Princípios e práticas de cibersegurança em dispositivos médicos

Guia nº 38/2020 – versão 1

ANVISA

Agência Nacional de Vigilância Sanitária - Anvisa

2020

Princípios e práticas de cibersegurança em dispositivos médicos

VIGENTE A PARTIR DE 24/09/2020

Início do período de contribuições: 25/09/2020
Fim do período de contribuições: 23/03/2021

Este Guia expressa o entendimento da Anvisa sobre as melhores práticas com relação a procedimentos, rotinas e métodos considerados adequados ao cumprimento de requisitos técnicos ou administrativos exigidos pelos marcos legislativo e regulatório da Agência.[1]

Trata-se de instrumento regulatório não normativo, de caráter recomendatório e não vinculante, sendo, portanto, possível o uso de abordagens alternativas às proposições aqui dispostas, desde que compatíveis com os requisitos relacionados ao caso concreto. A inobservância ao conteúdo deste documento não caracteriza infração sanitária, nem constitui motivo para indeferimento de petições, desde que atendidos os requisitos exigidos pela legislação.

As recomendações contidas neste Guia produzem efeitos a partir da data de sua publicação no Portal da Anvisa ficam sujeitas ao recebimento de sugestões da sociedade por meio de formulário eletrônico, disponível em https://pesquisa.anvisa.gov.br/index.php/56883?lang=pt-BR.

As contribuições[2] recebidas serão avaliadas e poderão subsidiar a revisão do Guia e a consequente publicação de uma nova versão do documento. Independentemente da decisão da área, será publicada análise geral das contribuições e racional que justifique a revisão ou não do Guia.

[1] Portaria nº 1.741, de 12 de dezembro de 2018, que dispõe sobre as diretrizes e os procedimentos para melhoria da qualidade regulatória na Agência Nacional de Vigilância Sanitária (Anvisa).

[2] A fim de garantir maior transparência ao processo de elaboração dos instrumentos regulatórios editados pela Anvisa, esclarecemos que os nomes dos responsáveis pelas contribuições (pessoas físicas e jurídicas) são considerados informações públicas e serão disponibilizados de forma irrestrita nos relatórios e outros documentos gerados a partir dos resultados deste Guia. Já o e-mail e o CPF dos participantes, considerados informações sigilosas, terão seu acesso restrito aos agentes públicos legalmente autorizados e às pessoas a que se referem tais informações, conforme preconiza o artigo 31, §1º, inciso I da Lei nº 12.527, de 18 de novembro de 2011. Outras informações que venham a ser consideradas sigilosas pelos participantes poderão ser apensadas em campo específico no formulário eletrônico.

SUMÁRIO

1. ESCOPO

Este guia faz parte do processo de internalização do IMDRF/CYBER WG/N60 – *Principles and Practices for Medical Device Cybersecurity*, elaborado pelo Fórum Internacional de Reguladores em Dispositivos Médicos (IMDRF, do inglês *International Medical Device Regulators Forum*) para fornecer recomendações sobre os princípios gerais e as boas práticas de cibersegurança em dispositivos médicos, inclusive dispositivos médicos para diagnóstico *in vitro*, para todos os intervenientes.

O texto apresenta recomendações para fabricantes de dispositivos médicos, serviços de saúde, Anvisa e usuários para minimizar riscos de cibersegurança que podem surgir com o uso do dispositivo para o uso pretendido; e para garantir a manutenção e continuidade da segurança do paciente e desempenho do dispositivo. Este documento considera cibersegurança no contexto de dispositivos médicos que contêm *software*, incluindo firmware e controladores lógicos programáveis (por exemplo, marca-passos, bombas de infusão) ou existem apenas como *software,* por exemplo, *software* como dispositivo médico (SaMD). É importante observar que o escopo deste guia de cibersegurança de dispositivos médicos é limitado ao potencial dano ao paciente. Por exemplo, estão no escopo deste guia, os riscos de cibersegurança que afetam o desempenho, afetam negativamente os resultados clínicos ou resultam em erros de diagnóstico ou erros terapêuticos. Embora outros tipos de danos sejam importantes, como os associados à violação da privacidade dos dados, eles não são considerados no escopo deste documento. Ademais, este documento reconhece a importância da cibersegurança para a empresa do fabricante. Contudo, a cibersegurança no viés da empresa não está no escopo deste guia. Para boas práticas adicionais relacionadas à segurança da empresa do fabricante, o *NIST Cybersecurity Framework* serve como um importante recurso.

Este documento tem como objetivo:

- Empregar uma abordagem baseada no risco para o projeto e desenvolvimento de dispositivos médicos com proteções de cibersegurança apropriadas;
- Contribuir para a garantia da segurança do paciente, desempenho e segurança de dispositivos médicos e a infraestrutura de serviços de saúde conectada ao dispositivo;
- Apontar que a cibersegurança é uma responsabilidade compartilhada entre todos os intervenientes, incluindo, mas não limitado a fabricante de dispositivos médicos, serviços de saúde, usuários, Anvisa e aqueles que encontram vulnerabilidades (cf. Seção 6.3.3);
- Fornecer recomendações aos intervenientes para ajudar a minimizar o risco de danos ao paciente durante o ciclo de vida do produto;
- Definir termos e descrever as boas práticas atuais para alcançar a cibersegurança de dispositivos médicos;
- Promover políticas de compartilhamento de informações sobre incidentes, ameaças e vulnerabilidades de cibersegurança, a fim de aumentar a transparência e fortalecer a resposta.

2. INTRODUÇÃO

A necessidade de cibersegurança[1] eficaz para garantir a funcionalidade dos dispositivos médicos e a segurança do paciente tem se tornado cada vez mais importante com o aumento do uso de dispositivos conectados à rede,

[1] Cibersegurança é um termo que designa um estado em que informações e sistemas são protegidos contra atividades não autorizadas, como acesso, uso, divulgação, interrupção, modificação ou destruição, a um nível em que os riscos relacionados à confidencialidade, integridade e disponibilidade sejam mantidos em um nível aceitável por todo o ciclo de vida. (ISO 81001-1).

cabeada ou sem fio, e à Internet. Os incidentes de cibersegurança tornam inoperantes os dispositivos médicos e as redes hospitalares, interrompendo a prestação de cuidado médico ao paciente nos serviços de saúde. Tais incidentes podem conduzir a dano ao paciente por meio de atrasos e ou erros no diagnóstico e ou nos tratamentos. Os intervenientes de serviços de saúde têm responsabilidade compartilhada em relação à cibersegurança de dispositivos médicos.
Este guia pretende ajudar todos os intervenientes a entender melhor seu papel na implementação de medidas de cibersegurança de forma proativa, de modo a proteger e fortalecer a segurança e eficácia de dispositivos médicos, em antecipação a futuros ataques, problemas ou eventos.

A convergência dos princípios e práticas globais de cibersegurança em serviços de saúde é necessária para garantir que a segurança do paciente e o desempenho do dispositivo médico sejam mantidos. Até o momento, entretanto, os regulamentos atuais entre os governos são díspares e carecem do alinhamento global necessário para garantir a cibersegurança dos dispositivos médicos.

O objetivo deste guia é fornecer princípios gerais e boas práticas para facilitar a convergência regulatória internacional aplicáveis ao processo de cibersegurança de dispositivos médicos. O documento está estruturado da seguinte forma:

- Escopo do documento;
- Introdução ao tema e bases legais;
- Visão geral dos princípios gerais da cibersegurança de dispositivos médicos;
- Recomendações para os intervenientes em relação às boas práticas no gerenciamento pré- e pós-mercado da cibersegurança de dispositivos médicos. Destaca-se que a abordagem de pré-mercado trata principalmente dos fabricantes de dispositivos médicos;
- Recomendações de pós-mercado para todos os intervenientes;
- Algumas considerações finais sobre cibersegurança;
- Glossário dos principais termos utilizados em cibersegurança.

Este é o primeiro guia a se concentrar exclusivamente na cibersegurança de dispositivos médicos. Entretanto, existem outros documentos do IMDRF ou de outros países ou regiões (e.g. União Europeia) que devem ser observados em termos de considerações gerais de segurança. O documento *IMDRF/GRRP WG/N47 FINAL:2018* fornece princípios essenciais harmonizados aplicáveis ao projeto e fabricação de dispositivos médicos, incluindo os para diagnóstico *in vitro*. Esses princípios essenciais devem ser considerados juntamente com este guia, sendo aplicáveis em todo o ciclo de vida de um dispositivo médico. O *IMDRF/SaMD WG/N12 FINAL:2014* descreve a importância da segurança da informação com relação às considerações de segurança do paciente na seção 9.3 e ilustra alguns fatores particulares que afetam a segurança da informação do SaMD.

3. BASE LEGAL

Conforme Art. 12 da Lei 6.360, de 23 de setembro de 1976, nenhum produto de interesse à saúde, seja nacional ou importado, poderá ser industrializado, exposto à venda ou entregue ao consumo no mercado brasileiro antes de registrado no Ministério da Saúde, com exceção dos indicados no § 1º do Art. 25 da referida Lei, que embora dispensados de registro, são sujeitos ao regime de Vigilância Sanitária.

Conforme Art. 8º da Lei 9.782, de 26 de janeiro de 1999, compete, à Agência Nacional de Vigilância Sanitária (Anvisa) regulamentar, controlar e fiscalizar os produtos e serviços que envolvam risco à saúde pública, o que incluiu, dentre outras atividades, a concessão de registro de produtos (inciso IX do Art. 7º).

A Resolução de Diretoria Colegiada 185, de 22 de outubro de 2001, da Anvisa, define produto médico como

> "Produto para a saúde, tal como equipamento, aparelho, material, artigo ou sistema de uso ou aplicação médica, odontológica ou laboratorial, destinado à prevenção, diagnóstico, tratamento, reabilitação ou anticoncepção e que não utiliza meio farmacológico, imunológico ou metabólico para realizar sua principal função em seres humanos, podendo, entretanto, ser auxiliado em suas funções por tais meios".

Portanto, os *softwares* sujeitos ao regime de vigilância sanitária são aqueles destinados à prevenção, diagnóstico, tratamento, reabilitação ou anticoncepção de seres humanos.

4. PRINCÍPIOS GERAIS

Esta seção fornece princípios gerais que orientam para a cibersegurança de dispositivos médicos, relevantes para todos os intervenientes considerarem ao desenvolver, regular, usar e monitorar dispositivos médicos e podem representar impacto positivo na segurança do paciente.

4.1. Harmonização global

A cibersegurança de dispositivos médicos é uma questão de interesse global. Os incidentes de segurança têm o potencial de ameaçar a segurança dos pacientes em todo o mundo, causando erros de diagnóstico ou terapêuticos, comprometendo o desempenho seguro de um dispositivo, afetando resultados clínicos ou negando o acesso do paciente a cuidados críticos. A convergência dos esforços globais para a cibersegurança de dispositivos médicos é necessária para garantir a segurança do paciente, enquanto se incentiva a inovação e se permite o acesso oportuno do paciente a dispositivos médicos seguros e eficazes. Todos os intervenientes são incentivados a adotar abordagens de cibersegurança no ciclo de vida do dispositivo médico. Isto inclui o projeto do produto, atividades de gerenciamento de riscos ao longo do ciclo de vida do dispositivo, rotulagem do dispositivo, requisitos de submissão regulatórios, compartilhamentos de informações e atividades pós-mercado.

4.2. Ciclo de vida do produto

Os riscos associados a ameaças e vulnerabilidades de cibersegurança devem ser considerados em todas as fases da vida de um dispositivo médico, desde a concepção inicial até o fim do suporte (EOS, do inglês *End of Support*). Para gerenciar efetivamente a natureza dinâmica do risco de cibersegurança, o gerenciamento de riscos deve ser aplicado em todo o ciclo de vida do produto (TPLC, do inglês *Total product life cycle*), em que o risco de cibersegurança é avaliado e mitigado nas várias fases do TPLC, incluindo, mas não se limitando a, projeto, fabricação, teste, e atividades de monitoramento pós-mercado.

É sabido que é necessário equilibrar segurança do paciente e segurança do dispositivo. Ao incorporar controles de cibersegurança e mitigação de riscos e danos, é fundamental que os fabricantes de dispositivos médicos assegurem que a segurança do paciente e desempenho essencial do dispositivo sejam mantidos.

4.3. Responsabilidade compartilhada

A cibersegurança de dispositivos médicos é uma responsabilidade compartilhada entre os intervenientes, incluindo fabricante, serviço de saúde, usuários, Anvisa e aqueles que encontram as vulnerabilidades (cf. Seção 6.3.3). Todos os intervenientes devem entender suas responsabilidades e trabalhar em estreita colaboração com outros intervenientes para continuamente monitorar, avaliar, mitigar riscos e danos, comunicar e responder aos potenciais riscos de cibersegurança e ameaças no ciclo de vida do dispositivo médico.

4.4. Compartilhamento de informações

Compartilhamento de informações de cibersegurança é um princípio fundamental na abordagem que envolve o ciclo de vida do produto visando dispositivos médicos seguros e protegidos. Todos os intervenientes são encorajados a adotar uma abordagem proativo de pré e de pós-mercado para o compartilhamento de informações de cibersegurança. A disponibilidade oportuna de informações fornece a todos os intervenientes uma capacidade aprimorada para identificar ameaças, avaliar riscos associados e responder de acordo. Todos os intervenientes responsáveis são, portanto, incentivados a participar ativamente de Organizações de Análise e Compartilhamento de Informações (ISAOs, do inglês *Information Sharing Analysis Organizations*), para fomentar a colaboração e comunicação de incidentes de cibersegurança, ameaças e vulnerabilidades que possam afetar a segurança do paciente, o desempenho, a integridade e a segurança dos dispositivos médicos e a infraestrutura do serviço de saúde conectada ao dispositivo. Esses esforços promovem a transparência. A divulgação coordenada de vulnerabilidades (CVD, do inglês *Coordinated vulnerability disclosure*) é outro mecanismo de compartilhamento de informações que é incentivada como uma boa prática. Além disso, os ecossistemas se beneficiariam com o desenvolvimento adicional de políticas de compartilhamento de informações que se estendem para além dos fabricantes, incluindo serviços de saúde, assim como usuários de dispositivos médicos. A Anvisa pretende compartilhar informações com outros reguladores da área da saúde para ajudar a proteger e manter, globalmente, a segurança do paciente.

5. CONSIDERAÇÕES PRÉ-MERCADO PARA CIBERSEGURANÇA DE DISPOSITIVOS MÉDICOS

Considerando que a cibersegurança de dispositivos médicos deva ser considerada ao longo do ciclo de vida do produto, há elementos importantes que um fabricante deve abordar durante o projeto e o desenvolvimento de um dispositivo médico antes da sua entrada no mercado. Esses elementos de pré-mercado incluem: projetar recursos de segurança no produto; aplicar estratégias de gerenciamento de risco; desenvolver testes de segurança; fornecer informações úteis para os usuários operarem o dispositivo com segurança; dispor de um plano para as atividades pós-mercado. Para os elementos pré-mercado, os fabricantes devem considerar o ambiente do uso pretendido, bem como os cenários de uso indevido previsíveis. As seções, a seguir, têm como objetivo introduzir esses conceitos e fornecer recomendações aos fabricantes na fase de pré-mercado. Destaca-se que as atividades do ciclo de vida para *software* de dispositivos médicos são especificadas na norma IEC 62304:2006/AMD1:2015.

5.1. Requisitos de segurança e projeto da arquitetura

Endereçar proativamente as ameaças de cibersegurança na fase de projeto (por exemplo, modelagem de ameaças) podem atenuar o potencial de danos ao paciente de forma mais efetiva do que pautar apenas em atividades reativas de pós-mercado. Esses insumos no projeto podem vir de várias fases do ciclo de vida do

produto, como captura de requisitos, teste de verificação de projeto ou atividades de gerenciamento de riscos no pré e pós-mercado.

Os requisitos de segurança também devem ser identificados durante a fase de captura de requisitos do projeto. Alguns requisitos de segurança e medidas de controle de risco de segurança podem ser encontrados nas normas AAMI TIR57:2016, IEC TR 80001-2-2, IEC TR 80001-2-8, a família ISO 27000 e recursos publicados pelo *National Institute Standards and Technologies*[2] (NIST) (por exemplo, *Secure Software Development Framework* - SSDF), *Open Web Application Security Project*[3] (OWASP) (por exemplo, *Security by Design Principles*) e a *US Healthcare and Public Health Sector Coordinating Council* (HPH SCC) *Joint Cyber Security Working Group* (JCWG) (por exemplo, o *Joint Security Plan*).

Embora a Tabela 1 não pretenda ser uma lista exaustiva, ela descreve alguns princípios de projeto que os fabricantes de dispositivos médicos devem considerar ao projetar seu produto.

Tabela 1 - Princípios a serem considerados no projeto de dispositivos médicos

Princípio do projeto	**Descrição**
Comunicações seguras	O fabricante deve considerar como o dispositivo faria interface com outros dispositivos ou redes. As interfaces podem incluir conexões com fio e ou sem fio. Exemplos de métodos de interface incluem *Wi-Fi*, Ethernet, *Bluetooth*, USB etc.
	O fabricante deve considerar projetar funcionalidades que atendam todas as entradas (não apenas externas) e levar em consideração a comunicação com dispositivos e ambientes que suportam apenas comunicação menos segura (por exemplo, um dispositivo conectado a uma rede doméstica ou a um dispositivo legado).
	O fabricante deve considerar como a transferência de dados de e para o dispositivo é protegida para impedir o acesso não autorizado, modificação ou reprodução (*replay*). Por exemplo, os fabricantes devem determinar: como as comunicações entre dispositivos/sistemas se autenticarão entre eles; se a criptografia é necessária; como a reprodução não autorizada de comandos ou dados transmitidos anteriormente será impedida; e se o encerramento de sessões de comunicação após um tempo pré-definido é apropriado.
Proteção de Dados	O fabricante deve considerar se os dados relacionados à segurança do paciente são armazenados ou transferidos para/do dispositivo requerem algum nível de proteção, tal como criptografia. Por exemplo, as senhas devem ser armazenadas como *hashes* criptograficamente seguros.
	O fabricante deve considerar se são necessárias medidas de controle de risco sobre a confidencialidade para proteger os campos de controle/sequenciamento de mensagens nos protocolos de comunicação ou para impedir o comprometimento dos materiais de codificação criptográfica.
Integridade do Dispositivo	O fabricante deve avaliar a arquitetura no nível do sistema para determinar se recursos de projeto são necessários para garantir o não repúdio dos dados (por exemplo, suporte a uma função de trilha de auditoria).
	O fabricante deve considerar riscos à integridade do dispositivo, tais como modificações não autorizadas no *software* do dispositivo.

[2] Órgão do Departamento do Comércio do governo dos Estados Unidos da América (EUA).

[3] É uma comunidade online que cria e disponibiliza de forma gratuita artigos, metodologias, documentação, ferramentas e tecnologias no campo da segurança de aplicações *web.*

	O fabricante deve considerar controles, tais como *anti-malware* para evitar vírus, *spyware*, *ransomware*, e outras formas de código malicioso de ser executado no dispositivo.
Autenticação do Usuário	O fabricante deve considerar controles de acesso do usuário que validem quem pode usar o dispositivo ou permita a concessão de privilégios a diferentes funções de usuário ou permita o acesso de usuários em caso de emergência. Ademais, as mesmas credenciais não devem ser compartilhadas entre dispositivos e usuários. Exemplos de autenticação ou autorização de acesso incluem senhas, chaves de *hardware*, biometria ou um sinal de intenção que não pode ser produzido por um outro dispositivo.
Manutenção de *software*	O fabricante deve estabelecer e comunicar um processo para implementação e implantação de atualizações periódicas.
	O fabricante deve considerar como operar o *software* do sistema, o *software* de terceiros ou como o *software* de código aberto será atualizado ou controlado. O fabricante também deve planejar como responder a atualizações de *software* ou ambientes operacionais desatualizados fora de seu controle (por exemplo, *software* de dispositivo médico executando em uma versão não segura de um sistema operacional).
	O fabricante deve considerar como o dispositivo será atualizado para protegê-lo contra vulnerabilidades de cibersegurança recém-descobertas. Por exemplo, pode-se considerar se as atualizações exigirão intervenção do usuário ou serão iniciadas pelo dispositivo e como a atualização pode ser validada para garantir que não tenha efeito adverso na segurança do paciente e no desempenho do dispositivo.
	O fabricante deve considerar quais conexões serão necessárias para realizar atualizações e a autenticidade da conexão ou atualização através do uso de assinatura de código ou de outros métodos semelhantes.
Acesso Físico	O fabricante deve considerar controles para impedir que uma pessoa não autorizada acesse o dispositivo. Por exemplo, os controles podem incluir bloqueios físicos ou restringir fisicamente o acesso às portas, ou não permitir o acesso com um cabo físico sem exigir autenticação.
Confiabilidade e disponibilidade	O fabricante deve considerar os recursos de projeto que permitirão ao dispositivo detectar, resistir, responder e se recuperar de ataques de cibersegurança, a fim de manter seu desempenho essencial.

Os princípios de desenvolvimento seguro são essenciais para o projeto seguro do dispositivo. Muitos modelos ou padrões atuais de ciclo de vida de desenvolvimento de *software* não incorporam esses princípios por padrão. É importante que os fabricantes de dispositivos que desenvolvem *software* de dispositivos médicos incorporem estes princípios de segurança no desenvolvimento de seu *software*. Para isso, é necessário que os fabricantes adotem uma abordagem holística de cibersegurança de dispositivos médicos, avaliando riscos e mitigações ao longo do ciclo de vida do produto.

5.2. Princípios de gerenciamento de risco para o ciclo de vida do produto

Os princípios sólidos de gerenciamento de riscos que tratam dos domínios de segurança do paciente e proteção devem ser incorporados ao longo do ciclo de vida de um dispositivo médico. Um risco de cibersegurança que afeta a segurança do paciente e o desempenho essencial do dispositivo, afeta negativamente os resultados clínicos ou resulta em erros de diagnóstico ou terapêuticos também devem ser considerados no processo de gerenciamento de riscos do dispositivo médico. O gerenciamento de risco, tal como descrito na norma ISO 14971:2019, e de gestão de riscos de cibersegurança (por exemplo, tal como descrito em AAMI TIR57:2016 e AAMI TIR97:2019), deve ser utilizado pelo fabricante, de modo a considerar os seguintes passos como parte do seu processo de gestão de riscos:

- Identificar qualquer vulnerabilidade de cibersegurança;
- Estimar e avaliar os riscos associados;
- Controlar esses riscos para um nível aceitável;
- Avaliar e monitorar a eficácia dos controles de risco; e
- Comunicar os riscos por meio de divulgação coordenada aos intervenientes.

A Figura 1 mostra o processo de gerenciamento de riscos de segurança proposto pela norma AAMI TIR57:2016. Esse pode ser um processo de gerenciamento de riscos especializado, executado como parte de uma gestão de riscos, ou pode ser parte integral do processo de gerenciamento de riscos como proposto pela norma ISO 14971:2019, com o apropriado mapeamento de vulnerabilidades, ameaças e outros critérios relacionados à segurança. O Anexo F disponibiliza a norma ISO/TR 24971:2020, um guia para ajudar a implementar a o gerenciamento de riscos de dispositivos médicos.

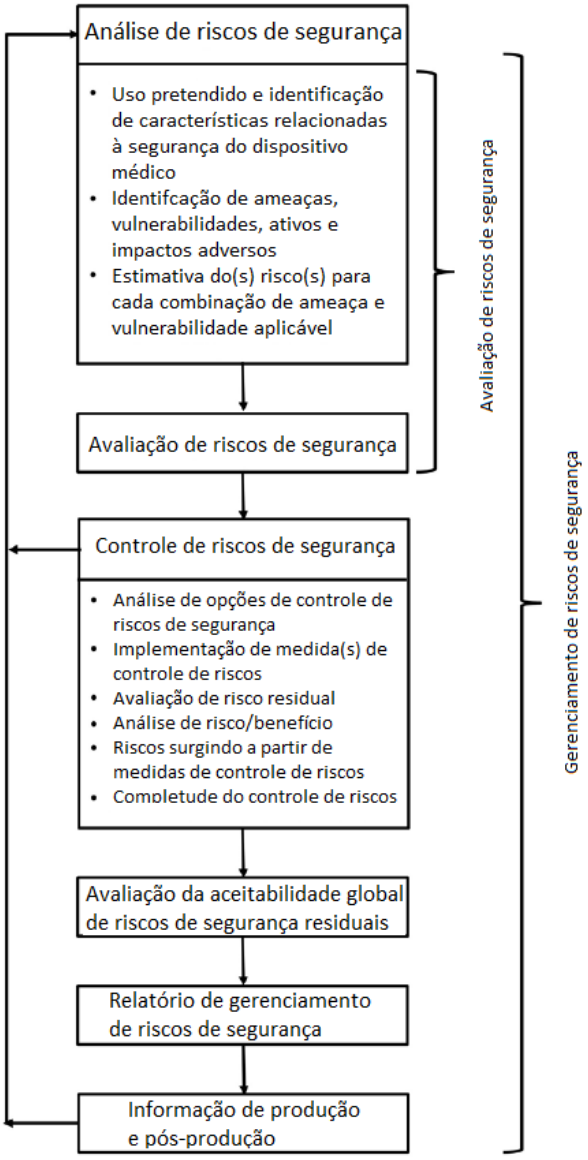


Figura 1 - Representação esquemática do processo de gerenciamento de riscos de segurança (com permissão da AAMI TIR57:2016.)

Com relação à cibersegurança na regulação de dispositivos médicos, as análises de risco devem se concentrar na avaliação do risco de danos ao paciente, considerando: 1) a possibilidade de explorar a vulnerabilidade de cibersegurança, e 2) a gravidade dos danos ao paciente se a vulnerabilidade estava a ser explorada. Essas análises também devem incorporar considerações sobre controles compensatórios e mitigações de risco.

As avaliações de risco conectam o projeto à modelagem de ameaças, dano ao paciente, mitigações dos riscos e testes de segurança. É, portanto, importante estabelecer um projeto de arquitetura segura de tal forma que o risco pode ser adequadamente gerenciado. Existem inúmeras ferramentas e abordagens que podem ser alavancadas nessa avaliação, incluindo, mas não se limitando à avaliação de riscos de segurança, modelagem de ameaças e pontuação de vulnerabilidades.

- **Avaliação de riscos de segurança**: os fabricantes devem considerar riscos, ameaças e controles de cibersegurança ao longo do ciclo de vida do produto. Onde aplicável, os requisitos de cibersegurança devem ser cruzados com ameaças e vulnerabilidades de cibersegurança específicas do dispositivo se os requisitos são mitigações dos riscos identificados.

- **Modelagem de ameaças**: a modelagem de ameaças é um processo para identificar, enumerar e mitigar riscos das ameaças em potencial do dispositivo e do sistema. Especificamente, a modelagem de ameaças inclui a consideração de riscos, abordando, mas não se limitando a riscos relacionados à cadeia de suprimentos (por exemplo, componentes do sistema), projeto, produção, implantação (por exemplo, em um ambiente hospitalar) e manutenção. Ademais, a criação de diagramas de sistema suficientemente detalhados ajuda a entender como os elementos de projeto de cibersegurança são incorporados a um dispositivo que ajuda ainda mais na modelagem de ameaças. Em gerar um modelo de ameaça e por orientação do OWASP, os fabricantes de dispositivos médicos devem responder a quatro questões básica, relativas a cibersegurança:

    1. O que estamos construindo?
    2. O que pode dar errado? (por exemplo, como poderia ser atacado)
    3. O que vamos fazer sobre isso?
    4. Fizemos um trabalho suficientemente bom?

    Estas perguntas podem ser feitas no contexto da arquitetura da aplicação, fluxo de dados operacionais ou modelagem de ameaças em nível mais amplo de sistema, conforme o caso. Ao determinar o que pode dar errado durante a modelagem de ameaças, os fabricantes devem considerar a configuração incorreta não intencional ou maliciosa de *software* e *hardware* (por exemplo, conectar um dispositivo à Internet que não foi projetado para isso).

- **Pontuação de vulnerabilidades**: a pontuação de vulnerabilidades fornece uma maneira de caracterizar e avaliar a possibilidade de explorar a vulnerabilidade e a gravidade de uma vulnerabilidade de cibersegurança. As vulnerabilidades e exposições comuns (CVE, do inglês *common vulnerabilities and exposures*) conhecidas e identificadas no projeto e desenvolvimento devem ser analisadas e avaliadas usando uma metodologia consistente de pontuação de vulnerabilidades, tal como o Sistema de Pontuação de Vulnerabilidade Comum (CVSS, do inglês *Common Vulnerability Scoring System*) ou qualquer outro sistema de pontuação de vulnerabilidade que venha a ser adotado no futuro. Riscos de cibersegurança, pontuação de vulnerabilidade e medidas de controle podem ser usadas para subsidiar a modelagem de ameaças e avaliações de riscos de segurança para novos produtos e outras ferramentas

de avaliação de riscos não específicas à cibersegurança, por exemplo, análise do modo e efeito de falha (FMEA, do inglês *Failure mode and effects analysis*).

Ao integrar um processo de gestão de riscos de cibersegurança a um processo de gerenciamento de riscos do dispositivo médico, conforme apresentado pela norma ISO 14971:2019, atividades que endereçam a segurança, tais como modelagem de ameaças e pontuação de vulnerabilidades, devem ser levadas em conta.

5.3. Teste de segurança

Na fase de verificação e validação no processo de projeto e desenvolvimento, o fabricante deve empregar vários tipos de testes de segurança para garantir que o código esteja livre de vulnerabilidades conhecidas e que os controles de segurança foram efetivamente implementados. Os testes devem levar em consideração o contexto de uso do dispositivo e seu ambiente de implantação. A aplicação de técnicas de verificação de *software* é recomendada para garantir que o *software* esteja em conformidade com as especificações e que as anomalias sejam minimizadas. Também é importante garantir que o dispositivo médico seja testado quanto a vulnerabilidades conhecidas que possam ser exploradas. Para fazer isso, o dispositivo médico deve passar por um processo de avaliação de segurança ou verificação de aceitação (por exemplo, teste de *software*, simulação de ataque). O teste de segurança é um componente do arcabouço de desenvolvimento seguro e a granularidade adicional em relação às considerações de teste podem ser encontradas nos padrões e recursos apresentados na Seção 5.1. deste documento. Os pontos abordados a seguir devem ser considerados pelos fabricantes de dispositivos médicos:

- Executar buscas direcionadas por vulnerabilidades conhecidas nos componentes do *software*/módulos ou fraquezas do *software* também durante a fase de desenvolvimento. Por exemplo, os testes periódicos de segurança podem incluir: análise estática de código, análise dinâmica, teste de robustez, varredura por vulnerabilidades ou análise da composição de *software*.
- Realizar análises técnicas de segurança (por exemplo, teste de penetração). Isso inclui esforços para identificar vulnerabilidades desconhecidas por meio de testes *fuzz*, por exemplo; ou verificar pontos de entrada alternativos, como leitura de arquivos ocultos, configurações, fluxos de dados ou registros de *hardware*.
- Completar uma avaliação de vulnerabilidades. Isto inclui uma análise de impacto da vulnerabilidade em outros produtos internos, isto é, análise de variância, a identificação de contramedidas e a reparação - ou a mitigação - da vulnerabilidade.

5.4. Plano de gerenciamento de cibersegurança para o ciclo de vida do produto

À medida que as ameaças de cibersegurança evoluem, os fabricantes devem, proativamente, monitorar, identificar e endereçar as vulnerabilidades e explorações como parte de seu plano de gerenciamento de cibersegurança por todo o ciclo de vida do produto. Um plano deve estar em vigor no momento de pré-mercado do desenvolvimento do produto e mantido idealmente em toda a organização do fabricante. Esse plano deve abordar:

- **Vigilância no TPLC**: o monitoramento proativo e identificação de vulnerabilidades de cibersegurança recém-descobertas, avaliação de suas ameaças e respostas apropriadas.

- **Divulgação de vulnerabilidades**: Um processo formalizado para coletar informações de quem encontra vulnerabilidades, desenvolver estratégias de mitigação e correção, e divulgar a existência de vulnerabilidades e abordagens de mitigação ou correção para os intervenientes.
- **Atualizações e correção**: um plano que descreve como o *software* será atualizado ou como outras ações corretivas serão aplicadas para manter a segurança e o desempenho contínuos do dispositivo regularmente ou em resposta a uma vulnerabilidade identificada.
- **Recuperação**: um plano de recuperação para o fabricante, usuário ou ambos, para restaurar o dispositivo à sua condição operacional normal após um incidente de cibersegurança.
- **Compartilhamento de informações**: participação em Organizações de Análise e Compartilhamento de Informações (ISAO, do inglês *Sharing Analysis Organizations*) ou em Centros de Análise e Compartilhamento de Informações (ISAC, do inglês *Information Sharing and Analysis Centers*), que promovem a comunicação e o compartilhamento de informações atualizadas sobre ameaças e vulnerabilidades de segurança.

5.5. Rotulagem e documentação de segurança do cliente

5.5.1. Rotulagem

A rotulagem expressa as informações relevantes de segurança para usuários finais, levando em consideração o relativo risco de cibersegurança. Ela deve incluir os seguintes elementos:

- Instruções do dispositivo e especificações do produto relacionadas aos controles de cibersegurança recomendados e apropriados para o ambiente de uso pretendido (por exemplo, *software* anti-*malware*, configuração de conectividade de rede, uso de um *firewall*).
- Uma descrição dos recursos e procedimentos para fazer cópia de segurança e restauração para recuperar configurações.
- Uma lista de portas de rede e outras interfaces que devem receber e ou enviar dados e uma descrição da funcionalidade da porta, bem como informações se as portas são de entrada ou saída. Ressalta-se que as portas não utilizadas devem ser desativadas.
- Diagramas de sistema suficientemente detalhados para usuários finais.

5.5.2. Documentação de segurança do cliente

Além das instruções de uso, a documentação técnica escrita para instalação, configuração do dispositivo, bem como os requisitos técnicos para seus ambientes de operação são particularmente importantes para a segurança do usuário e seu uso seguro. A documentação deve incluir os seguintes elementos:

- Orientação específica aos usuários sobre os requisitos de infraestrutura que suportará o dispositivo, para que este possa operar conforme o esperado.
- Uma descrição da situação de segurança do dispositivo e ou como pode a segurança pode ser aprimorada, usando configuração segura. Configurações seguras podem incluir proteções de dispositivos finais/terminais, tal como *anti-malware*, *firewall* ou regras de *firewall*, *whitelists*, parâmetros de evento de segurança, registro de parâmetros, detecção de segurança física.

- Onde aplicável, instruções técnicas para permitir a implantação e manutenção de redes seguras (conectadas) e instruções para os usuários sobre como responder após a detecção de uma vulnerabilidade ou incidente de cibersegurança.
- Uma descrição de como o dispositivo ou os sistemas que o suporta notificarão o usuário quando condições anômalas forem detectadas, ou seja, eventos de segurança, sempre que possível. Os tipos de eventos de segurança podem ser alterações de configuração, anomalias de rede, tentativas de login, tráfego anômalo, como por exemplo, enviar solicitações para entidades desconhecidas.
- Uma descrição dos métodos para retenção e recuperação da configuração do dispositivo por um usuário privilegiado autenticado.
- Onde aplicável, riscos de segurança e as consequências de alterações na configuração de segurança ou no ambiente de uso. Uma descrição dos procedimentos sistemáticos para usuários autorizados baixarem e instalarem atualizações do fabricante.
- Informações, se conhecidas, sobre o fim do suporte à cibersegurança do dispositivo. Sobre este tema, ver também a Seção 6.6.
- Uma Lista de materiais de *software* (SBOM, do inglês *Software Bill of Materials*) para informar e dar suporte aos operadores sobre a cibersegurança de componentes comerciais, de código aberto ou de *software* de prateleira, incluídos no dispositivo médico. Uma SBOM cria a transparência necessária por meio de uma lista que identifica cada componente de *software* por seu nome, origem, versão e compilação. As SBOM permitem que os operadores de dispositivos, incluindo pacientes e serviços de saúde, gerenciem efetivamente seus ativos e riscos relacionados, compreendam o impacto potencial das vulnerabilidades identificadas no dispositivo - e no sistema conectado - e apliquem contramedidas para manter a segurança do paciente e o desempenho essencial do dispositivo. Os operadores de dispositivos podem usar o SBOM para facilitar o trabalho com o fabricante do dispositivo para identificar os *softwares* que podem ter vulnerabilidades e os requisitos de atualização, bem como executar o processo de gerenciamento de riscos de segurança apropriado. O SBOM também ajuda na tomada de decisão da compra, fornecendo, com visibilidade aos possíveis compradores, os componentes usados nos aplicativos, que podem determinar o risco de segurança potencial. Os fabricantes devem alavancar as boas práticas da indústria para o formato, sintaxe e marcação usados para dispor o SBOM. Como o SBOM revela informações sensíveis sobre o dispositivo médico, sua distribuição é incentivada por meio de canais de comunicação confiáveis. Presume-se que os fabricantes determinarão maneiras confiáveis de comunicar os SBOM ao operador.

5.6. Documentação para submissão regulatória

Além das atividades descritas nas seções anteriores, os fabricantes de dispositivos médicos devem documentar e resumir claramente suas atividades relacionadas à cibersegurança. Dependendo da classe de risco do dispositivo, a Anvisa pode exigir documentação para avaliar o dispositivo médico antes da entrada no mercado ou pode solicitá-la durante a fase pós-mercado. Se necessário, para registrar o produto, deve ser apresentada documentação afeta à cibersegurança que descreva as características de projeto do dispositivo, as atividades de gerenciamento de riscos, os testes, a rotulagem e a evidência de um plano para monitorar e responder a ameaças que emergem ao longo do ciclo de vida do produto. A documentação para submissão regulatória de que trata esta seção compõe o dossiê técnico, conforme orienta a Nota Técnica 04/2012/GQUIP/GGTPS/Anvisa. As documentações são detalhadas nas subseções a seguir.

5.6.1. Documentação de projeto

O projeto deve conter documentação que descreva o dispositivo, incluindo quaisquer interfaces ou vias de comunicação ou componentes (*hardware* e *software*) e todas as características de projeto que foram incluídos para mitigar os riscos de cibersegurança relacionados aos danos ao paciente, tais como os descritos na Seção 5.1. Em particular, a razão e as premissas principais para a seleção das medidas para o controle do acesso, criptografia, atualizações seguras, registo, segurança física.

5.6.2. Documentação de gerenciamento de riscos

A documentação de gerenciamento de risco deve conter documentos que descrevam claramente ameaças e vulnerabilidades de cibersegurança, estimativa dos riscos associados, descrições dos controles em vigor para mitigar esses riscos e evidências para demonstrar que esses controles foram testados. Os fabricantes devem considerar incluir controles que maximizem a cibersegurança do dispositivo sem afetar indevidamente outros controles de segurança. Os documentos de gerenciamento de riscos relacionados à cibersegurança submetidos à Anvisa devem ser claros e usar como guia, um padrão de gerenciamento de riscos de cibersegurança, comopor exemplo, AAMI TIR57:2016 e AAMI TIR97:2019. Os resultados devem estar alinhados com os requisitos gerais da norma ISO 14971:2019, para garantir que a saída possa ser usada como insumo para o gerenciamento de riscos geral. Os documentos de gerenciamento de riscos relacionados à cibersegurança podem incluir:

- Documentação abrangente de gerenciamento de riscos, tal como um relatório de gerenciamento de riscos ou relatório de gerenciamento de riscos de segurança, que deve incluir qualquer modelagem de ameaças e ameaças de cibersegurança identificadas.
- Discussão sobre qualquer impacto das mitigações de riscos de segurança no gerenciamento de outros riscos.

5.6.3. Documentação de teste de segurança

Relatórios de teste que resumem todos os testes realizados para verificar a segurança do dispositivo e a eficácia de qualquer controle de segurança. Detalhes de testes específicos, tais como o cruzamento de componentes de *software* ou subsistemas com bancos de dados de vulnerabilidades conhecidas foram apresentados na Seção 5.3. Contudo, todos os documentos de teste devem conter:

- Descrições de métodos de teste, resultados e suas conclusões;
- Uma matriz de rastreabilidade entre riscos de segurança, controles de segurança e testes para verificar esses controles; e
- Referências a quaisquer padrões e procedimentos[4] e ou documentações internas usadas.

5.6.4. Documentação de planejamento de gerenciamento de cibersegurança do ciclo de vida do produto

A empresa deve dispor de um resumo do plano de manutenção do dispositivo que descreva os processos pós-mercado pelos quais o fabricante pretende garantir a segurança do paciente e o desempenho contínuos do dispositivo ao longo de seu ciclo de vida. Conforme descrito na Seção 5.4, esses processos podem

[4] Procedimento Operacional Padrão (POP).

incluir: vigilância no ciclo de vida do produto, divulgação de vulnerabilidades, atualizações e correção, recuperação e compartilhamento de informações.

5.6.5. Rotulagem e documentação de segurança do cliente

Inclui toda documentação afeta ao usuário, com informações relevantes, conforme descrito na Seção 5.5, para permitir que o usuário gerencie os riscos no ambiente pretendido do dispositivo.

6. CONSIDERAÇÕES PÓS-MERCADO PARA CIBERSEGURANÇA DE DISPOSITIVOS MÉDICOS

À medida que as vulnerabilidades mudam com o tempo, os controles projetados e implementados na fase de pré-mercado podem ser inadequados para manter um perfil de risco aceitável. Portanto, é necessária uma abordagem pós-mercado dinâmica, na qual vários intervenientes desempenham papel relevante. Essa abordagem pós-mercado abrange vários elementos e inclui a operação do dispositivo no ambiente pretendido, compartilhamento de informações, divulgação coordenada de vulnerabilidades, correção de vulnerabilidades, resposta a incidentes e dispositivos legados. As seções, a seguir, têm como objetivo introduzir esses conceitos e fornecer recomendações aos principais intervenientes na fase pós-mercado do produto.

6.1. Dispositivos em operação no ambiente de uso pretendido

6.1.1. Serviços de saúde e pacientes

6.1.1.1. Boas práticas de cibersegurança a serem adotadas pelos serviços de saúde

A cibersegurança de dispositivos médicos é uma responsabilidade compartilhada e requer a participação de todos os intervenientes, incluindo serviços de saúde. Esses devem considerar a adoção de um processo de gerenciamento de risco para lidar com a segurança do paciente, o desempenho e os aspectos de cibersegurança de dispositivos médicos que estão conectados à sua infraestrutura de tecnologia de informação (TI). O processo deve ser aplicado no(a):

- Desenvolvimento inicial da infraestrutura de TI;
- Integração de um novo dispositivo médico na rede de TI existente; e
- Mudança de sistemas operacionais, da rede de TI ou do próprio dispositivo médico (*software* e *firmware*) com atualizações ou modificações.

A fim de realizar o processo de gestão de riscos, os serviços de saúde podem se referir a padrões de relevância, tais como IEC 80001-1, ISO 31000:2018 e a série ISO 27000. Em particular, a ISO 27799:2016. Os documentos do *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* da FDA podem também servir como referência.

Além de adotar um sistema de gerenciamento de riscos, os serviços de saúde também devem aderir às seguintes práticas recomendadas de cibersegurança, as quais não devem ser encaradas como uma lista exaustiva, para manter a postura geral de segurança:

- Boa segurança física para impedir o acesso físico não autorizado a dispositivos médicos ou pontos de acesso à rede;
- Medidas de controle de acesso (por exemplo, baseado em papéis) para garantir que apenas pessoal autorizado tenha acesso a elementos da rede, informações armazenadas, serviços e aplicações;
- Empregar gerenciamento de configuração para identificar todos os ativos atuais e acompanhar futuras alterações na configuração;
- Aplicar as medidas de configuração e proteção, conforme recomendações do fabricante;
- Controlar o acesso à rede para limitar a comunicação com dispositivos médicos;
- Atualizar práticas de gerenciamento que garantem atualizações tempestivas de segurança;
- Aplicar medidas de proteção contra *malware* para impedir ataques; e
- Limitar o tempo máximo da sessão para impedir o acesso não autorizado a dispositivos desassistidos por um período prolongado.

A implementação dessas boas práticas deve ser contextualizada com o uso clínico do dispositivo. Por exemplo, a adesão a algumas dessas práticas recomendadas pode não ser viável em uma emergência médica. Muitas das práticas acima são descritas no *NIST Cybersecurity Framework*.

6.1.1.2. Treinamento/Educação para os usuários

Os profissionais de saúde devem adotar uma abordagem holística para contribuir para que incidentes de cibersegurança não ocorram em suas instituições. Assim, eles são encorajados a fornecer treinamento em cibersegurança no nível básico para criar conscientização entre os usuários (por exemplo, médicos, enfermeiros, engenheiros biomédicos, técnicos) sobre segurança e introduzir práticas de higiene cibernética. Isto inclui treinamento sobre a operação de dispositivos médicos de maneira segura (por exemplo, apenas conectar seus dispositivos à rede segura) e como identificar e relatar qualquer comportamento anormal no dispositivo (por exemplo, desligamentos/reinicializações arbitrárias, *software* de segurança desativado). Tal treinamento também deve ser estendido a pacientes se os dispositivos médicos conectados destinam-se a ser operados pelos próprios pacientes, como por exemplo, dispositivos de uso doméstico, tais como glicosímetro ou bomba de insulina portátil.

6.1.2. Fabricantes de dispositivos médicos

Além da informação contida na rotulagem do produto e a documentação de segurança do cliente, os fabricantes são incentivados a estabelecer parcerias com os de serviços de saúde, distribuidores e consumidores de seus produtos, quando possível, para garantir a melhor implantação e configuração de seus dispositivos.

6.2. Compartilhamento de informações

O compartilhamento de informações é uma ferramenta vital para gerenciar ameaças e vulnerabilidades de cibersegurança em vários setores da economia mundial. Padrões e boas práticas para compartilhamento de inteligência e ameaças têm sido desenvolvidas e implementadas em outros setores que não os serviços de

saúde. Intervenientes de dispositivos médicos são incentivados a adotar ferramentas validadas por outros setores para fortalecer a segurança do ecossistema mundial de dispositivos médicos.

Devido à variedade de acesso aos recursos, diferentes métodos e uma gama de níveis de maturidade entre os intervenientes, também há um espectro de abordagens válidas para o compartilhamento de informações. Ademais, boas práticas de cibersegurança continuam a evoluir e as decisões são tomadas baseadas em conhecimento por vários fatores, incluindo o tipo de dispositivo, a infraestrutura conectada, o tamanho, o nível organizacional e o nível da ameaça. Portanto, este documento não favorece uma abordagem específica em detrimento de outra. Em vez disso, articula princípios que devem ser seguidos em relação ao compartilhamento de informações. Os exemplos não pretendem especificar requisitos, mas servir como ilustrações.

6.2.1. Princípios-chave

- As informações relacionadas à segurança dos dispositivos médicos devem ser compartilhadas com qualquer pessoa que precise dessas informações para garantir que o dispositivo médico em questão possa ser usado com segurança (por exemplo, usuários, pacientes, outros fabricantes, distribuidores, prestadores de serviços de saúde, pesquisadores da área de segurança e o público).
- A informação compartilhada deve ser equilibrada de tal forma que seja significativa, consumível e acionável para distintos intervenientes (por exemplo, informações sobre um *chipset* mais seguro poderiam ser importante para os fabricantes, mas a informação pode não trazer benefícios para os usuários finais do dispositivo).
- As informações devem ser compartilhadas livremente e como um ato de boa-fé oportuno, com o objetivo de melhorar a segurança do paciente, independentemente dos interesses comerciais.
- Garantir, tanto quanto possível, informações globalmente consistentes que sejam compartilhadas oportunamente de forma síncrona entre jurisdições para permitir que os intervenientes em várias jurisdições respondam de acordo.

6.2.2. Principais intervenientes

O setor de dispositivos médicos é regulado e mundial. Consequentemente, as recomendações locais ou jurisdicionais para o compartilhamento de informações podem não ser suficientes para um fabricante que esteja fornecendo dispositivos para vários mercados. Estratégias para compartilhar informações relacionadas à segurança de dispositivos médicos precisam ser globais. Intervenientes podem, portanto, precisar se envolver em várias redes, reconhecendo que algumas redes podem ser internacionais.

6.2.2.1. Anvisa

A Anvisa é uma receptora importante de informações relacionadas à segurança dos dispositivos médicos e é frequentemente envolvida na disseminação de informações.

- Deve focar em criar processos que incentivem a divulgação tempestiva de informações relacionadas à cibersegurança de dispositivos médicos. Isto inclui compartilhamento de informações entre os reguladores internacionais da área da saúde para facilitar uma resposta mundialmente coordenada.

6.2.2.2. Fabricantes de dispositivos médicos

- Devem identificar, avaliar e compartilhar informações de vulnerabilidade, independentemente da origem dessas informações. Os fabricantes são incentivados a compartilhar qualquer informação que ajude o regulador a gerenciar as expectativas e facilitar os requisitos regulatórios.
- Deve ter como objetivo sincronizar a notificação de todos os reguladores, onde o produto afetado é distribuído, para garantir informações globalmente consistentes e, oportunamente, uma resposta globalmente alinhada.
- Deve usar linguagem simples, no nível de leitura apropriado para o usuário pretendido, para comunicar informações que requerem ações sobre ameaças e vulnerabilidades de cibersegurança de dispositivos médicos. Pode ser necessário incluir informações sobre os benefícios clínicos e riscos associados com a implantação de uma atualização ou controles compensatórios necessários até que a atualização esteja disponível.

6.2.2.3. Serviços de saúde

- São frequentemente responsáveis por tomar medidas ou facilitar ações. Portanto, eles devem ter acesso a qualquer informação necessária para implementar uma recomendação e garantir a proteção de seus pacientes.
- Também são geradores importantes de informações, pois trabalham com dispositivos médicos em campo e podem fornecer retroalimentação sobre quais dispositivos foram afetados, assim como facilitar ou tornar eficaz a implementação da correção ou mitigação em um cenário do mundo real.

6.2.2.4. Usuários finais (Equipe de saúde, Pacientes, Cuidadores e Consumidores)

- São, geralmente, os que fazem a escolha final sobre a implementação de uma atualização ou outra correção disponibilizada pelo fabricante. Portanto, eles precisam de informações claras e com significado para que possam tomar uma decisão respaldada em conhecimento suficiente.

6.2.2.5. Outros intervenientes, incluindo governos e entidades de compartilhamento de informações

- As autoridades policiais, a segurança nacional e outras agências governamentais podem precisar compartilhar informações sobre ameaças e vulnerabilidades de cibersegurança de dispositivos médicos em várias partes do governo para proteger os serviços de saúde e outras infraestruturas críticas.
- As entidades que coletam, compartilham informações ou fornecem orientações ou conhecimentos especializados em segurança também podem ser fontes importantes de informações em segurança, assim como fornecer suporte. Essas entidades podem ser organizações governamentais ou organismos privados. Exemplos incluem redes de compartilhamento de informações (por exemplo, ISAO e ISAC), agências de disseminação da informação - por exemplo, CERT, do inglês *Computer Emergency Response Team*) - e outros. Esses intervenientes provavelmente diferem entre jurisdições e mercados.

6.2.3. Tipos de informação

As vulnerabilidades de cibersegurança podem representar ameaças a vários componentes do produto, incluindo *software*, *hardware* e componentes próprios ou de terceiros. Para proteger os pacientes dos danos, as informações compartilhadas podem incluir, mas não estão limitadas a:

- Informações sobre produtos afetados por uma vulnerabilidade e como eles são afetados;
- Informações sobre vulnerabilidades de componentes usados em outros produtos;
- Informações sobre equipamentos de TI que podem afetar a segurança de dispositivos médicos;
- Informações sobre os ataques, potenciais ataques e disponibilidade de código para explorar a vulnerabilidade;
- Confirmação de incidentes (por exemplo, "Você também está vendo isso?");
- Disponibilidade de patches e outras mitigações de segurança, como controles compensatórios; e
- Instruções adicionais sobre o uso e a integração de dispositivos médicos como medida provisória.

Compartilhamento de informação também deve incluir práticas e métodos que podem mitigar ameaças. Por exemplo, como equipamentos de TI podem ser configurados para mitigar uma vulnerabilidade que afeta um dispositivo médico ou métodos para responder a explorações conhecidas.

6.2.4. Comunicação confiável

As redes de compartilhamento de informações devem ser construídas com o entendimento, por escrito, se necessário, de que as informações sejam compartilhadas para melhorar a segurança do produto e a segurança do paciente e que as informações compartilhadas não devem ser usadas para obter uma vantagem comercial. Uma maneira de incentivar o compartilhamento de informações é oferecer a possibilidade de compartilhamento anônimo.

6.3. Divulgação coordenada de vulnerabilidades

A transparência é um componente essencial da cibersegurança porque é difícil garantir o que não é conhecido. Um mecanismo que aumenta a transparência é a Divulgação Coordenada de Vulnerabilidades, do inglês, *Coordinated Vulnerability Disclosure* (CVD). A CVD estabelece processos formalizados para obter informações sobre vulnerabilidades de cibersegurança, avaliar vulnerabilidades, desenvolver mitigações e controles compensatórios e divulgar essas informações a vários intervenientes - incluindo clientes, pares (outras empresas), reguladores governamentais, organizações de compartilhamento de informações de cibersegurança e o público.

A adoção de políticas e procedimentos de CVD é uma abordagem proativa que permite que os usuários finais das tecnologias afetadas tomem decisões baseadas em suficiente conhecimento sobre as ações que podem ser adotadas para proteger melhor seus dispositivos médicos, a infraestrutura de TI na saúde e pacientes.

O envolvimento no processo de CVD é um mecanismo responsável por aumentar a conscientização sobre questões de segurança e deve ser visto como um sinal da maturidade de um fabricante relacionado à melhoria contínua da qualidade e ao gerenciamento de riscos, conforme observado em outros setores da indústria.

Embora uma postura vanguardista em relação à CVD seja um sinal de comportamento corporativo proativo e responsável, houve vários casos infelizes de fabricantes de dispositivos médicos enfrentando publicidade negativa como consequência da adoção dessas boas práticas. Como boa prática, a CVD deve ser realizada como uma regra e não como uma exceção, e os intervenientes em dispositivos médicos são incentivados a perguntar aos fabricantes sobre suas políticas de CVD para catalisar ainda mais a sua adoção.

6.3.1. Fabricantes de dispositivos médicos

À medida que o ecossistema de dispositivos médicos continua amadurecendo, os benefícios de se comportar de maneira transparente serão mais plenamente reconhecidos. A divulgação transparente é de extrema importância, protegendo preventivamente o público contra possíveis danos em vários produtos comercializados que podem ser afetados pela mesma vulnerabilidade. Os fabricantes também se beneficiam diretamente do comportamento transparente, pois permitem um projeto de segurança aprimorado para novos produtos. Prestadores de serviços de saúde e pacientes devem estar cientes de que as CVD dos fabricantes, por meio de equipes de resposta de questões computacionais - tais como CERT e CSIRT - ou reguladores do governo, são fontes primárias de informações sobre vulnerabilidades. Pode haver diferenças entre os países em relação a se, como e quando o regulador se comunica como parte da CVD. No entanto, espera-se que os fabricantes desenvolvam e distribuam informações por meio de boletins para usuários, notificações ou outros meios, de forma tempestiva, após a avaliação do assunto. Os fabricantes devem estar cientes dos requisitos jurisdicionais específicos em relação às comunicações tempestivas.

Nenhum dispositivo médico ativado por *software* está completamente livre de vulnerabilidades e, como tal, o envolvimento em CVD deve fazer parte da prática rotineira. Não é o número de vulnerabilidades que serve como um indicador da postura de cibersegurança de um fabricante, mas a consistência e a oportunidade com que responde. Portanto, CVD deve fazer parte da abordagem proativa dos fabricantes quanto à cibersegurança de dispositivos médicos, pois ajuda a melhorar a saúde e a segurança dos pacientes. No que se refere a uma CVD proativa, os fabricantes devem:

- Monitorar as fontes de informações de cibersegurança para identificação e detecção de vulnerabilidades de cibersegurança e riscos.
- Adotar política e práticas de divulgação coordenadas de vulnerabilidades (por exemplo, ISO/IEC 29147:2014: *Information Technology – Security Techniques – Vulnerability Disclosure*). Isso inclui confirmar o recebimento do relatório inicial de vulnerabilidade a quem encontra vulnerabilidades dentro de um período especificado.
- Estabelecer e comunicar processos para entrada e tratamento de vulnerabilidades (ISO/IEC 30111: 2013: *Information Technology – Security Techniques – Vulnerability Handling Processes*). Esses processos são claros, consistentes e reproduzíveis, independentemente da fonte de origem da vulnerabilidade (por exemplo, pesquisador de segurança ou prestador de serviço de saúde etc.).
- Avaliar as vulnerabilidades relatadas de acordo com as metodologias de avaliação de segurança estabelecidas (por exemplo, CVSS) e clínicas (por exemplo, ISO 14971:2019).
- Desenvolver uma correção, se possível. Se não for possível, desenvolver medidas para a mitigação adequada de vulnerabilidades e/ou controles compensatórios com os meios estabelecidos para relatar falhas de implantação e reverter alterações.
- Interagir com os reguladores internacionais da área da saúde, incluindo a Anvisa, quando necessário, para que eles tenham conhecimento das próximas divulgações de vulnerabilidades.
- Comunicar uma descrição da vulnerabilidade aos intervenientes, incluindo escopo, impacto, avaliação de risco com base no entendimento atual do fabricante e descrever as mitigações da vulnerabilidade e/ou controles compensatórios. Os intervenientes também devem ser atualizados conforme a situação muda de figura.

Além de suas próprias comunicações com os clientes, os fabricantes são incentivados a coordenar mundialmente a divulgação de suas vulnerabilidades. Os CERT e organizações equivalentes geralmente

trabalham em colaboração com quem encontra as vulnerabilidades e com o fabricante durante todo o processo de CVD. Em particular, os CERT frequentemente desempenham importante papel na divulgação pública por meio de recomendações globais e regionais traduzidas para as línguas locais. Para obter mais informações sobre CVD, consulte o Guia CERT® de Divulgação Coordenada de Vulnerabilidades (*CERT® Guide to Coordinated Vulnerability Disclosure*).

6.3.2. Anvisa

A Anvisa pode ajudar a apoiar a coordenação do processo de avaliar e estimar a vulnerabilidade, a análise de impacto, mitigação e correção entre o fabricante e quem encontra as vulnerabilidades, que, em última análise, pode levar a uma comunicação tempestiva ao público, a fim de reduzir o risco de que as vulnerabilidades sejam exploradas. Essa comunicação inclui comunicações globais simultâneas, conforme o caso, uma vez que a CVD é reconhecida como uma prática recomendada.

6.3.3. Aqueles que encontram vulnerabilidades (inclui pesquisadores da área de segurança e outros)

As vulnerabilidades, quando identificadas, devem ser relatadas diretamente ao fabricante ou a um coordenador terceiro, como uma entidade governamental. O fabricante, em seguida, coordena e se comunica com aquele que encontrou a vulnerabilidade, durante todo o processo de avaliação e implementação da correção. Por fim, quem identificou a vulnerabilidade e o fabricante devem coordenar a divulgação da vulnerabilidade publicamente. Desde que o fabricante concorde com quem identificou a vulnerabilidade e não haja nenhuma evidência de um ataque a utilizando, a divulgação coordenada requer que quem a identificou não a divulgue até que uma solução ou uma medida de correção esteja disponível. Se quem a identificou revela a vulnerabilidade antes de uma correção, ele e o fabricante devem ao menos coordenar a descrição de uma gama completa de possíveis medidas de mitigação, colocando os usuários, incluindo serviços de saúde e/ou pacientes, numa posição mais empoderada para operar seus dispositivos com segurança ao paciente/usuário e de forma segura.

6.4. Correção de vulnerabilidades

Ações associadas à correção da vulnerabilidade são essenciais para reduzir o risco de danos ao paciente. As correções podem incluir uma ampla gama de ações, incluindo notificações ao paciente. Como tal, vários grupos de intervenientes desempenham papéis críticos nesse processo e esses papéis são descritos em mais detalhes abaixo.

6.4.1. Fabricantes de dispositivos médicos

6.4.1.1. Gerenciamento de riscos

A primeira fase de qualquer resposta a uma vulnerabilidade de cibersegurança em um dispositivo médico é a avaliação de riscos. O gerenciamento de riscos descrito na norma ISO 14971:2019 é uma prática bem estabelecida e madura no setor de dispositivos médicos. Essa prática deve ser aplicada à avaliação do risco de cibersegurança de uma vulnerabilidade e, em seguida, para determinar o impacto na segurança do paciente por fabricantes e Anvisa, estabelecendo um processo de gerenciamento de risco de cibersegurança vinculado ao gerenciamento de risco do produto. Uma estratégia de correção que está bem fundamentada no contexto da segurança do paciente pode então ser desenvolvida e acordada. Para induzir a eficácia desta abordagem, a informação deve ser compartilhada entre fabricantes e a Anvisa e, especialmente no que diz respeito ao risco

percebido e a necessidade da ação, quando for o caso. No entanto, uma vez que a saída da avaliação de risco informa a priorização e o momento da correção, caso a percepção de risco entre fabricantes e Anvisa difiram significativamente, é improvável que estes concordem com uma estratégia de correção para o caso.

Os fabricantes e a Anvisa também precisam levar em consideração o risco percebido por outros intervenientes que possam estar menos familiarizados com o gerenciamento de riscos, a gestão da qualidade e a regulação. Isso pode levar a diferentes expectativas sobre como o fabricante deve responder a uma vulnerabilidade de segurança e dentro de uma janela de tempo. Similarmente, alguns intervenientes podem não entender os mecanismos de redução de risco como controles compensatórios, que podem ser implantados para proteger suficientemente um dispositivo vulnerável, reduzindo assim o risco de danos ao paciente para um nível aceitável. Informações imprecisas que superdimensionam o risco para os pacientes podem criar uma crise de confiança nas tecnologias em saúde.

Todos os intervenientes precisam reconhecer que, assim como outros riscos relacionados a dispositivos médicos, as vulnerabilidades de cibersegurança são gerenciadas de acordo com o risco que representam para pacientes e usuários.

6.4.1.2. Componentes de terceiros

Os componentes de terceiros são uma parte essencial da cadeia de suprimentos de dispositivos médicos, sejam eles *software* ou *hardware*. Esses componentes podem criar riscos próprios, que são gerenciados pelo fabricante por meio do gerenciamento de riscos, gestão da qualidade e escolhas no projeto. Fabricantes devem gerenciar as implicações de cibersegurança dos seus componentes de *software* e de *hardware*. Da mesma forma, problemas pós-mercado com um componente de terceiros também podem afetar a segurança do dispositivo médico e os fabricantes precisam gerenciar esse risco. Os usuários esperam que o fabricante entenda como uma vulnerabilidade de segurança em um componente subjacente, como um sistema operacional ou processador, afeta o dispositivo médico.

A resposta dos fabricantes a uma vulnerabilidade em um componente de terceiros deve ser a mesma das vulnerabilidades de componentes próprios, a saber, o gerenciamento contínuo de riscos e compartilhamento de informações com clientes e usuários. Mesmo que seja improvável que os fabricantes detenham o controle sobre o tempo da resolução de uma vulnerabilidade de terceiros (por exemplo, a disponibilidade de uma atualização), ainda se espera que os fabricantes tomem medidas para reduzir os riscos para pacientes e usuários.

6.4.1.3. Comunicação

Conforme discutido em outras seções, é essencial uma comunicação clara e concisa com aqueles que precisam de informações para gerenciar riscos. Além disso, aqueles que gerenciam riscos devem ter conhecimento técnico para entender a gravidade da situação e agir de forma coerente com a situação. A comunicação deve incluir as seguintes informações principais:

- Linha do tempo para a resolução de vulnerabilidades, por exemplo, quando uma correção estará disponível;
- Mecanismo de resolução, por exemplo, como ocorrerá a implantação da medida de correção;
- Pontuação de vulnerabilidade, como uma pontuação CVSS;
- Índice parar explorar uma vulnerabilidade, por exemplo, baixo nível de conhecimento para explorar uma vulnerabilidade;
- Método de explorar uma vulnerabilidade, por exemplo, remoto; e
- Medidas provisórias de mitigação de riscos, por exemplo, que ações devem ser tomadas, incluindo o uso de controles compensatórios, enquanto se aguarda uma resolução mais permanente.

6.4.1.4. Ação corretivas

As ações dos intervenientes dependerão de vários fatores, incluindo o tipo de dispositivo, a jurisdição regulatória, o risco para a segurança dos usuários e ou pacientes e a finalidade pretendida. Portanto, este documento não elabora ações específicas que são esperadas para todos os dispositivos, mas aponta princípios que devem estar subjacentes a todas as ações para correção de vulnerabilidades:

- Conformidade com os requisitos regulatórios locais;
- Adesão aos princípios de segurança do paciente e desempenho essencial;
- Compartilhamento de informações com os intervenientes para reduzir o risco a pacientes e usuários;
- Cooperação dos intervenientes para alcançar a correção acordada; e
- Correção tempestiva, relativa ao risco.

Quando o dispositivo não possui medidas de proteção fundamentais ou inerentes suficientes e as atualizações não são viáveis, alternativas de mitigação de riscos devem ser aplicadas como controles compensatórios. Os exemplos podem incluir a instalação de um *firewall* entre o dispositivo e a rede conectada, ou remover o dispositivo da rede conectada. Em alguns países, esses controles compensatórios são geralmente implementados pelo serviço de saúde com base na informação fornecida pelo fabricante. No Brasil, o detentor da regularização do dispositivo médico é o responsável legal por implementar os controles.

Os reguladores operam de acordo com a legislação de sua jurisdição, o que significa que eles podem impor requisitos específicos antes que a correção possa ser aplicada a dispositivos médicos no seu mercado. Os fabricantes precisam considerar isto ao planejar ações de correção de vulnerabilidades. A Anvisa deve ser informada o quanto antes de modo a não impedir ou retardar o prosseguimento das atividades de correção do fabricante. A notificação tempestiva à Anvisa[5] permite que a autoridade reguladora disponha de tempo necessário para iniciar qualquer processo regulatório ou ações necessárias, enquanto, concomitantemente, apoia a uma correção pertinente e auxilia no gerenciamento dos intervenientes e suas expectativas (por exemplo, usuários, mídia, público).

Informações sobre vulnerabilidades de segurança circulam rapidamente em uma economia global e explorações de vulnerabilidades de segurança podem alcançar o mundo todo em segundos. Consequentemente, é necessária uma estratégia coordenada e global para corrigir vulnerabilidades. Se uma vulnerabilidade é corrigida e divulgada em uma jurisdição, mas permanece sem tratamento em outra, ela pode dar uma vantagem ao "adversário" e deixar os pacientes e o setor de serviços em saúde expostos a ataques.

É esperado que os fabricantes, que fornecem para vários mercados, coordenem a divulgação de informações e correções para minimizar letargias. A coordenação do fabricante deve ser estendida para uma comunicação proativa com todos os reguladores onde o produto afetado está sendo distribuído.

Todos os intervenientes precisam reconhecer que a atualização imediata pode não ser possível ou desejável, e que medidas provisórias podem ser críticas para garantir a segurança do paciente e ou usuário. Isso é particularmente importante quando essas medidas devem ser implementadas pelos intervenientes fora do controle direto do fabricante ou da Anvisa. Por exemplo, algumas ações podem ser executadas apenas pelo departamento de TI do hospital. A execução bem-sucedida de estratégias de correção depende muitas vezes do compartilhamento eficaz das informações e do gerenciamento dos intervenientes (incluindo usuários e mídia). É importante observar que a correção, embora ideal, nem sempre é possível e, nesse caso, devem ser aplicadas mitigações de risco e controles compensatórios apropriados.

[5] No Brasil, é compulsória a realização e notificação de ação de campo, conforme regulação sanitária. Mais detalhes em http://portal.anvisa.gov.br/acao-de-campo.

6.4.2. Prestadores de serviços de saúde e pacientes

6.4.2.1. Atualizações

Os pacientes recebem atendimento médico em instalações dos serviços de saúde e no ambiente de serviços de atenção domiciliar. Cada ambiente de uso está associado a considerações exclusivas para atualização.[6] No ambiente de serviço de atenção domiciliar, por exemplo, o usuário pode ser o paciente, cuidador, vizinho de confiança ou um membro da família. Esta seção fornece orientação geral para atualização e as seções subsequentes descrevem considerações específicas para cada ambiente de uso.

A Cláusula 6.2.5 da norma IEC 62304: 2006 +AMD1:2015, *Medical device software — Software life cycle processes* exige que os fabricantes divulguem aos usuários e reguladores qualquer problema no *software* médico lançado e como obter e instalar atualizações. Espera-se que usuários específicos de um dispositivo médico, identificados pelo fabricante e aprovados pela Anvisa, implementem as atualizações fornecidas pelo fabricante de acordo com as instruções de instalação associadas. Esses usuários devem seguir as orientações do fabricante para acessar os boletins de serviço e outras informações normalmente fornecidas em uma página da *web*.

Quando uma atualização não pode ser aplicada dentro de um prazo razoável, o fabricante pode recomendar controles compensatórios (por exemplo, segmentação de uma rede de TI médica) ou alterações nas configurações programáveis pelo usuário do dispositivo médico. Para reduzir o risco de danos ao paciente por certos tipos de vulnerabilidades, a Anvisa pode direcionar o fabricante a desativar funcionalidades específicas do dispositivo médico, acessórios ou do ecossistema que o suporta, como por exemplo, servidores de atualização de *software*. Nos dois casos, os usuários devem seguir as orientações do fabricante e, conforme apropriado, avaliar os riscos associados ao ambiente de uso.[7]

A Tabela 2 é adaptada a partir dos métodos de correção documentados no Plano de Segurança Conjunto.[8] A coluna mais à direita da tabela descreve a principal responsabilidade do usuário identificado por implementar uma atualização aprovada pelo fabricante do dispositivo médico.

Tabela 2 - Métodos de atualização e responsabilidades do usuário na sua implantação

Método de atualização	Descrição resumida	Responsabilidade do usuário
Atualização remota	Atualizações aplicadas por meio de serviço remoto, seguro e autorizado e plataformas de suporte fornecidas pelo fabricante.	Garantir a conectividade remota de acordo com as instruções fornecidas pelo fabricante.
Administrada pelo usuário	As atualizações aprovadas estão disponíveis para recuperação e instalação pelo cliente a partir de uma fonte designada,	Recuperar e instalar a atualização de acordo

[6] IEC 60601-1-11:2015, *Medical electrical equipment — Part 1-11: General requirements for basic safety and essential performance – Collateral Standard: Requirements for medical electrical equipment and medical electrical systems used in the home healthcare environment* define o "ambiente de serviço de atenção domiciliar" como "local de moradia em que um paciente mora ou em outros locais em que estejam presentes, excluindo ambientes de estabelecimentos de serviços de saúde..." e inclui exemplos: "Em um carro, ônibus, trem, barco ou avião, em cadeira de rodas ou caminhando ao ar livre."

[7] É reconhecido que, em determinadas situações, o usuário não pode avaliar adequadamente os riscos.

[8] *Medical Device and Health IT Joint Security Plan*, *Healthcare and Public Health Sector Coordinating Council* (HSCC), janeiro de 2019. Observe que as duas primeiras colunas incorporam pequenas alterações para melhorar a clareza e o método de correção "ad hoc" é removido (somente as correções validadas são consideradas).

Método de atualização	Descrição resumida	Responsabilidade do usuário
	incluindo *download* direto de terceiros que fornecem o produto ou componente.	com as instruções fornecidas pelo fabricante.
Assistência técnica	O estabelecimento da assistência técnica presencial administra as atualizações de cibersegurança (inclui manutenção *in loco*). Observe que esse método é aplicável nos casos em que a atualização incorreta tem danos previsíveis e graves e o pessoal de serviço presencial pode ser necessário para a resolução.	Fornecer o dispositivo médico a um estabelecimento da assistência técnica, dar suporte à assistência técnica *in loco* ou viajar para um de serviço de saúde.

Observe que, para visitas de assistência técnica presencial, o usuário é responsável por interagir com um profissional qualificado para a instalação da atualização.

6.4.2.2. Considerações para o ambiente do serviço de saúde

Nas unidades de saúde do Brasil, os pacientes são atendidos por profissionais de saúde qualificados (por exemplo, enfermeiros, médicos) que devem estar registrados em seus respectivos conselhos de classe em função dos requisitos regulatórios locais. Espera-se que os pacientes sigam as instruções fornecidas pelos serviços de saúde, incluindo aqueles relacionados à segurança, para garantir a operação segura e eficaz de seus dispositivos médicos.

A cláusula 3.2 da IEC 80001-1: 2010, *Application of risk management for IT Networks incorporating medical devices — Part 1: Roles, responsibilities and activities* descreve as competências de gerenciamento de riscos da organização responsável, incluindo a manutenção de dispositivos médicos implantados em uma rede de TI médica. A organização responsável pode ser diferente do prestador de serviço de saúde imediato do paciente. A atualização é um tipo de medida de controle de risco e a Cláusula 4.4.4.3 fornece orientações específicas:

> As medidas de controle de risco no dispositivo médico devem ser implementadas apenas pelo fabricante do dispositivo médico ou pela organização responsável, seguindo as instruções de uso ou com a permissão documentada do fabricante do dispositivo médico. […] Quaisquer alterações em um dispositivo médico realizadas pela organização responsável sem o consentimento documentado do fabricante do dispositivo médico não são recomendadas.

Essas recomendações foram desenvolvidas para garantir o gerenciamento eficiente e seguro das redes de TI médicas. Leigos não devem ser autorizados a instalar atualizações de dispositivos médicos que estão ligados à rede de TI médica.

Conforme destacado na IEC 80001-1, os acordos de responsabilidade são uma opção para garantir que todas as partes entendam a responsabilidade compartilhada de gerenciar dispositivos em uma rede de TI médica. Se um fabricante é instruído a desativar certas funções do dispositivo médico, os prestadores de serviços de saúde devem avaliar seu fluxo de trabalho clínico para garantir que a segurança do paciente seja mantida.

6.4.2.3. Considerações para o ambiente de serviço de atenção domiciliar

O ambiente de serviço de atenção domiciliar acomoda um conjunto diversificado de usuários em potencial, conforme observado nas orientações da FDA, *Design Considerations for Devices Intended for Home Use*:

> Os usuários de dispositivos de uso doméstico são diferentes dos profissionais de saúde que normalmente operam dispositivos médicos em um estabelecimento profissional de saúde. Os usuários domésticos podem ter uma grande variedade de capacidades e deficiências físicas, sensoriais e cognitivas e diferenças emocionais que devem ser consideradas no projeto de dispositivos de uso doméstico.

A aplicabilidade dos métodos de atualização para o ambiente de serviço de atenção domiciliar é uma função de muitos parâmetros, incluindo a classificação de risco de dispositivos médicos, requisitos de recursos subjacentes (por exemplo, conexão à Internet de alta velocidade) e usabilidade. Devido à ampla variedade de necessidades do usuário, muitos dispositivos de uso doméstico exigem o método de atualização da "assistência técnica", listado na Tabela 2. A instalação da atualização para um dispositivo médico implantado pode exigir interação presencial com o prestador do serviço de saúde do paciente.

Alguns dispositivos de uso doméstico, especialmente aqueles classificados como SaMD, acomodam a atualização remota ou os métodos de aplicação de *patches* administrados pelo usuário. As atualizações remotas exigem a menor quantidade de interação do usuário, mas geralmente requerem o consentimento do paciente, de acordo com os processos estabelecidos pelo serviço de saúde. Com qualquer método de atualização, os pacientes devem seguir as instruções fornecidas pelo seu prestador de serviço de saúde e, conforme aplicável, pelo fabricante do dispositivo médico.

Se um paciente pretende viajar para o exterior, deve conversar com seu prestador de serviço de saúde ou fabricante do dispositivo médico para entender as opções de manutenção de *software* para seu dispositivo.

6.4.3. Anvisa

6.4.3.1. Atualizações pós-mercado

Os vetores de ameaças estão constantemente se adaptando e avançando nas técnicas de explorar vulnerabilidades. Como resultado, atividades frequentes de manutenção de *software* são recorrentemente necessárias para aprimorar a resiliência da cibersegurança de um dispositivo ("higiene cibernética"), corrigir vulnerabilidades ou mitigar o risco de vulnerabilidades que não podem ser remediadas. Se cada alteração feita "exclusivamente para fortalecer a cibersegurança" fosse submetida ao mais alto nível de análise regulatória, a carga resultante da análise logo sobrecarregaria a maioria das autoridades reguladoras.

No contexto da cibersegurança, a autoridade reguladora deve estabelecer duas questões fundamentais para determinar se uma alteração de *software* exige aprovação antes do lançamento:

1. A mudança é destinada a apenas fortalecer a cibersegurança e não tem qualquer outro impacto sobre o *software* ou dispositivo?

O fabricante deve avaliar seu sistema para garantir que tais alterações não afetem a segurança ou o desempenho do dispositivo, executando análises, verificações e ou validações necessárias. Se um fabricante tomar conhecimento de qualquer impacto acidental ou não intencional da alteração em outros aspectos do *software* ou dispositivo, em algumas jurisdições, a alteração deverá ser submetida, previamente à autoridade reguladora e esta decidir pelo processo regulatório apropriado.

2. A alteração visa corrigir ou reduzir o risco de uma vulnerabilidade associada a um risco residual inaceitável vinculado a danos ao paciente?

As avaliações pós-mercado de risco de vulnerabilidade devem basear-se na avaliação da potencialidade de explorar uma vulnerabilidade e na gravidade dos possíveis danos ao paciente e são usadas para determinar se o risco residual é aceitável ou inaceitável. Observe que a definição de "dano ao paciente" é um subconjunto do "dano", conforme definido na ISO 14971:2019, *Medical devices — Application of risk management to medical devices.*[9] A definição estrita de dano ao paciente tem o efeito líquido de permitir o tratamento excepcional da análise regulatória das alterações necessárias para proteger a saúde pública.

A Tabela 3 apresenta o arcabouço adotado pela Anvisa para o controle regulatório necessário para os vários tipos de atividades de manutenção de *software*. Observa-se que os níveis apresentados nesta tabela fornecem os seus respectivos procedimentos de supervisão regulatória. Isto é, o fabricante reportará as alterações à Anvisa somente quando o nível dos requisitos regulatórios for alto e em dois possíveis procedimentos:

1. Aprovação requerida, caso haja alteração de *software* de classe de risco III ou IV com novas indicações e funcionalidades.
2. Implementação imediata, caso contrário.

Tabela 3 - Atualizações de software e nível recomendado de controle regulatório

Objetivo da atualização		**Nível dos Requisitos Regulatórios**	**Exemplos**	**Procedimento a cerca de Alterações (RDC 340/2020)**
Melhorar a segurança (cibersegurança)		Baixo	Um fabricante de aplicativo ("app") SaMD é informado de uma atualização do sistema operacional subjacente que adiciona controles de segurança para suportar uma estratégia de defesa em profundidade. O aplicativo SaMD requer que a modificação seja compatível com alterações na interface de baixo nível no sistema operacional subjacente. As modificações associadas do aplicativo SaMD não estão relacionadas a nenhuma vulnerabilidade conhecida.	Não reportável
Correção de vulnerabilidade ou estratégia de redução de risco para vulnerabilidades que não podem ser corrigidas	Risco residual aceitável de danos ao paciente	Médio	Um fabricante de dispositivo recebe uma reclamação do usuário de que um analisador de gases no sangue foi infectado por *malware* e houve uma preocupação de que o *malware* possa alterar os dados no dispositivo. O resultado de uma investigação e avaliação de impacto do fabricante confirma a presença de *malware* e descobre que o *malware* não resulta na manipulação de dados não criptografados armazenados e fluindo através do dispositivo. A segurança do paciente e o desempenho essencial do dispositivo não são afetados pelo *malware* e a avaliação de risco do fabricante determina que o risco de	Não reportável

			danos ao paciente devido à vulnerabilidade é aceitável.[9]	
	Risco residual inaceitável de danos ao paciente	Alto	Um fabricante é informado que há portas de comunicação abertas e não utilizadas. O fabricante reconhece o recebimento do relatório de vulnerabilidade para quem encontrou a vulnerabilidade e a análise subsequente determina que as funcionalidades projetadas do dispositivo não impedem que uma ameaça baixe *firmware* não autorizado no dispositivo, o que pode ser usado para comprometer a segurança e o desempenho essencial do dispositivo. Embora não haja relatos de eventos adversos graves ou mortes associadas à vulnerabilidade, a avaliação de risco conclui que o risco de danos ao paciente é inaceitável.[10]	Aprovação requerida, caso haja alteração de *software* de classe de risco III ou IV com novas indicações e funcionalidades Implementação imediata, caso contrário.

Se a mudança proposta do *software* afetar várias vulnerabilidades ou, alternativamente, melhorar a "higiene cibernética" e afetar pelo menos uma vulnerabilidade, o fabricante deverá considerar o nível mais alto aplicável na Tabela 3 para informar as ações subsequentes. Por exemplo, uma única alteração de *software* pode aumentar a segurança do sistema, reduzir o risco de vulnerabilidade A (risco residual aceitável de dano ao paciente) e corrigir a vulnerabilidade B (risco residual inaceitável de dano ao paciente). Nesse caso, o nível alto de requisitos regulatórios associados à vulnerabilidade B seria a aplicável.

Para qualquer nível, a autoridade reguladora pode, a seu critério, solicitar evidências de que o fabricante está seguindo os processos estabelecidos do ciclo de vida e outros requisitos regulamentares para a manutenção do *software*, incluindo os identificados na norma IEC 62304:2006/AMD 1:2015.

6.5. Resposta a incidentes

6.5.1. Fabricantes de dispositivos médicos

Os fabricantes de dispositivos médicos devem se preparar para responder a incidentes e eventos de cibersegurança que possam afetar seus produtos e clientes, incluindo pacientes. Como tal, os fabricantes devem estabelecer uma política de gerenciamento de resposta a incidentes que possa ser escalável e criar uma equipe de resposta a incidentes com base em seu portfólio de produtos. O objetivo de uma equipe de resposta a incidentes é fornecer poder adequado para a avaliação, respondendo e aprendendo com incidentes de cibersegurança, e fornecer a coordenação, gestão, feedback e comunicação necessários, para a ação tempestiva e pertinente no próximo incidente.

A preparação inclui estabelecer uma política de gerenciamento de incidentes, desenvolver planos detalhados de resposta a incidentes, formar uma equipe de resposta a incidentes, testar e exercitar rotineiramente a resposta a incidentes e melhorar continuamente esse recurso por meio das lições aprendidas.

[9] Adaptado dos exemplos fornecidos em *Guidance for Industry and Food and Drug Administration Staff*, *Postmarket Management of Cybersecurity in Medical Devices*. Dezembro de 2016.
[10] Ibid.

Gerenciamento de incidentes, conforme definido na norma ISO/IEC 27035 inclui, em alto nível, o seguinte[11]: planejar e preparar, detectar e reportar, avaliar e decidir, responder e registrar as lições aprendidas. Cada tópico está detalhado no Apêndice A: Funções de resposta a incidentes (Norma ISO IEC 27.035).

6.5.1.1. Papéis e responsabilidades

A equipe de resposta a incidentes pode ser dividida nos seguintes grupos: gerência, planejamento, monitoramento, resposta, implementação, análise, e, por vezes, especialistas externos. Cada grupo tem diferentes papéis e responsabilidades. A equipe deve designar membros para esses grupos com base em suas habilidades e conhecimentos e algumas das posições podem ser preenchidas por mais de um membro da equipe. Os membros designados para os grupos relevantes devem ser responsáveis pelo mesmo trabalho ou trabalho semelhante. Informações mais detalhadas sobre as funções desses grupos são fornecidas no Apêndice A: Funções de resposta a incidentes (Norma ISO IEC 27.035).

6.5.1.2. Expectativas de comunicação

Os clientes devem receber informações de contato do fabricante do dispositivo médico para relatar incidentes e eventos de cibersegurança, bem como ser orientados a submeter os relatos por meio de canais regulares de suporte ao cliente. A equipe de resposta a incidentes deve estabelecer uma rotina compassada para fornecer atualizações a todos os intervenientes afetados por um incidente e trabalhar no sentido de fornecer comunicações direcionadas ao cliente o mais precocemente, após a identificação inicial de incidentes e eventos de cibersegurança. Destaca-se que os fabricantes devem estar cientes dos requisitos jurisdicionais específicos em relação às comunicações tempestivas. Atingir o prazo supramencionado para boletins ou notificações do fabricante durante incidentes pode depender de comunicação tempestiva e precisa com os clientes.

No Brasil, é compulsória a realização e notificação de ação de campo, conforme regulação sanitária. Os incidentes de cibersegurança de dispositivos médicos que afetam a segurança do paciente e ou do usuário e a sua privacidade devem ser relatados à Tecnovigilância da Anvisa. Mais detalhes em http://portal.anvisa.gov.br/acao-de-campo. Quando a atividade criminosa for identificada no curso da investigação, os organismos policiais locais e aplicáveis devem ser notificados. CERT e ISAO devem ser contatados para uma maior coordenação em ataques e eventos de cibersegurança globais.

6.5.2. Serviços de saúde

Os serviços de saúde devem estabelecer políticas para lidar com incidentes de segurança e mecanismos para mitigar ou resolver um incidente de segurança e divulgar as informações relacionadas para intervenientes internos e externos. Para este propósito, os serviços de saúde devem considerar o planejamento e o gerenciamento de recursos para mitigar as vulnerabilidades do dispositivo. Isto possivelmente inclui garantir que dispositivos sobressalentes ou partes extras estejam disponíveis, se necessário, durante um incidente.

6.5.2.1. Política e funções

Políticas e papéis do gerenciamento de vulnerabilidade ou incidentes de segurança devem ser efetivos nos serviços de saúde. Essas políticas devem estabelecer o modo como os serviços de saúde receberão e disseminarão informações dos documentos de divulgação do fabricante , como por exemplo, a Declaração de

[11] Para maiores informações, consultar o item 6.5.1.1. Papéis e responsabilidades.

Divulgação de Informações do Fabricante para a Segurança de Dispositivos Médicos (MDS2), SBOM e informações de vulnerabilidade/atualizações, bem como informações de instituições que compartilham informações ou de participantes de ISAO. Para este fim, deve ser mantida e verificada periodicamente uma lista de pontos de contatos para informar e ser informado. Da mesma forma, os acordos de nível de serviço (ANS), estabelecidos antes da instalação e revisados periodicamente, fornecem os termos contratuais que os fabricantes e outros fornecedores são obrigados a cumprir, durante ou em resposta a um incidente. Os serviços de saúde são incentivados a estabelecer sua própria equipe de resposta a incidentes de segurança.

6.5.2.2. Treinamento por funções

Os requisitos para o treinamento de cada papel relevante devem ser estabelecidos e revisados periodicamente para determinar se precisam ser atualizados. Os especialistas em segurança que avaliam evidências de incidentes de segurança devem receber treinamento em análise forense de segurança, além de experiência prática. Aqueles que participam do processo de resposta a incidentes devem ser treinados nesse processo e na teoria de resposta a incidentes, além da experiência prática. Os processos de treinamento devem ser avaliados periodicamente e podem ser realizadas simulações - exercício de resposta a um incidente - para realizar essa avaliação.

6.5.2.3. Análise e resposta

Os serviços de saúde devem avaliar o impacto de qualquer incidente ou vulnerabilidade relatada e cooperar com os intervenientes, incluindo o fabricante do dispositivo médico, fornecendo informações que descrevem o resultado de qualquer investigação. Quando são necessárias ações para a resolução, o status da investigação e seu cronograma devem ser incluídos no resultado. Os serviços de saúde devem manter os pacientes atualizados com informações relacionadas com a segurança do paciente, incluindo as boas práticas e medidas de mitigação. Quando a resolução inclui correção, a validação, incluindo o teste de regressão, deve ser realizada antes de aplicar a correção a todo o estabelecimento. Aqueles testes devem garantir que a correção não interrompa a funcionalidade do sistema existente. Os serviços de saúde devem atualizar a informação sobre a correção e a mitigação, quando necessário.

6.5.3. Reguladores de dispositivos médicos

A Anvisa também deve estar envolvida na resposta a incidentes de cibersegurança de dispositivos médicos. Conforme observado na seção de resposta dos fabricantes (6.5.1 Fabricantes de dispositivos médicos), a Anvisa deve ser notificada sobre incidentes de cibersegurança, para que esteja ciente, possa solicitar informações adicionais para a tomada de decisões regulatórias e tomar ações adicionais, quando necessário. Conforme o caso, ações adicionais podem incluir, entre outras, a avaliação do impacto na segurança do paciente, a avaliação do benefício/risco da mitigação proposta pelo fabricante, a comunicação com os intervenientes (incluindo partes interessadas não tradicionais, tais como pesquisadores de cibersegurança) e o envolvimento de outras agências governamentais e reguladores internacionais da área da saúde.

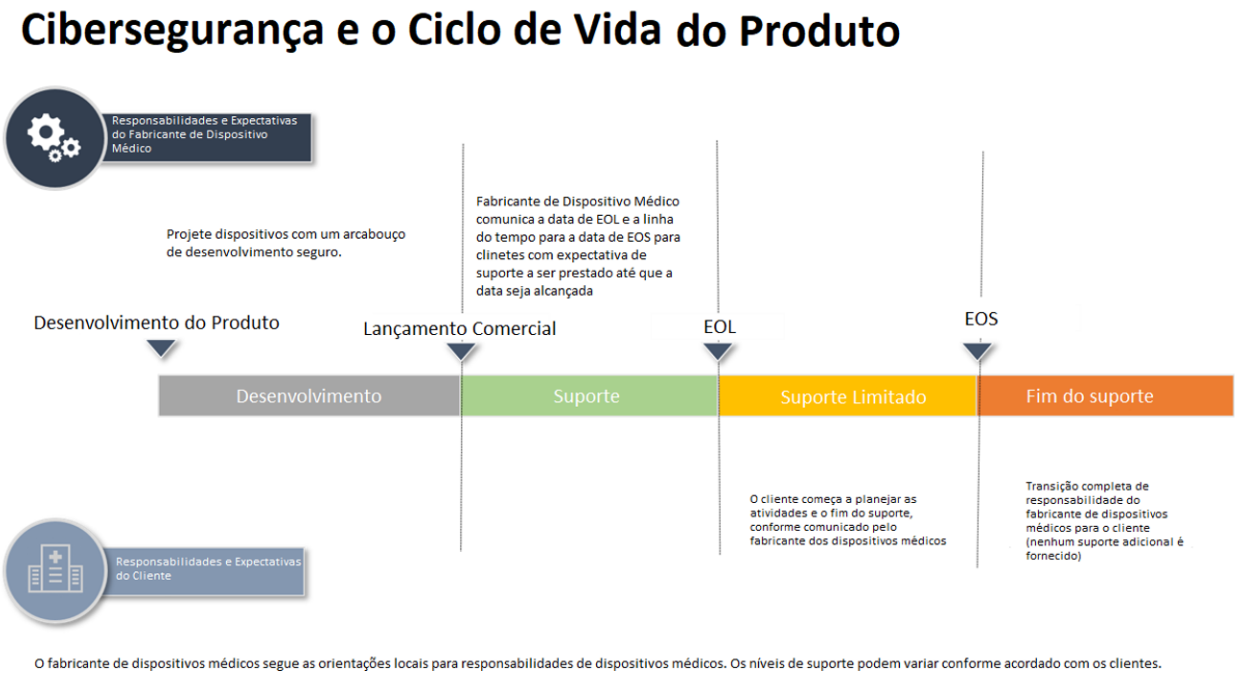
6.6. Dispositivos médicos legados

Para os fins deste guia, os dispositivos médicos que não podem ser razoavelmente protegidos (por atualizações e ou controles compensatórios) contra as ameaças de cibersegurança atuais são considerados dispositivos legados. A condição de legado representa um desafio especialmente complexo para o presente estado do ecossistema de serviços de saúde a nível mundial, pois a cibersegurança do dispositivo pode não ter sido considerada na fase inicial do seu projeto e mantida para muitos dispositivos em uso atualmente. O desafio é

ainda agravado pelo fato de que a utilidade clínica de um dispositivo muitas vezes supera a sua capacidade de suporte à segurança, enquanto a transformação para a tecnologia digital de dispositivos médicos ofereceu funcionalidade expandida que nunca poderia ter sido realizada em dispositivos analógicos mais antigos. Embora benéfica ao cuidado do paciente, a combinação de *software*, *hardware* e conectividade de rede nessas tecnologias impõem novas demandas sobre a vida útil do dispositivo, que geralmente consiste em equipamentos de capital (por exemplo, *hardware* de scanner), assim como componentes básicos (por exemplo, servidores, estações de trabalho, bancos de dados e sistemas operacionais). É importante observar, no entanto, que a idade do dispositivo não é o único determinante do status de legado. Em outras palavras, um dispositivo que não pode ser razoavelmente protegido contra as ameaças atuais de cibersegurança pode ter menos de cinco anos; independentemente de sua idade, este dispositivo ainda seria considerado legado. Por outro lado, um dispositivo pode ter 15 anos, mas se mantiver a capacidade de estar razoavelmente protegido contra as ameaças atuais de cibersegurança, não será considerado legado.

À medida que os esforços para abordar o TPLC da cibersegurança de dispositivos médicos continuam a avançar a partir do estágio inicial de projeto e desenvolvimento de dispositivos, a disponibilidade de dispositivos que mantêm a capacidade de proteção razoável contra ameaças à cibersegurança ao longo de sua vida útil se tornará cada vez mais a regra, e o desequilíbrio observado em relação à multiplicidade de dispositivos legados no uso clínico atual - representando uma ameaça à segurança dos serviços de saúde e suas redes - diminuirá. As subseções a seguir deste guia articulam um arcabouço conceitual que conduz a um estado futuro ideal de cibersegurança de dispositivos médicos, no qual dispositivos legados (aqueles que não podem ser razoavelmente protegidos contra as ameaças atuais de cibersegurança) são descontinuados/desativados, com notificação adiantada adequada para os serviços de saúde, de modo a permitir o planejamento da continuidade dos negócios (Figura 2).

Figura 2 - Arcabouço conceitual do dispositivo legado em função do ciclo de vida do produto para a cibersegurança



6.6.1. Fabricantes de dispositivos médicos

A atenção para a cibersegurança de dispositivo médico inicia na fase de elaboração do projeto e desenvolvimento do dispositivo, bem antes do lançamento comercial, como mostrado na Figura 2. O alinhamento com o arcabouço TPLC e o suporte completo de dispositivos médicos para assegurar uma proteção

razoável contra ameaças de cibersegurança atuais devem continuar além da data de fim de vida (EOL) publicada pelo fabricante. A data de EOL de cibersegurança do fabricante significa capacidade reduzida de fornecer suporte abrangente à cibersegurança do dispositivo médico. Ao se aproximar da data de EOL de cibersegurança, o fabricante deve enviar um comunicado para seus clientes, notificando-os do suporte limitado que permanece disponível além da data de EOL, com comunicação clara da data de término do suporte (EOS) da cibersegurança do dispositivo. Não deve ser esperado suporte para nenhum dispositivo médico após a data estabelecida de EOS de cibersegurança.

De acordo com esse arcabouço conceitual, quando um dispositivo médico atinge sua data de EOS de cibersegurança, é considerado um dispositivo médico legado que não pode ser razoavelmente protegido contra as ameaças atuais de cibersegurança e deve ser descontinuado/desativado. A responsabilidade por manter a segurança do dispositivo e assumir riscos por seu uso após a data de EOS seria transferida nesse momento, para o cliente, por exemplo, os serviços de saúde.

É importante observar que, embora as alterações de projeto em alguns dispositivos possam não ser viáveis (por exemplo, um sistema operacional obsoleto que não é mais suportado e não pode ser corrigido por motivos de segurança), os controles compensatórios podem fornecer algum nível de proteção. Na presença de controles compensatórios disponíveis e implantados com sucesso, o dispositivo médico não seria considerado legado por este arcabouço. Conforme o caso, a Anvisa pode incentivar os fabricantes de dispositivos médicos a alavancar os controles compensatórios para enfrentar os desafios atuais de segurança de dispositivos após a data de EOL, para dar tempo suficiente aos serviços de saúde conduzirem o planejamento de continuidade de negócios para a data de EOS, quando não houver mais suporte de segurança disponível do fabricante. O projeto de dispositivos, o gerenciamento de vulnerabilidades e as comunicações com os clientes desempenham um papel importante no tratamento dos desafios de cibersegurança dos dispositivos. As recomendações para os fabricantes em função do estágio do ciclo de vida do dispositivo incluem o seguinte:

- Desenvolvimento:

    a. Levar em consideração o ciclo de vida do suporte de componentes de *hardware* e *software* que compõem o dispositivo médico. Para fornecer suporte abrangente a um dispositivo médico, o fabricante deve poder obter suporte dos fornecedores de *hardware* e *software* correspondentes, por meio de atualizações de *software*/*firmware* que tratam de questões de qualidade, desempenho e segurança. Um fabricante deve antecipar a necessidade de apoiar a segurança do paciente e a eficácia de um produto ao longo de seu uso. O fabricante deve considerar que o suporte de um fornecedor de terceiros a um componente pode terminar dentro da vida útil projetada do dispositivo e isso pode afetar negativamente a capacidade do fabricante de oferecer suporte à operação segura do dispositivo.
    b. Projetar e desenvolver dispositivos sob um arcabouço de desenvolvimento seguro para minimizar o número de dispositivos legados no futuro. Esses dispositivos, no mínimo, devem atender a uma base de referência de segurança e incluir mecanismos para atualizações e *patches*.

- Suporte:

    a. Monitorar dispositivos médicos em busca de vulnerabilidades com risco inaceitável e fornecer uma resposta com o melhor esforço possível e manter a documentação de riscos continuamente alinhada ao ciclo de vida do produto como parte do gerenciamento de riscos.
    b. Comunicar, claramente, marcos-chave do ciclo de vida, incluindo datas de EOL de cibersegurança de dispositivos como parte dos processos de aquisição e instalação - responsabilidades do cliente devem ser integradas às comunicações em todos esses momentos.
    c. Notificar proativamente clientes sobre as datas de EOS de fornecedores terceiros dos componentes do dispositivo.
    d. Publicar alerta ao cliente que sinaliza o suporte em curso, mas limitado até a data de EOS de cibersegurança. Após essa data, o dispositivo seria considerado sem suporte e em um estado de

legado. O momento desse comunicado ao cliente deve ocorrer ao se aproximar da data de EOL e permitirá um aviso adiantado para descontinuação/desativação do dispositivo e o planejamento de continuidade de negócios para os serviços de saúde. A comunicação clara ajuda as organizações de serviços de saúde a entender suas responsabilidades e os riscos do dispositivo, para que possam planejar a desativação do equipamento, a substituição e o orçamento do dispositivo de acordo com o caso.

- Suporte limitado (data de EOL começa aqui):

    a. Continuar a comunicar a linha do tempo para as datas de EOS de cibersegurança, para permitir tempo suficiente para os clientes se prepararem para a data de EOS e as responsabilidades associadas.
    b. Dar continuidade às ações "a" e "c" da fase de Suporte do ciclo de vida, acima.

- Fim do suporte (o legado começa aqui):

    a. Transferência total de responsabilidade do fabricante para o cliente. Após a data de EOS formal de cibersegurança do dispositivo, os usuários de dispositivos não devem esperar qualquer nível de suporte.

6.6.2. Serviços de saúde

Muitos serviços de saúde planejam o uso do dispositivo por muito mais tempo do que a vida útil fornecida pelo fabricante na data de EOL de cibersegurança divulgada. No entanto, à medida que o cenário de ameaças muda com o tempo e novas ameaças surgem, o risco e os custos do uso de tecnologia desatualizada aumentam e devem ser contabilizados por meio de uma responsabilidade compartilhada entre o fabricante do dispositivo médico e o serviço de saúde. As recomendações, a seguir, em função da fase do ciclo de vida do dispositivo, podem ajudar a tratar os desafios dos serviços de saúde com dispositivos médicos, para planejar com antecedência uma data bem definida de EOS de cibersegurança:

- Suporte:

    a. Solicitar pontos de contato e processos de comunicação claros com os fabricantes de dispositivos para assegurar o planejamento, entendimento e a transparência do ciclo de vida do produto.
    b. Solicitar uma SBOM, pois os componentes de *software* com o menor ciclo de vida do suporte afetarão a capacidade de suporte e a segurança desses dispositivos. A obtenção de um SBOM ajuda o cliente a entender melhor os componentes que afetam o ciclo de vida do dispositivo e pode incluir informações de *hardware* adicional para medidas de controle de riscos, como controles compensatórios.
    c. Garantir apoio adequado e manutenção de seus dispositivos médicos enquanto estiverem em uso, seja por meio do fabricante de dispositivos médicos, agentes de serviços de terceiros ou de recursos e controles internos. Isto inclui suporte adequado à segurança da rede, segurança de ativos, gerenciamento de identidade e acesso e operações de segurança.
    d. Avaliar os riscos novos e em evolução no seu ambiente e unir todos os esforços para controlar os riscos por meio de mitigações adequadas, incluindo, mas não limitando à segmentação de rede, funções de acesso do usuário, avaliação de riscos, testes de segurança, monitoramento de rede etc.
    e. Planejar com antecedência a data de EOS de cibersegurança do fabricante, para que um dispositivo legado sem suporte (que possa comprometer a segurança do paciente e a segurança da rede do serviço de saúde) possa ser adequadamente eliminado e substituído por um dispositivo médico protegido e com suporte.

- Suporte limitado:

a. Continuar as ações "c", "d" e "e" na fase de Suporte do ciclo de vida do dispositivo, acima.

- Fim do suporte:

a. Aceitar a responsabilidade pelo gerenciamento da segurança do dispositivo e assumir o risco de segurança pelo uso contínuo além da data de EOS de cibersegurança, se não for possível descontinuar/desativar o dispositivo sem afetar a continuidade dos cuidados ao paciente.

7. APÊNDICES

7.1. Apêndice A: funções de resposta a incidentes (da norma ISO/IEC 27035)

Gerenciamento de Incidentes – ISO/IEC 27035	
Planejar e preparar	Estabelecer uma política de gerenciamento de incidentes de segurança da informação, formar uma equipe de resposta a incidentes etc.
Detectar e reportar	Alguém precisa identificar e relatar eventos que podem ser ou se transformar em incidentes.
Avaliar e decidir	Alguém deve avaliar a situação para determinar se é de fato um incidente.
Responder	Conter, erradicar, recuperar e analisar forensicamente o incidente, quando for o caso
Lições aprendidas	Fazer melhorias sistemáticas no gerenciamento de riscos de informações da organização como consequência de incidentes experimentados.

Equipe de resposta a incidentes		
Funções	**Responsabilidades**	**Principais ações**
Gerente	Lidera e toma decisões sobre questões importantes relacionadas à resposta a incidentes de cibersegurança	a) comprometer-se e apoiar a resposta a incidentes, incluindo o fornecimento dos recursos necessários (mão de obra, financeira e material); b) revisar e aprovar políticas e planos de resposta a incidentes e supervisar a implementação; c) revisar e criticar os planos de resposta a incidentes; d) coordenar internamente e externamente a equipe.
Grupo de Planejamento	Opera a resposta a incidentes	a) estabelecer e planejar políticas de segurança; b) implementar processos de segurança; c) ajustar as prioridades de risco; d) comunicar com organizações de nível superior e outras organizações de terceiros; e) apoiar a administração; f) discutir/registrar/aprovar relatórios de vulnerabilidade nas organizações alvo; g) realizar outras atividades dirigidas pelo gerente.
Grupo de Monitoramento	Executa as atividades de monitoramento de segurança em tempo real	a) monitorar e operar diariamente; b) detectar a intrusão, registrar incidentes e executar as primeiras respostas; c) executar as atualizações de segurança;

		d) implementar política de segurança e gerenciamento de cópia de segurança; e) realizar suporte técnico; f) gerenciar instalações; g) realizar outras atividades dirigidas pelo gerente.
Grupo Respondente	Fornece serviços como respostas em tempo real, suporte técnico	a) propagar e informar incidentes; b) analisar correlação entre sistemas de monitoramento; c) apoiar investigação e recuperação de incidentes; d) analisar vulnerabilidade no incidente alvo; e) realizar outras atividades dirigidas pelo gerente.
Grupo de Implementação	Executa a ação total da resposta a incidentes	a) analisar os requisitos de resposta a incidentes; b) determinar políticas e níveis de resposta a incidentes; c) implementar políticas e planos de resposta a incidentes; d) projetar planos de resposta a incidentes; e) resumir o trabalho e o relatório de resposta a incidentes; f) implantar e usar os recursos de resposta a incidentes; g) realizar outras atividades dirigidas pelo gerente.
Grupo de Análise	Executa análise de incidentes	a) planejar a análise de vulnerabilidade para a equipe; b) aprimorar as ferramentas de análise de segurança e a lista de verificação; c) melhorar as regras de monitoramento; d) publicar boletim informativo; e) realizar outras atividades dirigidas pelo gerente.

7.2. Apêndice B: recursos jurisdicionais para divulgação coordenada de vulnerabilidades

Austrália
CERT Austrália
https://www.cert.gov.au/

AusCERT
https://www.auscert.org.au/

Brasil
Todos os CERTs no Brasil
https://www.cert.br/csirts/brazil/

Canadá

Centro Canadense de Segurança Cibernética
https://www.cyber.gc.ca/

Europa
União Europeia CERT
https://cert.europa.eu

França
ANSM
https://ansm.sante.fr/

https://www.ansm.sante.fr/Declarer-un-effet-indesizable/Votre-declaration-concerne-un-dispositif-medical/Votre-declaration-concerne-un-dispositif-medical/(offset)/0

Ministério da Saúde e Solidariedade da França
https://solidarites-sante.gouv.fr/soins-et-maladies/signalement-sante-gouv-fr/

Agência de Sistemas Compartilhados de Informação em Saúde
https://www.cyberveille-sante.gouv.fr/

ANSSI - Agência Nacional de Segurança de Sistemas de Informação
https://www.ssi.gouv.fr/en/

Alemanha
CERT Alemanha
https://www.cert-bund.de/

Itália
https://www.csirt-ita.it/

Japão
CERT do Japão/Centro de Coordenação (JPCERT / CC)
https://www.jpcert.or.jp/vh/top.html ou https://www.jpcert.or.jp/english/

Cingapura
Singer
https://www.csa.gov.sg/singcert/news/advisories-alerts

Estados Unidos
CERT de Sistemas de Controle Industrial (ICS-CERT)
https://www.us-cert.gov/ics

US CERT
https://us-cert.cisa.gov/

8. CONSIDERAÇÕES FINAIS

Suportes lógicos (*softwares*) destinados à diagnóstico ou terapia em saúde, ou que comandem um produto médico ou que tenham influência em seu uso também são considerados dispositivos médicos e estão sujeitos à regulação da Anvisa[12]. São exemplos: *softwares* de processamento de imagens para diagnósticos, *softwares* de

[12] Mais detalhes em http://portal.anvisa.gov.br/2017-2020/produtos/regulamento-de-software-medico.

diagnóstico em saúde (ex: glicemia), *software* de planejamento de radioterapia e, até mesmo, certos aplicativos de celular podem ser considerados *softwares* como dispositivos médicos.

Os *softwares* como dispositivos médicos podem ser autônomos, operando como dispositivos com fim em si mesmo ou em combinação com outro(s) dispositivo(s). No primeiro caso, existem os aplicativos móveis para diagnósticos, por exemplo, cálculo de doses de insulina. No último caso, há *softwares* utilizando medições a partir de um sensor, como as bombas de infusão e marcapassos. O escopo do tema são os dispositivos médicos que contêm *firmware*, controladores programáveis ou *softwares* que se conectam em rede.

Segundo a norma 81001-1, cibersegurança é um estado em que informações e sistemas são protegidos contra atividades não autorizadas, como acesso, uso, divulgação, interrupção, modificação ou destruição, a um nível em que os riscos relacionados à confidencialidade, integridade e disponibilidade sejam mantidos em um nível aceitável por todo o ciclo de vida. A necessidade de cibersegurança eficaz para garantir a funcionalidade dos dispositivos médicos e a segurança do paciente tem se tornado cada vez mais importante com o aumento do uso de dispositivos conectado à rede cabeada ou sem fio e à Internet. Os incidentes de cibersegurança podem tornar inoperantes os dispositivos médicos e as redes hospitalares, interrompendo a prestação de cuidado médico ao paciente nas instalações de serviços de saúde. Há estudos que apontam que este tipo de ataque alcançou a marca de 94% dos serviços de saúde. Portanto, não apenas os dispositivos médicos necessitam de atenção, mas o próprio ambiente em que eles se encontram, sendo este um meio para alcançar aqueles. Tais incidentes podem conduzir a dano ao paciente através de atrasos e/ou erros no diagnóstico e/ou nos tratamentos etc. A cibersegurança destes dispositivos inclui não somente a proteção da informação, mas a proteção de outros ativos como a própria pessoa.

Este guia pretende ajudar todos os intervenientes a entender melhor seu papel no suporte à cibersegurança proativa, que ajuda a proteger e fortalecer dispositivos médicos em antecipação a futuros ataques, problemas ou eventos. Ademais, há necessidade de convergência regulatória internacional com o Fórum Internacional de Reguladores de Dispositivos Médicos (IMDRF), do qual o Brasil é membro. No intuito de demonstrar convergência regulatória e harmonização nas discussões do IMDRF, é proposto a internalização de guias sobre *software* que orientam temas já formalizados na regulamentação da Anvisa sobre dispositivos médicos. Neste caso, este guia de princípios e práticas de cibersegurança em dispositivos médicos, que é resultado do grupo de trabalho homônimo do IMDRF, agrega ao arcabouço regulatório da Anvisa.

9. GLOSSÁRIO

Para os propósitos deste documento, os termos e definições fornecidos no IMDRF/GRRP WG/N47 FINAL:2018 e os seguintes se aplicam.

Ameaça: potencial de violação da segurança, que existe quando há uma circunstância, capacidade, ação ou evento que poderia violar a segurança e causar danos (Guia ISO / IEC 120)

Ataque: tentativa de destruir, expor, alterar, desativar, roubar ou obter acesso não autorizado ou fazer uso não autorizado de um ativo (ISO/IEC 27000:2018)

Ativo: entidade física ou digital que tem valor para um indivíduo, uma organização ou um governo (ISO/IEC JTC 1/SC 41 N0317, 12/11/2017)

Atualização: modificações corretivas, preventivas, adaptativas ou perfectivas feitas no *software* de um dispositivo médico

NOTA 1: Derivada das atividades de manutenção de *software* descritas na ISO/IEC 14764:2006.

NOTA 2: As atualizações podem incluir patches e alterações na configuração

NOTA 3: Modificações adaptativas e perfectivas são aprimoramentos no *software*. Essas modificações são aquelas que não estavam nas especificações de projeto do dispositivo médico.

Autenticação: garantia de que uma característica reivindicada de uma entidade está correta (ISO/IEC 27000: 2018)

Autenticidade: propriedade que uma entidade é o que afirma ser (ISO/IEC 27000: 2018)

Autorização: concessão de privilégios, que inclui a concessão de privilégios para acessar dados e funções (ISO 27789:2013)

NOTA: Derivado da ISO 7498-2: concessão de direitos, que inclui a concessão de acesso com base em direitos de acesso.

Cibersegurança: um estado em que informações e sistemas são protegidos contra atividades não autorizadas, como acesso, uso, divulgação, interrupção, modificação ou destruição, a um nível em que os riscos relacionados à confidencialidade, integridade e disponibilidade sejam mantidos em um nível aceitável por todo o ciclo de vida. (ISO 81001-1)

Confidencialidade: propriedade de que as informações não são disponibilizadas ou divulgadas a indivíduos, entidades ou processos não autorizados (ISO / IEC 27000: 2018)

Dano ao paciente: lesão física ou danos à saúde do paciente (Modificado da ISO/IEC Guia 51:2014)

Desempenho essencial: desempenho de uma função clínica, além da relacionada à segurança básica, em que a perda ou degradação além dos limites especificados pelo fabricante resulta em um risco inaceitável (IEC 60601-1:2005+AMD1:2012)

Disponibilidade: propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada (ISO / IEC 27000:2018)

Dispositivo médico legado (Dispositivo legado): dispositivos médicos que não podem ser razoavelmente protegidos contra ameaças atuais de cibersegurança

Divulgação Coordenada de Vulnerabilidades (CVD): processo pelo qual pesquisadores e outros intervenientes trabalham em cooperação com um fabricante na busca de soluções que reduzam os riscos associados à divulgação de vulnerabilidades (AAMI TIR97:2019)

NOTA: Esse processo abrange ações como relatar, coordenar e publicar informações sobre uma vulnerabilidade e sua resolução.

Fim da vida útil (EOL): estágio do ciclo de vida de um produto, que começa quando o fabricante não o vende mais além da vida útil, conforme definido pelo fabricante, e o produto passa por um processo formal de data de EOL, incluindo notificação aos usuários.

Fim do suporte (EOS): o estágio do ciclo de vida de um produto, iniciado quando o fabricante encerra todas as atividades de suporte de serviço e o suporte de serviço não se estende além desse ponto.

Integridade: propriedade pela qual os dados não foram alterados de maneira não autorizada desde que foram criados, transmitidos ou armazenados (ISO/IEC 29167-19:2016)

Medida de controle de compensação de risco (Controle de compensação): tipo específico de medida de controle de risco implementada no lugar ou na ausência de medidas de controle de risco implementadas como parte do projeto do dispositivo (AAMI TIR97:2019)

> NOTA: Uma medida de controle de risco compensatório pode ser permanente ou temporária (por exemplo, até que o fabricante possa fornecer uma atualização que incorpore medidas adicionais de controle de risco).

Modelagem de ameaças: processo exploratório para expor qualquer circunstância ou evento com potencial de causar danos a um sistema na forma de destruição, divulgação, modificação de dados ou negação de serviço (Adaptado da ISO/IEC/IEEE 24765-2017)

Não repúdio: capacidade de provar a ocorrência de um evento ou ação reivindicados e suas entidades originárias (ISO/IEC 27000:2018)

Privacidade: libertação da intrusão na vida privada ou nos negócios de um indivíduo quando essa invasão resultar de coleta e uso indevido ou ilegal de dados sobre esse indivíduo (ISO/TS 27799:2009)

Validação: confirmação, através do fornecimento de evidência objetiva, de que os requisitos para um uso ou aplicação específicos pretendidos foram cumpridos (ISO 9000:2015)

> NOTA 1: O termo "validado" é usado para designar o status correspondente.
>
> NOTA 2: As condições de uso para validação podem ser reais ou simuladas.

Verificação: confirmação, através do fornecimento de evidência objetiva, de que os requisitos especificados foram cumpridos (ISO/IEC Guia 63)

> NOTA 1: A evidência objetiva necessária para uma verificação pode ser o resultado de uma inspeção ou de outras formas de determinação, como a realização de cálculos alternativos ou a análise de documentos.
>
> NOTA 2: As atividades realizadas para verificação às vezes são chamadas de processo de qualificação.
>
> NOTA 3: A palavra "verificado" é usada para designar o status correspondente.

Vulnerabilidade: fraqueza de um ativo ou controle que pode ser explorado por uma ou mais ameaças (ISO/IEC 27000:2018)

10. REFERÊNCIAS BIBLIOGRÁFICAS

10.1. Documentos do IMDRF

1. *Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations* IMDRF/SaMD WG/N12:2014 (setembro de 2014)
2. *Essential Principles of Safety and Performance of Medical Devices and IVD Medical Devices* IMDRF/GRRP WG/N47 FINAL:2018 (novembro de 2018)

10.2. Padrões

3. AAMI TIR57:2016 *Principles for medical device security—Risk management*
4. AAMI TIR 97:2019, *Principles for medical device security—Postmarket risk management for device manufacturers*
5. IEC 60601-1:2005+AMD1:2012, *Medical electrical equipment - Part 1: General requirements for basic safety and essential performance*
6. IEC 62304:2006/AMD 1:2015, *Medical device software – Software life cycle processes*
7. IEC 62366-1:2015*, Medical devices - Part 1: Application of usability engineering to medical devices*
8. IEC 80001-1:2010, *Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities*
9. IEC TR 80001-2-2:2012, *Application of risk management for IT-networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls*
10. IEC TR 80001-2-8:2016, *Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2*
11. ISO 13485:2016, *Medical devices – Quality management systems – Requirements for regulatory purposes*
12. ISO 14971:2019, *Medical devices – Application of risk management to medical devices*
13. ISO/TR 80001-2-7:2015, *Application of risk management for IT-networks incorporating medical devices – Application guidance – Part 2-7: Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1*
14. Família ISO/IEC 27000 - *Information security management systems*
15. ISO/IEC 27035-1:2016*, Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management*
16. ISO/IEC 27035-2:2016, *Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response*
17. ISO/IEC 29147:2018, *Information Technology – Security Techniques – Vulnerability Disclosure*
18. ISO/IEC 30111:2013, *Information Technology – Security Techniques – Vulnerability Handling Processes*
19. ISO/TR 24971:2020, *Medical devices – Guidance on the application of ISO 14971*
20. UL 2900-1:2017, *Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements*
21. UL 2900-2-1:2017, *Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems*

10.3. Outros guias regulatórios

22. Alemanha (BSI): *Cyber Security Requirements for Network-Connected Medical Devices* (novembro de 2018)
23. Austrália (TGA): *Medical device cybersecurity - Consumer information* (julho de 2019)
24. Austrália (TGA): *Medical device cybersecurity guidance for industry* (julho de 2019)
25. Austrália (TGA): *Medical device cybersecurity information for* users (julho de 2019)
26. Canadá (*Health Canada*): *Pre-market Requirements for Medical Device Cybersecurity* (junho de 2019)
27. China (CFDA): *Medical Device Network Security Registration on Technical Review Guidance Principle* (janeiro de 2017)
28. Comissão Europeia: *REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC* (maio de 2017)
29. Comissão Europeia: *REGULATION (EU) 2017/746 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU* (maio de 2017)
30. Estados Unidos (FDA) (Minuta): *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* (outubro de 2018)
31. Estados Unidos (FDA): *Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software* (janeiro de 2005)

32. Estados Unidos (FDA): *Design Considerations for Devices Intended for Home Use* (novembro de 2014)
33. Estados Unidos (FDA): *Postmarket Management of Cybersecurity in Medical Devices* (dezembro de 2016)
34. França (ANSM) (Minuta): *Cybersecurity of medical devices integrating software during their life cycle* (julho de 2019)
35. Japão (PMDA): *Ensuring Cybersecurity of Medical Device: PFSB/ELD/OMDE Notification No. 0428-1* (abril de 2015)
36. Japão (PMDA): *Guidance on Ensuring Cybersecurity of Medical Device: PSEHB/MDED-PSD Notification No. 0724-1* (julho de 2018)
37. Singapura: *Singapore Standards Council Technical Reference 67: Medical device cybersecurity* (2018)

10.4. Outros recursos e referências

38. Guia CERT® para divulgação coordenada de vulnerabilidades
https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf
39. NIST *Cybersecurity Framework*
https://www.nist.gov/cyberframework
40. NIST *Secure Software Development Framework* (SSDF)
https://csrc.nist.gov/CSRC/media/Publications/white-paper/2019/06/07/mitigating-risk-of-software-vulnerabilities-with-ssdf/draft/documents/ssdf-for-mitigating-risk-of-software-vulns-draft.pdf
41. Medical *Device and Health IT Joint Security Plan* (janeiro de 2019)
https://healthsectorcouncil.org/wp-content/uploads/2019/01/HSCC-MEDTECH-JSP-v1.pdf
42. MITRE *medical device cybersecurity playbook* (outubro de 2018)
https://www.mitre.org/publications/technical-papers/medical-device-cybersecurity-regional-incident-preparedness-and
43. MITRE *CVSS Healthcare Rubric*
https://www.mitre.org/publications/technical-papers/rubric-for-applying-cvss-to-medical-devices
44. Nota Técnica 04/2012/GQUIP/GGTPS/Anvisa
http://portal.anvisa.gov.br/documents/33912/447671/NOTA+TÉCNICA+GQUIP+N°+04+de+2012
45. Health *Industry Cybersecurity Practices: Managing Threats and Protecting Patients* (HICP)
https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx
46. Open *Web Application Security Project* (OWASP)
https://www.owasp.org/index.php/Main_Page
47. Declaração *de Divulgação de Informações do Fabricante para a Segurança de Dispositivos Médicos* (MDS2)
https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx
48. ECRI *approach to applying the NIST framework to MD*
https://www.ecri.org/components/HDJournal/Pages/Cybersecurity-Risk-Assessment-for-Medical-Devices.aspx
49. National *Telecommunications and Information Administration (NTIA) / US Department of Commerce, Vulnerability Disclosure Attitudes and Actions: A Research Report from the NTIA Awareness and Adoption Group*
https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf
50. https://republicans-energycommerce.house.gov/wp-content/uploads/2018/10/10-23-18-CoDis-White-Paper.pdf
51. https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

Agência Nacional de Vigilância Sanitária – Anvisa

SIA Trecho 5, Área Especial 57, Lote 200

CEP: 71205-050

Brasília – DF

www.anvisa.gov.br

www.twitter.com/anvisa_oficial

Anvisa Atende: 0800-642-9782

ouvidoria@anvisa.gov.br