselho Federal de Medicina).

Por serem arquivados em *softwares*, as informações estão sujeitas a serem hackeadas, e caso isso ocorra há um grande prejuízo para o hospital, uma vez que há a perda da credibilidade e, caso alguém o processe, ele precisa indenizar por danos morais.

Segundo Van Bemmel (1997 *apud* AZEVEDO NETO, 2003), o prontuário em papel vem sendo utilizado desde o século V a.C. Na época, Hipócrates já orientava os médicos a registrarem os dados em ordem cronológica, o chamado "Prontuário Orientado pelo Tempo", onde cada médico realizava anotações por datas, sendo um prontuário para cada médico, de forma que além de dificultar a procura por dados, elevava o número de prontuários por paciente e dificultava o cruzamento das informações obtidas.

Lawrence Weed (1969 *apud* AZEVEDO NETO, 2003) inseriu a ideia de um prontuário para cada problema, onde as anotações são registradas de acordo com a estrutura SOAP, onde:

S – Subjetivo (Queixas e sintomas do paciente);

O – Objetivo (encontrados por exames);

A– Abordagem diagnóstica (testes laboratoriais, por imagem, etc.);

P – Plano (terapêutico e cuidados), assim como são formados os prontuários hoje.

2.6. Aparelhos eletrônicos

No cotidiano de um hospital, mesmo se um elevador parar de funcionar, pode ser prejudicial para o paciente. Por serem dispositivos eletrônicos, muitos aparelhos presentes nos hospitais são vulneráveis a serem hackeados, já que precisam de um *software* para gerenciá-lo.

Se um dispositivo, como o respirador por exemplo, for alvo de um *hacker*, ele pode ter acesso a quantidade de oxigênio liberado para o paciente; pode desligar o aparelho e por fim acabar matando o paciente.

Vulnerabilidades e ameaças de *cyber* segurança podem impactar nas redes de TI e dos dispositivos médicos além de outros sistemas conectados na rede. Com o ataque, os pacientes, podem sofrer tanto dos impactos na segurança e privacidade de seus dados, como podem ser fisicamente afetados por ameaças e vulnerabilidades de segurança de seus dispositivos. Esse dano pode derivar do desempenho do próprio dispositivo, impedindo operações hospitalares ou a incapacidade de prestar cuidados. (NIST, 2018, Tradução nossa, *apud* MEURER, 2018),

> A vulnerabilidade dos dispositivos estava no Bluetooth onde em poucos segundos era possível infectar o dispositivo com um *malware*. Após infectado o dispositivo poderia infectar o computador de seus usuários e a partir dali abrir uma porta de acesso aos invasores. A partir deste momento as possibilidades obtidas pelos invasores vai até onde podemos facilmente imaginar. Além a falha de segurança dos dispositivos o vazamento de informações pessoais como de localização, rotina, batimentos cardíacos entre outros são muito críticos, pois além da comercialização dos dados existe o risco de manipulação dos mesmos. (ANDERSON, 2015 *apud* MEURER, 2018).

Segundo AbuDalbouh (2014 *apud* Magnagnagno, 2015), a utilização de dispositivos móveis nos ambientes hospitalares tem crescido devido à facilidade no

acompanhamento e evolução do paciente, uma vez que permite que médicos e enfermeiros possam verificar as condições dos pacientes, renovando e acrescentando as informações com agilidade. Porém, a utilização de aplicativos móveis muitas vezes transmite uma grande quantidade de dados pessoais em tempo real, tornando forte potencial de invasão de privacidade (FTC, 2009 *apud* Magnagnagno, 2015). Outra preocupação é principalmente com o acesso e manuseio interno de prontuário eletrônico, as informações de um paciente, estão contidas no documento e são registradas pela equipe médica, esse é um dos documentos que as pessoas mais têm o desejo e muitas vezes a necessidade de preservar (GAERTNER e SILVA, 2005 *apud* Magnagnagno, 2015).

2.7. Privacidade das informações dos pacientes

Ao falar de privacidade deve-se saber a definição da palavra. Para Silva (2001) privacidade pode ser entendida como um conjunto de informações acerca do indivíduo o qual ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em quais condições, sem a isso ser legalmente sujeito. Moreira (2001) diz que a privacidade de um indivíduo e de suas informações é um direito de cada cidadão e a ele pertence. Desta forma, nenhuma organização deve negligenciar esta responsabilidade nem descuidar de nenhuma informação que lhe for confiada. (FONTES, 2006)

As informações a respeito de um paciente se multiplicaram muito, com isso, gestores de instituições da área da saúde reconhecem a importância das informações para o gerenciamento da qualidade dos serviços médicos (OLIVEIRA; JANSSEN, 2007 *apud* BRAGANÇA, 2010). Por isso, a troca dos prontuários de papéis para os Registros Eletrônicos de Saúde (RES) foi essencial para essa nova etapa da tecnologia médica.

O risco da perda de dados dos pacientes sempre existiu, no caso dos prontuários de papel, se armazenados de maneira incorreta, poderiam acarretar na perda de uma ou de várias informações, simplesmente esquecendo uma folha ou até mesmo trocando a ficha médica para o arquivo de outra pessoa. Com os prontuários eletrônicos não é diferente, estes dados podem estar sujeitos a vulnerabilidades, como por exemplo: acesso não autorizado (seja em nuvem, banco de dados ou servidores), no canal de comunicação, ou entre outras partes envolvidas no gerenciamento de dados.

Raghupathi e Tan (2002) afirmam que “o prospecto de armazenar informações em saúde na forma eletrônica suscita discussões acerca de padrões, ética, privacidade, confidencialidade e segurança”.

Uma forma de manter informações íntegras e oferecer uma forma de segurança para todos os usuários do sistema é manter a privacidade, recorrendo a métodos e funções criptográficas, que devem ser implementadas para dificultar acessos indevidos a dados pessoais ou ao banco de dados. Contudo, aumentar a segurança da informação pode implicar na perda de usabilidade, logo é importante garantir que a usabilidade não se torne muito baixa ao aumentar da segurança dos dados.

2.7.1. Riscos da informação na área da saúde

Dados médicos são informações muito importantes sobre uma pessoa, uma vez que com eles atualizados, tem-se acesso a todos exames feitos recentemente, quais procedimentos foram realizados como cirurgias, atestados, internações entre outros.

Todas essas informações ficam armazenadas nos prontuários dos pacientes e por possuir todas essas informações importantes, os prontuários são alvos de *hackers*, que tentam invadir o *software* do hospital para roubar esses dados e até modifica-los.

Se algum *hacker* encontrar alguma falha de segurança nos *softwares* de um hospital, certamente ele irá explorar essas vulnerabilidades e roubar os dados dos pacientes ou até mesmo infectar a rede com malware. Se o *software* for hackeado, o *hacker* pode ter acesso à todas as informações dos pacientes e alterar os prontuários eletrônicos, resultados de exames, assim, prejudicando a saúde do paciente, transforando uma pessoa saudável em uma doente, e vice-versa. Também é possível que ele consiga hackear dispositivos médicos, ajustando a quantidade de ar que um respirador manda para o paciente, a frequência de batidas em um marca-passo, parar elevadores no meio de uma emergência, etc.

Segundo a afirmação de Scudere (2014), os “médicos poderão operar pacientes visualizando pelo *glass* cenas e/ou rotinas do melhor procedimento a seguir, validadas pela base de dados do hospital [….]”, mas a dúvida se inicia no momento em que não se sabe mais se os dados do prontuário do paciente do hospital não foram manipulados por um *hacker* com intuito, de direto ou indireto, de prejudicar o médico ou paciente.

2.7.2. Vazamento de dados

Todas as organizações da área da saúde devem se adequar as normas da LGPD, já que é uma forma de prevenção contra vazamentos de dados dos pacientes, ataques *hackers* ou até falha humana. Um estudo sobre privacidade de pacientes e segurança de dados mostrou que 94% dos hospitais tiveram pelo menos uma violação de segurança nos últimos dois anos em sua maioria os ataques ocorreram por parte de agentes internos da organização (GOLDSHIMIDT, 2021).

Se for comprovado que ocorreu o descumprimento da LGPD, a organização pode sofrer com punições pelo vazamento dos dados, alguns exemplos são: advertência, multa simples, de até 2% do faturamento da pessoa jurídica, limitados até R$ 50.000.000,00 por infração, multa diária; bloqueio dos dados pessoais e eliminação dos dados, dentre outros, todas elencadas no art. 52 da LGPD, sem contar os danos reputacionais e possíveis ações judiciais por parte dos titulares dos dados .Outra punição prevista nessa lei é a possibilidade de publicização da infração após apuração e confirmação da ocorrência, o que acarretaria no descrédito do profissional em relação aos pacientes, podem comprometer gravemente a continuidade do trabalho da instituição.

2.7.2. Hospital de Câncer de Barretos – São Paulo

Segundo Koike e Central de jornalismo (2017), o maior Ciberataque mundial, ocorreu em junho de 2017, no hospital de câncer de Barretos, interior de São Paulo, causado por um *ransomware*, vírus que "sequestra" computadores. Todas as unidades do hospital em Barretos, Jales e Porto Velho foram afetadas, no mínimo 350 exames foram interrompidos e o atendimento dos 6 mil pacientes diários do complexo hospitalar foram prejudicados.

Segundo Ferrari (2017) as primeiras estimativas colocam o Ciberataque como potencialmente maior do que o *WannaCry*, que ocorreu no último mês de maio de 2017. O mesmo explica o que é *ransomware*:

> [...] ocorre quando um *hacker* invade o computador, o *smartphone* ou algum dispositivo conectado à *internet*, bloqueia informações por meio de criptografia. Se o dono das informações quiser vê-las novamente, precisa pagar um resgate, *ransom*, em inglês. Chamada de *notpetya*, um tipo de vírus que sequestra dados digitais e afetou grandes empresas em dezenas de países. No Brasil o Hospital de Câncer de Barretos interior

> de São Paulo (SP) foi o mais afetado pela invasão dos *hackers*, dados foram criptografados e bloqueou 1 mil computadores além de prejudicar consultas, exames e até sessões de radioterapia.

Segundo Koike (2017), Paulo de Tarso o diretor clínico do hospital na época, relatou que os *hackers* pediram 300 bitcoins por computador, como pagamento para que os equipamentos sejam desbloqueados. Como o pagamento não foi realizado todos os pacientes do Hospital, e das demais unidades, estavam sujeitos a terem seus dados pessoais usados indevidamente. Contudo, de acordo com o hospital, as informações dos pacientes ficaram "seguras e preservadas".

3. Estudo de Caso

3.1. Internet das coisas (*IoT*)

Segundo Ashton (2009) o termo Internet das Coisas, ou *Internet of Things* (*IoT*) em inglês, foi apresentado por Kevin Ashton em uma apresentação o ano de 1999 para a empresa Procter & Gamble. Segundo o mesmo autor, seu objetivo era falar sobre uma realidade na qual os computadores coletariam dados e assim saberiam tudo sobre as coisas.

Segundo Research (2013), "A *IoT* descreve um sistema em que os elementos no mundo físico, e sensores dentro ou acoplados a esses elementos, estão conectados à Internet através de conexões de Internet sem fio e com fio. Os sensores podem usar vários tipos de conexões de área local como RFID, NFC, Wi-Fi, Bluetooth e Zigbee." Com isso entende- se que a *IoT* é um sistema capaz de conectar elementos do mundo físico à internet através de conexões de Internet com e sem fio. A *IoT* irá:

- Conectar objetos inanimados e seres vivos;
- Usar sensores para coleta de dados;
- Alterar quais tipos de itens se comunicam em uma rede IP.

3.2. *IoT* nos hospitais

O uso de dispositivos *IoT* estão cada vez mais presentes na sociedade, como os carros autônomos, pulseiras que monitoram o desempenho dos atletas e na medicina não é diferente, os dispositivos trazem vários benefícios para os pacientes, pesquisadores, unidades e profissionais da saúde.

Segundo Maia (2017) a *IoT* está presente na medicina desde 1950 quando a Agência Espacial dos Estados Unidos (NASA) utilizava a tecnologia de transmissão de dados para monitorar os sinais vitais dos astronautas.

A *IoT* pode transformar totalmente a forma como os hospitais, e outras unidades de saúde coletam e usam os dados de seus pacientes. Os objetos físicos como os sensores integrados e outros dispositivos coletam os dados e transmitem informações em tempo real, esses dados podem ser analisados para (ENTERPRISE, Alcatel Lucent, 2019):

- melhorar o tratamento ao paciente;
- otimizar processos;
- conhecer mais sobre as necessidades e preferências dos pacientes;
- tornar as redes hospitalares mais inteligentes.

Segundo o Dr. José Aldair Morsch (2019), a *IoT* pode trazer diversas vantagens na medicina, e são elas:

- Registro autônomo de informações;
- Monitoramento contínuo do paciente;
- Facilidade no compartilhamento de dados;
- Maior acesso às informações sobre saúde;
- Armazenamento automático na nuvem;
- Histórico médico mais completo, com apoio a diagnósticos assertivos;
- Empoderamento do paciente;
- Fortalecimento de ações preventivas e de autocuidado.

A implementação do *IoT* nos hospitais também pode ajudar a superar problemas comuns, como por exemplo a redução no tempo na sala de espera, desperdício de insumos hospitalares, medicamentos, vacinas, materiais e tecidos biológicos.

3.2.1. *Iot* em dispositivos hospitalares

As inovações tecnológicas que ocorreram na área da saúde vão muito além dos aplicativos de celulares e de *wearables*. Entre eles estão os seguintes dispositivos *IoT*:

- Marcapassos cardíacos;
- Monitoramento contínuo inteligente de glicose (CGM);
- Respiradores conectados;

- Lentes de contato inteligentes;
- Projeto BlueSky – monitoramento de pacientes com Parkinson;
- Dispositivo para diabéticos.

Para Morsch (2019), a utilização desses dispositivos médicos permite que o hospital, ou outra organização da saúde reduza custos na contratação de especialistas e agrega na agilidade da emissão dos resultados dos exames. Além de melhorar a qualidade de vida dos pacientes, uma vez que esses dispositivos irão monitorar os dados dos pacientes e fornecerá informações em tempo real (MAISLAUDO, 2019).

3.2.2. Problemas da *IoT* nos hospitais

Por serem dispositivos físicos conectados à rede com e sem fio, os dispositivos *IoT* podem ser alvos de ataques caso não estejam devidamente protegidos. Algumas vulnerabilidades que podem acontecer são: *malwares*, má gestão e configuração incorreta do dispositivo e atualizações.

Segundo Gomes (2019), os dispositivos *IoT* na área da saúde são alvos mais atraentes para os *hackers* pelas seguintes razões:

- Possui muitos equipamentos ligados à rede e pode haver lacunas de segurança num determinado equipamento;
- Os equipamentos *IoT* pessoais transportados pelas famílias e ou funcionários não são analisados pelas equipas de sistemas de informação locais;
- Estes equipamentos contêm informações valiosas tais como dados pessoais e histórico de saúde pessoal, que podem ser exploradas para obter um determinado lucro;

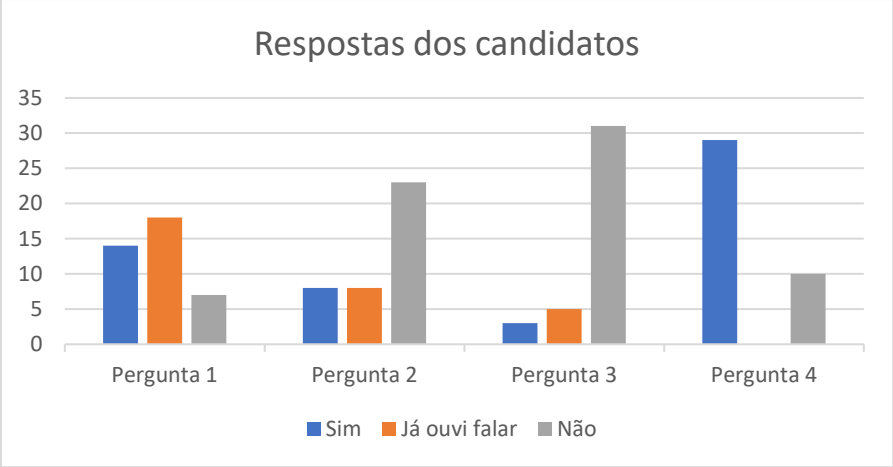
3.3. Pesquisa

Este trabalho tem como base um procedimento de pesquisa descritiva, cujo principal objetivo é proporcionar uma nova visão sobre o tema abordado. Para o resultado dessa pesquisa foi realizada uma abordagem qualitativa, houve um levantamento e coleta de dados cujo principal objetivo é compreender e interpretar determinadas opiniões e percepções do público alvo a respeito da importância da segurança da informação nos hospitais.

Em uma pesquisa realizada com 39 pessoas, entre estudantes, de faculdades como FAM Americana e Barceló (Argentina) e profissionais da área da saúde, de instituições como o Hospital Alemão Oswaldo Cruz e o Centro Municipal de Saúde de Tocantins, foram cometidas 14 perguntas, entre elas as mais importantes são:

1- Você sabe o que é segurança da Informação?
2- Sabe o que significa a lei LGPD?
3- Você sabe o que é *IoT*?
4- Você sabe a importância de se aplicar a segurança da informação nos hospitais e em organizações da saúde?

Para uma melhor compreensão dos resultados dessa pesquisa, foi elaborado um gráfico de barras para ilustrar as respostas dos candidatos.



Por meio desta pesquisa, pode-se analisar que apenas 36% das pessoas sabem o que é a segurança da informação. 21% sabem o que é LGPD, 8% sabem o que é *IoT* e 74% entendem a importância de se aplicar a segurança da informação nos hospitais.

3.4. Soluções para os problemas

Apesar de possuírem muitas vulnerabilidades, os dispositivos eletrônicos fazem parte do avanço tecnológico e por isso métodos de proteção foram desenvolvidos para impedir que esses dispositivos sejam hackeados.

> Para ter uma boa segurança desses dispositivos deve-se cumprir 3 etapas. Na hora da compra, escolher produtos e serviços de fabricantes conhecidos, verificar se o fabricante projetou e arquitetou o dispositivo *IoT* levou em consideração a segurança. No caso de realizar a configuração e o provisionamento na instalação dos dispositivos não

> deve permitir senhas padrão, os dados devem ser criptografados, as conexões web deve ser seguras e o acesso à rede limitado; possuir políticas de segurança, tais como, de privacidade, retenção de dados, acesso remoto, entre outros. Sempre aplicar a administração e gerenciamento adequados, como por exemplo, as atualizações de segurança devem ser instaladas automaticamente, configurar limites para conexões de entrada e saída, tipos de dados, portas e configurações de segurança. (MCAFEE, 2017).

De acordo com a mesma empresa, outros procedimentos e políticas que sempre devem ser seguidos para melhor proteção de dispositivos *IoT* são:

- Analisar o histórico de segurança do dispositivo *IoT*;
- Manter o *software* de todos os dispositivos *IoT* sempre atualizado;
- Usar senhas fortes e diferentes do padrão;
- Aproveitar as configurações de segurança da *IoT*.
- Conectar os dispositivos *IoT* em Wi-Fi seguro.
- Restringir o acesso físico aos dispositivos *IoT*.
- Reiniciar os dispositivos *IoT* periodicamente.

Conforme o Hospital Brasil (2021) para manter a segurança dos dispositivos *IoT* deve-se seguir algumas práticas, como por exemplo, basear-se no tipo de dispositivo médico, níveis de ameaça, padrões de uso e outras características de perfil de dispositivo usando configurações de VLAN ou políticas de firewall, além disso, separar aqueles em execução em um sistema operacional em fim de vida daqueles com patches de segurança atualizados, implementar processos para modificar as credenciais do fornecedor padrão na implantação do dispositivo e monitoramento para rede fora de banda, IP ou varreduras de porta também podem ajudar a reduzir os ataques.

4. Conclusão

Como foi abordado na pesquisa, uma pequena porcentagem dos entrevistados sabem o que é segurança da informação, LGPD e *IoT*, por isso, uma maneira de resolver esse problema é investir no setor de TI, uma vez que os profissionais dessa área estarão preparados para os eventos que podem ocorrer; conscientizar os profissionais da área a se informar sobre o assunto, já que, 67% dos entrevistados relataram que as faculdades não possuem nenhuma aula/disciplina na qual expliquem a importância da proteção de dados dos pacientes.

Os dispositivos *IoT* estão se tornando muito comuns nessa área, por isso é necessário que os profissionais da área saibam identificar esses dispositivos, uma vez que 92% dos entrevistados responderam que não sabem onde os dispositivos *IoT* se encontram em um hospital. Além disso, as instituições devem possuir políticas e regras de segurança da informação para delimitar o acesso dos funcionários a certos tipos de ações referentes às informações dos pacientes.

Referências bibliográficas

ABNT. NBR ISO/IEC 27002:2005: **Tecnologia da Informação** – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005. 120p

ALVES, G. A. **Segurança da Informação**: uma visão inovadora da gestão. Rio de Janeiro: Ciência Moderna Ltda, 2006.

ASHTON, K. **That 'Internet of Things' thing**. Publicado no RFID Journal, 2009. Disponível em: http://www.rfidjournal.com/article/view/4986. Acesso em 24 mar 2022.

AZEVEDO NETO, R. S. et al. **O Prontuário Eletrônico do Paciente**, 1 ed., Área de Prestação de Serviços de Saúde e Tecnologia Unidade de Organização dos Serviços de Saúde Organização Pan Americana da Saúde Oficina Sanitária Pan Americana, Organização Mundial da Saúde Washington, D.C., 2003

BRAGANÇA, C. E. B. A. **Privacidade em informações de saúde:** uma análise do comportamento percebido por profissionais de saúde de instituições hospitalares do Rio Grande do Sul. 2010. Dissertação (Mestre em Administração e Negócios) - Faculdade de Administração, Contabilidade e Economia da Pontifícia, Universidade Católica do Rio Grande do Sul. Disponível em: https://tede2.pucrs.br/tede2/bitstream/tede/5608/1/426897.pdf

BRASIL, Governo Federal. **Proteção de Dados – LGPD**. 2020. Disponível em: **Erro! A referência de hiperlink não é válida.** Acesso em 21 mar 2022

CENTRAL DE JORNALISMO. **Crueldade -** Hackers invadem sistema do Hospital de Câncer de Barretos e pedem resgate. 2017. Disponível em: https://www.tudoemdia.com/2017/06/28/crueldade-hackers-invadem-sistema-do-hospital-de-cancer-de-barretos-e-pedem-resgate. Acesso no dia 27 abr 2022

CONSELHO FEDERAL DE MEDICINA. **Prontuário médico**. 1999. Disponível em: https://portal.cfm.org.br/artigos/prontuario-medico/#:~:text=O%20prontu%C3%A1rio%20m%C3%A9dico%20%C3%A9%20um%20documento%20elaborado%20pelo,exames%2C%20al%C3%A9m%20das%20indica%C3%A7%C3%B5es%20de%20tratamentos%20e%20prescri%C3%A7%C3%B5es.?msclkid=8c47bdcfd08711ec8c212b46cc475695. Acesso no dia 10 maio 2022.

DEMO, F.; PRIESNITZ FILHO, W. **Gestão de Privacidade no Armazenamento de Dados do Paciente em Registros Médico-Hospitalares Eletrônicos.** *In*: ESCOLA REGIONAL DE REDES DE COMPUTADORES (ERRC), 17. 2019,

Alegrete. **Anais** [...]. Porto Alegre: Sociedade Brasileira de Computação, 2019. p. 57-64. DOI: https://doi.org/10.5753/errc.2019.9212. Acesso em 21 mar 2022

DONDA, D. **Padrões e normas relacionadas à Segurança da Informação**. 2016. Disponível em: https://danieldonda.com/padres-e-normas-relacionadas-segurana-da-informao/?msclkid=c5002d32d08311ec9e3f3d9d5bf5b616. Acesso dia 10 maio 2022.

Dr. MORSCH, J. A. **9 exemplos de como a internet das coisas avança na saúde.** 2019. Disponível: em https://telemedicinamorsch.com.br/blog/iot-na-medicina?msclkid=3796ddebd16011ec899939b66ca426d1. Acesso em: 12 maio 2022

ENTERPRISE, A. L. (2019) A internet das Coisas (IoT) em assistência de saúde. Artigo. Disponível em: https://www.al-enterprise.com/-/media/assets/internet/documents/iot-for-healthcare-solutionbrief-ptbr.pdf?msclkid=3795f9f6d16011ec929a6cb7db9186a9.

FEDERAÇÃO BRASILEIRA DE HOSPITAIS**, Guia LGPD para o setor hospitalar**. São Paulo. [s.n], 2020. Disponível em: https://www.fbh.com.br/wp-content/uploads/2021/02/Guia-LGPD.pdf

FERRARI, B. **A tecnologia por trás de mais um mega-ataque cibernético global**. 2017. Disponível em: https://epoca.oglobo.globo.com/tecnologia/experiencias-digitais/noticia/2017/06/tecnologia-por-tras-de-mais-um-mega-ataque-cibernetico-global.html - Acesso em 27 abr 2022

FONTES, E. **Segurança da Informação:** o usuário faz a diferença, Rio de Janeiro: Editora Saraiva, 2006.

GASETA, E. R. (2022). Sistema de gestão de segurança da informação. [PowerPoint de apoio à disciplina de gestão de segurança da informação, lecionada na Fatec Americana] Disponível em: https://fatecspgov.sharepoint.com/sites/Section_ISG016.A585.M.097.004.20221/Material%20de%20Aula/Sistema%20de%20Gest%C3%A3o%20de%20Seguran%C3%A7a%20da%20Informa%C3%A7%C3%A3o.pdf?CT=1654191479550&OR=ItemsView

GOLDSHIMIDT, G. **ARTERIAL:** Um Modelo para a Prevenção ao Vazamento de Informações de Prontuários Eletrônicos utilizando Processamento de Linguagem Natural. 2021. Dissertação (Doutor em computação aplicada) – Universidade do Vale do Rio dos Sinos, UNISINOS. Disponível em: http://repositorio.jesuita.org.br/bitstream/handle/UNISINOS/10900/Guilherme%20Goldschmidt_.pdf?Sequence=1&isallowed=y

GOMES, J. T. C. **Riscos e vulnerabilidades dos equipamentos IoT em unidades de saúde.** 2019. Dissertação (Mestrado de Cibersegurança e Informática Forense) – Escola superior de tecnologia e gestão, Instituto Politécnico de Leiria, 2019. Disponível em: https://iconline.ipleiria.pt/bitstream/10400.8/4680/1/Riscos%20e%20vulnerabilidades%20dos%20equipamentos%20IoT%20em%20unidades%20de%20sa%C3%BAde.pdf

GORDON, S. R.; GORDON, J. R. Sistemas de informação: uma abordagem gerencial. 3. ed. Rio de Janeiro: LTC, 2011.

HELMS, M. M.; MOORE, R.; AHMADI, M**. Information technology and healthcare industry:** a Swot analysis. *International Journal of Healthcare Information Systems and Informatics*, v. 3, n. 1, p. 75-92, 2008.

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

HOSPITAL BRASIL, Portal. **Artigo** – Como manter a segurança da Internet das Coisas Médicas?. 2021. Disponível em: https://portalhospitaisbrasil.com.br/artigo-como-manter-a-seguranca-da-internet-das-coisas-medicas/. Acesso em 22 maio 2022

https://www.herrero.com.br/files/revista/file9035c2d4bad4b6fc952182ce1b7aafcd.pdf

JUNIOR, A. E. A., e SANTOS, E. M., **Segurança da informação em hospitais**: a percepção da importância de controles para gestores e profissionais de TI. Revista Gestão e Saúde, Curitiba, v. 4, n. 2, p.1-14. 2012.

KOIKE, B. **Hospital de Câncer de Barretos é alvo de ciberataque**. 2017. Disponível em: https://valor.globo.com/empresas/noticia/2017/06/27/hospital-de-cancer-de-barretos-e-alvo-de-ciberataque.ghtml. – Acesso em 27 abr 2022.

MAGNAGNAGNO, O. A. **Mecanismos de proteção da privacidade das informações de prontuário eletrônico de pacientes de instituições de saúde.** 2015. Dissertação (mestre em administração e negócios) - Faculdade de Administração, Contabilidade e Economia, Pontifícia Universidade católica do Rio Grande do Sul. Disponível em: https://tede2.pucrs.br/tede2/bitstream/tede/6417/2/476570%20-%20Texto%20Completo.pdf

MAIA, U. **Como a IoT está mudando os hospitais e o mercado de saúde.** 2017. Disponível em: https://docmanagement.com.br/03/02/2017/como-iot-esta-mudando-os-hospitais-e-o-mercado-de-saude/. Acesso em: 11 maio 2022

MAISLAUDO. **IoT na medicina:** exemplos de como a Internet das Coisas avança na área da saúde. 2019. Disponível em: https://maislaudo.com.br/blog/iot-na-medicina/. Acesso em: 12 maio 2022

MCAFEE. **Proteção de dispositivos IoT como defesa contra ataques**. 2017. Artigo Disponível em: https://www.mcafee.com/enterprise/pt-br/assets/solution-briefs/sb-quarterly-threats-mar-2017-1.pdf.

MEURER, M. **Uso do IOT na saúde e segurança da informação**. 2018. Artigo (Especialista em Gestão da Segurança da Informação) - Universidade do Sul de Santa Catarina. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/3705

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

MOREIRA, N. S. **Segurança Mínima**: Uma visão corporativa da Segurança da Informação, Rio de Janeiro: Axcel Books, 2001.

RAGHUPATHI, W., Tan, J. (2002), Strategic IT applications in health care, Communications of the ACM, v. 45 n. 12, p. 56-61.

RESEARCH, L. **Uma introdução à Internet da Coisas (IoT).** 2013. Artigo. Disponível em:

https://www.cisco.com/c/dam/global/pt_br/assets/brand/iot/iot/pdfs/lopez_research_an_introduction_to_iot_102413_final_portuguese.pdf

SCUDERE, L. **Risco Digital na Web 3.0** - Criando Estratégias de Defesas Cibernéticas. Editora Campus, São Paulo, 2014.

SÊMOLA, M. **Gestão de Segurança da Informação** – uma visão executiva. 8ª ed, Rio de Janeiro: Elsevier, 2003.

SILVA, J, A. **Curso de Direito Constitucional Positivo**, 19ª Ed. p. 206. São Paulo: Malheiros, 2001