UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE ENGENHARIA ELÉTRICA
GRADUAÇÃO EM ENGENHARIA BIOMÉDICA

Adriano Reis da Silva Júnior

Cibersegurança em Dispositivos Médicos: Estudo da ABNT IEC/TR60601-4-5 de Junho de 2022

Uberlândia
Junho 2023

Adriano Reis da Silva Júnior

Cibersegurança em Dispositivos Médicos: Estudo da ABNT IEC/TR60601-4-5 de Junho de 2022

Trabalho apresentado como requisito parcial de avaliação na disciplina Trabalho de Conclusão de Curso de Engenharia Biomédica da Universidade Federal de Uberlândia.

Orientador: Adriano Alves Pereira

Assinatura do Orientador

Uberlândia
Junho 2023

Dedico este trabalho aos meus pais, pelo estímulo, carinho e compreensão.

Agradecimentos

Primeiramente agradeço a Deus por toda ajuda durante o semestre e toda minha vida.
À minha família e à minha noiva, pelo apoio e paciência durante todos esses anos da graduação.
À minha avó, por ter me acompanhado na cidade de Uberlândia durante toda minha graduação.
Ao professor Adriano, pela orientação na elaboração desse trabalho.

Resumo

A *internet* conectou pessoas e disponibilizou o acesso a diversos conteúdos, de textos a vídeos, podendo ser utilizada como ferramenta de trabalho e com fácil acesso através dos *smartphones*. Entretanto, ela também pode oferecer perigos aos seus utilizadores, tornando-os expostos para ataques cibernéticos, ameaças, golpes e outros crimes digitais. Dispositivos médicos também se conectaram e, da mesma forma, estão expostos aos ataques existentes na *internet*, sendo necessário buscar informações sobre os requisitos e recomendações de cibersegurança para dispositivos médicos. Dessa forma, o presente trabalho busca realizar um estudo para compreender as recomendações de segurança da informação para dispositivos médicos presentes na norma ABNT IEC/TR60601-4-5, de junho de 2022. Este trabalho buscou explorar as práticas definidas apenas na norma ABNT IEC/TR 60601-4-5, de junho de 2022, por ser uma norma brasileira e que trata especificamente da segurança cibernética em dispositivos médicos, diferentes de outras normas cujos contextos são diferentes dos existentes nesses dispositivos. A norma estudada visa oferecer os requisitos necessários para atingir níveis adequados de cibersegurança em dispositivos médicos, mostrando que um modelo mais simplificado de Confidencialidade, Integridade e Disponibilidade não pode ser utilizado no contexto de dispositivos médicos devido a toda complexidade existente. Outros conceitos importantes também são definidos por essa norma, como o de contramedidas e *firecalls*, para garantirem que os dispositivos executem sua função essencial mesmo sob eventos de segurança. Por fim, percebe-se que dispositivos médicos possuem uma alta especificidade, onde normas mais genéricas de cibersegurança podem não atender a esses requisitos corretamente, mostrando a importância de normas específicas e exclusivas para dispositivos médicos.

Palavras Chave: Segurança da informação, Cibersegurança, Dispositivos médicos.

Abstract

The internet has connected people and provided access to various contents, from texts to videos, and can be used as a work tool and with easy access through smartphones. However, it also brought dangers to its users, making them exposed to cyber attacks, threats, scams and other digital crimes. Medical devices have also become connected and, likewise, are also exposed to existing attacks on the internet, so it is necessary to seek information on cybersecurity requirements and recommendations for medical devices. Thus, the present academic work seeks to understand the information security recommendations for medical devices present in the ABNT IEC/TR60601-4-5 standard of June 2022. This academic work sought to explore the practices defined only in the ABNT IEC/TR 60601-4-5 June 2022 standard, as it is a Brazilian standard and specifically deals with cybersecurity in medical devices, unlike other standards whose contexts are very different from those existing on these devices. The standard studied aims to provide the necessary requirements to achieve adequate levels of cybersecurity in medical devices, showing that a more simplified model of Confidentiality, Integrity and Availability cannot be used in the context of medical devices, due to all the existing complexity. Several important concepts are also defined by this standard, such as countermeasures and firecalls, to ensure that the devices perform their essential function even under security events. Finally, it is clear that medical devices have a very high specificity, where more generic cybersecurity standards may not meet these requirements correctly, showing how essential the standards specifically for medical devices are.

Keywords: Information security, Cybersecurity, Medical devices.

Lista de ilustrações

Lista de quadros

Lista de abreviaturas e siglas

ARPA	Advanced Research Projects Agency
CA	Certificate Authority
CD	Confidencialidade dos Dados
CIA	Controle de Identificação
CID	Confidencialidade, Integridade e Disponibilidade
CU	Controle de Uso
DDoS	Distributed Denial of Service
DR	Disponibilidade de Recurso
DoS	Denial of Service
FRD	Fluxo Restrito de Dados
HTML	Hypertext Markup Language
IDS	Intrusion Detection System
IP	Internet Protocol
IS	Integridade do Sistema
IoMT	Internet of Medical Things
MAC	Message Autentication Code
NIST	National Institute of Standards and Technology
NS-A	Nível de Segurança Alvo
NS-C	Nível de Segurança de Capacidade
NS-O	Nível de Segurança Obtido
NS	Nível de Segurança
ROE	Reação Oportuna de Eventos
TCP	Transmission Control Protocol
TI	Tecnologia da Informação
WWW	World Wide Web

Sumário

1 Introdução

A *internet*, atualmente, é utilizada por diversas pessoas em todo o planeta, disponibilizando acesso a uma vasta gama de conteúdos, de textos a mídias digitais, como imagens, vídeos e músicas, e até mesmo oferecendo serviços, possibilitando à humanidade acessar informações com as pontas dos dedos, por meio dos *smartphones* (GRALLA, 1998; COMER, 2018). Além de entretenimento e informação, ela é utilizada como uma ferramenta de trabalho, necessária para a realização da função de muitos profissionais, bem como a realização de reuniões de forma remota (CENDON, 2000; COMER, 2018).

A *internet* é formada por uma rede de computadores espalhados pelo mundo, estes estão interligados e se comunicam através de alguns protocolos específicos, como o *Transmission Control Protocol* (TCP), e o *Internet Protocol* (IP) (CENDON, 2000; GRALLA, 1998; COMER, 2018). A fim de garantir que o conteúdo e os serviços encontrados nessa rede permaneçam disponíveis no caso de uma falha no caminho da conexão entre dois dispositivos, existem vários caminhos alternativos que permitem a transmissão da informação desejada até o ponto que a solicitou (CENDON, 2000).

As origens do que é atualmente conhecido como *internet* se dá no contexto da Guerra Fria, na década de 1960, onde o Departamento de Defesa dos Estados Unidos e a Administração dos Projetos de Pesquisas Avançada (ARPA, sigla em inglês) começaram a experimentar uma rede de computadores como uma forma de comunicação para que, em casos de ataques nucleares, a mesma não fosse destruída, conceito idealizado previamente por Paul Baran, cujo trabalho foi de extrema importância para tratar a respeito dos detalhes de como essa nova rede funcionaria. Essa rede de computadores recebeu o nome de ARPANET (CENDON, 2000; ABREU, 2009; ROSA, 2012).

A ideia de Baran se baseava em uma rede redundante (que permite o acesso a um nó por diversos caminhos diferentes), que, em caso de perda da conexão com algum dos computadores (ou nós, estações de comunicação), existiria outra rota pela qual a conexão poderia ser estabelecida (CENDON, 2000; ROSA, 2012). Outro ponto importante era a decentralização dessa rede, que garantiria a redundância desejada, pois, em uma rede centralizada, a destruição do nó central traria o fim das comunicações entre todos os computadores (BARAN, 1962; CENDON, 2000).

Apesar da rede descentralizada já trazer benefícios, caso uma certa quantidade de nós fossem destruídos, a comunicação também seria interrompida. Uma forma de evitar isso é pela utilização das redes distribuídas, que traria uma redundância maior ao sistema e as conexões são distribuídas o máximo possível, assegurando que a conexão fosse preservada (BARAN, 1962; ABREU, 2009).

Desde seu início, a *internet* foi pensada, planejada e estruturada de forma interdisciplinar, tendo sido possível sua criação devido à tais esforços. Após a ARPANET, outras

redes de computadores começaram a surgir, sendo necessário conectá-las, permitindo, então, que qualquer computador pudesse ser ligado à rede (ROSA, 2012; COMER, 2018).

Isso se tornou possível graças ao estabelecimento de protocolos, como o TCP, que permitia os computadores se comunicarem por pacotes, isto é, quebra-se a informação em pedaços, enviando-os para o destino (COMER, 2018; ROSA, 2012; ABREU, 2009). Com o passar do tempo, diversas empresas criaram os seus protocolos de comunicação, buscando se tornarem o padrão utilizado, porém, por conta das vantagens sobre outros protocolos e da vasta diversidade de redes, o TCP se sobressaiu e tornou-se o padrão (ROSA, 2012).

Em 1975 a *internet* já contava com quase 2000 usuários e possibilitava que pesquisadores a utilizassem para compartilhar informações. Com a popularização da *internet*, o correio eletrônico começou a ser utilizado por várias comunidades, com sistemas diferentes, porém interligados, e empresas começaram a oferecer serviços por meio dessa rede, permitindo que ela se tornasse uma forma de negócio, como no caso dos provedores de *internet* (ABREU, 2009; LEINER et al., 2009).

Até então, o uso da *internet* era limitado, porém, após o surgimento da *World Wide Web* (WWW), em 1989, se tornou possível a criação de servidores que fornecessem informações como texto, imagens e outros tipos de mídia, utilizando hipertexto, no formato HTML, possibilitando formatar textos e inserir mídias e *hiperlinks* entre documentos e páginas. Com a WWW, o crescimento da *internet* acelerou, tanto que, 7 anos depois, já existiam mais de 50 milhões de usuários em todo o mundo (ROCHA; FILHO, 2016; GOETHALS; AGUIAR; ALMEIDA, 2000).

A *internet* se popularizou rapidamente e cada vez mais pessoas passaram a utilizá-la, com propagandas e diversos outros serviços sendo oferecidos por ela. Não só serviços, mas a *internet* passou a ser utilizada na educação, possibilitando a disseminação de conteúdo e novas formas de aprender. Outro produto resultante da *internet* foram as redes sociais, as quais permitem que os usuários troquem mensagens e compartilhem conteúdos sobre assuntos de seus gostos, sendo mais pessoais. Entretanto, também existem redes sociais que são de uso profissional, permitindo compartilhar suas experiências de trabalho (ROCHA; FILHO, 2016; ABREU, 2009; GOETHALS; AGUIAR; ALMEIDA, 2000).

Em 2016, mais de 90% dos brasileiros já estavam conectados à *internet*, acessando redes sociais e conteúdos, como o Facebook e até mesmo o YouTube, possuindo acessos tanto de computadores, quanto de dispositivos móveis, como celulares (ROCHA; FILHO, 2016).

A *internet* permitiu que todos os seus utilizadores conseguissem se comunicar e entrar em contato com mais facilidade. Contudo, não apenas coisas boas vêm desse novo meio, existem diversos perigos aos quais todos os usuários da *internet* estão expostos diariamente (SCREMIN; WANZINACK, 2017; JOSÉ; BARBAS, 2020).

Com essa exposição pública, facilidade para criação de grupos, comunidades e dis-

cussões, todos estão expostos a perigos como ataques cibernéticos, roubo de dados e de identidade, por exemplo. Não obstante, a *internet* facilita o compartilhamento de fotos pessoais, sejam sozinhos, com família e amigos, ou até mesmo fotos íntimas, onde existe o risco de que essas fotos sejam compartilhadas sem permissão (SCREMIN; WANZINACK, 2017; JOSÉ; BARBAS, 2020).

É possível também que predadores digitais criem perfis em redes sociais ou aplicativos de relacionamento com histórias, fotos e nomes falsos para enganar as pessoas e as levarem a compartilhar informações, dinheiro, ou até mesmo fotos íntimas. Pessoas de todas as idades podem ser vítimas desses predadores, inclusive crianças e jovens, os quais, caso tenham fotos íntimas compartilhadas indesejadamente, podem sofrer danos psicológicos, podendo levá-los até mesmo a tirarem sua própria vida (SCREMIN; WANZINACK, 2017; JOSÉ; BARBAS, 2020).

Nessa lista de perigos digitais também encontram-se os grupos e *sites* com conteúdos violentos e de disseminação de ódio ou conteúdo racista, que podem estimular ações violentas contra pessoas, grupos ou etnias (JOSÉ; BARBAS, 2020).

O advento da tecnologia trouxe também o que é conhecido como Internet das Coisas (IoT, do termo em inglês), onde o avanço dos sistemas embarcados e das redes de computadores permitem que objetos comuns do cotidiano possam se conectar à *internet* e, assim, realizar novas funções(SANTOS et al., 2016).

Esses objetos que agora recebem a capacidade de se conectar com a *internet*, normalmente fazem uma combinação de sensores e dados coletados para realizar o processamento dessas informações na *internet* e, por essa competência, recebem o nome "objetos inteligentes"(SANTOS et al., 2016; POPPER, 2018).

Entre as áreas de aplicação das tecnologias IoT está a área da saúde, onde já existem relógios capazes de medir desempenho físico, havendo a possibilidade do surgimento de vestimentas e acessórios com sensores capazes de medir dados relacionados à saúde (POPPER, 2018; MASSOLA; PINTO, 2018).

A coleta de dados de saúde como pressão arterial, temperatura corporal, batimentos cardíacos, entre outros, podem ser utilizados para auxílio de diagnóstico médicos, pois seriam enviados para aplicativos e analisados por profissionais da área da saúde (POPPER, 2018; MASSOLA; PINTO, 2018).

Atualmente, já existem exemplos dessa tecnologia sendo utilizada em prol da saúde, como a utilização de pulseira para realizar acompanhamento de recém-nascidos, alertando enfermeiros sobre informações importantes como alterações na oxigenação ou na frequência cardíaca (MASSOLA; PINTO, 2018).

Contudo, toda essa conectividade apresenta riscos relacionados a cibersegurança, como a abertura para *hackers* explorarem vulnerabilidades e controlar esses dispositivos, ou até mesmo sequestrarem os dados neles contidos; por serem dispositivos conectados, eles podem servir como porta para invasões em outros sistemas na mesma rede. Além do

mais, existem muitas informações pessoais e sensíveis transmitidas por esses dispositivos, o que pode causar danos a indivíduos, inclusive podendo ameaçar suas vidas, como em casos de próteses ou bombas de insulina, por exemplo (MASSOLA; PINTO, 2018).

Diante desse cenário, conhecendo a importância deste tema e possuindo um grande interesse na área, este trabalho busca tratar sobre a segurança da informação nos dispositivos médicos tratados em normas, especificamente na ABNT IEC/TR60601-4-5 de junho de 2022.

1.1 Objetivo Geral

O objetivo deste trabalho é realizar um estudo sobre os requisitos e recomendações para atingir níveis adequados de cibersegurança em dispositivos médicos, utilizando como base as informações contidas na norma ABNT IEC/TR60601-4-5, de junho de 2022.

1.2 Objetivos Específicos

O presente trabalho possui os seguintes objetivos específicos:

- Compreender a norma ABNT NBR IEC TR 60601-4-5.
- Discorrer sobre a segurança da informação em dispositivos médicos.
- Entender os requisitos para caminhar rumo à cibersegurança dos dispositivos médicos.

1.3 Justificativa

A *internet* cresceu de tal forma que se tornou algo comum do cotidiano. Cada vez mais dispositivos se tornam conectados, oferecendo compartilhamento e processamento de dados pela *internet*. Devido à popularização desses dispositivos inteligentes, diversos setores passaram a utilizar equipamentos que se comunicam através de uma rede de computadores, abrindo espaço para a existência de vulnerabilidades expostas ao público e, consequentemente, podendo se tornar alvos por usuários maliciosos.

Esse cenário também se tornou realidade para os dispositivos médicos, como, por exemplo, equipamentos de imagens que se comunicam diretamente com servidores para o armazenamento de exames de pacientes, dispositivos de monitoramento que auxiliam no tratamento e identificação de problemas, relógios inteligentes capazes de monitorar a frequência cardíaca e nível de oxigenação do sangue, entre outros. Todos esses dispositivos utilizam protocolos de comunicação que podem apresentar vulnerabilidades.

Ataques a sistemas de informação são recorrentes, e, muitas vezes, causam grandes danos às entidades alvo. Quando os alvos são hospitais ou dispositivos médicos, dados

sensíveis de pacientes estão sob ameaça. Informações sobre tratamentos, doenças, alergias e dados pessoais podem ser perigosos se obtidos por pessoas maliciosas, podendo se tornar um risco à vida, principalmente pessoas publicamente expostas, como políticos, por exemplo.

O roubo de informações sensíveis não é o único risco nesse cenário, devido à possibilidade de dispositivos inteligentes serem utilizados como ferramentas de auxílio de tratamentos, estes também podem possuir vulnerabilidades que permitiriam aos atacantes modificarem dados ou injetarem comandos para atrapalhar o funcionamento normal do aparelho. É possível imaginar cenários onde uma bomba de insulina é invadida, fazendo com que uma dose letal seja aplicada ao paciente, ou então um marcapasso que possui vulnerabilidades que o fazem parar de funcionar.

1.4 Motivação

Conhecendo os riscos provenientes de dispositivos conectados, percebe-se a importância da cibersegurança nesses cenários. Considerando ainda que dispositivos médicos se tornaram conectados, é possível notar a relevância desse tema, já que esses dispositivos estão expostos aos mesmos perigos que os demais, porém, os dispositivos médicos tratam de dados mais sensíveis e existe a possibilidade de danos à vida. Surgindo a necessidade de uma pesquisa para entender e discorrer sobre a cibersegurança em dispositivos médicos.

2 Fundamentação Teórica

Com as redes de computadores e os diferentes tipos de informação transmitidas por elas, o que normalmente ficava no mundo físico, foi transferido para um mundo virtual. A esse mundo virtual costuma-se dar o nome ciberespaço. O termo "ciberespaço"foi popularizado por conta das obras do escritor William Gibson, especificamente em sua obra conhecida como *Neuromancer* (MONTEIRO; PICKLER, 2007).

Na obra de Gibson, o ciberespaço é uma forma de materializar e abstrair dados e informações. Contudo, na atualidade esse termo é utilizado para representar o sistema de comunicação entre computadores e bancos de dados, isto é, as redes de computadores de uma sociedade onde as informações são disponibilizadas (MONTEIRO; PICKLER, 2007).

2.1 Ataques na Internet

A *internet* e o ciberespaço abriram portas para ataques a outros dispositivos, como os ataques de negação de serviço (DoS), onde um usuário malicioso faz uso de um computador ou dispositivo conectado à rede para realizar várias solicitações a outro dispositivo ou servidor para sobrecarregá-lo e torná-lo indisponível aos outros dispositivos e usuários da rede. A forma mais básica de realizar esse ataque é enviando uma solicitação para o endereço de transmissão (*broadcast*) da rede colocando o IP da vítima no pacote emitido, assim, os demais computadores da rede enviariam uma resposta para o dispositivo da vítima (DOMINGOS, 2018).

Uma evolução desse tipo de ataque é o ataque de negação de serviço distribuído (DDoS), cuja premissa é similar ao DoS, porém utilizam-se vários dispositivos conectados para enviar as solicitações a um único alvo. Essa rede de dispositivos que realizam o ataque normalmente são máquinas que foram infectadas, permitindo que um *hacker* ordene os ataques em todas essas máquinas zumbis. Nos anos 2000, um grupo de *hackers* invadiu redes de universidades norte-americanas e utilizou os dispositivos presentes nelas para atacar vários *sites*, afetando economicamente seus alvos (CORTEZ; KUBOTA, 2013; DOMINGOS, 2018).

Vírus, de forma geral, são programas maliciosos, também conhecidos como *malwares*, criados para causar danos a dispositivos ou para roubar dados contidos nos mesmos. Eles são instalados contra a vontade do usuário quando um programa infectado é executado. Podem existir diversas categorias de vírus, algumas delas serão citadas a seguir (OLIVEIRA, 2013; DOMINGOS, 2018). É possível encontrar algumas categorias de vírus com uma breve descrição sobre eles no Quadro 1.

Um desses vírus são os chamados *worms*, que possuem a habilidade de se espalharem pelo computador e por outros dispositivos que estejam na rede. Outra característica

Quadro 1 – Categorias de vírus e descrições

Categoria de Vírus	**Descrição**
Vírus de arquivos	Utilizam os arquivos do sistema operacional para se propagar.
Vírus de setor de *boot*	Se localizam nos setores de inicialização do sistema operacional, impedindo que o mesmo inicialize.
Vírus de *e-mail*	Recebidos e propagados por correio eletrônico, normalmente induzem o usuário a executar um arquivo para infectar o computador e se espalhar para os contatos da vítima
Vírus de *script*	Possuem esse nome por serem feitos em linguagem de *script*. Normalmente são recebidos por páginas da *internet* ou *e-mail*, podendo até serem executados de forma automática.
Vírus de macro	Utilizam linguagens de macro para infectar os arquivos das aplicações que possuem essas linguagens, como o Excel ou PowerPoint, por exemplo.
Vírus de celular	Podem se espalhar por meio do *bluetooth* ou por mensagens. O dispositivo é infectado quando o usuário executa um arquivo malicioso. Esse vírus consegue controlar o celular e até mesmo exportar a agenda telefônica da vítima.

Fonte: Elaborado pelo autor com base em Oliveira (2013) e Domingos (2018).

desse tipo de *malware* é que eles consomem muitos recursos do computador, prejudicando o desempenho do dispositivo (DOMINGOS, 2018; SERAZZI; ZANERO, 2003; AYCOCK, 2006).

Outro tipo de vírus são os *spywares*, com finalidade de monitorar todas as atividades de um dispositivo, porém, nem sempre eles são maliciosos, pois podem ser instalados pelo dono do dispositivo. Existem categorias de *spywares*, como *keyloggers*, que monitoram as teclas digitadas, e *screenloggers*, que capturam informações do mouse, como posição e cliques (DOMINGOS, 2018; AYCOCK, 2006; ERBSCHLOE, 2004).

Existem também os *trojans*, que permitem que usuários maliciosos consigam acessar os computadores infectados. Os *trojans* são capazes de instalar outros programas maliciosos no computador da vítima, permitem que o atacante acesse de forma remota o alvo ou que o dispositivo alvo seja utilizado para realizar ataques de negação de serviço, podem apagar arquivos, controlar a navegação do usuário e até mesmo utilizar *spywares* para monitorar a vítima (DOMINGOS, 2018; AYCOCK, 2006; ERBSCHLOE, 2004).

Os ataques do tipo *phishing* tem por objetivo o roubo de informações. Nesses ataques, são utilizados *sites* e *e-mails* falsos para enganar as vítimas, obtendo seus dados pessoais ou financeiros por meio das de técnicas de engenharia social. Normalmente, os golpistas se passam por entidades conhecidas, tais como bancos, por exemplo (BASTOS; NEVES et al., 2021; DOMINGOS, 2018).

Outro tipo de vírus e ataque comum é o de *ransomware*, que é o sequestro com extorsão dos dados de um computador. Em muitos cenários, os atacantes infectam os computadores das vítimas, sequestram os dados presentes no computador e depois criptografam

o dispositivo da vítima, solicitando um pagamento por parte da vítima para liberarem os arquivos. Outra vertente desse ataque é bloquear o acesso ao dispositivo, também cobrando um pagamento da vítima para liberar o acesso. Mesmo pagando, nada garante que os atacantes realmente vão liberar o acesso aos dados ou ao dispositivo, nem que o *ransomware* será removido do computador (BASTOS; NEVES et al., 2021; LISKA; GALLO, 2019).

2.2 Técnicas de Cibersegurança

A *internet* ajudou o crescimento econômico e se tornou um recurso para a sociedade, disponibilizando novas oportunidades e sendo a infraestrutura crítica para muitos serviços. Logo, esses ataques descritos promovem perigo à esses serviços, pois os atacantes podem utilizar as vulnerabilidades existentes no ciberespaço para prejudicar os sistemas de informação (NUNES, 2012).

A fim de amenizar e até mesmo impedir que essas ameaças consigam avançar, foi criado o conceito de cibersegurança, isto é, a segurança do ciberespaço. O objetivo da cibersegurança é controlar o acesso às informações de forma que pessoas não autorizadas não consigam obter acesso a esses dados. Além disso, ela busca encontrar formas de verificar mensagens, bem como garantir sua autenticidade, para que se possa ter certeza com quem se está falando ou quem enviou uma determinada mensagem (TELES, 2015).

A segurança da informação possui três conceitos básicos: a confidencialidade, a integridade e a disponibilidade. A Confidencialidade está relacionada com a permissão do acesso à informação, sendo restrito apenas aos usuários que possuam autorização. A integridade está relacionada com a completude da informação, isto é, garantir que a informação não foi modificada. A disponibilidade, por sua vez, está relacionada com a disponibilidade da informação, ou seja, é garantir que a informação esteja sempre disponível para os usuários permitidos (DOMINGOS, 2018; SANTOS, 2014; MONTEIRO; GIORDANO; POSSAMAI, 2019).

Existem outras duas propriedades relacionadas com a autoria de mensagens e informações: a Autenticação e o Não Repúdio. Autenticação é a capacidade de atestar que uma informação ou usuário são legítimos, enquanto o Não Repúdio é a garantia que o sistema possui que determinada pessoa executou uma ação ou enviou uma mensagem. Essas propriedades permitem a validação de informações, contudo, vale ressaltar que, para que se tenha o Não Repúdio, é necessário que exista a Autenticidade e Integridade das informações (DOMINGOS, 2018; MONTEIRO; GIORDANO; POSSAMAI, 2019).

Entre as tecnologias e técnicas utilizadas para garantir a segurança do ciberespaço está o *hashing*. Uma *hash*, de forma simplificada, é uma função cujo objetivo é resumir um conjunto de dados. Uma propriedade que torna essa função interessante é a unidirecionalidade, que indica que o processo é de via única, ou seja, uma entrada produzirá uma

saída, porém dessa saída, não se pode voltar à entrada original (TELES, 2015; ADÃO; SILVEIRA; SILVEIRA, 2017; JESUS; ALVES; AMÉRICO, 2018; SENDIN, 1999).

Devido a essa propriedade, pode-se utilizar esses algoritmos para verificar a integridade dos dados, pois, caso estejam corrompidos ou alterados, produzirão uma *hash* diferente. Também é comum utilizar *hashs* para validar que uma mensagem foi realmente gerada por uma parte conhecida, chamados de códigos de autenticação de mensagens (MAC). Para a obtenção dos MACs, necessita-se de uma chave secreta compartilhada entre duas partes, a qual é utilizada em uma *hash* em conjunto com a mensagem a ser transmitida, que efetivamente é o MAC. Esse MAC gerado é enviado com a mensagem, assim a outra parte pode ler a mensagem e recalcular o MAC com a chave secreta que ela também possui e comparar com o MAC recebido para validação (TELES, 2015; SENDIN, 1999).

Exemplificado: Alice e Bob compartilham uma chave k. Alice deseja enviar uma mensagem m para Bob. Alice gera uma *hash* da junção da chave e da mensagem, produzindo MAC_A. Alice envia $m + \text{MAC}_A$ para Bob. Bob computa uma *hash* da junção da mensagem recebida (m) com a sua chave secreta (k), produzindo MAC_B. Se MAC computado por Bob for igual ao MAC recebido, ele pode ter certeza que a mensagem está íntegra e que o remetente realmente foi Alice (TELES, 2015; SENDIN, 1999).

Outra aplicação das *hashs* é para auxiliar o controle de acesso. Por serem unidirecionais, pode-se armazenar apenas a *hash* da senha de um usuário, calculando novamente a *hash* da senha em todo o login, e comparando com o valor de *hash* armazenado no banco de dados, impedindo que sua senha fique salva de forma que todos consigam ler, tornando esse armazenamento mais seguro (SENDIN, 1999).

Outra ferramenta são as cifras, conhecidas por criptografia, que permitem tornar dados confidenciais. As cifras são funções que utilizam chaves para cifrar uma determinada mensagem, impedindo a leitura do conteúdo criptografado a menos que se possua a chave para decifrar a mensagem. Os modelos de criptografias podem ser simétricos, ou assimétricos. Nos modelos simétricos, utiliza-se uma mesma chave para trocar uma mensagem cifrada entre duas partes, isto é, a mesma chave utilizada para cifrar, é a que se utiliza para decifrar. Já, na criptografia assimétrica, utilizam-se chaves diferentes, uma pública, que pode ser compartilhada com todos, e uma privada, que deve pertencer apenas ao dono da chave (TELES, 2015; OLIVEIRA, 2012).

Por meio das chaves públicas e privadas, pode-se utilizar um sistema de assinatura digital, onde a chave privada de uma pessoa é usada para cifrar uma *hash* de uma mensagem, podendo ser descriptografada por qualquer pessoa por meio da chave pública do autor da mensagem. Assim, é possível comprovar quem realmente escreveu aquela mensagem, provendo integridade (por conta da *hash* que se alteraria caso a mensagem fosse modificada), autenticidade e não repúdio, isto é, não poder negar quem é o autor da mensagem. Contudo, vale lembrar que a utilização dessa sistemática para assinaturas digitais não garantirá que a mensagem seja confidencial, permitirá apenas verificar sua

autenticidade (OLIVEIRA, 2012; TELES, 2015).

Para a utilização de assinaturas digitais e criptografias de chave pública e privada, é necessário distribuir as chaves públicas de todos os usuários, para facilitar quando quiser se comunicar com alguém. Contudo, existe a possibilidade de um usuário malicioso querer se passar por outra pessoa, podendo se aproveitar disso para iniciar ataques. Para evitar esse tipo de problema, existem os certificados digitais, que contém informações individuais em conjunto com a chave pública daquela pessoa, e esse certificado é assinado por uma autoridade de certificação (CA), podendo ser validado com a chave pública dessa autoridade (OLIVEIRA, 2012; NOBRE et al., 2007)

Para garantir uma maior segurança, existe ainda uma cadeia de autenticação. Os certificados são emitidos pelas autoridades certificadoras, que, por sua vez, precisam estar abaixo de outra autoridade certificadora que seja superior a ela. Da mesma forma, essa autoridade superior está abaixo de outra autoridade, seguindo assim até a autoridade raiz, formando uma cadeia de autoridades (NOBRE et al., 2007).

Mesmo utilizando todas essas técnicas citadas anteriormente, ainda é importante cuidar do tráfego dos dados que circulam pela rede. Para isso, existem algumas ferramentas, como, por exemplo, o *Firewall*, colocado entre a rede de uma empresa e a *internet*. O *Firewall* ajuda a controlar os pacotes que chegam da *internet* para a rede da empresa e vice e versa. Todos os pacotes passarão por ele, logo é possível adicionar regras de segurança, bloqueando ou permitindo a entrada de pacotes específicos, funcionando como um filtro de pacotes na rede (TELES, 2015).

Outra ferramenta que pode ser utilizada como complemento ao *Firewall* são os Sistemas de Detecção de Intrusão (IDS), que também monitoram os pacotes, porém, possuem a capacidade de alertar os administradores de rede caso seja detectada alguma violação nas regras de segurança estabelecidas. Normalmente, essas ferramentas possibilitam configurar alertas para ataques ou ações específicas, como, por exemplo, alertar caso exista algum usuário escaneando portas abertas na rede. A principal diferença entre o IDS e um *Firewall* é que um IDS possui uma memória acerca dos pacotes, isto é, existe um histórico. O *Firewall* consegue bloquear ou permitir um determinado pacote, enquanto o IDS consegue identificar que muitos pacotes semelhantes, ou suspeitos, estão vindo de um determinado dispositivo (TELES, 2015)

2.3 Ataques em Dispositivos Médicos

Apesar da existência dessas técnicas e ferramentas, é necessário melhorá-las, mantê-las atualizadas, e, em alguns casos, fazer adaptações, pois não são apenas os computadores que estão vulneráveis a ataques, mas outros dispositivos conectados à *internet* também podem ser alvos, como dispositivos inteligentes e câmeras de segurança. Há histórico de *hackers* infectarem esses dispositivos e provocarem ataques por meio deles. Um exem-

plo disso foi o ataque conhecido como Mirai, que em 2016 infectou vários dispositivos inteligentes, se espalhando como um *worm* pela rede. Com vários dispositivos infectados, criou-se uma rede zumbi com 100 mil dispositivos, os quais foram utilizados para realização de ataques de negação de serviço distribuído (CLOUDFLARE, 20-; GREENE, 2016; BUXTON, 2022).

Por esse fato, dispositivos médicos conectados à *internet* ou a rede de um hospital também estão em risco de ataques. Em 2017, um ataque de *ransomware* conhecido como *Wanna Cry* comprometeu a rede de equipamentos radiológicos de diversos hospitais, provocando reagendamentos dos exames já marcados (NEWS, 2022)

Ataques do tipo *ransomware* se tornaram mais frequentes em hospitais e instituições de saúde, mostrando que uma parte considerável dos dispositivos médicos são vulneráveis. Muitos desses ataques ocorreram no ano de 2021 e, segundo o levantamento divulgado no relatório "State of Healthcare IoT Device Security Report"de 2022, os casos de *ransomware* em instituições de saúde aumentaram consideravelmente. Esse estudo também reportou que as bombas de infusão eram os equipamentos que mais apresentavam riscos, onde cerca de 73% delas possuíam vulnerabilidades conhecidas (NEWS, 2022; BUSINESS, 2022).

Outro exemplo de vulnerabilidade existente em dispositivos médicos pode ser encontrado em redes corporais sem fio, conhecidas como WBAN, as quais são uma rede de sensores (vestíveis ou implantados) que possuem comunicação sem fio, e monitoram sinais de forma contínua. Nessas aplicações, a integridade e autenticação são de difícil implementação devido às limitações presentes nos sensores utilizados (DARWISH; HASSANIEN, 2011).

Cenários onde os dados transmitidos são sensíveis necessitam da garantia de uma boa segurança, sendo necessário desenvolver métodos de criptografias mais eficientes e que consumam menos energia. A autenticação também é de extrema importância, pois pode acontecer de os pacientes estarem inconscientes, então não conseguirão digitar suas senhas. Para isso, existem estudos que buscam utilizar sinais fisiológicos únicos como formas de autenticação (DARWISH; HASSANIEN, 2011).

Em dispositivos implantáveis existe uma dificuldade muito grande na autenticação e garantia da confidencialidade dos dados, principalmente por limitações de consumo de energia, onde sistemas criptográficos mais seguros podem consumir mais. Ataques de falsa identidade, alteração de mensagem, escuta de mensagem, drenagem de bateria, bloqueio de sinal e ataques internos são os mais comuns nos dispositivos médicos implantáveis (STRYDIS et al., 2013; GOLDSCHMIDT et al., 2019).

O ataque de falsa identidade se dá quando um usuário malicioso se passa por um implante ou como um leitor de implante, reenviando mensagens já transmitidas ou alterando a ordem dos pacotes enviados, podendo atrapalhar os tratamentos (STRYDIS et al., 2013).

A alteração de mensagem, como o próprio nome diz, é a modificação do conteúdo das mensagens enviadas e recebidas pelo implante. O risco desses ataques é a possibilidade de se injetar um código malicioso que pode prejudicar o implante. Por outro lado, a escuta de mensagens permite um usuário malicioso ler o conteúdo que está sendo enviado/recebido pelo implante, correndo o risco de expor dados sensíveis do paciente (STRYDIS et al., 2013).

Os ataques de drenagem de bateria são categorias de ataques de negação de serviço, que tornam o implante indisponível, forçando que a bateria se drene até que acabe. Podem acontecer por meio da repetição de determinadas ações, como envio de mensagens de autenticação, que exige que o implante valide as mensagens, e, consequentemente, gaste mais bateria (STRYDIS et al., 2013).

No bloqueio de sinal, o atacante envia diversas mensagens de forma repetida, impedindo que o implante consiga se comunicar. Por último, os ataques internos são aqueles onde um usuário autorizado, isto é, que possua acesso ao implante, modifique dados do implante a fim de esconder evidências (STRYDIS et al., 2013).

Os ataques a dispositivos médicos são perigosos pois podem provocar atrasos em hospitais, ou até impossibilitar que um tratamento ocorra, colocando em risco os pacientes. Deixar de atualizar dispositivos e *software* antigos com vulnerabilidades, permitir o acesso não autorizado à rede, utilização de senhas fracas, configurações de redes que não sigam boas práticas são exemplos de riscos que estabelecimentos de saúde estão expostos (MEURER, 2018).

Não oferecer atualizações de segurança, não utilizar protocolos de criptografia, métodos de autenticação insuficientes, utilizar interfaces inseguras, deixar portas abertas para modificações no *software* de dispositivos médicos e a exposição de dados de pacientes são riscos que devem ser tratados pelos fabricantes de dispositivos médicos (MEURER, 2018).

Para se proteger de alguns desses ataques, pode-se utilizar as ferramentas citadas previamente. Um exemplo do uso de um desses métodos de segurança citados, aplicados em cenários de dispositivos médicos, se dá em imagens de telerradiografia, fazendo o uso de certificados digitais para disponibilizar acesso às imagens dos pacientes por meio da *internet* de forma segura e autêntica, podendo incluir laudos, assinados de forma digital, garantindo que seus dados são íntegros e que foram enviados pelo remetente esperado (NOBRE et al., 2007).

2.4 A Cibersegurança

A cibersegurança pode ser vista como a aplicação de técnicas para proteger informações que trafegam nas redes. Os dispositivos médicos, por possuírem *hardware* e *software*, também estão sujeitos às boas práticas existentes na segurança da informação, buscando prevenir possíveis ataques e riscos que possam surgir. É necessário entender as carac-

terísticas de cada dispositivo, bem como a possibilidade de existirem vulnerabilidades em alguns recursos presentes no uso do dispositivo (BRAZ; PONTES; SOUZA, 2019)

Apesar disso, garantir a segurança de alguns dispositivos é algo desafiador, por não possuírem todos os recursos, já que, em muitos cenários, esses dispositivos se apresentam como dispositivos de baixo custo. Falhas de segurança em ambientes hospitalares podem acarretar vazamentos de informações de pacientes, comprometendo o sigilo, sendo necessário a utilização de técnicas de criptografias e a determinação de níveis de permissões para limitar o acesso à certas informações (CIPRIANO, 2021)

Por possuir uma estrutura muitas vezes desatualizada, a área da saúde se torna um alvo para ataques. Equipamentos mais modernos se tornam mais conectados, porém, a preocupação com a cibersegurança ainda deixa a desejar. As diversas inovações, como a Internet das Coisas Médicas (IoMT), que buscam conectar dispositivos médicos com a *internet*, os registros eletrônicos de pacientes e atendimentos pela *internet* abrem as portas para novos ataques (DIAS et al., 2021).

Existem muitas vantagens em utilizar a tecnologia dessa forma, como, por exemplo, permitir o monitoramento de pacientes em tempo real, ou transmitir os dados deles por meio da *internet* para um médico. Outro exemplo é a telemedicina, que permitiu a realização de consultas e diagnósticos de forma *online*. Contudo, mesmo com essas vantagens, por possuírem vulnerabilidades, toda essa conectividade pode colocar em risco os pacientes, sendo necessário estabelecer e seguir padrões de cibersegurança (DIAS et al., 2021).

3 Metodologia

O presente trabalho tem características de uma pesquisa exploratória, cujo objetivo é esclarecer os conceitos relacionados com o tema do mesmo, neste caso, sobre as normas e legislações em vigência a respeito da segurança cibernética em dispositivos médicos (GIL, 2008).

Esse tema foi escolhido por conta da abundante quantidade de dispositivos médicos que possuem conexão com a *internet*, e principalmente pela importância da segurança dos dados que esses dispositivos operam, podendo conter informações sensíveis dos pacientes.

Existem diversas normas com o tema de cibersegurança, como a série ISO 27000 e série NIST SP 800, que tratam a respeito da segurança da informação. Outras normas de gerenciamento de risco também poderiam ser utilizadas para tratar do tema de segurança cibernética em dispositivos médicos, sem contar recomendações de autoridades regulatórias. Já normas diretamente relacionadas à segurança cibernética de dispositivos médicos, as opções são mais limitadas, como, por exemplo, a norma ABNT IEC TR 60601-4-5 e a IEC 80001-5-1, podendo ser complementadas seguindo as demais recomendações da série 60601 da ABNT.

Ainda para complementar, poderiam ser utilizadas normas que tratem o gerenciamento de risco, e gerenciamento de risco em redes de TI que possuam dispositivos médicos, como a IEC TR 80001-2-x.

Outro exemplo de norma que poderia abranger os dispositivos médicos, é a Estrutura em Segurança Cibernética e Publicações Especiais do NIST (National Institute of Standards and Technology), que tem como alvo redes de TI que sejam críticos para segurança cibernética nacional. Porém, como o objetivo deste trabalho é tratar sobre a cibersegurança especificamente em dispositivos médicos, será considerado tema desse estudo, apenas a norma ABNT IEC TR 60601-4-5, deixando como sugestão uma análise mais profunda de como essas outras normas citadas possam, ou não, ser utilizadas no domínio dos dispositivos médicos.

Portanto, como referência às práticas que devem ser seguidas, será utilizada a norma ABNT IEC/TR 60601-4-5, de junho de 2022, cujo título é "Equipamento eletromédico - Parte 4-5: Orientações e interpretação - Especificações técnicas de cibersegurança relacionada à segurança". Para fins desse trabalho, serão considerados apenas os cenários descritos que envolvam os dispositivos médicos, bem como seus *softwares*.

As especificações de segurança cibernética relacionadas à rede da tecnologia da informação (TI) médica, e que não tratem a respeito de dispositivos médicos, salvo se o funcionamento do dispositivo depender dessa especificação da rede de TI, estão fora do tema principal de estudo.

Na seção A.7 da ABNT IEC 60601-4-5 existem algumas partes de outras normas

utilizadas para a elaboração do documento em questão. Nessa parte do documento, foi possível ter um breve contato com essas demais normas. Portanto, esses trechos, que estavam diretamente relacionados a dispositivos médicos, também foram utilizados para a elaboração deste trabalho.

4 Resultados e Discussões

4.1 Objetivos da Norma

O objetivo da norma ABNT NBR IEC TR 60601-4-5 é oferecer alguns requisitos para que ensaios de cibersegurança possam ser realizados de forma que os níveis de segurança garantam um certo nível de resistência em situações de ataques nos dispositivos médicos. Seu papel não é definir níveis de segurança específicos, pois isso depende de uma análise e gerenciamento de risco, que cabe ao fabricante realizar e descrever, bem como declarar o nível de segurança do dispositivo e suas limitações (ABNT, 2022).

Essa norma também pode ser utilizada para ensaios de tipo, isto é, aqueles que utilizam um equipamento para representar vários outros, por conta do grande estresse e esforço pelo quais os equipamentos passam, que pode reduzir sua vida útil. O objetivo desse ensaio é mostrar que todos os equipamentos desse mesmo tipo obedecerão às mesmas especificações que normalmente não são identificadas em ensaios de rotina (PORTO, 2009; BOLOTINHA, 2015).

Porém, quando a norma ABNT NBR IEC TR 60601-4-5 for utilizada nessas situações, a pessoa responsável por realizar os testes apenas verificará o que foi relatado pelo fabricante. Deve-se ressaltar que esses ensaios não avaliam se, no ambiente de uso pretendido, o nível de segurança de capacidade é o adequado, isso será responsabilidade do gerenciamento de risco, analisando os impactos sobre a segurança, as exposições às ameaças, verificando o quão significativas são as vulnerabilidades, os valores dos ativos, e, dessa forma, é possível avaliar as contramedidas definidas para cada nível de segurança (ABNT, 2022).

4.2 Modelos de Segurança da Informação

Segundo a subseção 5.2 da IEC TS 62443-1-1, de julho de 2009, citada na norma ABNT NBR IEC TR 60601-4-5, a segurança da informação visa a Confidencialidade, Integridade e Disponibilidade (modelo CID). Em algumas estratégias, a confidencialidade é priorizada, deixando a disponibilidade com a menor das prioridades. Em outros cenários, como em situações de sistemas industriais de controle e automação, essa ordem é invertida, sendo a disponibilidade a maior prioridade e a confidencialidade a última, já que os dados sozinhos não são tão sensíveis, visto que só funcionam dentro daquele contexto. Assim, o contexto e as condições do sistema a ser estruturado podem alterar a ordem das prioridades CID (ABNT, 2022; IEC/TS, 2009).

Todavia, o modelo simples de CID não é o suficiente para entender completamente

os requisitos de cibersegurança, para isso, a subseção 5.3 da IEC TS 62443-1-1 lista 7 requisitos importantes a serem seguidos: Controle de Identificação e Autenticação (CIA); Controle de Uso (CU); Integridade do Sistema (IS); Confidencialidade dos Dados (CD); Fluxo Restrito de Dados (FRD); Reação Oportuna de Eventos (ROE); e Disponibilidade de Recurso (DR) (ABNT, 2022; IEC/TS, 2009).

O Controle de Identificação e Autenticação (CIA) gerencia o acesso a dispositivos ou informações específicas, evitando que pessoas não autorizadas obtenham esse acesso. De forma similar, o Controle de Uso (CU) serve para impedir o uso não autorizado a um dispositivo ou informação (ABNT, 2022; IEC/TS, 2009).

A Integridade do Sistema (IS) assegura a completude da informação, a fim de evitar alterações não autorizadas. A confidencialidade dos Dados (CD) é o requisito que busca proteger contra o vazamento de informações, por exemplo, garantindo que a mesma é confidencial (ABNT, 2022; IEC/TS, 2009).

O Fluxo Restrito de Dados (FRD) é o requisito que limita o curso dos dados e da informação pelos meios de comunicação, evitando que os mesmos sejam publicados em fontes não autorizadas. A Reação Oportuna de Eventos (ROE) está relacionada com a ação de notificar as autoridades sobre violações de cibersegurança, mostrando evidências e as ações para a correção após os eventos. Por fim, a Disponibilidade de Recurso (DR) é o que assegura que todos os recursos de rede estarão disponíveis a fim de evitar ataques do tipo de negação de serviço (ABNT, 2022; IEC/TS, 2009).

4.3 Público Alvo da Norma

O primeiro passo a ser dado a respeito da norma ABNT NBR IEC TR 60601-4-5 é a definição do seu público alvo, que, segundo ela mesma, são os fabricantes de dispositivos médicos e a equipe responsável por integrar esses dispositivos a uma rede de TI médica, visando dar orientações a respeito da cibersegurança desses dispositivos (ABNT, 2022).

Logo de início, a norma já determina algumas responsabilidades que convém aos fabricantes. Contudo, antes de falar sobre essas responsabilidades, é necessário definir alguns termos que são muito utilizados no decorrer da norma e que serão importantes para o melhor entendimento deste trabalho (ABNT, 2022).

4.4 Conceitos Importantes

Um dos conceitos importantes é a função essencial de um dispositivo médico, representando um conjunto básico de funcionalidades que permitam o uso e disponibilidade clínica do equipamento. É ela que permite o dispositivo de cumprir com o mínimo de sua função clínica, estando sempre disponível para ser utilizado, com o desempenho mínimo

necessário e com uma segurança básica, isto é, sem falhar no seu papel e que ainda possa ser considerado seguro (ABNT, 2022).

A função essencial de um dispositivo médico dependerá de uma análise comparando os riscos e os benefícios, verificando quais funcionalidades devem sempre estar acessíveis, e quais podem ser bloqueadas em determinadas situações (ABNT, 2022).

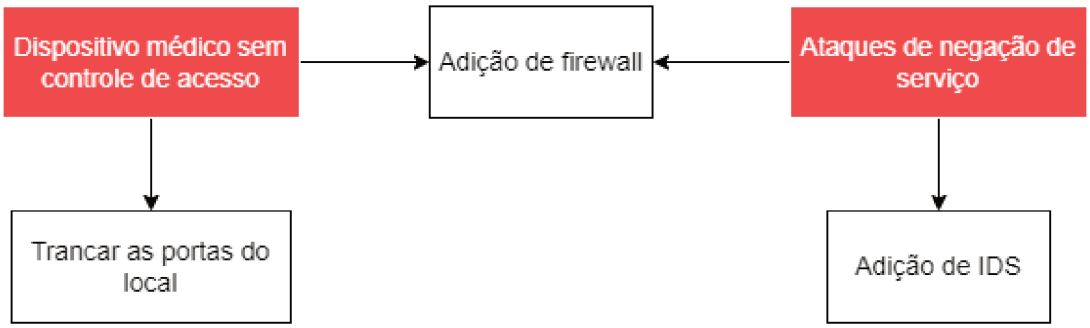
Eventos ou incidentes de segurança são situações adversas que colocam em risco a segurança da rede ou o dispositivo, tornando-os vulneráveis, ou que violem as políticas de segurança estabelecidas. São os casos de ataques diretos ao dispositivo, à rede médica à qual ele está conectado, ou a algum serviço/servidor com o qual esse dispositivo se comunica, bem como tentativas de acesso não autorizado (DURBANO, 2019; ABNT, 2022; SOUZA, 2022).

Outro termo importante é o termo *Firecall*, que representa uma função de emergência para o dispositivo. Em caso de um evento de segurança, onde o dispositivo médico está comprometido, a fim de garantir que a função essencial dele se cumpra, é necessário que existam funções para acesso emergencial (ABNT, 2022).

As contramedidas são medidas de cibersegurança estabelecidas, tanto para dispositivos médicos, quanto para a rede de tecnologia da informação (TI), para controlar e amenizar os riscos e vulnerabilidades de cibersegurança, cujo objetivo é diminuir os danos que podem surgir em uma situação de ataque ou falha. Elas podem ser classificadas em técnicas, como no caso do uso de um *software* para proteção contra vírus; administrativas, como procedimentos ou políticas internas; e físicas, como o trancar de uma porta ou bloqueio ao acesso direto às placas de circuito impresso de um dispositivo (ABNT, 2022).

Alguns exemplos de contramedidas podem ser encontrados nas Figuras 1, 2 e 3, onde, nos blocos em vermelho, estão os exemplos de ataques, que se conectam por meio de setas aos blocos em branco, que representam as contramedidas que podem ser adotadas nesses cenários. Exemplos para dispositivos que estejam conectados a uma rede de internet e estão sujeitos a ataques, como ataques de DoS e DDoS, e vulnerabilidades, como não possuírem acesso por credenciais, podem ser encontrados na Figura 1.

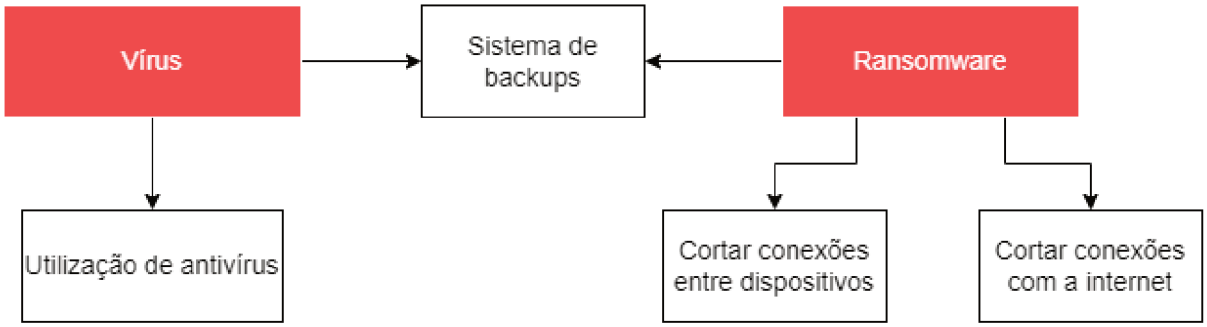
Figura 1 – Exemplos de contramedidas para alguns ataques para dispositivos conectados à rede



Fonto: Elaborada pelo autor, 2023

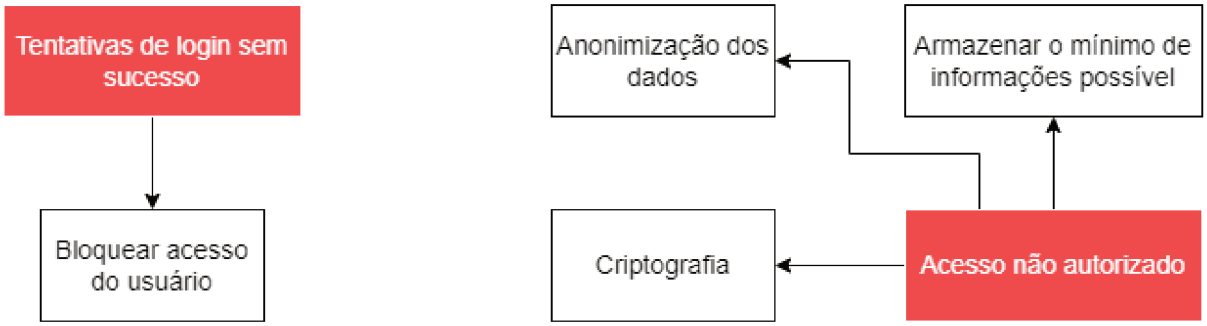
Na Figura 2, encontram-se exemplos de contramedidas que podem ser tomadas para ataques que estejam relacionados com vírus. Enquanto isso, na Figura 3, estão exemplos de contramedidas para ataques que estejam relacionados com a tentativa de obter acesso às informações confidenciais do dispositivo.

Figura 2 – Exemplos de contramedidas para alguns ataques relacionados com vírus



Fonto: Elaborada pelo autor, 2023

Figura 3 – Exemplos de contramedidas para alguns ataques relacionados com o acesso às informações



Fonto: Elaborada pelo autor, 2023

O documento também faz o uso de três níveis de segurança diferentes, conforme a IEC 62443-3-3, de agosto de 2013, o Nível de Segurança Alvo, Nível de Segurança de Capacidade e Nível de Segurança Obtido. O Nível de Segurança Alvo (NS-A) é o nível de segurança desejado, determinado pelo nível de risco e a segurança necessária para que tudo funcione corretamente; Nível de Segurança de Capacidade (NS-C) é o nível de segurança que pode ser oferecido pelo dispositivo médico, mediante uma configuração correta. Indica que o dispositivo consegue, ou não, atender os requisitos do nível de segurança alvo. Por fim, o Nível de Segurança Obtido (NS-O) é o nível de segurança real para a rede de TI médica. É utilizado para determinar se um sistema de cibersegurança satisfaz os objetivos definidos (ABNT, 2022).

Os níveis de segurança auxiliam a tomada de decisões e a utilização de contramedidas, pois serve para abordar de forma qualitativa a cibersegurança para um determinado dispositivo. Por ser qualitativo, seu intuito é poder facilitar a comparação e permitir um

melhor gerenciamento da cibersegurança. Cabe a cada organização definir cada nível de segurança e determinar a forma de medi-lo de forma consistente para toda organização. O nível de segurança representa a eficácia necessária pelas contramedidas, bem como pelas propriedades de segurança cibernética do dispositivo, podendo ser utilizado na identificação de estratégias para a defesa contra eventos de segurança (ABNT, 2022; IEC/TS, 2009).

Os níveis de segurança são divididos em quatro níveis, e suas definições são dadas pela IEC 62443-3-3, de agosto de 2013, sendo as seguintes: O NS 1 visa impedir que informação chegue nas mãos de pessoas não autorizadas, por meio de espionagem ou por exposição casual. O NS 2 busca impedir o acesso não autorizado à informação por entidades que as estejam procurando através de formas simples, com poucos recursos, habilidades e motivações. O NS 3 procura impossibilitar o acesso não autorizado às entidades que buscam informações com um nível moderado de recursos, habilidades e motivação. Enquanto no NS 4, essa entidade que busca essas informações de forma ativa possui um alto nível de recursos, habilidades e de motivação (ABNT, 2022; IEC/TS, 2013).

O nível de segurança alvo e o nível de segurança de capacidade são definidos pelos fabricantes. Para a declaração do nível de segurança de capacidade, deve-se basear no nível de segurança alvo especificado, considerando o ambiente que o mesmo será utilizado. Após a equipe responsável pela instalação e integração do dispositivo com a rede de TI médica ter finalizado essa incorporação do equipamento, pode-se gerenciar o nível de segurança obtido, e, assim, estabelecer as devidas contramedidas necessárias. Para dispositivos médicos utilizados fora de ambientes profissionais de saúde, utilizar um nível de segurança de capacidade consoante ao nível de segurança alvo é o que se considera apropriado (ABNT, 2022).

O nível de segurança obtido diminui conforme o tempo por conta da degradação das contramedidas e pelo surgimento de novas vulnerabilidades, porém, as mesmas podem ser revisadas em uma atualização do dispositivo. O importante é garantir que o nível de segurança obtido seja sempre maior ou igual ao nível de segurança alvo determinado (ABNT, 2022).

A norma ABNT NBR IEC TR 60601-4-5, em sua subseção 4.6.3, fornece alguns exemplos de seleção do nível de segurança alvo, contando também com uma tabela de exemplo mostrando critérios que podem ser utilizados na hora de definir o nível de segurança alvo, como, por exemplo, as consequências da perda de segurança, se existem dados de pacientes, se permite o acesso a outros ativos, qual o tipo de usuário que utiliza esse dispositivo, qual o ambiente que ele é utilizado, entre outros (ABNT, 2022).

Com base nos níveis de segurança determinados pode-se definir os requisitos de segurança do dispositivo. Na ABNT NBR IEC TR 60601-4-5 também é possível encontrar uma tabela que relaciona os requisitos de cibersegurança com os requisitos fundamentais,

quando se considera um determinado nível de segurança de capacidade. Como, por exemplo, a identificação/autenticação de usuário humano, deve ser feita em todos os 4 níveis de segurança, porém, a identificação/autenticação única são requisitos apenas nos níveis 2, 3 e 4; e a autenticação de vários fatores para todas as interfaces é requisito apenas nos níveis 3 e 4 (ABNT, 2022).

O ideal seria que fosse escolhido apenas um nível de segurança de capacidade para um determinado dispositivo médico, e assim o dispositivo seguiria todos os requisitos necessários do nível correspondente, porém, podem existir cenários onde isso não é necessariamente adequado. Para isso, é possível atribuir níveis de segurança de capacidade para cada requisito fundamental e utilizar a notação de vetor de nível de segurança, estabelecida na norma IEC 62443-3-3, de agosto de 2013, em sua seção A.3.3. Nesse vetor de nível de segurança serão mapeados os 7 requisitos fundamentais da IEC TS 62443-1-1, citados anteriormente, onde os valores desse vetor representarão o nível de segurança de capacidade, de 0 a 4, para cada um desses requisitos fundamentais (ABNT, 2022; IEC/TS, 2013).

4.5 Responsabilidades e Cuidados

Estabelecidos esses termos principais, pode-se dar início às responsabilidades estabelecidas na ABNT IEC TR 60601-4-5. Aos fabricantes, caberá determinarem a segurança básica, desempenho e função essencial que garantam a disponibilidade em situações de ameaças ou ataques, bem como funções para acesso de emergência (*Firecall*) e seus gerenciamentos segundo as prioridades dos eventos de segurança, e um nível de segurança alvo mínimo que seja adequado para todos os ambientes onde pretende-se utilizar o dispositivo. Tanto as entidades responsáveis pela rede quanto os fabricantes compartilham a responsabilidade sobre o gerenciamento de risco (ABNT, 2022).

Ademais, como documentos complementares, os fabricantes de dispositivos médicos deverão entregar às entidades responsáveis por toda parte legal e moral da utilização e/ou manutenção do dispositivo eletromédico, descrições técnicas que contenham os seguintes itens (ABNT, 2022):

- os grupos que receberão as informações relacionadas à cibersegurança, e seus níveis de permissão no dispositivo;
- uma demonstração clara de como utilizar o dispositivo de forma segura, bem como informações necessárias para poderem discutir com os seus pacientes a respeito dos riscos da cibersegurança;
- diagramas de sistema com detalhes suficientes sobre segurança cibernética;

- uma lista com materiais de cibersegurança que permitam os grupos-alvo gerenciarem os dispositivos e entenderem os riscos envolvidos;
- os requisitos mínimos (como *hardware* e *software*) dos dispositivos que podem ser utilizados em conjunto com o principal;
- a lista e descrição dos recursos de cibersegurança, as quais protegem a função essencial do dispositivo;
- informar como a blindagem pode ser alcançada e como conseguir níveis de segurança diferentes de forma configurável;
- lista de ameaças;
- informações dos riscos de utilizar o dispositivo fora do ambiente pretendido;
- a lista de contramedidas existentes para cada ameaça listada;
- recomendações de configurações que garantam um uso seguro;
- avisos para desativarem quaisquer aplicações ou portas que não sejam utilizadas;
- informações de como utilizar mecanismos padrões de TI para garantir a segurança;
- documentação das interfaces, locais de acesso, componentes que podem ser conectados, dados que são transmitidos ou recebidos, protocolos utilizado, bem como as portas de redes, suas funções e descrição, a forma que os dados são tratados e o caminho que fazem;
- explicação de como o dispositivo indicará que ocorreu uma anomalia/evento de segurança;
- detalhamento de como reagir em eventos de segurança;
- descrição da função essencial do dispositivo durante um evento de segurança, incluindo o que o operador deverá fazer;
- explicação de qual forma as evidências forenses são coletadas, arquivos de registro e sua localização, e como o mesmo pode ser utilizado para uma análise
- instruções para criação de *backup* e restauração dos mesmos (com a devida autenticação do usuário);
- descrições para garantir que uma manutenção remota atrapalhe o uso do dispositivo
- detalhamentos sobre o fim do suporte à cibersegurança, quando estes são conhecidos

Um requisito importante das contramedidas é que todas devem garantir que os dispositivos médicos possam continuar operando com o seu desempenho essencial e funcionamento mínimo. Como, por exemplo, um dispositivo que, para ser utilizado, possua um sistema de controle de acesso por meio de credenciais e que faça o uso da *internet* está sendo atacado e, como contramedida, resolvam cortar a conexão com a *internet*, o que impediria o uso do dispositivo. De mesmo modo, um ataque de negação de serviços não deve impedir que o dispositivo seja utilizado em sua função mínima (ABNT, 2022).

Outro ponto relevante são sobre os ativos, ou seja, objetos, sejam físicos ou lógicos, que possuam um valor real ou percebido para o dispositivo médico ou à rede de TI médica, como componentes, equipamentos, ou informações. Conforme o nível de risco e ameaça aos quais os dispositivos estão submetidos, os dispositivos médicos devem conseguir proteger esses ativos que sejam críticos através do *hardware*, seguindo especificações de cibersegurança já aceitas e comprovadas e baseadas em outras normas, como o uso de travas ou *tokens* de segurança (ABNT, 2022).

Existem cuidados, em relação à cibersegurança, que devem ser tomados quando se projeta um dispositivo médico, aspectos importantes como protocolos de comunicação, bem como a segurança dos dados dos pacientes, por exemplo. Para a segurança das comunicações entre um dispositivo médico e meios externos, convém que se faça o uso de chaves únicas e individuais para a comunicação de cada dispositivo com métodos criptográficos seguros, assim, conhecer a chave de um dispositivo não quebra a comunicação de outros dispositivos, por usarem chaves diferentes (ABNT, 2022).

Em relação às informações de pacientes, os dispositivos médicos precisam passar por manutenções, para isso, os dados de pacientes não podem ser expostos, logo os dispositivos precisam conseguir remover quaisquer informações que identifiquem pacientes por um usuário não autorizado. Essa função de anonimizar os dados deve ser executada antes do dispositivo ser enviado para manutenção, ou antes que seja descartado para evitar vazamento de informações (ABNT, 2022).

Não somente isso, mas, quando se trata de um dispositivo médico, atender apenas aos requisitos de uma segurança básica e que garantam o desempenho essencial, não é o suficiente para todos os casos. Logo, caberá ao fabricante tomar algumas medidas. Por exemplo, em caso de um ataque, é necessário que existam contramedidas apropriadas para garantir que o equipamento continue oferecendo um certo nível de cuidados médicos, ou seja, deve-se manter certa funcionalidade clínica. Desse modo, percebe-se a importância da função essencial, que foi definida para garantir o uso do dispositivo médico em situações como a acima, pois a funcionalidade clínica e disponibilidade mínimas são essenciais para garantir a continuidade da prestação de serviços de cuidado à saúde mesmo durante ataques. Além disso, corrigir problemas de cibersegurança, seja no *hardware*, seja no *software*, pode levar bastante tempo, sem contar o tempo para a validação, logo, a função essencial do dispositivo precisa garantir o funcionamento do mesmo durante esse intervalo

de tempo (ABNT, 2022).

Deve-se tomar cuidado em relação a quais funções estarão presentes para garantir o suporte da função essencial, pois uma funcionalidade específica pode implicar, em casos de um ataque, a perda da disponibilidade ou confidencialidade do dispositivo, sendo necessário fazer uma análise de risco-benefício, incluindo onde armazenar as informações, se existirão *Firecalls* que possam ser executadas para garantir a funcionalidade clínica, se cada ação de emergência será devidamente registrada de alguma forma, entre outros aspectos a serem analisados (ABNT, 2022).

Para exemplificar um cenário onde a análise de risco-benefício não foi eficiente, pode-se imaginar uma rede de TI médica que foi infectada por um *ransomware*, o qual se espalhará para os demais dispositivos da rede criptografando todo conteúdo armazenado neles. Utilizar como contramedida o encerramento de todas as conexões da rede pode ser extremamente problemático caso exista algum dispositivo que utilize um sistema de autenticação que dependa de uma conexão com a rede, o que tornaria o dispositivo inutilizável, perdendo sua funcionalidade clínica (ABNT, 2022).

Quanto à confidencialidade dos dados, em geral, existem requisitos diferentes dentro de cada país. A norma estudada indica que seu escopo é restrito apenas às especificações de cibersegurança, porém recomenda a norma IEC 62443-4-2, de fevereiro de 2019, seção 8, como uma base para os aspectos de cibersegurança e para o gerenciamentos dos requisitos de outros tipos de dispositivos (não médicos) que estejam conectados na rede de TI médica (ABNT, 2022).

A criação de uma norma própria para dispositivos médicos facilita a integração dos dispositivos médicos às redes de TI, e garantindo que apresentem segurança e que continuem funcionando conforme o proposto. Para que essa norma fosse elaborada, várias outras normas que tratavam o tema de segurança cibernética foram utilizadas como referências, porém, segundo o que a ABNT IEC/TR 60601-4-5 relata, essas demais normas utilizadas costumam seguir duas metodologias diferentes. Uma delas é se baseando em uma análise de risco, para que se possa encontrar uma forma de controlá-los e amenizá-los, enquanto a outra se inicia com a seleção de um nível de segurança, baseando-se no risco geral, para poder determinar os demais níveis de segurança (ABNT, 2022).

No caso da norma ABNT NBR IEC TR 60601-4-5, por se basear em diversas outras normas, a abordagem escolhida é de seguir uma filosofia híbrida, na qual se baseia na ABNT NBR ISO 14971, de julho de 2020, para determinar o risco e, conforme o nível de risco escolhido, será determinado um nível de segurança em conformidade à série de normas IEC 62443, sendo esse nível de segurança que determinará quantas e quais contramedidas estarão presentes no dispositivo médico (ABNT, 2022).

4.6 Comparações com outros países

A *General Data Protection Regulation* (GDPR), da União Europeia, diz que, quando se coleta informações, é necessário que o sujeito que teve esses dados coletados possa ter acesso a todos os dados coletados, incluindo dados da saúde. A ABNT IEC/TR 60601-4-5 não trata de especificações sobre o acesso às informações por parte do paciente. Outro ponto bastante defendido pela GDPR é a proteção e privacidade dos dados, que também é uma preocupação na ABNT IEC/TR 60601-4-5, já que ela coloca como requisito o uso de chaves únicas e individuais, para cada dispositivo, bem como funções para anonimizar dados (EUROPEAN PARLIAMENT, 2016; ABNT, 2022).

Ainda relacionado com a proteção de dados, a GDPR trata da realização de uma avaliação de impacto de proteção de dados quando essas informações processadas apresentarem um alto risco para os direitos e liberdades das pessoas, isto é, dados sensíveis, como dados de saúde. Para essa avaliação, deve existir um detalhamento do processamento de dados, incluindo a justificativa para esse processamento, quais dados estão envolvidos, quem receberá esses dados. Outro requisito é avaliar os riscos e impactos à privacidade dos indivíduos, bem como possíveis vulnerabilidades ou ameaças. Além disso, é necessário definir as medidas que serão implementadas para amenizar esses riscos. De forma geral, é bem similar com o que é solicitado na ABNT IEC/TR 60601-4-5, a qual requer a determinação de contramedidas e existe essa preocupação com a segurança dos dados (EUROPEAN PARLIAMENT, 2016; ABNT, 2022).

Outra semelhança entre a GDPR e a ABNT IEC/TR 60601-4-5 é que, na GDPR existe a necessidade de notificar as violações de dados pessoais, enquanto na ABNT IEC/TR 60601-4-5 existe a reação oportuna de eventos, que também está relacionada com a notificação em casos de violações das políticas de cibersegurança (EUROPEAN PARLIAMENT, 2016; ABNT, 2022).

O NIST SP 800-53 é um conjunto de diretrizes para segurança cibernética *National Institute of Standards and Technology* (NIST) dos Estados Unidos. Dentre essas diretrizes estão o controle de acesso, relacionado com a autenticação em dois fatores, controle de acesso aos sistemas e política para as senhas. A proteção dos dados, abordando a criptografia tanto para dados em repouso, isto é, que permanecem no dispositivo, quanto para dados em trânsito, isto é, enviados para outros locais, além da separação das funções para impedir um acesso não autorizado. Controle de acesso e políticas para impedir o acesso não autorizado também estão presentes ABNT IEC/TR 60601-4-5, porém o NIST SP 800-53 possui um nível maior de detalhes (NIST, 2022; ABNT, 2022).

O gerenciamento de riscos também é citado em ambas as normas, contudo o NIST SP 800-53 fornece diretrizes para realizar a avaliação dos riscos e também implementar formas de amenizá-los. Algo que está presente no NIST SP 800-53 e não na ABNT IEC/TR 60601-4-5 são as especificações para controles de detecção e respostas a violações da cibersegurança, tratando sobre a identificação e análise de eventos de segurança. Outro ponto

positivo e fundamental que está presente apenas no NIST SP 800-53 é sobre treinamentos e políticas de conscientização sobre a cibersegurança, e papeis e responsabilidades de cada um (NIST, 2022; ABNT, 2022).

Uma semelhança entre a ABNT IEC/TR 60601-4-5 e o NIST SP 800-53 é sobre a continuidade do funcionamento essencial e à recuperação de desastres, onde existe a preocupação em garantir que exista uma forma de continuar utilizando o equipamento mesmo mediante a um evento de segurança (NIST, 2022; ABNT, 2022).

5 Conclusão

A utilização de normas específicas para a cibersegurança em dispositivos médicos é fundamental, pois a maioria das normas presentes sobre cibersegurança, inclusive utilizadas como referência para a norma explorada nesse documento, são desenvolvidas para outros ambientes, como, por exemplo, normas para automação industrial e de sistema de controle, normas de redes e segurança de sistemas em geral, para o gerenciamento de riscos em redes de TI, e normas para dispositivos que se conectem à *internet*.

A utilização de normas que não estejam inseridas no contexto de dispositivos médicos muitas vezes não pode ser aplicada, como o caso das capacidades de cibersegurança definidas na IEC 62443, fortalecendo a importância da existência de normas e documentos voltados para segurança cibernética específica de dispositivos médicos, já que o contexto que eles são aplicados é diferente. Equipamentos médicos possuem peculiaridades a mais, por conta da exposição que apresentam, alto contato com diferentes pessoas, e pelos dados sensíveis que circulam por esses aparelhos e por toda a rede de TI médica no local onde ele é instalado.

Parte dessas especificidades que os dispositivos médicos apresentam é que em unidades de atendimento e cuidados na área saúde, por exemplo, existem restrições de acesso físico aos dispositivos, e os mesmos não podem ter sua operação afetada no caso de um ataque, logo é necessário um conjunto particular de instruções e orientações de como agir nesses cenários ou evitar situações como essas.

Claro que existem partes de normas que podem ser aplicadas para dispositivos médicos, como a parte que abrange os requisitos de cibersegurança na série de normas IEC 62443, todavia, dentro dessa mesma série de normas, para que pudesse ser aproveitado algo, foi necessário que adaptações fossem realizadas.

De forma geral, a preocupação com a segurança e proteção dos dados é algo fundamental para os dispositivos médicos. Percebe-se que alguns princípios também eram tratados em outras normas de forma similar alguns conceitos estabelecidos na ABNT IEC/TR 60601-4-5. Um exemplo é a busca por impedir o acesso não autorizado a informações sensíveis, também tratado na GDPR, outro é a necessidade de dar continuidade ao funcionamento do dispositivo, contido na NIST-SP800-53.

Com isso em mente, maiores pesquisas permitirão explorar, entender e listar as particularidades dos dispositivos médicos e das redes de TI médicas, como a sensibilidade dos dados que podem circular neles e a necessidade de estarem operantes mesmo mediante a uma situação de ataque direto e/ou indireto. Com essas particularidades bem definidas e conceituadas, pode-se então iniciar um processo de diferenciação entre as normas de segurança cibernética já existentes e, assim, avaliar quais demais normas genéricas podem ser utilizadas como complementos dentro dos contextos de dispositivos médicos e se existem

outros requisitos importantes que não foram contemplados na ABNT IEC/TR 60601-4-5.

Referências

ABREU, K. C. K. História e usos da internet. *BOCC–Bliblioteca Online de Ciências da Comunicação*, p. 1–9, 2009.

ADÃO, J. M. R.; SILVEIRA, S. I. da; SILVEIRA, D. R. da. *A função do algoritmo hash md4*. [S.l.]: UNIESP, 2017.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT IEC/TR60601-4-5 DE 06/2022*: Equipamento eletromédico - parte 4-5: Orientações e interpretação - especificações técnicas de cibersegurança relacionada à segurança. Rio de Janeiro, 2022.

AYCOCK, J. *Computer viruses and malware*. [S.l.]: Springer Science & Business Media, 2006. v. 22.

BARAN, P. *On Distributed Communications Networks*. Santa Monica, CA: RAND Corporation, 1962.

BASTOS, N. B. N. de L.; NEVES, L. N. L. M. et al. Ransomware e phishing durante a pandemia covid-19 (coronavírus). *Revista Tecnológica da Fatec Americana*, v. 9, n. 01, p. 68–83, 2021.

BOLOTINHA, M. *TRANSFORMADORES DE POTÊNCIA - ENSAIOS EM FÁBRICA*. 2015. Disponível em: ⟨https://pt.linkedin.com/pulse/transformadores-de-pot\%C3\%AAncia-ensaios-em-f\%C3\%A1brica-manuel-bolotinha⟩.

BRAZ, H. L. A.; PONTES, P. E. A. K.; SOUZA, R. C. R. de. Biohacking e segurança da informação: Vulnerabilidades em dispositivos implantáveis. 2019.

BUSINESS, S. *Mais da metade dos dispositivos hospitalares apresentam falhas de segurança*. 2022. Disponível em: ⟨https://www.saudebusiness.com/ti-e-inovacao/mais-da-metade-dos-dispositivos-hospitalares-apresentam-falhas-de-seguranca⟩.

BUXTON, O. *What Is the Mirai Botnet?* 2022. Disponível em: ⟨https://www.avast.com/c-mirai⟩.

CENDON, B. A internet. In: _____. [S.l.: s.n.], 2000. p. 275–300.

CIPRIANO, W. F. A segurança da informação com o advento da internet das coisas em ambientes hospitalares: uma abordagem bibliográfica. 2021.

CLOUDFLARE. *O que é a botnet Mirai?* 20–. Disponível em: ⟨https://www.cloudflare.com/pt-br/learning/ddos/glossary/mirai-botnet/⟩.

COMER, D. E. *The Internet book: everything you need to know about computer networking and how the Internet works*. [S.l.]: Chapman and Hall/CRC, 2018.

CORTEZ, I. S.; KUBOTA, L. C. Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras. *Revista de Administração*, Elsevier, v. 48, n. 4, p. 757–769, 2013.

DARWISH, A.; HASSANIEN, A. E. Wearable and implantable wireless sensor network solutions for healthcare monitoring. *Sensors*, Molecular Diversity Preservation International (MDPI), v. 11, n. 6, p. 5561–5595, 2011.

DIAS, F. M. et al. Elaboração e avaliação de uma estrutura teórico-prática para a gestão de riscos de cibersegurança para o setor de saúde. Universidade Nove de Julho, 2021.

DOMINGOS, F. d. S. Segurança da informação: vírus ataques e contramedidas. Universidade Federal Fluminense, 2018.

DURBANO, V. *CSIRT: o que são os grupos de Resposta a Incidente de Segurança?* 2019. Disponível em: ⟨https://blog.ecoit.com.br/csirt-o-que-sao-os-grupos-de-resposta-incidente-de-seguranca/⟩.

ERBSCHLOE, M. *Trojans, worms, and spyware: a computer security professional's guide to malicious code*. [S.l.]: Elsevier, 2004.

EUROPEAN PARLIAMENT. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. 2016. Disponível em: ⟨https://eur-lex.europa.eu/eli/reg/2016/679/oj⟩.

GIL, A. C. *Métodos e técnicas de pesquisa social*. São Paulo: Atlas, 2008. ISBN 9788522451425.

GOETHALS, K.; AGUIAR, A.; ALMEIDA, E. História da internet. *Faculdade de Engenharia da Universidade do Porto, Mestrado em Gestão da Informação*, 2000.

GOLDSCHMIDT, G. et al. Segurança da informação na comunicação de dispositivos médicos: uma revisão quasi-sistemática. *Journal of Health Informatics*, v. 11, n. 2, 2019.

GRALLA, P. *How the Internet works*. [S.l.]: Que Publishing, 1998.

GREENE, T. *DDoS attack takes down Krebs site*. 2016. Disponível em: ⟨https://www.csoonline.com/article/3123785/largest-ddos-attack-ever-delivered-by-botnet-of-hijacked-iot-devices.html⟩.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. *IEC/TS 62443-1-1 DE 2009*: Industrial communication networks – network and system security – part 1-1: Terminology, concepts and models. [S.l.], 2009.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. *IEC 62443-3-3 DE 2013*: Industrial communication networks - network and system security - part 3-3: System security requirements and security levels. [S.l.], 2013.

JESUS, W. S. C. D.; ALVES, G. R. T.; AMÉRICO, P. A. Autenticação de certificados emitidos em eventos usando algoritmo message-digest algorithm 5. 2018.

JOSÉ, M. R. V.; BARBAS, M. P. Estudo sobre os perigos da internet: O fenómeno do catfishing em contexto de produção multimédia em educação. *Revista da UI_IPSantarém-Unidade de Investigação do Instituto Politécnico de Santarém*, v. 8, n. 2, p. 47–56, 2020.

LEINER, B. M. et al. A brief history of the internet. *SIGCOMM Comput. Commun. Rev.*, Association for Computing Machinery, New York, NY, USA, v. 39, n. 5, p. 22–31, oct 2009. ISSN 0146-4833. Disponível em: ⟨https://doi.org/10.1145/1629607.1629613⟩.

LISKA, A.; GALLO, T. *Ransomware: defendendo-se da extorsão digital*. [S.l.]: Novatec Editora, 2019.

MASSOLA, S. C.; PINTO, G. S. O uso da internet das coisas (iot) a favor da saúde. *Revista Interface Tecnológica*, v. 15, n. 2, p. 124–137, 2018.

MEURER, M. Uso do iot na saúde e segurança da informação. *Gestão da Segurança da Informação-Unisul Virtual*, 2018.

MONTEIRO, G. T.; GIORDANO, L. A.; POSSAMAI, V. A. O uso da inteligência artificial na segurança das criptomoedas. *PROJETOS E RELATÓRIOS DE ESTÁGIOS*, v. 1, n. 1, 2019.

MONTEIRO, S. D.; PICKLER, M. E. V. O ciberespaço: o termo, a definição e o conceito. *DataGramaZero-Revista de Ciência da Informação*, v. 8, n. 3, p. 1–21, 2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Security and Privacy Controls for Federal Information Systems and Organizations*. [S.l.], 2022. Disponível em: ⟨https://doi.org/10.6028/NIST.SP.800-53r5⟩.

NEWS, T. H. *Are Medical Devices at Risk of Ransomware Attacks?* 2022. Disponível em: ⟨https://thehackernews.com/2022/01/are-medical-devices-at-risk-of.html⟩.

NOBRE, L. F. et al. Certificação digital de exames em telerradiologia: um alerta necessário. *Radiologia Brasileira*, SciELO Brasil, v. 40, p. 415–421, 2007.

NUNES, P. F. V. A definição de uma estratégia nacional de cibersegurança. *Nação e defesa*, Instituto da Defesa Nacional, 2012.

OLIVEIRA, F. B. de. Malware, o vírus que oculta arquivos: como recuperar arquivos afetados por esse vírus de computador. *Múltiplos Olhares em Ciência da Informação*, v. 3, n. 2, 2013.

OLIVEIRA, R. R. Criptografia simétrica e assimétrica-os principais algoritmos de cifragem. *Segurança Digital [Revista online]*, v. 31, p. 11–15, 2012.

POPPER, M. A. Internet das coisas: potencialidades e perigos. *Gestão da Segurança da Informação-Unisul Virtual*, 2018.

PORTO, B. P. d. S. Disjuntores de potência: uma breve introdução à teoria e ensaios básicos em laboratório. Universidade Federal de Campina Grande, 2009.

ROCHA, G. d.; FILHO, V. B. S. Da guerra às emoções: história da internet e o controverso surgimento do facebook. *Encontro Regional Norte de História da Mídia*, v. 4, 2016.

ROSA, A. M. As origens históricas da internet: uma comparação com a origem dos meios clássicos de comunicação ponto a ponto. 2012.

SANTOS, B. P. et al. Internet das coisas: da teoria à prática. 2016.

SANTOS, E. P. dos. Segurança da informação: Como garantir a integridade, a confidencialidade e a disponibilidade das informações em uma organização educacional privada de teresina/information security: How to ensure integrity, confidentiality and availability of the infor. *Revista FSA (Centro Universitário Santo Agostinho)*, v. 7, n. 1, 2014.

SCREMIN, S. de F.; WANZINACK, C. Sexting: Perigos na internet, um estudo de caso com uma amostragem de acadêmicos/as da universidade federal do paraná. *Razón y palabra*, Universidad de los Hemisferios, v. 21, n. 97, p. 746–761, 2017.

SENDIN, I. da S. Funções de hashing criptográficas. 1999.

SERAZZI, G.; ZANERO, S. Computer virus propagation models. In: SPRINGER. *International workshop on modeling, analysis, and simulation of computer and telecommunication systems*. [S.l.], 2003. p. 26–50.

SOUZA, T. *Evento vs. Incidente: Desmistificando os conceitos - Auditoria de TI, Segurança Cibernética, Riscos e Controles*. 2022. Disponível em: ⟨https://tiagosouza.com/evento-incidente-seguranca-cibernetica-o-que-e-conceitos/⟩.

STRYDIS, C. et al. A system architecture, processor, and communication protocol for secure implants. *ACM Transactions on Architecture and Code Optimization (TACO)*, ACM New York, NY, USA, v. 10, n. 4, p. 1–23, 2013.

TELES, T. M. F. P. d. S. *Cibersegurança - Deteção de outliers*. Tese (Mestrado em Ciências Militares Navais) — Escola Naval Talant De Bien Faire, 2015.