Henrique Lima Alves Braz

Paulo Eduardo A. Klerk Pontes

Raul Cândido Ruiz de Souza

BIOHACKING E SEGURANÇA DA INFORMAÇÃO: VULNERABILIDADES EM DISPOSITIVOS IMPLANTÁVEIS

SÃO CAETANO DO SUL - SP
2019

Henrique Lima Alves Braz

Paulo Eduardo A. Klerk Pontes

Raul Cândido Ruiz de Souza

BIOHACKING E SEGURANÇA DA INFORMAÇÃO: VULNERABILIDADES EM DISPOSITIVOS IMPLANTÁVEIS

Trabalho de Conclusão de Curso apresentado à Faculdade de Tecnologia de São Caetano do Sul, sob a orientação da Prof. Me. Edna Mataruco Duarte, como requisito parcial para a obtenção do diploma de Graduação no Curso de Tecnologia em Segurança da Informação.

SÃO CAETANO DO SUL - SP
2019

Dedicamos este trabalho de conclusão de curso, aos nossos pais, filhos, e irmãos, principalmente aqueles que conquistaram este lugar durante a elaboração deste trabalho. Dedicamos também aos nossos professores e outros pesquisadores que por meio de seus exemplos nos inspiraram a compor este trabalho. E por último a todos aqueles que possuam um dispositivo implantado em seus corpos, que desejamos encontrem neste trabalho um recurso para o resguardo de sua própria integridade física.

RESUMO

ALMEIDA DE KLERK, P. E.; BRAZ, H. L. A.; DE SOUZA, R. C. R. **Segurança da Informação em Dispositivos Implantáveis**. 53 f. Trabalho de Graduação – Faculdade de Tecnologia de São Caetano do Sul, São Caetano do Sul, 2018.

Os dispositivos implantáveis, como recurso que ficará introduzido no corpo humano após a intervenção, são considerados neste Trabalho de Conclusão de Curso como ativos, e como tal, estão sujeitos a vulnerabilidades de segurança da informação principalmente por apresentarem: dados que identifiquem software e hardware, dados do usuário, capacidade de armazenamento, transmissão, monitoramento e processamento de dados. Neste contexto, conforme publicado em diferentes mídias nacionais e internacionais há vários casos de ameaças que exploram vulnerabilidades.

No entanto, no Brasil, não temos nenhuma regulamentação ou lei específica que trate deste problema. Diante desta lacuna, este trabalho tem como objetivo descrever vulnerabilidades em dispositivos implantáveis (DI) com vistas a elaboração de um relatório que poderá contribuir com a prática de segurança da informação, tendo como base as leis que tratam destes recursos e por meio de aproximações com leis nacionais que podem servir como aporte jurídico. O método utilizado foi bibliográfico, utilizando-se artigos, livros, reportagens e apresentações relacionadas ao tema.

Ao final, foi possível constatar que este é um cenário que demanda estudo e é ainda carente de regulamentação que trate especificamente do assunto, como já ocorre em outros países. O relatório apresentado neste trabalho, representa um primeiro passo, em uma busca por elencar pontos importantes de observação necessário nesta área de conhecimento.

Palavras-chave: Segurança da Informação; Dispositivos Médicos; Cibersegurança; Relatório; Vulnerabilidades.

ABSTRACT

ALMEIDA DE KLERK, P. E .; BRAZ, H. L. A.; DE SOUZA, R. C. R. Information Security in Implantable Devices. 53 f. Graduation Work – Faculdade de Tecnologia de São Caetano do Sul, São Caetano do Sul, 2018.

Implantable devices, as a resource that will be introduced into the human body after the intervention, are considered in this Course Completion Work as assets, and as such, are subject to information security vulnerabilities mainly because they present: data that identifies software and hardware, user data, storage capacity, transmission, monitoring and data processing. In this context, as published in different national and international media there are several cases of threats that exploit vulnerabilities.

However, in Brazil, we do not have any specific regulations or law that addresses this problem. Given this shortcoming, this paper aims to describe vulnerabilities in implantable devices (DI) with a view to elaborating a report that can contribute to the practice of information security, based on the laws that deal with these resources and by means of approximations with laws that can serve as a legal contribution. The method used was bibliographic, using articles, books, reports and presentations related to the theme.

In the end, it was possible to verify that this is a scenario that requires study and is still lacking in regulations that deal specifically with the subject, as is already the case in other countries. The report presented in this paper represents a first step in a quest to list important points of observation needed in this area of knowledge.

Keywords: Information Security; Medical devices; Cyber security; Report; Vulnerabilities.

Lista de Figuras

Lista de Siglas

ANVISA - Agência Nacional de Vigilância Sanitária

CDI - Cardio Desfibrilador Implantável

DCEI - Dispositivos Cardíacos Eletrônicos Implantáveis

DMI – Dispositivo Médico Implantável

DMIA – Dispositivos Médicos Implantáveis Ativos

e-PHI - *eletronic personal health information*

FDA – Food and Drug Administration

GDPR - Regulamento Geral sobre a Proteção de Dados

HIPPA - Health Insurance Portability and Accountability Act

LGPDP - Lei Geral de Proteção de Dados Pessoais

MiTM – Man in The Middle

Wi-Fi – Wireless Fidelity

SUMÁRIO

INTRODUÇÃO

A Segurança da Informação, enquanto ciência busca a construção de conhecimento e a compreensão de suas potenciais aplicações em benefício da sociedade, por meio do desenvolvimento e controle de tecnologias, que visem o resguardo de informações úteis a uma organização, estado ou indivíduo. Para que este objetivo possa ser atingido se faz necessário definir quais ativos devem ser resguardados pela Segurança da Informação.

Devido à grande relevância das tecnologias médicas e seus benefícios para sociedade optamos por tomar como objeto de estudo os ativos de informação no campo da Medicina, mais especificamente dispositivos implantáveis.

Tecnologias médicas são essenciais ao diagnóstico, tratamento e reabilitação e desempenham papel crucial para a saúde dos indivíduos e da sociedade como um todo. Devido às constantes inovações destas tecnologias, que contribuem para melhorar a acurácia e qualidade dos processos diagnósticos, o aumento da eficiência dos cuidados em saúde, em todos os níveis, permite tratar mais pacientes em menores intervalos de tempo. (HEALTHCARE, 2015, p. 38)

Dentro de deste campo de estudo os ativos são definidos seguindo padrões diversos, porém nosso trabalho propõe recomendações direcionadas ao cenário Nacional, com este intuito consideramos aqui a definição adotada pelo Governo Federal Brasileiro que considera “ativos de informação, os meios de armazenamento, transmissão e processamento da informação, os sistemas de informação, bem como os locais onde se encontram esses meios e, as pessoas que a eles têm acesso." Sendo assim todo dispositivo implantável que venha a armazenar informações ou ser identificável por meio de informações únicas será aqui considerado um ativo, bem como os indivíduos que tenham contato com estes dispositivos.

Neste trabalho será apresentada uma análise das normas e demais padrões internacionais de Segurança da Informação aplicáveis aos Dispositivos Implantáveis. Equipamentos estes que estão sujeitos à critérios de segurança estabelecidos no âmbito de diversas ciências e campos do saber, entretanto ainda não possuem em língua portuguesa material suficiente com relação a Segurança da Informação e, área esta que tem nitidamente

sofrido ataques, por meios de vulnerabilidades, conforme demonstraremos neste trabalho.

Sendo assim, o objetivo principal é analisar e descrever vulnerabilidades em Dispositivos Implantáveis (DI) com vistas a elaboração de um relatório de Gestão de Vulnerabilidades em Segurança da Informação. Além disso, apresentar como objetivos específicos, classificar e definir os Dispositivos Implantáveis e as metodologias, normas e demais padrões de Segurança da Informação abordados e aplicáveis a estes dispositivos.

Também objetivando lograr o êxito em observar por meio de relatos publicados na mídia, órgãos competentes e em entrevistas, as ameaças, no tangente a Segurança da Informação, as quais estão expostos os Dispositivos Implantáveis.

A produção do estudo científico para o Trabalho de Conclusão de Curso (TCC), apresentou tema relevante quanto a vulnerabilidade de dispositivos implantáveis, pois não há em nosso território qualquer normativa no âmbito da Segurança da Informação, que forneça supedâneo para discussão do assunto em tela. Tal produção de conhecimento visa apresentar e fomentar a discussão no que tange a Segurança da Informação em dispositivos específicos, pois muito se trata de vulnerabilidades em computadores, celulares e outros *gadgets*, contudo, dispositivos inseridos ao corpo humano, que por vezes substituem em parte ou por completo determinado órgão, ou auxiliam algum órgão em sua finalidade que está prejudicada, sendo, portanto, equipamentos de sobrevida, possuem estudo insuficiente nesta área.

Quando ocorre inserção de tais dispositivos no corpo humano, espera-se que não ocorram falhas na área de Segurança da Informação, assim tais equipamentos não possuem padrão ou regulamentação suficientes no âmbito Nacional. Desta forma o presente TCC, abordará os principais aspectos, visando apresentar boas práticas de segurança da informação voltada aos dispositivos implantáveis.

Ante a um cenário irreversível no mundo no que se refere ao crescimento de ataques cibernéticos, que com o advento de novas tecnologias e a necessidade constante da humanidade de se conectar de múltiplas formas, por meio de diversos dispositivos entre software e hardware

que se propagam mais rápido que o profissional de segurança é capaz de se especializar. Há a necessidade de normatizar e criar regras para determinadas tecnologias como forma de propor melhores práticas, tanto para que o usuário que estará exposto, quanto aos profissionais que irão implementá-lo.

Em outra vertente, partindo para tendências pessoais, o corpo humano deve ser respeitado em sua integridade, nos basilares mais arraigados da Carta Magna Brasileira de 1988, cuida da matéria em diversos dispositivos legais. No *caput* do art. 5º, garante a inviolabilidade dos direitos coligados à vida, bem como à integridade física: “ninguém será submetido a tortura nem a tratamento desumano ou degradante”, as garantias individuais priorizam o respeito à pessoa e à sua personalidade, abrangendo à integridade física e a dignidade moral, como previsto pela Constituição Federativa do Brasil.

A integridade física e dignidade moral são garantias individuais, portanto, afeto a segurança jurídica dada à cada Brasileiro, que por sua vez deverá por meio da segurança da informação, via normatização, ter como parâmetro que o profissional ao desenvolver seu mister deverá atender essa garantia legal com a sustentação da norma ora proposta, visando proteger o ativo mais importante, o ser humano.

Nossa metodologia está baseada em pesquisa de cunho documental e bibliográfico, com base em artigos e livros orientados ao tema, eventos relevantes ocorridos até o desenvolvimento do presente TCC, registros de incidentes, tendências e ocorrências existentes no que se refere a Dispositivos Implantáveis, caracterizado pela metodologia qualitativa com o intuito de acrescentar uma produção textual que explore a possibilidade de preencher as lacunas das práticas identificadas.

A análise realizada com base nestes registros tem como fulcro classificar as características dos Dispositivos Implantáveis e suas vulnerabilidades inerentes aos materiais ou tecnologias empregadas. Utilizando então, esta classificação, para propor um conjunto de boas práticas de modo que possibilite uma melhoria indutiva aos que necessitem ou optem pela utilização dos Dispositivos Implantáveis.

Buscando alcançar o objetivo traçado, por meio de literatura e demais publicações, para uma melhor compreensão do tema e a formação de uma

proposta de metodologia para a tratativa quando houver a possibilidade de existência de vulnerabilidades e ameaças em Segurança da Informação aos dados armazenados, transmitidos e processados pelos Dispositivos Implantáveis, podendo então com base nos estudos previamente publicados identificar, avaliar e compilar um conjunto de boas práticas, padrões e normas e regulamentos que venham a ser úteis para a formação do processo de gestão de vulnerabilidades especificas ao tema abordado.

1 SEGURANÇA DA INFORMAÇÃO

Diversas áreas de conhecimento e atuação profissional possuem alguma normatização ou padronização definidas de forma a especificar termos e utilizações de nomes, ações, recomendações, regras, regidas por leis específicas. Para a segurança da informação em si, pode-se aproximar leis brasileiras que tangem a propriedade física e os acessos realizados a meios eletrônicos que armazenam informações digitalmente.

Quanto ao que cerca os objetivos gerais da discussão deste trabalho, destacamos abaixo os conceitos de Segurança da Informação que tomamos como imprescindíveis.

Como basilares da Segurança da Informação, existem conceitos adotados em padrão por profissionais de diversos seguimentos e especificações da área de conhecimento. Começando por "Confidencialidade", que vem a ser uma delimitação de exclusividade de acesso, contemplando um número limitado de pessoas envolvidas com o tema, onde não exista a inclusão indireta de acesso por outras pessoas (MORENO, 2015, p.17).

A Autenticidade é a garantia de legitimidade do envio de uma informação, onde não tenha sido possível adulterar de algum modo a informação em trânsito (MORENO, 2015, p. 17).

A Disponibilidade é a garantia de que a informação poderá ser acessada e utilizada sempre que necessária (MORENO, 2015, p.17).

A Integridade sendo então a garantia de que a informação não sofreu alterações não autorizadas de qualquer gênero ou intensidade durante suas transferências, acessos ou armazenamentos (MORENO, 2015, p.17).

A Legalidade é a relação direta da informação e seus processos de controle e gestão seguindo as delimitações da legislação de determinado país. (MORENO, 2015, p. 17).

Outra definição que aborda conceitos muito utilizados para a compreensão de cenários e descrições de eventos em geral é a de Ameaças, especificando meios, ferramentas, ações que possibilitem o comprometimento de qualquer um dos princípios de Segurança da Informação, considerando tanto o âmbito lógico como o físico (MORENO, 2015, p. 17).

Uma vulnerabilidade é definida por características que componham a descrição de uma fragilidade de um ativo ou grupo de ativos, com alguma possibilidade de exploração por meio de uma ameaça (ABNT NBR ISO/IEC 27002, 2005, p. 96).

Um Risco, por sua vez, é a probabilidade de ocorrência de combinação de situações e fatores que propiciem a ocorrência de um evento, com as respectivas consequências (ABNT NBR ISO/IEC 27002, 2005, p. 6). Ainda lidando com este termo, uma análise/avaliação de risco vem a ser um processo abrangente e completo de análise e avaliação de riscos. O processo de gestão de riscos envolve a coordenação de atividades com o objetivo de tomar o controle dos riscos que afetem uma organização como um todo (ABNT NBR ISO/IEC 27002, 2005, p. 21).

Ocorre que estas definições devem também abranger dispositivos ou meios eletrônicos que possuem dados sensíveis, no sentido de não disporem de livre acesso a todos, tendo então alguma restrição de acesso.

Em 2014, a *Food and Drug Administration* (FDA) adotou as seguintes definições em cibersegurança como um processo, que deve ter o enfoque em prevenção de processos ou eventos que venham a ferir de algum modo um dos pilares estabelecidos, estabelecidos para Segurança da Informação, especificando-os como processos envolvendo acessos de informações diretamente ligadas a um dispositivo médico, envolvendo, de algum modo, um outro dispositivo que seja alheio (Samaras, 2016, p. 226–234).

É possível visualizar a cibersegurança como uma gama mais abrangente que envolve características ativas em sistemas informatizados, objetivando proteção de informações ou dados que interagem, trafegam ou que sejam armazenados pelo dito sistema (Samaras, 2016, p. 226–234).

No Brasil, existem leis que contemplam etapas regularizadoras como as leis Carolina Dieckmann, Lei n. 12.737/2012, sancionada em 30 de novembro de 2012, que propôs alterações no Código Penal Brasileiro; O Marco Civil da Internet, Lei n. 12.965/2014, que regula o uso da Internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede mundial de computadores, bem como determina diretrizes para atuação do Estado; E a Lei Geral de Proteção de Dados Pessoais -

LGPDP, Lei n. 13.709/2018, A citada lei regula as atividades de tratamento de dados pessoais e altera os artigos 7 e 16 do Marco Civil da Internet.

Existem definições internacionais, como a Americana *Health Insurance Portability and Accountability Act* (HIPAA), que é uma Lei de portabilidade e responsabilidade de provedores de saúde, de 1996. E a Europeia *General Data Protection Regulation* (Regulamento Geral sobre a Proteção de Dados – GDPR), Lei que trata sobre a privacidade, Proteção de dados pessoais e exportação de dados pessoais para territórios não pertencentes à União Europeia ou Espaço Econômico Europeu.

Os aspectos Jurídicos e de Segurança da Informação serão abordados em minúcias posteriormente neste trabalho no capítulo 3.

Quanto aos objetivos gerais do presente trabalho, as descrições do próximo capítulo tratarão do cerne da pesquisa realizada.

2 DISPOSITIVOS MÉDICOS

Em seu intuito de manter e restaurar a saúde, a Medicina se vale de Dispositivos Implantáveis, dispositivos estes, constituídos de material orgânico ou inorgânico destinados a inserção temporária ou permanente dentro do corpo humano.

Diferentes países que têm como oficial a língua portuguesa, aplicam diferentes terminologias e classificações aos Dispositivos Implantáveis. Portugal define como Dispositivo Médico Implantável Ativo, qualquer dispositivo médico que seja concebido para ser total ou parcialmente introduzido através de uma intervenção médica no corpo humano, seja cirurgicamente ou num orifício natural sem cirurgia e destinado a ficar implantado. Conforme apresenta o Guia de Interpretação de Exclusões para Dispositivos Médicos Implantáveis Ativos (DM e DMIA) - Decreto-Lei n. º 152-D/2017, de 11 de dezembro de Portugal.

No Brasil a Agência Nacional de Vigilância Sanitária (Anvisa), propõe o termo Dispositivos Médicos Implantáveis (DMI), e os define como:

> “Qualquer produto médico projetado para ser totalmente introduzido no corpo humano ou para substituir uma superfície epitelial ou ocular, por meio de intervenção

> cirúrgica, e destinado a permanecer no local após a intervenção" e ainda considera como Dispositivo Médico Implantável, qualquer produto médico "destinado a ser parcialmente introduzido no corpo humano por meio de intervenção cirúrgica e permanecer após esta intervenção por longo prazo" (ANVISA, 2001, item 3.15- RESOLUÇÃO-RDC No. 185, DE 22 DE OUTUBRO DE 2001).

Dentre estes dispositivos estão os implantes eletrônicos e bioeletrônicos, a serem utilizados isoladamente ou em combinação, e servem a diversos propósitos, a saber: substitutos de membros ou outros órgãos do corpo; liberação controlada de fármacos, como terapia hormonal, bombas de insulina ou analgesia; monitoram funções corporais ou provêm suporte a órgãos e tecidos, para fins de diagnóstico e tratamento de doenças, lesões ou deficiências.

Assim, alguns exemplos de dispositivos médicos implantáveis são: Os desfibriladores e marca-passos cardíacos; marca-passos gástricos; neuroestimuladores cerebrais destinados ao tratamento do Mal de Parkinson; neuroestimuladores medulares para tratamento de dor crônica e intratável dos membros ou do tronco; neuromodulador sacral para controle da bexiga; os implantes cocleares para habilitação e reabilitação auditiva neurossensorial.

Os Dispositivos Implantáveis sendo compostos de hardware, e muitas vezes também software, devem como todos os ativos de segurança serem analisados individualmente segundo parâmetros que permitam sua classificação e qualificação. Porém por estarem sujeitos a constante evolução, bem como diversidade, isto se torna um desafio tendo em vista a sua falta de similaridade apesar de possuírem semelhantes finalidades, apresentando variação constante em relação a seus componentes, materiais e funcionalidades. (HEALTHCARE, 2015).

Sendo estes dispositivos produzidos ou configurados utilizando conjuntos de hardware e software, não seria improvável serem objetos de estudo, prototipagem de dispositivos de aplicação em mesma área de conhecimento ou adotados como objetos em *hobbys*, os dados apresentados neste trabalho acerca das boas práticas de segurança da informação serão aplicáveis, respeitando-se os limites de órgãos regulamentadores, aos demais dispositivos implantáveis com finalidade não médica.

Ademais, com o surgimento das ciências Cibernética e Bioeletrônica, a possibilidade de se implantar dispositivos se tornou constante objeto de pesquisa, incluso em áreas experimentais e amadoras como é o caso do *Biohacking* e *Bioart*. Estes implantes além de oferecerem recursos para dar suporte, melhorar ou substituir operações do organismo, podem ainda trazer novas funções como é o caso dos biossensores e microchips de *Radio Frequency Identification (*RFID*)*. (SERRUYA, 2017, p. 4)

Estas possibilidades de implementação trazem a necessidade de uma criteriosa avaliação dos impactos da área da Segurança da Informação com o objetivo de prevenir e mitigar riscos que podem trazer profundo ônus a sociedade em áreas vitais, como a segurança nacional, a ciência forense e o meio ambiente. (KATZ, Evgeny, 2014, p. XV)

A seguir, é apresentado um histórico de ocorrências, estudos ou projetos realizados voltados ao tema, que servem, de certa forma como fornecedores do supedâneo para a elaboração dos objetivos apresentados no presente trabalho.

2.1 BREVE HISTÓRICO DOS DISPOSITIVOS IMPLANTÁVEIS COM RELAÇÃO A SEGURANÇA DA INFORMAÇÃO

Em 11 de Novembro de 1997 Eduardo Kac, bio-artista brasileiro, executou uma performance na qual implantou sob a própria pele uma cápsula de vidro cirúrgico contendo um chip de RFID, um implante destinado a identificação de animais (CARVALHO, 1997). No ano seguinte, o professor Kevin Warwick realizou um procedimento semelhante com fins acadêmicos, o que ficou conhecido como *Project Cyborg 1.0* (Warwick, 2003), e que iniciaria uma nova área de pesquisa no campo da cibernética e áreas correlatas. Em 2002 o professor Warwick foi além realizando uma conexão entre seu organismo e o corpo de sua esposa por meio inorgânico, o *Project Cyborg 2.0* (Revista Super Interessante, 2002).

O surgimento de novos implantes experimentais implicou na constante pesquisa com relação a segurança física dos seus usuários, no entanto os riscos concernentes à segurança da informação não receberam a mesma atenção embora tem crescido de forma alarmante. Em julho de 2007 a *Baxter Healthcare Corporation* declarou, por duas vezes, ter identificado um comportamento anômalo em diversas de suas bombas de insulina inclusive utilizando o termo "*buffer overflow*" para descrever o ocorrido (FDA, 2007). No mesmo ano Dick Cheney, o então vice-presidente dos Estados Unidos da América, requisitou modificações em seu implante, um desfibrilador cardíaco, devido ao risco de um cyber ataque (The Guardian, 2013). No ano seguinte durante o 29º *Annual IEEE Symposium on Security and Privacy* foram apresentados ataques a Marca-passos e Desfibriladores Cardíacos por meio de softwares de radiofrequência e ataques do tipo "*Zero-Power Defenses*" (HALPERIN, IEEE, 2008). Em 16 de Março de 2009 Mark N. Gasson se tornou o primeiro ser humano infectado por um "*Malware*", um vírus de computador, em uma autoinfecção utilizada como prova de conceito (The Telegraph, 2010).

Nos anos seguintes surgiram diversas publicações alertando sobre as vulnerabilidades destes dispositivos bem como a sua aplicação em diversas áreas (GAZZIRO, 2010). Em 2011 a *BlackHat*, uma das maiores conferências de Segurança da Informação apresentou uma palestra dedicada ao *Hacking* de Dispositivos Médicos, em 2012 uma vulnerabilidade apresentada em

marca passos foi descrita como liberando uma descarga potencialmente fatal de 830-volt (COMPUTERWORLD, 2012). Também em 2013 o Jack Barnaby Michael Douglas descreveu ataques com risco de fatalidade para os usuários de dispositivos implantáveis cardíacos (BARNABY, 2013). Posteriormente a pesquisadora Marie Moe apresentou uma palestra onde apresentava-se tanto como especialista em Segurança da Informação como possível alvo de ataques por possuir um implante cardíaco. Cabe ressaltar aqui que o trabalho desta pesquisadora tem contribuído, até o momento desta publicação, para o desenvolvimento de um projeto para o governo Norueguês que visa justamente a proteção de dispositivos médicos.

Ainda em 2012 um outro trabalho foi dedicado a Interfaces Implantáveis, em 27 de abril de 2015 o pesquisador Seth Wahle (FORBES, 2015), usou seu implante subcutâneo como vetor de ataque a um *smartphone*. Em 2015 novamente foram demonstradas vulnerabilidades em bombas de insulina da Hospira bem como a resistência da empresa em colaborar com o pesquisador para saná-las (VICE, 2015). Já em 2016 cerca de 10 Milhões de registros de saúde foram colocados à venda por cibercriminosos (Healthcare IT News, 2016), e semelhante vazamento teria ocorrido em terreno nacional em princípios de 2019, o vazamento de dados pessoais de 2,4 milhões de usuários do SUS - Sistema Único de Saúde (UOL, 2019).

Em 2017 Lou Maresca e Brian Chee publicaram a análise de sete marca-passos de quatro diferentes fabricantes nos quais identificaram 19 vulnerabilidades de Segurança da Informação (CHEE; MARESCA, 2019.). No mesmo ano foi anunciado um *recall* de quase 500.000 marca-passos devido a falhas desta natureza. Uma atualização de *Firmware* foi descrita em um comunicado oficial do FDA (THE GUARDIAN, 2017). Cabe ressaltar que este também é o ano de surgimento do Rim Biônico (UCSF, 2017).

Em 2018 o Conselho de Eletrofisiológica do Colégio Americano de Cardiologia declarou no jornal da instituição que os atacantes poderiam desativar ou reprogramar certos recursos do marca-passo, causando choques elétricos, esgotamento da bateria e interrupção das comunicações sem fio que ajudam os médicos a monitorar as condições dos pacientes (JOURNAL OF THE AMERICAN COLLEGE OF CARDIOLOGY, 2018).

Dado o citado histórico fica estabelecido que os Dispositivos Implantáveis devido às suas diversas e variáveis características precisam ser avaliados caso a caso seguindo metodologias já utilizadas para outros ativos bem como específicas para cada dispositivo. Os citados dispositivos podem: conter dados que identifiquem seu hardware e software, bem como os dados do usuário ou usuários (*Project Cyborg 2.0*), sendo assim armazenadores de informação; transmitir e receber dados, podendo ser alvo de ataques (GASSON, 2013) ou ainda meio de ataque (FORBES, 2015); monitorar e processar dados em relação a saúde do usuário, como no caso de marca-passos, bombas de insulina e demais sensores, ou ainda dados de comunicação como no caso dos implantes cocleares ou próteses oculares que implementem câmeras.

Estes mesmos Dispositivos Implantáveis ainda podem incorrer em falhas de segurança associadas a sistemas externos devido as suas possibilidades de comunicação via RFID (GAZZIRO, M. A. et al, 2010), *bluetooth* (ČAPKUN; BODMER, 2010), *wireless*, conexão com bancos de dados online e leitores externos.

Todas as características apresentadas acima, podem implicar no risco físico ao paciente bem como ônus aos dados sensíveis deste usuário. Devido a sua diversidade de características, faz-se necessário descrevê-los e estabelecer suas características para então avaliar suas vulnerabilidades. Após elencar um histórico em geral de eventos e estudos envolvidos com a área de conhecimento do tema, os próximos tópicos apresentados serão voltados a explanar vulnerabilidades possíveis em dois dispositivos implantáveis, considerados aqui devido a características de suporte a saúde humana e reposição parcial ou não de funcionalidade do corpo.

3 VULNERABILIDADES DE DISPOSITIVOS IMPLANTÁVEIS

Os dispositivos implantáveis e os diversos incidentes apresentados em mídias e literaturas levantam relevantes questões no que concerne a segurança da informação, mais especificamente sobre a confidencialidade dos dados de seus usuários. Serão abordados apenas dois tipos de dispositivos implantáveis como exemplo neste capítulo, tendo em vista a impossibilidade de cobrir o grande número de dispositivos existentes e já citados, bem como seguir a recomendação sobre a abrangência dos exemplos, direcionando-os a riscos que afetem diversos dispositivos.

Os exemplos utilizados aqui serão os Implantes Cocleares (IC), dispositivos que são individualmente configurados para cada usuário, sendo definida sua intensidade de estimulação, isto é, as saídas de nível de corrente dos eletrodos, com base no perfil do paciente. Durante esse procedimento, também são definidos os parâmetros de processamento de voz. Apesar desta configuração específica este DI necessita muitas vezes de posterior configuração realizada pelo próprio usuário, conforme artigo publicado em 2010 *On the Security and Privacy Risks in Cochlear Implants*.

É destacada, a possibilidade de controle remoto de ICs, isto para que usuários tenham como modificar configurações do IC, seja afetando o programa ou algum parâmetro (Čapkun; Bodmer, 2010, p. 2).

Foi possível notar uma possibilidade de inserção de falhas ou vulnerabilidades oriundas de configurações realizadas pelo próprio usuário, independentemente da intenção deste em alcançar tal façanha. Utilizando deste tipo de possibilidade, um atacante pode vir a inserir instruções especificas em um dos implantes deste tipo de função, induzindo sinais que sejam interpretados como sons específicos não necessariamente reais ou oriundos do ambiente onde o usuário estiver, uma vez que o microfone padrão pode ser ignorado (Čapkun; Bodmer, 2010, p. 2).

Com o potencial de registrar sons captados pelo microfone do dispositivo, é possível ao atacante se utilizar disto para obter acesso aos dados auditivos pertencentes a conversas e ambientes onde o usuário trafegar em uma jornada comum do dia a dia. Caso venha a obter persistência na coleta de informações, é possível que o atacante seja capaz de reconstruir

a rotina do usuário com base nos sons ambiente coletados continuamente. Neste cenário em específico, a possibilidade de ferir a privacidade de terceiros que interagiram em algum momento com o usuário também poderá ser constatada, possibilitando traçar então um perfil do comportamento do usuário perante outras pessoas com as quais interage em sua rotina costumeira. (Čapkun; Bodmer, 2010).

Outro aspecto de risco com relação a privacidade dos ICs e seus dispositivos de controle remoto é o fato de poderem ser voluntariamente ou involuntariamente descobertos (dentro de sua faixa de frequência operacional) e rastreados. Estes cenários em que os dispositivos são involuntariamente descobertos são extremamente impactantes no tocante à privacidade, pois os usuários podem não necessariamente querer divulgar que estão usando um dispositivo de IC. As razões típicas são que isto pode ter implicações sociais e econômicas. Os dispositivos de IC podem transportam outros dados sensíveis relacionadas ao usuário como nome, data de nascimento, e caso possuam identificadores únicos, estes podem ser enquadrados como dados sensíveis tratados por legislações específicas como *General Data Protection Regulation (GDPR)* na Europa e Lei Geral de Proteção de Dados Pessoais (Brasil - Lei 13.709/2018).

No caso elencado dos IC poderiam ser implementados procedimentos e metodologias de Segurança da Informação objetivando mitigar estas vulnerabilidades, por exemplo o pareamento entre as partes citadas utilizar-se-ia de chaves criptográficas, permitindo autenticação mútua e proteção a integridade de sua comunicação (ČAPKUN; BODMER, 2010, p. 2). Igualmente, em caso de substituição de hardware (IC), haverá a necessidade de novo emparelhamento com o novo processador de fala, seja por dano causado ao mesmo ou necessidade de *upgrade.*

São diversas as interferências sobre Dispositivos Cardíacos Eletrônicos Implantáveis (DCEI) consideradas em trabalhos acadêmicos e em Diretrizes da Sociedade Brasileira de Cardiologia (SBC), considerando desde a presença de sinais elétricos, fenômenos mecânicos ou químicos extrínsecos, sendo estas de natureza eletromagnética ou mecânica, entre elas telefones celulares, telefones sem fio, *bluetooth, walkie talkie*, redes *wireless* ou *Wi-Fi*. Estas interferências podem resultar em variações

inapropriadas da frequência de estimulação, provocar reversão do marca-passo e falha das funções do Cardio Desfibrilador Implantável (CDI) (MARTINELLI FILHO; ZIMERMAN, 2007).

Com a crescente necessidade de implementação de dispositivos médicos com funcionalidades tecnológicas avançadas, envolvendo captação, armazenamento e processamento de dados, leva a uma necessidade de segurança cibernética para garantir a funcionalidade e a segurança, possuindo conectividade (FDA, 2014, p.1). Tendo como premissa que fraquezas e vulnerabilidades dependem de gestão para que exista a possibilidade de realizar atividades de mitigação, visando evitar que ocorra, de alguma maneira a exploração de falhas identificadas (FDA, 2014, p. 4).

Tendo apresentado os motivos e exemplos gerais para a preocupação com a segurança da informação de dispositivos médicos, a seguir, serão apresentadas algumas das regulações que afetam direta ou indiretamente, devido à ausência de regulamentação específica em vigor, a postura que deverá ser adotada por quem fabrica, fornece ou realiza o procedimento cirúrgico ou a manutenção destes dispositivos, uma vez que estes, tenham a possibilidade de armazenar, processar ou transmitir informações pessoais.

3.1 O ÂMBITO LEGAL E A PROTEÇÃO DOS DISPOSITIVOS IMPLANTÁVEIS

A proteção dos Dispositivos Implantáveis está associada a identificação do hardware e software utilizado nos referidos dispositivos, bem como seu comportamento quanto ao tratamento dos dados e informações por ele armazenados, processados ou transmitidos.

Se faz importante avaliar as características dos dispositivos de modo que sejam comtempladas características amplas de seu uso ou funcionamento. Considerar a possibilidade de “conexão” ou “conectividade”, podem ser apresentadas como opções mais claras em relação a termos técnicos que especifiquem demais a característica, como “conectado à rede”, ou com especificação de protocolo. É importante que haja a consideração da possibilidade de exploração de algum dos fatores envolvidos na utilização do dispositivo implantável para que se leve em conta a possibilidade de

exploração de algum dos fatores envolvidos na utilização ou manipulação do dispositivo. (FU, 2016, 1)

Quanto a devida proteção legal está relacionada às normatizações de cada País, embora de forma independentes, ou seja, há Leis de temas amplos que abordam à proteção de dados como a LGPDP (Brasil - Lei 13.709/2018) que entrará em vigor em fevereiro de 2020 e a GDPR (Europeia).

A LGPDP discorre sobre a proteção, armazenamento e meios de comunicação em segurança da informação; embora o foco abordado na referida Lei neste trabalho será, em especial, as áreas da Saúde e Medicina, onde se englobam os referidos Dispositivos aqui tratados.

Nessa toada, os Estados Unidos possuem diversas regulamentações, contudo no que se refere à área da saúde, a Agência Federal Americana que pertence ao FDA é responsável pela proteção e promoção da saúde pública por meio de controle e supervisão de produtos de tabaco, segurança alimentar, suplementos dietéticos, medicamentos, vacinas, transfusões de sangue, Dispositivos Médicos entre outros insumos congêneres a sua atividade.

Sua fiscalização é feita pelo Escritório de Assuntos Regulatórios da agência, realizando a grande maioria do trabalho da FDA em campo. Os agentes de segurança do consumidor, são os indivíduos que inspecionam as instalações de produção e armazenagem, investigam queixas, doenças ou surtos e revisam a documentação no caso de dispositivos médicos, medicamentos, produtos biológicos e outros itens onde pode ser difícil para realizar um exame físico ou tomar uma amostra física do produto.

Possui ainda a HIPAA, aprovada em 1996, a referida Lei trata da portabilidade e responsabilidade de informações de saúde, entre elas o acesso às informações, Compartilhamento de informações e Proteção de suas informações, além de Assegurar a confidencialidade, integridade e disponibilidade de todos os e-PHI (*eletronic personal health information*) que criam, recebem, mantêm ou transmitem; Identificar e proteger contra ameaças razoavelmente antecipadas à segurança ou integridade da informação e Proteger contra usos ou divulgações razoavelmente antecipadas, inadmissíveis.

Na Europa o GPDR, são regras sobre a privacidade de dados pessoais do indivíduo e possui validade não somente na União Europeia, mas também em outros Países, inclusive o Brasil, pois os dados poderão ser migrados, copiados ou acessados, se o usuário desejar e, quando cabível. As empresas e organizações deverão seguir regras rígidas para coletar, processar, compartilhar e resguardar dados pessoais de qualquer cidadão de um dos Países do bloco Europeu, em conformidade com a Lei GPDR.

Enquanto no Brasil, temos leis relativamente novas para o âmbito informático, conforme citadas abaixo:

1. **Lei Nº 12.737/2012 (conhecida como Lei Carolina Dieckmann)** - Introduziu três tipos penais específicos envolvendo crimes informáticos: i) invasão de dispositivo informático alheio (artigo 154-A do Código Penal); ii) interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (artigo 266, §§ 1º e 2º do Código Penal); e iii) falsificação de cartão de crédito ou débito (artigo 298 do Código Penal). Observa-se que a referida Lei entrou efetivamente em vigor em 03 de abril de 2013, alterando o Código Penal Brasileiro (CPB). A partir desse momento os crimes enquadrados nesta Lei passarão a ser penalizados, o que antes não ocorriam. No escopo no nosso trabalho o enfoque desta Lei está nas vulnerabilidades cibernéticas que por ventura ocorram, além dos planos de continuidade que por ventura possam ter, ainda há o embasamento legal para dar resposta no âmbito criminal ao autor do delito, se for identificado.

2. **Decreto Nº 7.962/2013** - Regulamentou o **Código de Defesa do Consumidor (CDC) - Lei n. 8078/1990**, para dispor sobre a contratação no comércio eletrônico. Traz diversos esclarecimentos sobre atendimento ao consumidor em relação às compras realizadas pela internet, direito de arrependimento

em comércio eletrônico, incluindo ainda a obrigatoriedade de disponibilizar, em local de fácil visualização, qualquer risco e a segurança dos consumidores no que se refere a qualquer atividade exercida por meios eletrônicos. Exemplo de compra de um chip RFID para uso subcutâneo, ou seja, é um dispositivo implantável.

Na mesma esteira, ambas dentro do CDC, há a seguinte garantia legal:

3. **Lei 8078/1990**. **Código de Defesa do Consumidor – CDC-** Art. 12. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos.

   § 1º O produto é defeituoso quando não oferece a segurança que dele legitimamente se espera, levando-se em consideração as circunstâncias relevantes, entre as quais:

   I - Sua apresentação;

   II - o uso e os riscos que razoavelmente dele se esperam;

   III - a época em que foi colocado em circulação.

   § 2º O produto não é considerado defeituoso pelo fato de outro de melhor qualidade ter sido colocado no mercado.

   § 3º O fabricante, o construtor, o produtor ou importador só não será responsabilizado quando provar:

   I - que não colocou o produto no mercado;

   II - que, embora haja colocado o produto no mercado, o defeito inexiste;

   III - a culpa exclusiva do consumidor ou de terceiro.

O fabricante de implantes só não será responsabilizado quando a culpa for exclusiva do médico ou do paciente, ou eventuais terceiros que venham a manipular o dispositivo, uma vez que já tenha sido comprovado o correto funcionamento antes de tal manipulação.

Nesta toada, o CDC acoberta em direitos o usuário que por ventura venham a adquirir, por exemplo, um implante coclear, que usando de tecnologia *bluetooth* venha a oferecer riscos e vulnerabilidades ao seu cliente ou usuário em decorrência da ausência de informações claras sobre o pareamento dessa tecnologia de transmissão e/ou comunicação, já amplamente difundida e igualmente pacificada nas possíveis vulnerabilidades possíveis; no seguinte cenário fictício, em miúde, seu usuário uma pessoa influente e detentora de informações sigilosas de uma determinada organização, teve a seu dispositivo auditivo interceptado que possui o transmissor e receptor *bluetooth ativo* e toda sua audição ambiental passou a ser uma escuta ambiental e, essas informações sigilosas foram vazadas por falha ou vulnerabilidade de tal tecnologia que tenha sido explorada naquele instante (ČAPKUN; BODMER, 2010, p. 2).

4. **Lei Nº 12.965/2014 (Marco Civil da Internet)** - Estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil, tanto para provedores de conexão, provedores de aplicação e usuários da Internet. É um marco mundial, no que concerne ao tratamento da Internet sob a ótica do Direito Civil, sendo referenciado por alguns como a "Constituição da Internet", tendo em vista o caráter de princípio lógico da norma. Tendo os capítulos 7 e 16, abaixo integralmente destacadas do corpo da referida Lei, contudo futuramente alteradas pela **Lei Geral de Proteção de Dados Pessoais** (LGPDP), que serão explicitadas no item 5 deste trabalho.

- **Lei Nº 12.965/2014 - Marco Civil da Internet.** CAPÍTULO II - DOS DIREITOS E GARANTIAS DOS USUÁRIOS

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;

V - manutenção da qualidade contratada da conexão à internet;

VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;

XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e

XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no **caput**, tais como aquelas que:

I - Impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou

II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

- **Lei Nº 12.965/2014 - Marco Civil da Internet.** Subseção III - Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações da

Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:

I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º; ou

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.

5. **Lei Geral de Proteção de Dados Pessoais-** LGPDP -Lei n. 13.709/2018, regula as atividades de tratamento de dados pessoais e alterou os artigos 7 e 16 do Marco Civil da Internet, enfatizando conforme segue:

- **Dados pessoais**: é toda informação relacionada a pessoa natural identificada ou identificável, tal como nome, RG, CPF, e-mail, etc. Dados relativos a uma pessoa jurídica (tais como razão social, CNPJ, endereço comercial, etc.) não são considerados dados pessoais.

- **Dados pessoais sensíveis**: é todo dado pessoal que pode gerar qualquer tipo de discriminação, tais como os dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

- **Tratamento**: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento,

eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

- **Controlador**: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

- **Processador**: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

- **Consentimento**: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada**.**

- **Anonimização**: processos e técnicas por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

- **Dado anonimizado**: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. O dado anonimizado não é considerado dado pessoal para fins de aplicação da LGPDP.

- **Pseudononimização**: processos e técnicas por meio dos quais um dado tem sua possibilidade de associação dificultada. O dado pseudonimizado é considerado dado pessoal para fins de aplicação da LGPDP, tendo em vista a possibilidade de associação desse dado a uma pessoa natural.

  O LDPDP vem com intuito de preservar os dados pessoais e tornar possível sua portabilidade, dando principalmente autonomia sobre os dados ao seu real proprietário, resguarda o

usuário (pessoa física) nas garantias e deveres que as empresas (pessoas jurídicas), devem tratar de seus dados, assim gerará uma obrigação legal quanto a proteção de dados pessoais. Está prevista para entrar em vigor em fevereiro de 2020 e fora dado 18 meses (*Vacatio Legis*) desde sua publicação, 14 de gosto de 2018, para as organizações e empresas se adaptarem.

6. **Normativa n. 2830 Anvisa – Responsável pelo uso e operação do equipamento médico.**

Responsável pelo uso e operação do equipamento médico

- Procedimentos necessários antes do uso do equipamento médico
- Formas de utilização do equipamento

- Informações quanto à indicação de que o equipamento médico deve ser usado ou operado somente por profissional com habilitação definida ou treinado especificamente pela empresa é prerrogativa do fabricante do equipamento.

- Procedimentos necessários antes do uso do equipamento médico

- Todos os procedimentos a serem adotados antes de utilizar o equipamento médico devem estar descritos nas suas instruções de uso, o que inclui procedimentos clínicos de preparação do paciente e procedimentos técnicos e operacionais para preparar o equipamento para uso (ex.: esterilização, teste de alarmes, calibração, montagem, configuração de parâmetros etc.).

- Formas de utilização do equipamento

- O fabricante do equipamento deverá informar as suas formas de utilização:

- os procedimentos técnicos necessários para o usuário ou operador conectar, manusear e utilizar as partes e acessórios com o equipamento, incluindo informações gráficas, tais como figuras ou fotos inteligíveis, para melhor entendimento da descrição dos procedimentos;

- a descrição dos procedimentos para uso e operação completa do equipamento; e

- se necessária, a indicação de que o equipamento somente pode ser usado ou operado por profissional com habilitação definida ou que possua treinamento específico providenciado pela empresa.

Conforme se lê na normativa Anvisa, há recomendações para o profissional técnico e o usuário que fará uso de equipamentos médicos, entretanto é evidente sua subjetividade e portanto clara evidência de omissão na cautela dos princípios da segurança da informação, deixando o fabricante organizar, dentro dessa recomendação, a melhor formar de informar sobre o equipamento, não gerando requisitos mínimos padronizados para boas práticas no que tange a segurança e portanto, riscos de morte do paciente em decorrência de possíveis vulnerabilidades cibernéticas e ou ambientais.

7. **Lei n. 9695/1998.** Acrescenta incisos ao art. 1º da Lei nº 8.072 de 25 de julho de 1990, que **dispõe sobre os crimes hediondos**, e altera os arts. 2º, 5º e 10 da Lei nº 6.437, de 20 de agosto de 1977, e dá outras providências.

Art. 1º O art. 1º da Lei nº 8.072, de 25 de julho de 1990, alterado pela Lei nº 8.930, de 6 de setembro de 1994, passa a vigorar acrescido dos seguintes incisos:

VII-B - falsificação, corrupção, adulteração ou alteração de produto destinado a fins terapêuticos ou medicinais (art. 273, *caput* e § 1º, § 1º-A e § 1º-B, com a redação dada pela Lei nº 9.677, de 2 de julho de 1998)."

LEI Nº. 9.677, DE 2 DE JULHO DE 1998.

Altera dispositivos do Capítulo III do Título VIII do Código Penal, incluindo na classificação dos delitos considerados hediondos crimes contra a saúde pública, e dá outras providências.

"Art. 273. Falsificar, corromper, adulterar ou alterar produto destinado a fins terapêuticos ou medicinais:"(NR)

"Pena - reclusão, de 10 (dez) a 15 (quinze) anos, e multa."(NR)

"§ 1º Nas mesmas penas incorre quem importa, vende, expõe à venda, tem em depósito para vender ou, de qualquer forma, distribui ou entrega a consumo o produto falsificado, corrompido, adulterado ou alterado."(NR)

"§ 1º-A. Incluem-se entre os produtos a que se refere este artigo os medicamentos, as matérias-primas, os insumos farmacêuticos, os cosméticos, os saneantes e os de uso em diagnóstico."

"§ 1º-B. Está sujeito às penas deste artigo quem pratica as ações previstas no § 1º em relação a produtos em qualquer das seguintes condições:

> I - sem registro, quando exigível, no órgão de vigilância sanitária competente;
>
> II - em desacordo com a fórmula constante do registro previsto no inciso anterior;
>
> III - sem as características de identidade e qualidade admitidas para a sua comercialização;
>
> IV - com redução de seu valor terapêutico ou de sua atividade;
>
> V - de procedência ignorada;
>
> VI - adquiridos de estabelecimento sem licença da autoridade sanitária competente."

Esta Lei foca em delitos praticados com produtos, insumos, de uso de diagnóstico, matérias primas de uso médicos ou terapêuticos, dando a devida importância aos riscos à saúde pública, que por ventura, tais equipamentos médicos implantáveis podem esbarrar na referida Lei, se não observadas as questões legais pertinentes.

A segurança da informação é sem dúvida o objeto a ser evidenciado neste trabalho, mas destacamos como forma de uma iniciação do relatório no capítulo seguinte, que a segurança jurídica somada com a segurança da informação tornará este relatório substancial em forma e conteúdo, pois será construído com pilares que norteiam os usuários e os futuros estudiosos que com esta singela contribuição, construirão e elevarão a produção de conhecimento na área crescente de Biohacking.

Dada as responsabilidades cabíveis aos fornecedores e envolvidos profissionalmente com os dispositivos médicos implantáveis, visto que este podem acarretar em comprometimento de dados pessoais, da privacidade e da saúde de um usuário, é de suma importância que ocorra um processo de gestão de descritivos que informem a respeito das informações que estarão

contidas em um dispositivo médico implantável, sem que, deste modo, sejam feridos os direitos do usuário.

No próximo capítulo, serão descritos os processos que podem ser seguidos em ideias gerais para a possibilidade de gestão de segurança da informação, levando em conta as características abrangentes, que se submetem aos requerimentos gerais das regulamentações citadas. Além de apresentar as ideias gerais do processo, há um exemplo em quadro sobre como pode ser realizada a elaboração do relatório descrito.

4 RELATÓRIO DE SEGURANÇA DA INFORMAÇÃO PARA DISPOSITIVOS IMPLANTÁVEIS.

O primeiro passo para a proteção de um dispositivo é a compreensão do mesmo, sendo assim se faz necessário descrevê-lo. Devido às suas diversas e variadas características, os Dispositivos Implantáveis precisam ser avaliados caso a caso seguindo metodologias já utilizadas para outros ativos bem como específicas para cada dispositivo. Devido a sua diversidade de características, faz-se necessário descrevê-las para então avaliar suas vulnerabilidades. Apresentados a seguir, um relatório elaborado com o propósito de propiciar a criação de um modelo de relatório, que convém que seja mantido para vias de gestão da Segurança da Informação com relação à Dispositivos Implantáveis.

Todos os processos descritos deverão ser desenvolvidos com vistas a compor uma documentação que possibilite posterior consulta e atualização. Conforme descrito neste trabalho, os citados dispositivos apresentam:

- Dados que identifiquem seu hardware e software
- Dados do usuário ou usuários
- Armazenar, transmitir e receber dados
- Monitorar e processar dados
    - De saúde do usuário
    - Dados de comunicação com outros dispositivos

Para identificação destes critérios, abaixo é apresentado um esquema detalhado de atividades que cobre cada etapa necessária para elaboração do citado relatório.

Esquema detalhado de atividades

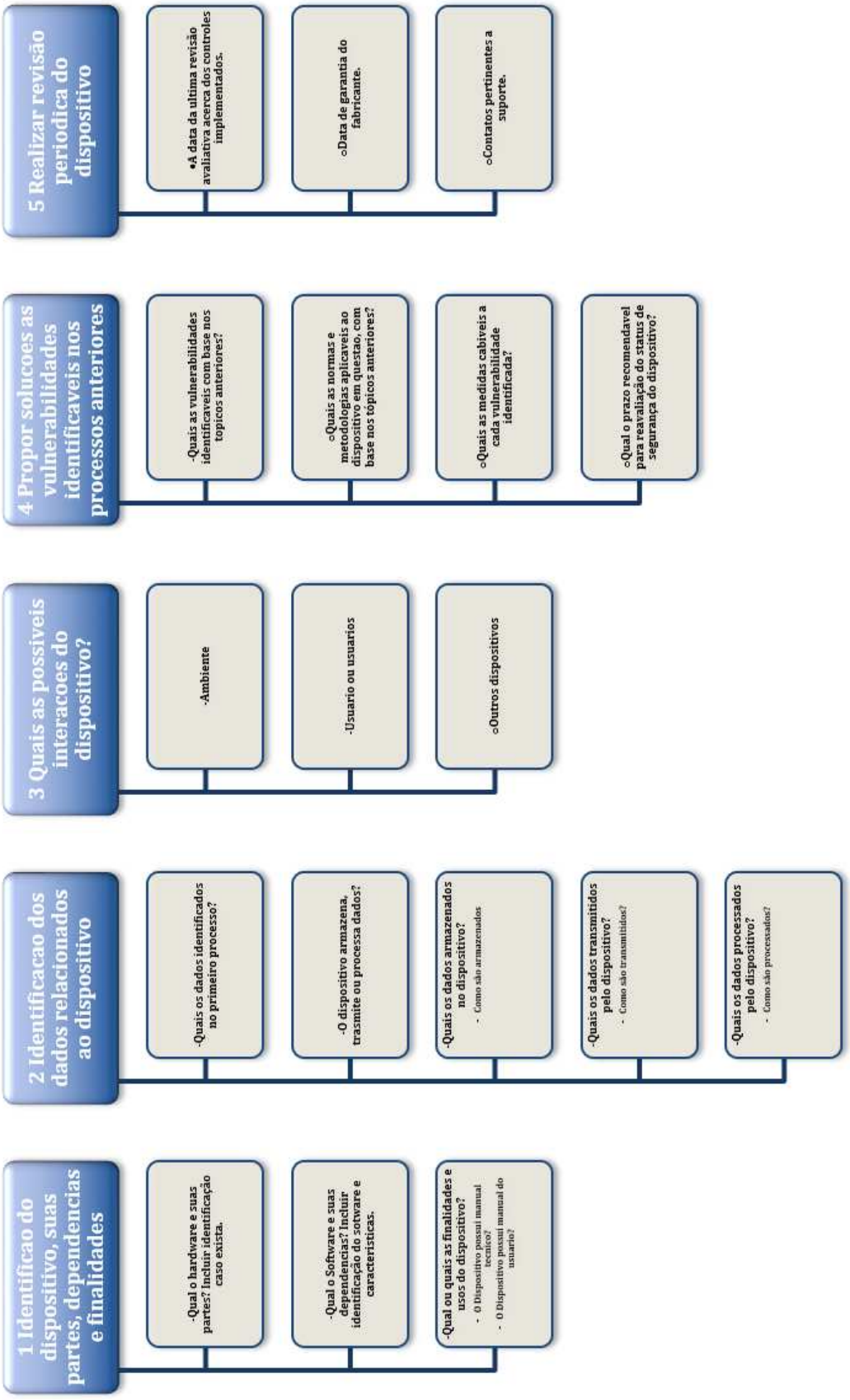

Figura 1 - Esquema detalhado de atividades - Fonte: Autores

Descrição das etapas que compõem o esquema de atividades:

1. Identificação do dispositivo, suas partes, dependências e finalidades

- Qual o hardware e suas partes?
  - Incluir identificação caso exista. Ex: Serial Number, MAC Adress, características visíveis.
- Qual o Software e suas dependências?
  - Incluir identificação do software e características. Ex: Versão, funcionalidade, data de atualização
- Qual ou quais as finalidades e usos do dispositivo? Obs: Todos os manuais identificados devem ser anexados ao relatório final.
  - O Dispositivo possui manual técnico?
  - O Dispositivo possui manual do usuário?

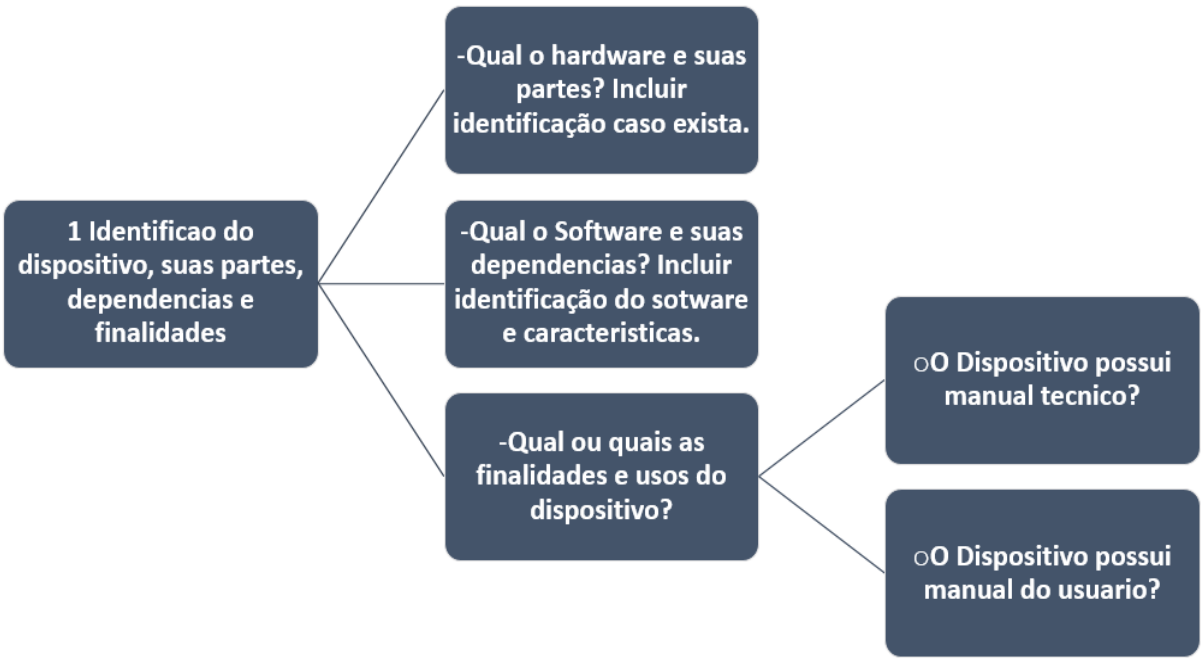

Figura 2 – Fonte: Autores

2. Identificação dos dados relacionados ao dispositivo: Conforme orientação oriunda de normas, legislações e demais fontes pertinentes, elencar o ciclo de vida dos dados e sua tratativa em cada uma das fases deste ciclo: Armazenamento, transferência, acesso e outros (ver LGPDP etc.)

- Quais os dados identificados no primeiro processo?
- O dispositivo armazena, transmite ou processa dados?
- Quais os dados armazenados no dispositivo?
  - Como são armazenados?
- Quais os dados transmitidos pelo dispositivo?
  - Como são transmitidos?

- Quais os dados processados pelo dispositivo?
    - Como são processados?

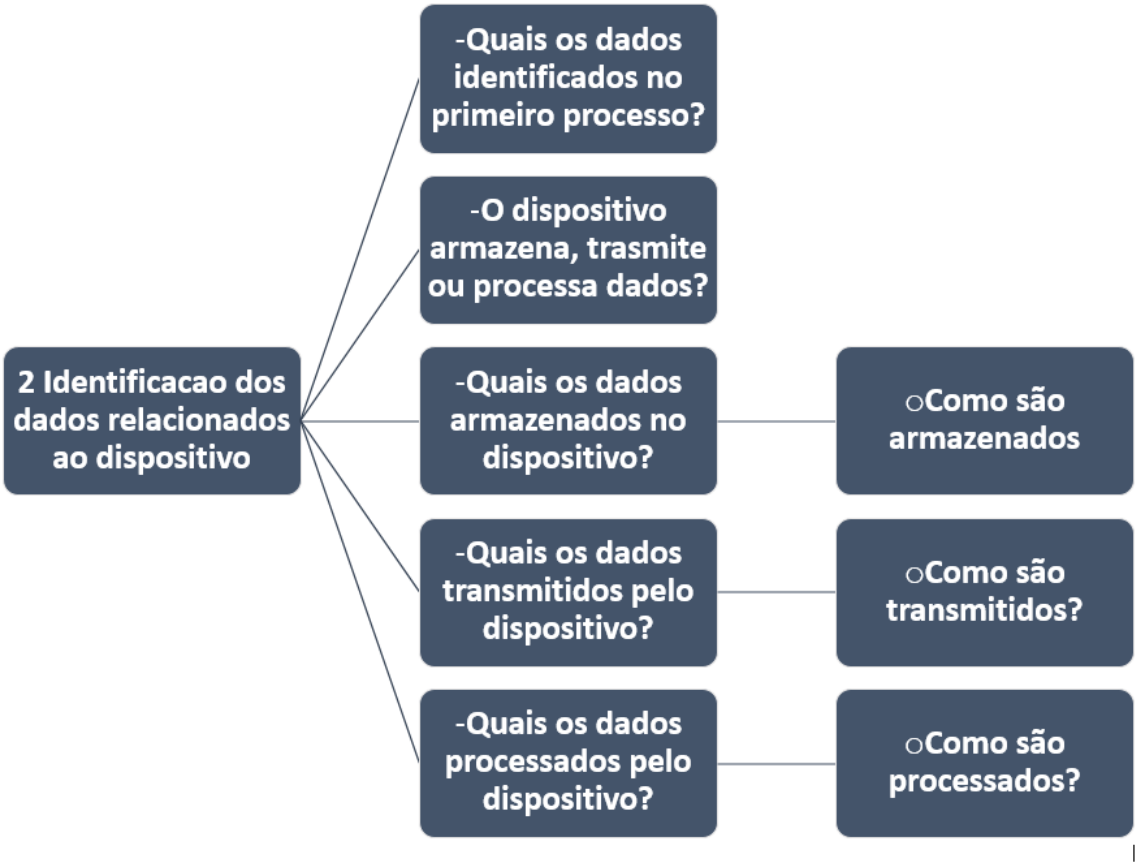

Figura 3 – Fonte: Autores

3. Quais as possíveis interações do dispositivo com relação à:

- Ambiente
- Usuário ou usuários
    - Identificar possíveis interações dos usuários com estes dispositivos. Quais as possíveis customizações e usos acessíveis ao usuário ou usuários (pareamento, manutenção, configurações de desempenho Ex: volume de áudio, ritmo cardíaco, compartilhamento de dados)
    - Outros dispositivos – Quando existir pareamento (via Bluetooth, RFid ou demais possibilidades):
        - Com quais tipos de dispositivos ou equipamentos o DI pode interagir e por quais meios?

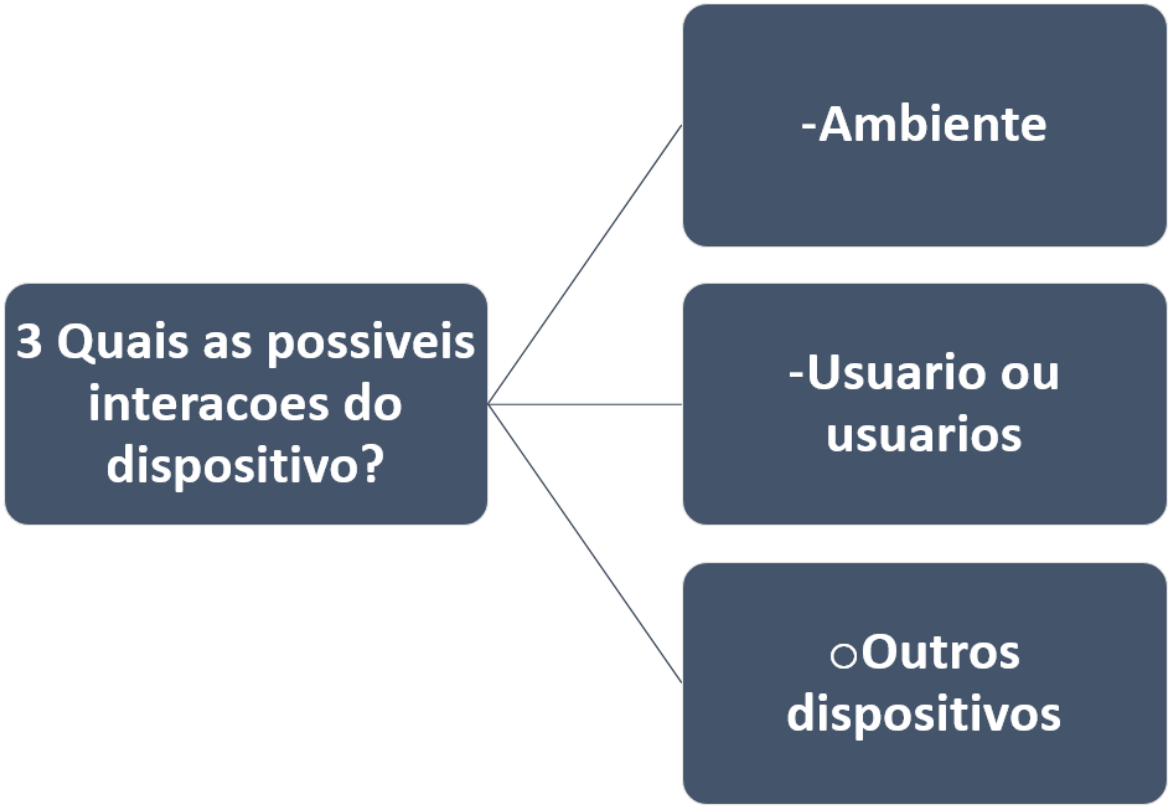

Figura 4 – Fonte : Fonte: Autores

4. Propor soluções às vulnerabilidades identificáveis ou identificadas nos processos anteriores:

- Compor relatório que elenque os seguintes quesitos:
  - Quais as vulnerabilidades identificáveis com base nos tópicos anteriores?
    - Neste ponto é válido levar em conta uma abrangência genérica para determinar uma gama maior de possíveis falhas de segurança, podendo assim tornar o todo do processo mais eficaz para futuras atualizações dos componentes descritos.
  - Quais as normas e metodologias aplicáveis ao dispositivo em questão, com base nos tópicos anteriores?
  - Quais as medidas cabíveis a cada vulnerabilidade identificada?
  - Qual o prazo recomendável para reavaliação do status de segurança do dispositivo?

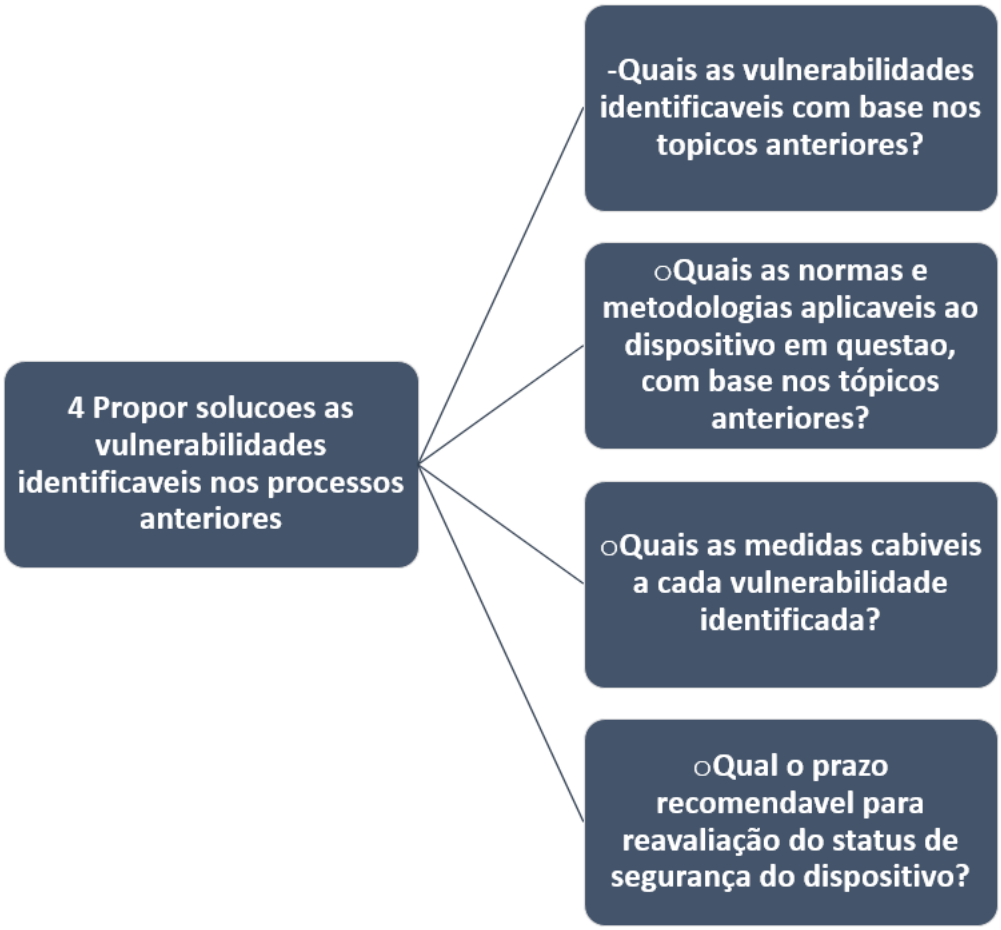

Figura 5 – Fonte: Autores

5. Realizar revisão periódica do dispositivo:

- Aqui todas as partes documentadas devem ser relacionadas para determinar o período de validade do atual relatório. Serão apresentadas aqui (quando existirem):
    - A data da última revisão avaliativa acerca dos controles implementados.
    - Data de garantia do fabricante.
    - Contatos pertinentes a suporte.

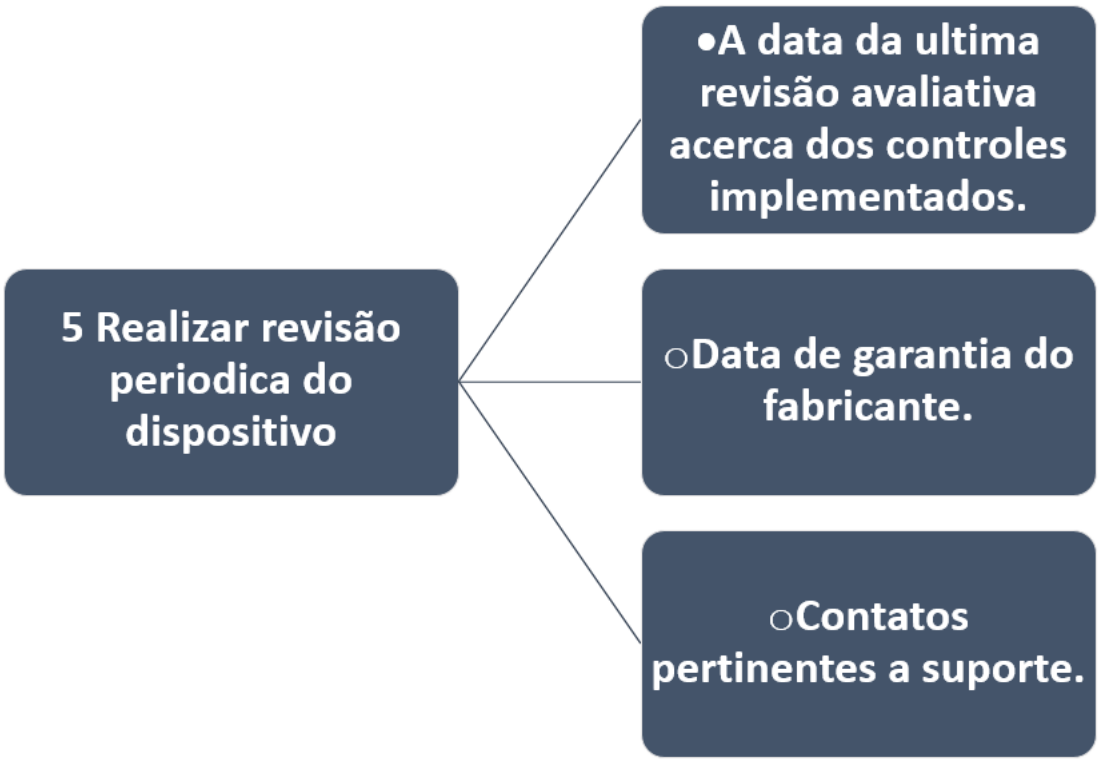

Figura 6 – Fonte: Autores

As questões levantadas em cada uma das etapas elencadas acima podem ser agrupadas em uma ficha em formato de relatório, possibilitando então um registro padronizado em meio acessível para os profissionais que necessitem obter acesso à informação anteriormente registrada para perpetuar um controle preciso e conciso acerca dos Dispositivos Médicos Implantáveis e suas características que possivelmente venham a lhe deixar com passíveis à exploração de vulnerabilidades que venham a ser descobertas.

Exemplo de relatório.

Relatório de Vulnerabilidades	Identificações do dispositivo	Software e Dependências
Identificação		
	Finalidades de Uso	
	Possui Manual Técnico?	
	Possui manual do usuário?	
	Armazena dados?	
	Transmite dados?	
	Processa dados?	
Descrição	Quais os dados transmitidos pelo dispositivo?	
	Quais os dados processados pelo dispositivo?	
	Quais os dados armazenados pelo dispositivo?	
	Como são transmitidos?	
	Como são processados?	
	Como são armazenados?	
Quais as possíveis interações do dispositivo?	Ambiente	Outros dispositivos
	Usuário ou usuários	

<table>
<tr><td rowspan="15">Vulnerabilidades</td><td>Quais as vulnerabilidades identificaveis com base nos tópicos anteriores?</td><td>Quais as normas e metodologias aplicáveis ao dispositivo em questão com base nos tópicos anteriores?</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Quais as medidas cabíveis a cada vulnerabilidade?</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>Quais as medidas cabíveis para cada vulnerabilidade identificada?</td><td>Prazo para Reavaliar a Segurança dispositivos</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td rowspan="5">Realizar a revisão periódica da segurança do dispositivo</td><td>Data da ultima avaliação:</td><td>Contatos pertinentes a suporte</td></tr>
<tr><td></td><td></td></tr>
<tr><td rowspan="2">Data de garantia do Fabricante:</td><td></td></tr>
<tr><td></td></tr>
<tr><td></td><td></td></tr>
</table>

Em vistas de manter o processo abrangente, o quadro acima apresentado segue a ordem geral dos passos a serem seguidos, podendo então o profissional encarregado pela gestão de vulnerabilidades em dispositivos

implantáveis tomar outras decisões cabíveis para complementar os campos do quadro de forma a melhor se adequar à particularidades do caso proposto.

CONSIDERAÇÕES FINAIS

Após realizar a leitura dos referenciais ao tema, foi possível compreender a complexidade exigida no que tange empregar controles de Segurança da Informação em dispositivos implantáveis. Há, fora do país, inúmeras iniciativas voltadas ao estudo do tema, abrangendo não apenas os dispositivos, mas, equipamentos que tem interações diretas com os dispositivos, mesmo que variando em finalidade, propõem melhorias em âmbitos tecnológicos e legais, além da existência de orientações quanto a adoção regularizada destas normas dentro das regulamentações gerais de instituições responsáveis.

Devido a sua grande necessidade por disponibilidade em detrimento dos demais pilares de segurança da informação, não consideramos possível empregar certas técnicas já reconhecidas e eficazes, aplicáveis a outros cenários de dispositivos eletrônicos e informáticos de forma geral, regularizados por diversos órgãos, padrões e legislações recomendáveis para o ganho de resiliência em proteção de dados pessoais, uma vez que estas práticas tem a possibilidade de tornar indisponível o acesso ao dispositivo implantável em situações críticas para a vida humana.

No cenário nacional, há muito o que se desenvolver, tanto em permissividade de estudo quanto em incentivo. Hoje, existem normas de biossegurança que tangem apenas os estudos voltados a tecidos vivos, enxergamos isto como um limitador, que impõe apenas a possibilidade de experimentações clandestinas envolvendo dispositivos eletrônicos implantáveis, com finalidades variadas. Acreditamos que o incentivo a pesquisa e aprofundamento no tema, trará benefícios a todo e qualquer usuário que tenha a necessidade de possuir um dispositivo eletrônico implantado em seu corpo, bem como para instituições com dedicação ao estudo e desenvolvimento cientifico voltado ao benefício geral da população, para fornecer, através do dispositivo, uma funcionalidade ou suporte a saúde de maneira geral.

REFERÊNCIAS

AZIZ, H. A.; GULED, A. Cloud computing and healthcare services. 2016.

JACK, Barnaby. Implantable medical devices: Hacking humans. Black Hat USA, 2013.

ČAPKUN, Srdjan; BODMER, Daniel. On the security and privacy risks in cochlear implants. Technical report/Swiss Federal Institute of Technology Zürich, Department of Computer Science, v. 677, 2010.

CHEE, Brian; MARESCA, Lou. Pacemakers with Vulnerabilities 2017. (12m47s). Disponível em: <https://youtu.be/3XvnaonC0U8>. Acesso em: 20/05/2019.

CHENG, Michael. Medical device regulations: global overview and guiding principles. World Health Organization, 2003.

CLARK, Shane S.; FU, Kevin. Recent results in computer security for medical devices. In: International Conference on Wireless Mobile Communication and Healthcare. Springer, Berlin, Heidelberg, 2011. p. 111-118.

COMPUTERWORLD, 17/10/2012. Disponível em <https://www.computerworld.com/article/2492453/malware-vulnerabilities/pacemaker-hack-can-deliver-deadly-830-volt-jolt.html>, Acessado em 20/05/2019.

SILVA, Rafael Pinto da et al. Brasil informacional: a segurança cibernética como desafio à segurança nacional. Enancib, v. 17, 2016.

DENNING, Tamara; FU, Kevin; KOHNO. Tadayoshi. Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security. In: HotSec. 2008.

FRIED, Inbar. What about security? Medical Applications and Implantable Medical Devices. 2014.

FU, K. Infrastructure Disruption: Internet of Things Security, Testimony before the US House of Representatives Committee on Energy and Commerce, Subcommittee on Communications and Technology and Subcommittee on Commerce, Manufacturing, and Trade (Nov. 16, 2016).

FU, Kevin. Software issues for the medical device approval process. Statement to the Special Committee on Aging, United States Senate, Hearing on a Delicate Balance: FDA and the Reform of the Medical Device Approval Process, 2011.

GASSON, Mark N.; KOOPS, Bert-Jaap. Attacking human implants: a new generation of cybercrime. Law, Innovation and Technology, v. 5, n. 2, p. 248-277, 2013.

GAZZIRO, M. A. et al. Smart Gun with Implantable RFid Match System–A practical approach. In: Proceedings of the European conference of chemical engineering, and European conference of civil engineering, and European conference of mechanical engineering, and European conference on Control. World Scientific and Engineering Academy and Society (WSEAS), 2010. p. 223-226.

GLADDEN, Matthew E. Critical Challenges in Information Security for Advanced Neuroprosthetics. Synthypion Academic, 2015.

GOLLAKOTA, Shyamnath et al. They can hear your heartbeats: non-invasive security for implantable medical devices. In: ACM SIGCOMM Computer Communication Review. ACM, 2011. p. 2-13.

GUARDIAN, Jornal The, 19/10/2013 Disponível em <https://www.theguardian.com/world/2013/oct/19/dick-cheney-heart-assassination-fear>. Acesso em 05/05/2019.

GUARDIAN, Jornal The, 31/08/2017 Disponível em <https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update>. Acesso em 05/05/2019.

HADDOW, Gill; HARMON, Shawn HE; GILMAN, Leah. Implantable smart technologies (IST): Defining the 'sting'in data and device. Health Care Analysis, v. 24, n. 3, p. 210-227, 2016.

HALPERIN, Daniel et al. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In: Security and Privacy, 2008. SP 2008. IEEE Symposium on. IEEE, 2008. p. 129-142.

HALPERIN, Daniel et al. Security and privacy for implantable medical devices. IEEE pervasive computing, v. 7, n. 1, 2008.

HANNA, Steve et al. Take Two Software Updates and See Me in the Morning: The Case for Software Security Evaluations of Medical Devices. In: HealthSec. 2011.

HEALTHCARE Management 38, 2015 Disponível em< http://studylibpt.com/doc/1541206/dispositivos-m%C3%A9dicos-implant%C3%A1veis>. Acesso em 19/04/2018

HEALTHCARE IT NEWS, 28/06/2016. Disponível em https://www.healthcareitnews.com/news/millions-patient-records-reportedly-sale-dark-web-after-ransom-demand. Acesso em 19/04/2018

HOLZ, Christian et al. Implanted user interfaces. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2012. p. 503-512.

IENCA, Marcello. HACKING MINDS, HACKING BRAINS, HACKING AUGMENTED BODIES: ETHICAL ASPECTS OF NEUROHACKING. In: The First Biannual Neuroadaptive Technology Conference. 2017. p. 113.

KNOW, What Should You. Cybersecurity for Cardiac Implantable Electronic Devices. JOURNAL OF THE AMERICAN COLLEGE OF CARDIOLOGY, v. 71, n. 11, 2018.

KAYACIK, Hilmi Günes; ZINCIR-HEYWOOD, A. Nur; HEYWOOD, Malcolm. Evolving successful stack overflow attacks for vulnerability testing. In: 21st Annual Computer Security Applications Conference (ACSAC'05). IEEE, 2005. p. 8 pp.-234.

KASPER, Timo; OSWALD, David; PAAR, Christof. Sweet dreams and nightmares: security in the internet of things. In: IFIP International Workshop on Information Security Theory and Practice. Springer, Berlin, Heidelberg, 2014. p. 1-9.

KATZ, Evgeny (Ed.). Implantable bioelectronics. John Wiley & Sons, 2014.

KOBES, Shelby David. Security implications of implantable medical devices. 2014.

KRAMER, Daniel B. et al. Security and privacy qualities of medical devices: An analysis of FDA postmarket surveillance. PLoS One, v. 7, n. 7, p. e40200, 2012.

MADARY, Jennifer. Addressing Cyber Security Vulnerabilities and Threats to Implantable Medical Devices. 2016.

MARTINELLI FILHO, Martino; ZIMERMAN, Leandro Ioschpe. Diretrizes brasileiras de dispositivos cardíacos eletrônicos implantáveis (DCEI). Arquivos brasileiros de cardiologia. São Paulo. Vol. 89, n. 6 (2007), p. e210-e237, 2007.

MOE, Marie EG. Unpatchable - Living with a Vulnerable Implanted Device 2015. (52m25s). Disponível em: <https://www.youtube.com/watch?v=ffpkFvRZWB8>. Acesso em: 28/05/2019.

MORENO, Daniel. Introdução ao Pentest. 1ª. Ed. São Paulo: Novatec, 2015.

VICE, 01/12/2015. Disponível em <https://motherboard.vice.com/en_us/article/78kp3x/drug-pump-maker-denies-security-patch-to-researcher-who-found-vulnerabilities>, Acessado em 20/05/2019

NAVON, Daniel. The Security of Medical Devices: How and Why Poor Security Puts People's Lives In Danger. 2016.

CARVALHO, Mario Cesar. Disponível em <https://www1.folha.uol.com.br/fsp/1997/11/11/cotidiano/13.html>. Acesso em 05/05/2019.

PERSPECTIVE, A. Managerial. Implantable Computers and Information Security.

SALAJEGHEH, Mastooreh; MOLINA, Andres; FU, Kevin. Home Telemedicine: Encryption is Not Enough. Journal of Medical Devices, v. 3, n. 2, p. 027503, 2009.

SAMARAS, Elizabeth Averill; SAMARAS, George Michael. Confronting systemic challenges in interoperable medical device safety, security & usability. Journal of biomedical informatics, v. 63, p. 226-234, 2016.13

SAMETINGER, Johannes et al. Security challenges for medical devices. Communications of the ACM, v. 58, n. 4, p. 74-82, 2015.

SCHECHTER, Stuart. Security that is Meant to be Skin Deep. Microsoft Research, Tech. Rep, 2010.

SENGUPTA, Korok. Development and Concerns for Wearable Ubiquitous Technology.

SUPER INTERESSANTE, Revista Disponível em <https://super.abril.com.br/tecnologia/kevin-warwick-o-ciborgue-numero-1/>. Acesso em 05/05/2019.

TELEGRAPH, Jornal The, 26/05/2010 Disponível em <https://www.telegraph.co.uk/technology/news/7767369/Scientist-is-first-man-to-be-infected-by-computer-virus.html>. Acesso em 05/05/2019.

UCSF - University of California San Francisco, 2017, Disponível em < https://pharm.ucsf.edu/kidney>. Acesso em 05/05/2019.

UOL, Márcio Padrão em 11/04/2019, Disponível em < https://noticias.uol.com.br/tecnologia/noticias/redacao/2019/04/11/dados-pessoais-de-24-milhoes-de-usuarios-do-sus-sao-vazados-na-internet.htm>. Acessado em 20/05/2019

US FOOD AND DRUG ADMINISTRATION et al. Content of premarket submissions for management of cybersecurity in medical devices: draft guidance for industry and food and drug administration staff. Retrieved May, v. 1, p. 2014, 2013.

WALKER, Glenn M. et al. A Framework for Bioelectronics: Discovery and Innovation. National Institute of Standards and Technology, 2009.

WARWICK, Kevin et al. The application of implant technology for cybernetic systems. Archives of neurology, v. 60, n. 10, p. 1369-1373, 2003.

FORBES, 2015 - Seth Wahle, used his hand implant to launch exploits on Google Android phones - <https://www.forbes.com/sites/thomasbrewster/2015/04/27/implant-android-attack/#7a72fee01d23> Acessado em 12/11/2018

SERRUYA, Ariel. The Extent of Biohacking and Its Security Implications, 2017.

Lei Nº. 9.677, DE 2 DE JULHO DE 1998. Disponível <http://www.planalto.gov.br/ccivil_03/Leis/L9677.htm> Acessado em 28/05/2019.

Lei Nº. 9695/1998 Disponível em <http://www.planalto.gov.br/ccivil_03/leis/L9695.htm> Acessado em 28/05/2019.

Normativa n. 2830 Anvisa – Responsável pelo uso e operação do equipamento médico

Lei Nº. 13.709/2018. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm> Acessado em 28/05/2019.

Lei Nº 12.965/2014. Disponível em < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acessado em 28/05/2019.

Lei Nº. 8078/1990. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm> Acessado em 28/05/2019.

ABNT NBR ISO/IEC 27002, 31/08/2005.