Infarmed
Autoridade Nacional
do Medicamento
e Produtos de Saúde, I.P.

WEBINAR 10

CONTEXTO REGULAMENTAR DAS TECNOLOGIAS DIGITAIS NA SAÚDE

19 DE FEVEREIRO DE 2025 10:00 - 11:00

VIGILÂNCIA E CIBERSEGURANÇA

RAQUEL ALVES

INFARMED, I.P.

19.FEV.2026

REPÚBLICA PORTUGUESA
SAÚDE

Infarmed
Autoridade Nacional do Medicamento e Produtos de Saúde, I.P.

SUMÁRIO

1

CIBERSEGURANÇA

Infarmed
Autoridade Nacional do Medicamento
e Produtos de Saúde, I.P.

CIBERSEGURANÇA

Assunto da atualidade e da maior importância num mundo cada vez mais conectado

«Cibersegurança», todas as atividades necessárias para **proteger de ciberameaças** as redes e os sistemas de informação, os seus utilizadores e outras pessoas afetadas; (…)

TECNOLOGIA

DMs

PESSOAS

AdobeStock © InfiniteFlow

!!!! RESPONSABILIDADE PARTILHADA !!!!

+

PARTILHA DE INFORMAÇÃO

Vária legislação a nível europeu, exemplos:

- Ato de Cibersegurança (Regulamento (UE) 2019/881)
- NIS 2 (Diretiva (UE) 2022/2555)
- **Regulamento de Ciber-Resiliência** (Regulamento (UE) 2024/2847)

20 jan 2026 – **Novo pacote de cibersegurança** – Proposta de revisão do ato de cibersegurança

ATO DE CIBER-RESILIÊNCIA - CRA

Exclui os dispositivos médicos

Artigo 2.º

Âmbito de aplicação

1. O presente regulamento é aplicável aos produtos com elementos digitais disponibilizados no mercado cuja finalidade prevista ou utilização razoavelmente previsível inclua uma conexão de dados lógica ou física, direta ou indireta, a um dispositivo ou a uma rede.

2. O presente regulamento não é aplicável aos produtos com elementos digitais aos quais sejam aplicáveis os seguintes atos jurídicos da União:

a) Regulamento (UE) 2017/745;

b) Regulamento (UE) 2017/746;

c) Regulamento (UE) 2019/2144.

(25) O Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho ([9]) estabelece regras relativas aos dispositivos médicos e o Regulamento (UE) 2017/746 do Parlamento Europeu e do Conselho ([10]) estabelece regras relativas aos dispositivos médicos para diagnóstico in vitro. Os referidos regulamentos abordam os riscos de cibersegurança e seguem abordagens específicas que também são contempladas no presente regulamento. Mais especificamente, os Regulamentos (UE) 2017/745 e (UE) 2017/746 estabelecem requisitos essenciais para os dispositivos médicos que funcionam através de um sistema eletrónico ou que constituem, por si mesmos, *software*. Os referidos regulamentos abrangem igualmente certos tipos de *software* não incorporado, bem como a abordagem de todo o ciclo de vida. Esses requisitos obrigam os fabricantes a desenvolver e construir os seus produtos aplicando princípios de gestão dos riscos e estabelecendo requisitos de segurança informática, bem como os correspondentes procedimentos de avaliação da conformidade. Além disso, desde dezembro de 2019, existem diretrizes específicas em matéria de cibersegurança dos dispositivos médicos, que fornecem aos fabricantes de dispositivos médicos, incluindo dispositivos para diagnóstico in vitro, orientações sobre a forma de cumprir todos os requisitos essenciais pertinentes previstos no anexo I desses regulamentos no que diz respeito à cibersegurança. Os produtos com elementos digitais a que se aplique qualquer um desses regulamentos não deverão, por conseguinte, ser abrangidos pelo presente regulamento.

MDR E IVDR

«Risco», a combinação da probabilidade de ocorrência de dano e a severidade desse dano;

Foco SAFETY/PERFORMANCE,
mas inclui SECURITY (que inclui cibersecurity)

tudo tem de ser incluído na avaliação do risco, mesmo que não seja explicito ao longo do texto do MDR e IVDR

CRA

«Risco de cibersegurança», o potencial de perda ou perturbação causada por um incidente, expresso como uma combinação da magnitude dessa perda ou perturbação e da probabilidade de ocorrência do incidente;
«Risco de cibersegurança significativo», um **risco de cibersegurança** que, com base nas suas características técnicas, se possa considerar altamente suscetível de dar origem a um incidente com impacto negativo grave, causando, nomeadamente, perturbações ou perdas materiais ou imateriais consideráveis

Foco CIBERSECURITY
(IT SECURITY, OPERATION SECURITY, INFORMATION SECURITY – confidencialidade, integridade, autenticidade e disponibilidade da informação)

Não inclui SAFETY

A CIBERSEGURANÇA NOS DISPOSITIVOS MÉDICOS

Produtos com elementos digitais

+

Concebidos

Fabricante

Ligados Net
(diretamente ou através de outros dispositivos)

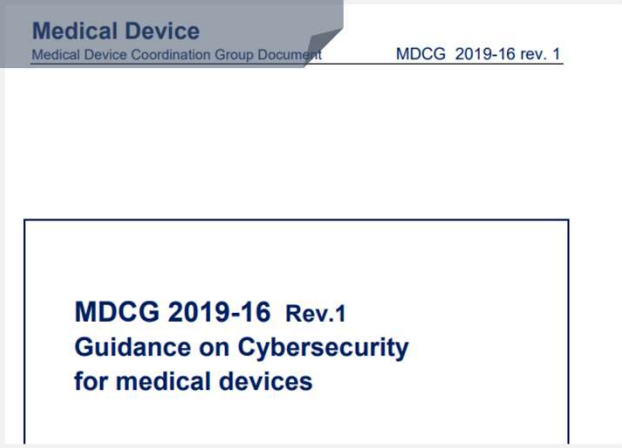
→

Cibersegurança

é um aspeto a ser avaliado, monitorizado e gerido continuamente

MDR Reg 745/2017

IVDR Reg 746/2017


Medical Device
Medical Device Coordination Group Document MDCG 2019-16 rev. 1

MDCG 2019-16 Rev.1
Guidance on Cybersecurity for medical devices

REQUISITOS GERAIS DE SEGURANÇA E DESEMPENHO RGSD – SOFTWARE

"Security "– segurança da informação
"Safety "– segurança do doente

"Safety & Security"

Ciber

Os dois Regulamentos MDR e IVDR cobrem os aspetos de "security" que engloba "cybersecurity"

- Anexo I

- Requisitos Gestão do Risco
  (SAFETY e SECURITY BY DESIGN)
- Requisitos Informação a ceder com DM

✖ Requisitos Conceção e Fabrico:
- Interação com o ambiente
- Sistemas eletrónicos programáveis e software (incluem os aspectos de pré e pós mercado)

I

Main topic	Section number MDR Annex I	Section number IVDR Annex I
Device performance	1	1
Risk reduction	2	2
Risk management system	3	3
Risk control measures	4	4
Minimisation of foreseeable risks, and any undesirable side-effects	8	8
✖ Combination/connection of devices/systems	14.1	13.1
✖ Interaction between software and the IT environment	14.2.d	13.2.d
✖ Interoperability and compatibility with other devices or products	14.5	13.5
✖ Repeatability, reliability and performance	17.1	16.1
✖ Development and manufacture in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation	17.2	16.2
✖ Minimum IT requirements	17.4	16.4
✖ Unauthorised access	18.8	-
Lay persons	22.1	-
Residual risks (information supplied by the manufacturer)	23.1 g	20.1 g
Warnings or precautions (information on the label)	23.2 m	20.2 m
Residual risks, contra-indications and any undesirable side-effects, (information in the instructions for use)	23.4 g	-
Minimum IT requirements (information in the instructions for use)	23.4.ab	20.4.1.ah

REQUISITOS GERAIS

RGSD (1- 9)

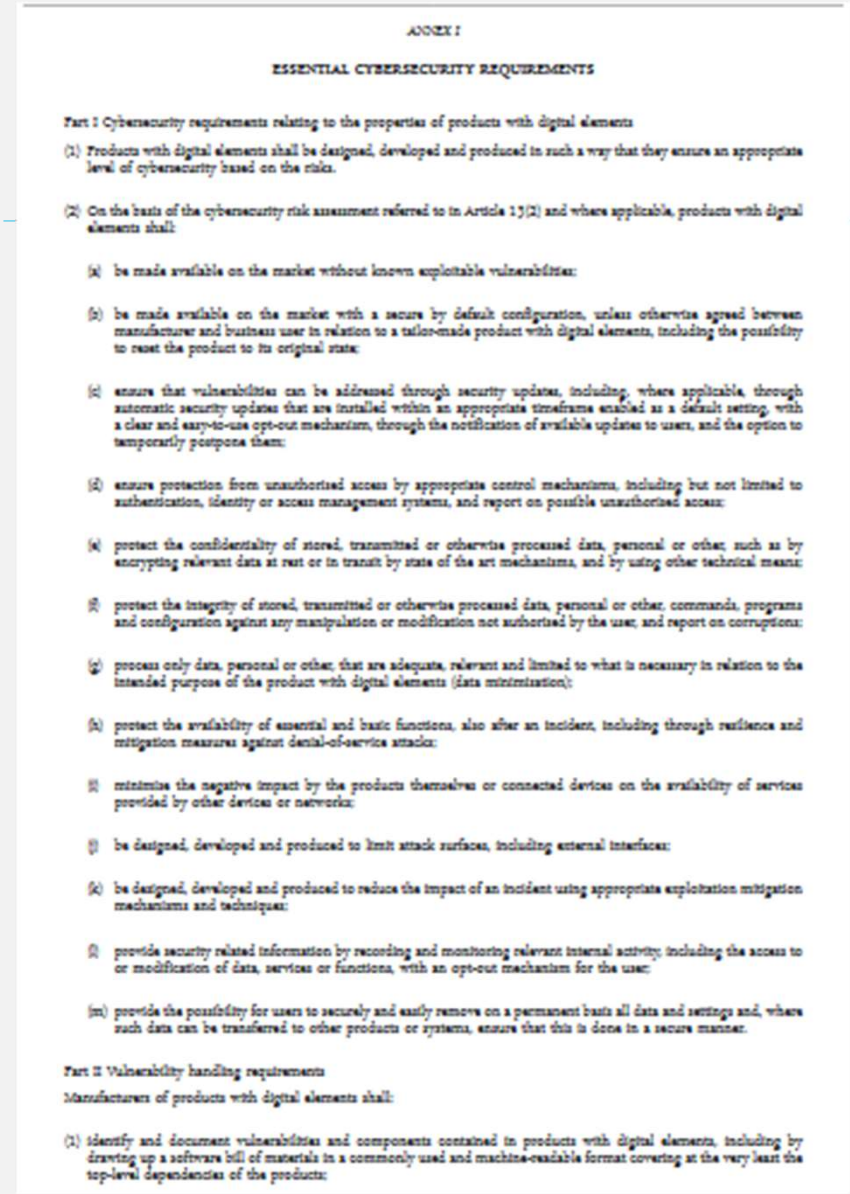
"Os dispositivos devem **atingir o desempenho previsto pelo fabricante** e ser **concebidos e fabricados de tal modo** que, em condições normais de utilização, **se adequem à finalidade prevista**. Devem ser **seguros e eficazes** e **não podem comprometer o quadro clínico** nem a segurança dos doentes, nem tão pouco a segurança e a saúde dos utilizadores ou, se for caso disso, de outras pessoas, desde que **os eventuais riscos associados à sua utilização constituam riscos aceitáveis quando ponderados pelo benefício** proporcionado aos doentes e sejam compatíveis com um elevado grau de proteção da saúde e da segurança**, atendendo ao estado atual dos conhecimentos geralmente reconhecido**."

- Performance Characteristics & Safety Features
- Risk Management System
- Usability and Ergonomic features
- Characteristics and performance during lifetime of the device
- Undesirable side-effects

Safety by design | **Risk Management** | **Benefit-Risk Analysis**

INFORMAÇÃO A CONSIDERAR

CRA – ANEXO I
Requisitos essenciais de cirbersegurança
A considerar aqueles que sejam possíveis aplicar



ANNEX I

ESSENTIAL CYBERSECURITY REQUIREMENTS

Part I Cybersecurity requirements relating to the properties of products with digital elements

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.

(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:

(a) be made available on the market without known exploitable vulnerabilities;

(b) be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;

(c) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;

(d) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;

(e) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means;

(f) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;

(g) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation);

(h) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;

(i) minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;

(j) be designed, developed and produced to limit attack surfaces, including external interfaces;

(k) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

(l) provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user;

(m) provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.

Part II Vulnerability handling requirements

Manufacturers of products with digital elements shall:

(1) identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;

(2) in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;

(3) apply effective and regular tests and reviews of the security of the product with digital elements;

(4) once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;

(5) put in place and enforce a policy on coordinated vulnerability disclosure;

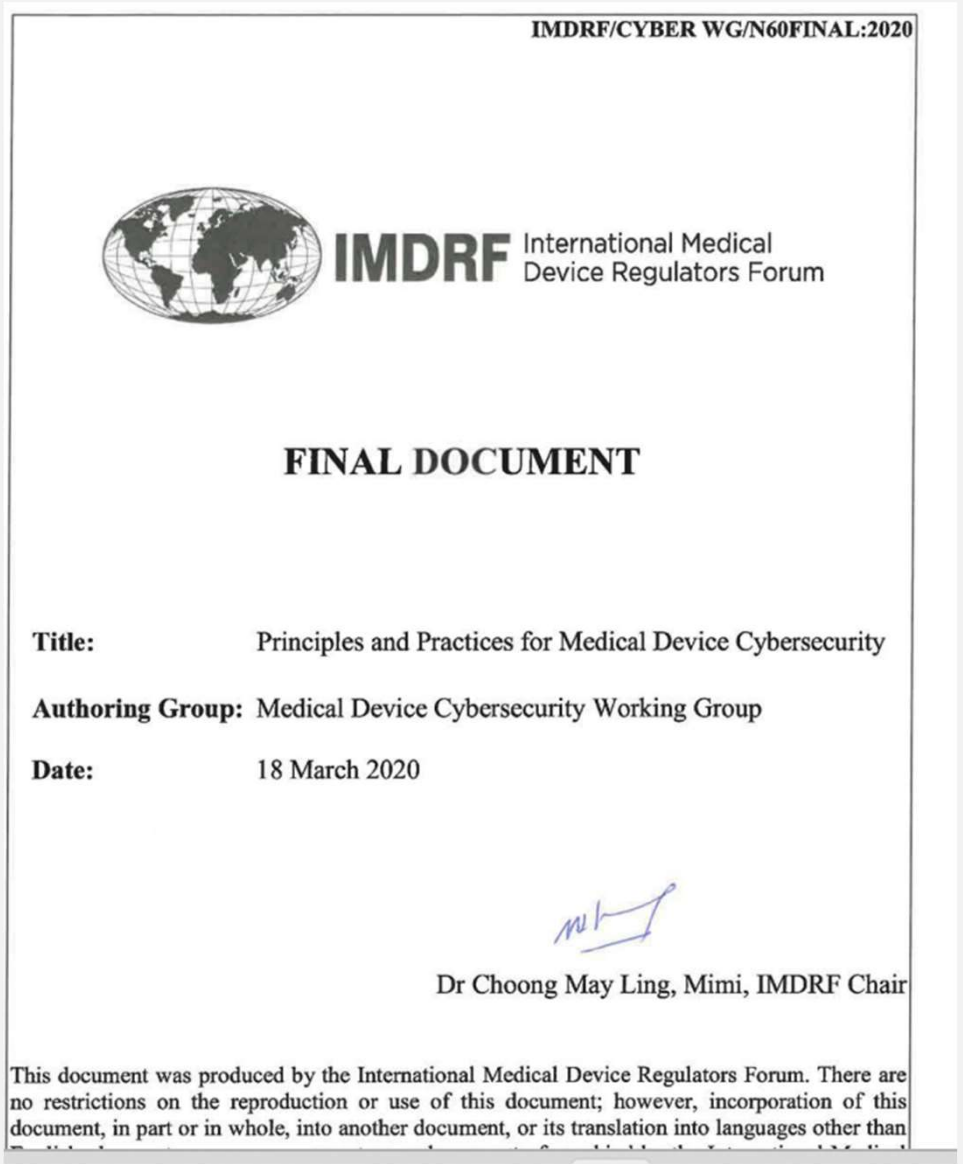
(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;

(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner;

(8) ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

NORMAS E OUTRAS GUIDANCES

- EN ISO 14971 Risk Management (Product)
- EN 62304 Software Lifecycle
- EN ISO 31000 Risk Management (Organisation) or particular standards under ISO 31xxx.
- EN ISO/IEC 27000 Information technology — Security techniques — Information security management systems (ISMS) — Overview and vocabulary
- EN ISO/IEC 27001 Information Technology – Security techniques – Information Security management Systems – Requirements.
- EN ISO/IEC 60601-1-x
- IEC 82304-1 Health Software Part 1: General requirements for Product Safety
- ISO/IEC 80001-1 Application of Risk Management for IT networks Incorporating Medical Devices
- ISO/IEC 80001-5-1 Application of Risk Management for IT networks incorporating medical device – Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software – Part 5-1: Activities in the product life-cycle.
- IEC/TR 80001-2-2 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
- IEC/TR 80001-2-8 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 TR 80001-2-2
- ISO/IEC 80001-xx including IEC/TR 80001-2-1, IEC/TR 80001-2-3, IEC/TR 80001-2-4, IEC/TR 80001-2-5, ISO/TR 80001-2-6, ISO/TR 80001-2-7 or other
- EN ISO 62366 / ISO 60601-4 Usability Engineering
- IEC 62443-4-2 Security for industrial automation and control systems. Part 4-2: Technical security requirements for IACS components.
- IEC 62443-4-1 Security for industrial automation and control systems. Part 4-1: Secure product development lifecycle requirements.
- IEC/TR 60601-4-5 Medical Electrical Equipment – Part 4-5. Safety related technical security specifications for medical devices.



IMDRF/CYBER WG/N60FINAL:2020

IMDRF International Medical Device Regulators Forum

FINAL DOCUMENT

Title: Principles and Practices for Medical Device Cybersecurity

Authoring Group: Medical Device Cybersecurity Working Group

Date: 18 March 2020

Dr Choong May Ling, Mimi, IMDRF Chair

This document was produced by the International Medical Device Regulators Forum. There are no restrictions on the reproduction or use of this document; however, incorporation of this document, in part or in whole, into another document, or its translation into languages other than

SAFETY E SECURITY

Guidance on Cybersecurity for medical device MDCG 2019-16 rev.1

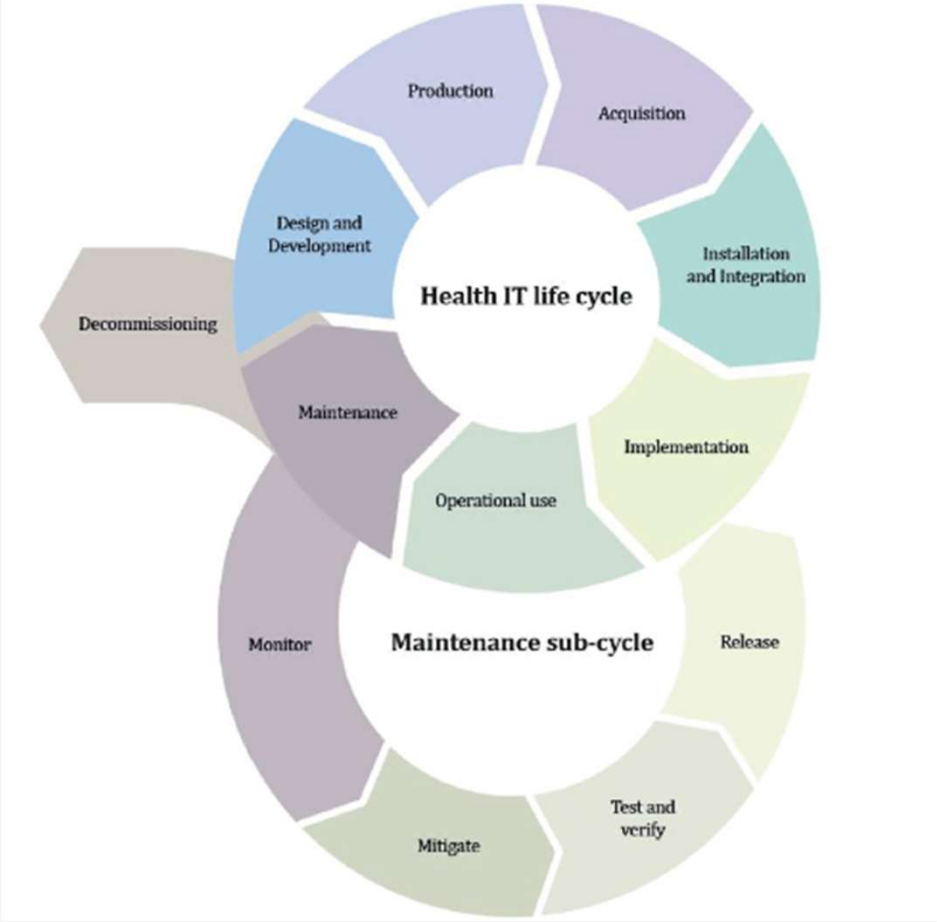
Medidas de "**security"** podem ter **impacto no safety**, por exemplo:

- **"Security" reduzida** - um controlo fraco do acesso **pode permitir a modificação do funcionamento** de um dispositivo implantável cardíaco
- **"Security" restritiva** – o uso **de medidas de security demasiado restritivas** com um elevado nível de proteção podem ter um **impacto na segurança, senão forem bem concebidas** (por exemplo **o acesso a um dispositivo numa situação de emergência vs medidas de security fortes numa situação normal**)
- **Na avaliação do risco os aspetos de "security" não podem ser avaliados de forma isolada, mas sempre considerando os aspetos de "safety".**

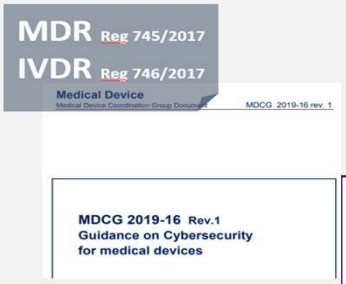
OUTROS ASPECTOS

- Finalidade prevista e ambiente operacional de uso
  - ✓ **os requisitos de cibersegurança** devem ter em conta a **natureza do dispositivo**, incluindo o tipo de dispositivo e a **tecnologia de comunicação** prevista usar. Em circunstâncias específicas com **base na avalição safety e security**, o fabricante pode ter que adotar medidas de controlo security menos restritivas.
  - ✓ um dispositivo deve ser concebido por uma **abordagem de defesa em camadas** e **não deve apoiar-se em controlos de security dependents do ambiente operacional**, apesar deste ambiente operacional dever também seguir boas práticas de cibersegurança.
- Uso indevido razoavelmente previsivel
  - ✓O uso de um cartão/pen de memória para fornecer dados a Sistema IT pode ser um exemplo.
- Responsabilidade partilhada de todos os que contactam com o dispositivo (instalação, atualização, manutenção, e utilização)

CIBERSEGURANÇA
AO LONGO DO CICLO DE VIDA DO DM



Guidance on Cybersecurity for medical device [MDCG 2019-16 rev.1]



A considerar:
Legislação transversal
Normas
Guidances
Outra informação

ESTADO DA ARTE (SOTA)

CONSIDERAR TODA A INFORMAÇÃO DISPONíVEL

Safety - Perigos relativos à segurança (mais estáveis)
Security - Vulnerabilidades (mudam rapidamente)

GESTÃO DO RISCO

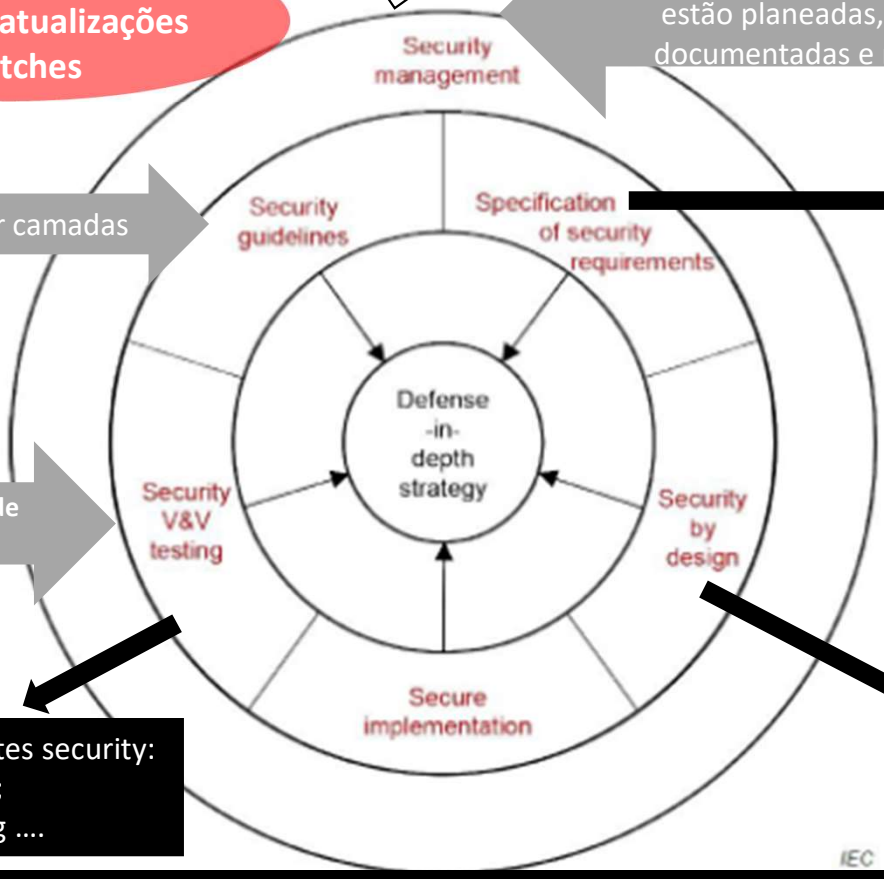
ELIMINAR OU REDUZIR O RISCO

reduzir tanto quanto possível os riscos sem afetar adversamente a relação benefício-risco

“SECURE BY DESIGN” - SEGURANÇA POR CAMADAS

problemas de “security”, atualizações e patches

Atividades de “security” estão planeadas, documentadas e registadas



Doc segurança por camadas

Garantir requisitos de security

Vários tipos de testes security: robustness testing; penetration testing ….

ex: funcionalidades de “security”

Automatic Logoff
Audit Controls
Authorization
Configuration of Security Features
Cybersecurity Product Upgrades
Personal Data De-Identification
Data Backup and Disaster Recovery
Emergency Access
Personal Data Integrity and Authenticity
Malware Detection / Protection
Node Authentication
Person Authentication
Physical Locks
System and OS Hardening
Security and Privacy Guides
Personal Data Storage Confidentiality
Transmission Confidentiality
Transmission Integrity

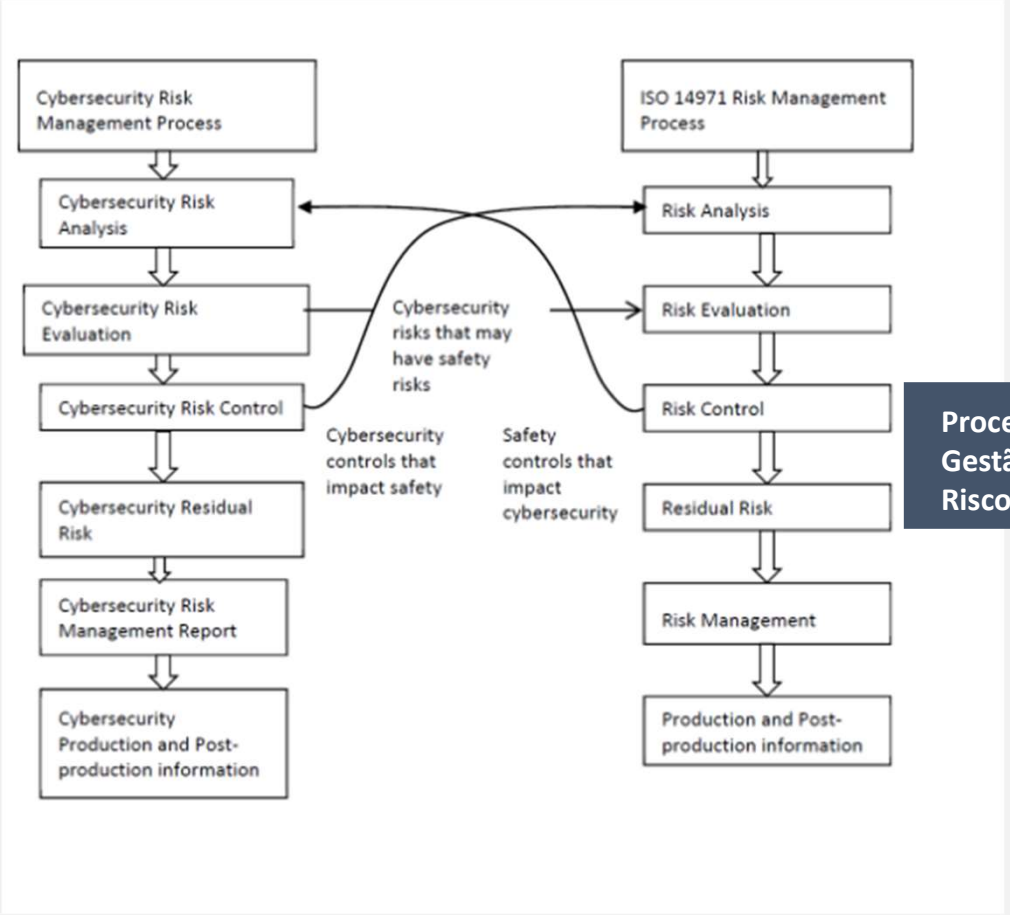
(medidas de proteção/controlo)

! SAFETY

Comunicações seguras;
Proteção de dados; Integridade do dispositivo;
Autenticação; Manutenção software; Acesso físico;
Fiabilidade e Disponibilidade

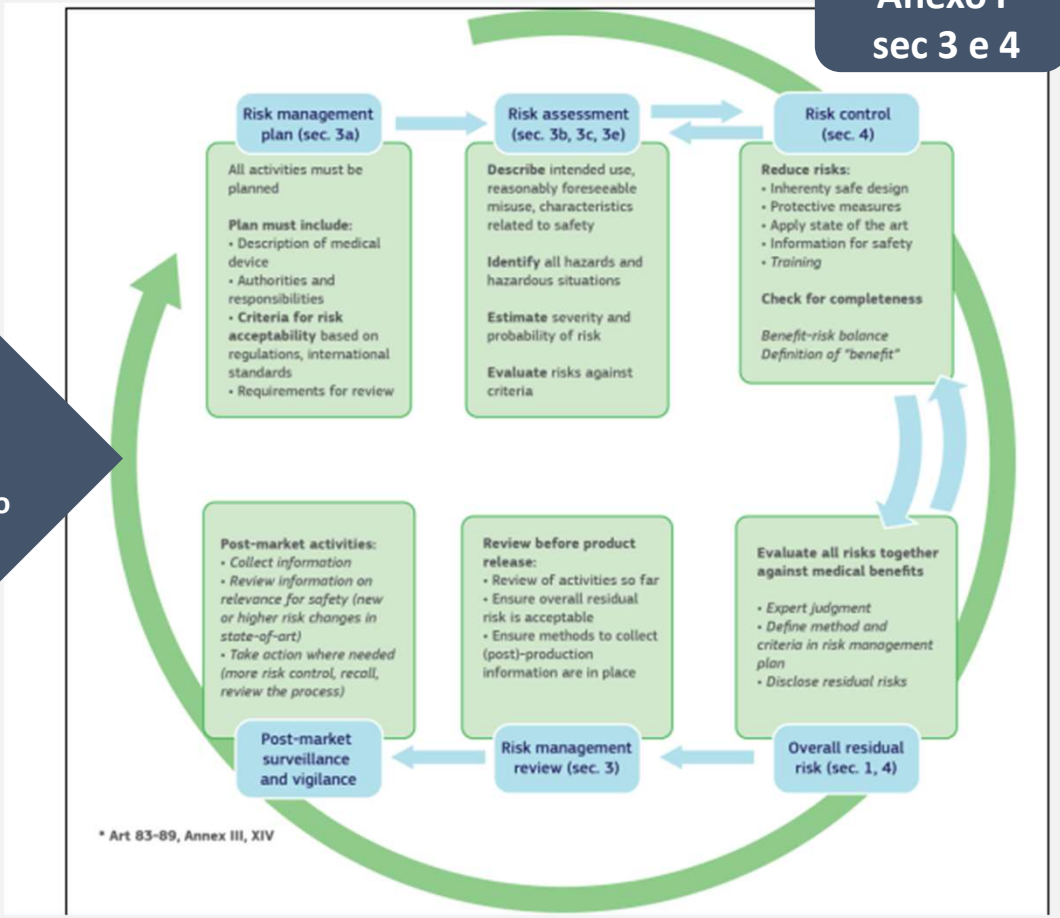
Garantir a confidencialidade, integridade e disponibilidade da informação

GESTÃO DO RISCO – “SECURITY” E “SAFETY”



Processo de Gestão do Risco Integrado

MDR Anexo I sec 3 e 4



Guidance on Cybersecurity for medical device [MDCG 2019-16 rev.1]

SECURITY RISK ASSESSMENT E SECURITY BENEFIT RISK ANALYSIS

Security Risk Assessment

- ✓ **Técnicas de modelagem de ameaças** - abordagem sistemática para **análise da "security"** de um produto de uma forma estrutural para que as **vulnerabilidades possam ser identificadas, enumeradas e priorizadas**, considerando um ataque hipotético.

Dispositivos, software, redes, processos de negócio …

Vulnerabilidade **desconhecida** – identificada – **conhecida**
Priorização – Common Vulnerability Scoring System (CVSS)

Security benefit risk analysis

- ✓ Não é efetuada individualmente para cada risco de "security"
- ✓ Deve ser efetuada de uma forma global estabelecendo critérios de aceitação do risco e medidas minimização dos riscos "security"
- ✓ Considerar a finalidade, o uso pretendido, o ambiente de funcionamento, e a possibilidade do impacto na segurança e desempenho utilizando a avaliação do risco do "safety"

INSTRUÇÕES DE UTILIZAÇÃO - CIBERSEGURANÇA
ANEXO I

23.4 (j) MDR "any requirements for special facilities, or special training, or particular qualifications of the device user and/or other persons;"

- Requisitos dos utilizadores no que respeita a treino /competências, incluindo de IT para a instalação, configuração e funcionamento do dispositivo

23.4 (q) MDR "for devices intended for use together with other devices and/or general purpose equipment:

— information to identify such devices or equipment, in order to obtain a safe combination, and/or

— information on any known restrictions to combinations of devices and equipment;"

- Requisitos mínimos das workstations destinadas às operações dos utilizadores: características do hardware, versões dos sistemas operativos, dispositivos periféricos …

INFORMAÇÃO SOBRE O AMBIENTE DE USO PRETENDIDO

PROFISSIONAIS DE SAÚDE

Exs:

- Controlos de cibersegurança recomendados (ex: software anti – virus; firewall, ...)
- Descrição das características de backup and restore e procedimentos para recuperar as configurações
- Diagramas suficientemente detalhados da network para os utilizadores
- Riscos de utilizar o dispositivo for a do ambiente de uso pretendido

- Nota 1: Os médicos devem informar os doentes sobre a utilização, benefícios e riscos, dos dispositivos inclundo os riscos de cibersegurança
- Nota 2: A informação a ser fornecida com do software deve ter em consideração o ambiente de uso (no domicílio com uma limitada ciberproteção, ou ambiente público, …)

DOCUMENTAÇÃO

- Sistema de Gestão do Risco
- Sistema de Gestão da Qualidade
- Documentação Técnica – Anexos II e III MDR e IVDR

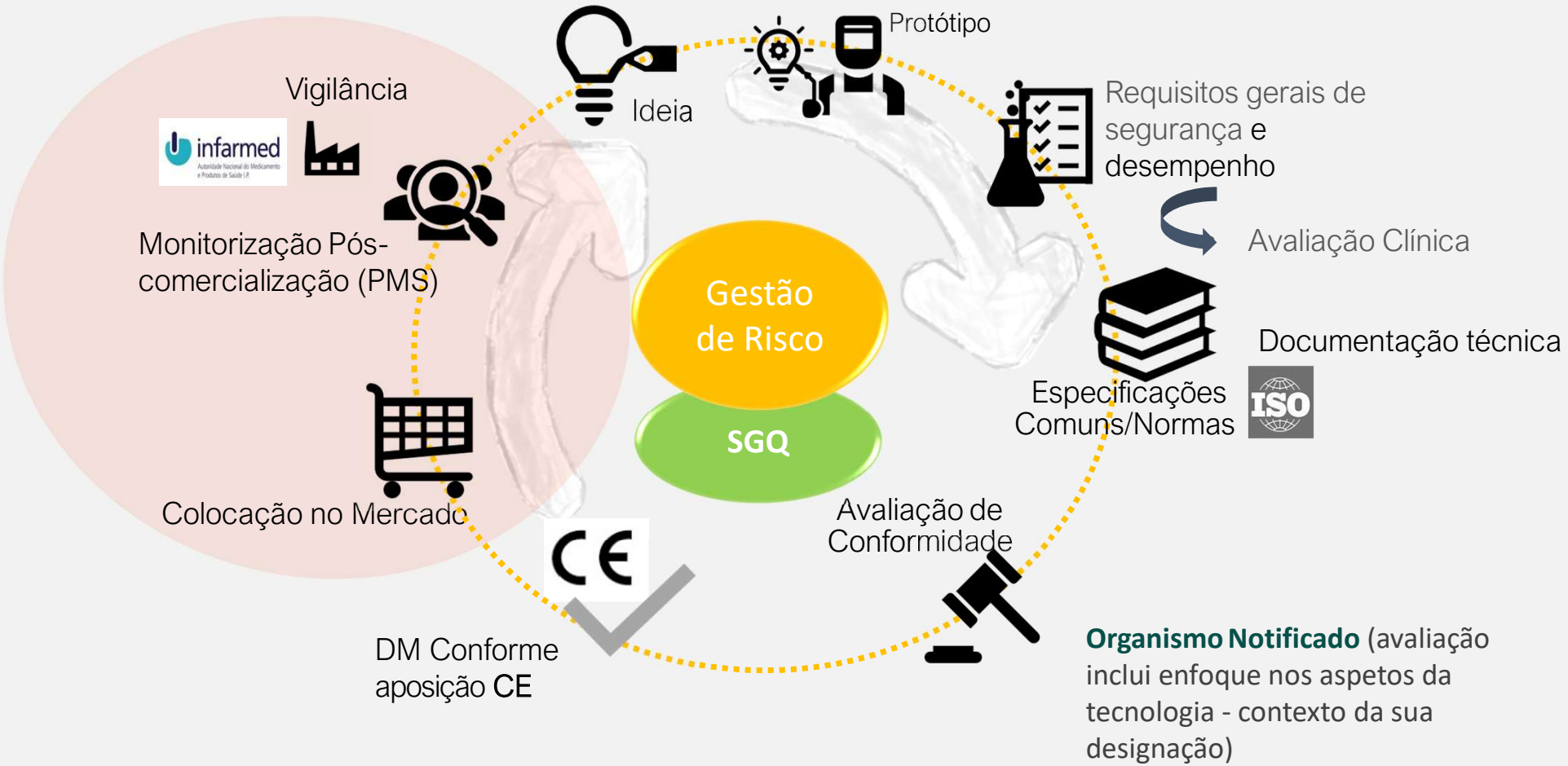
(engloba a demonstração do cumprimento dos **requisitos gerais de segurança e desempenho o que inclui os requisitos de "security", e ainda justificação, validação e verificação das soluções adotadas para o cumprimento dos requisitos**)

2

MONITORIZAÇÃO PÓS-COMERCIALIZAÇÃO (PMS)

Infarmed
Autoridade Nacional do Medicamento e Produtos de Saúde, I.P.

CICLO DE VIDA DO DISPOSITIVO MÉDICO



Regulamento MDR – Capítulo VII e Anexo III

Capítulo VII - 3 seções

- Sistema de monitorização pós-comercialização (fabricante)
- Vigilância (AC e fabricante)
- Fiscalização (AC)

Anexo III

- Documentação técnica relativa à monitorização pós-comercialização

Monitorização pós-comercialização, Vigilância e Fiscalização

Autoridade Competentes

Fabricante

Fiscalização do mercado

Vigilância

Sistema de Monitorização pós-comercialização

Vigilância

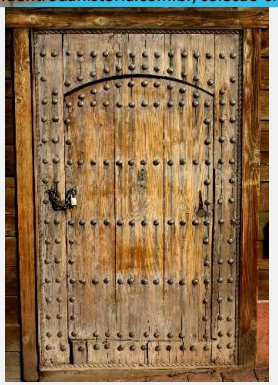
Vigilância

Maior gravidade
Maior risco

(Incidentes graves e ações corretivas de segurança)

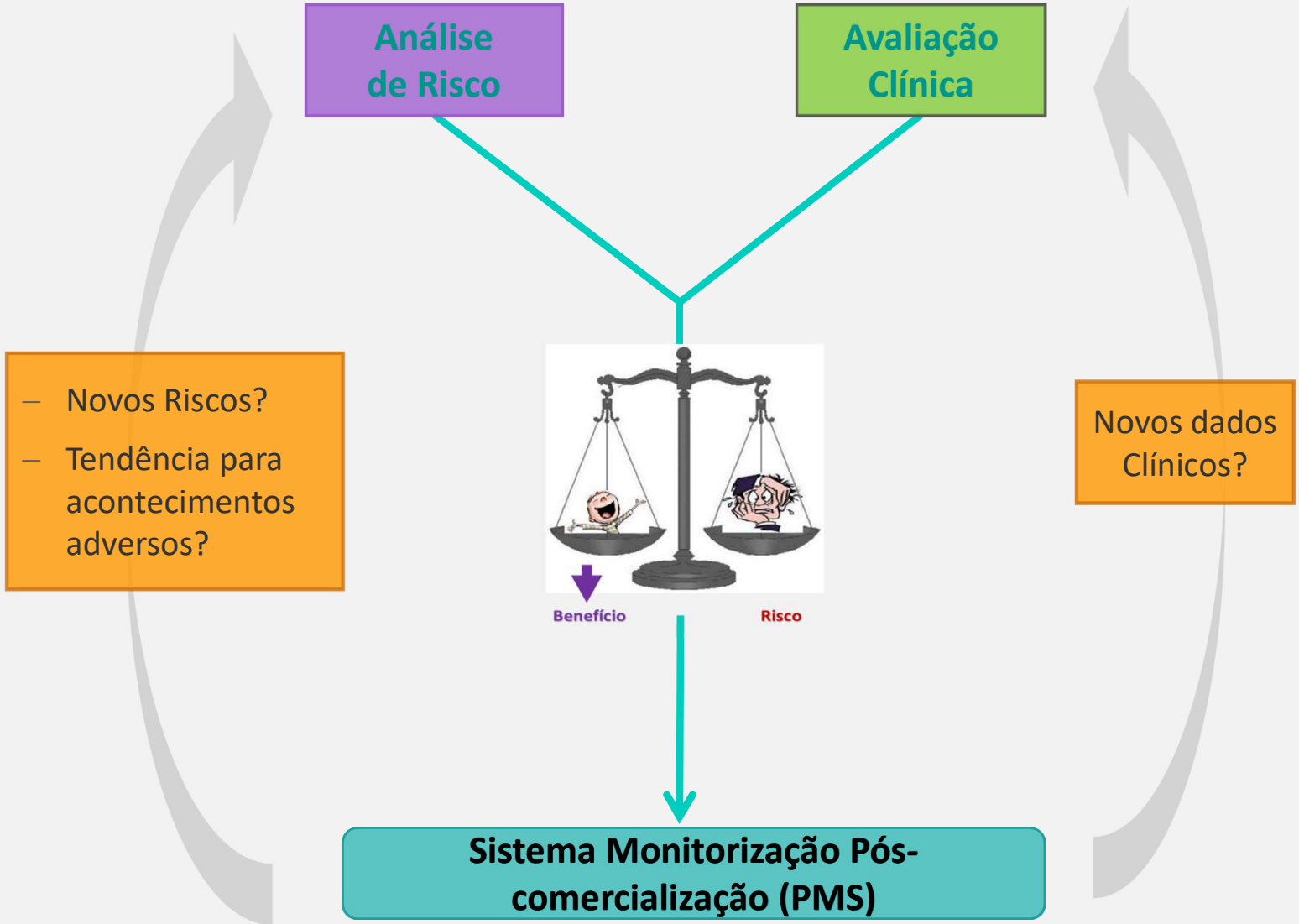
“SECURITY” E “SAFETY” NO PÓS-MERCADO

https://www.dentrodahistoria.com.br/colecao-classicos/o-conto-dos-tres-porquinhos/



Sistema PMS

Gestão do risco contínua…



Monitorização pós-comercialização – definição (MDR art 2º)

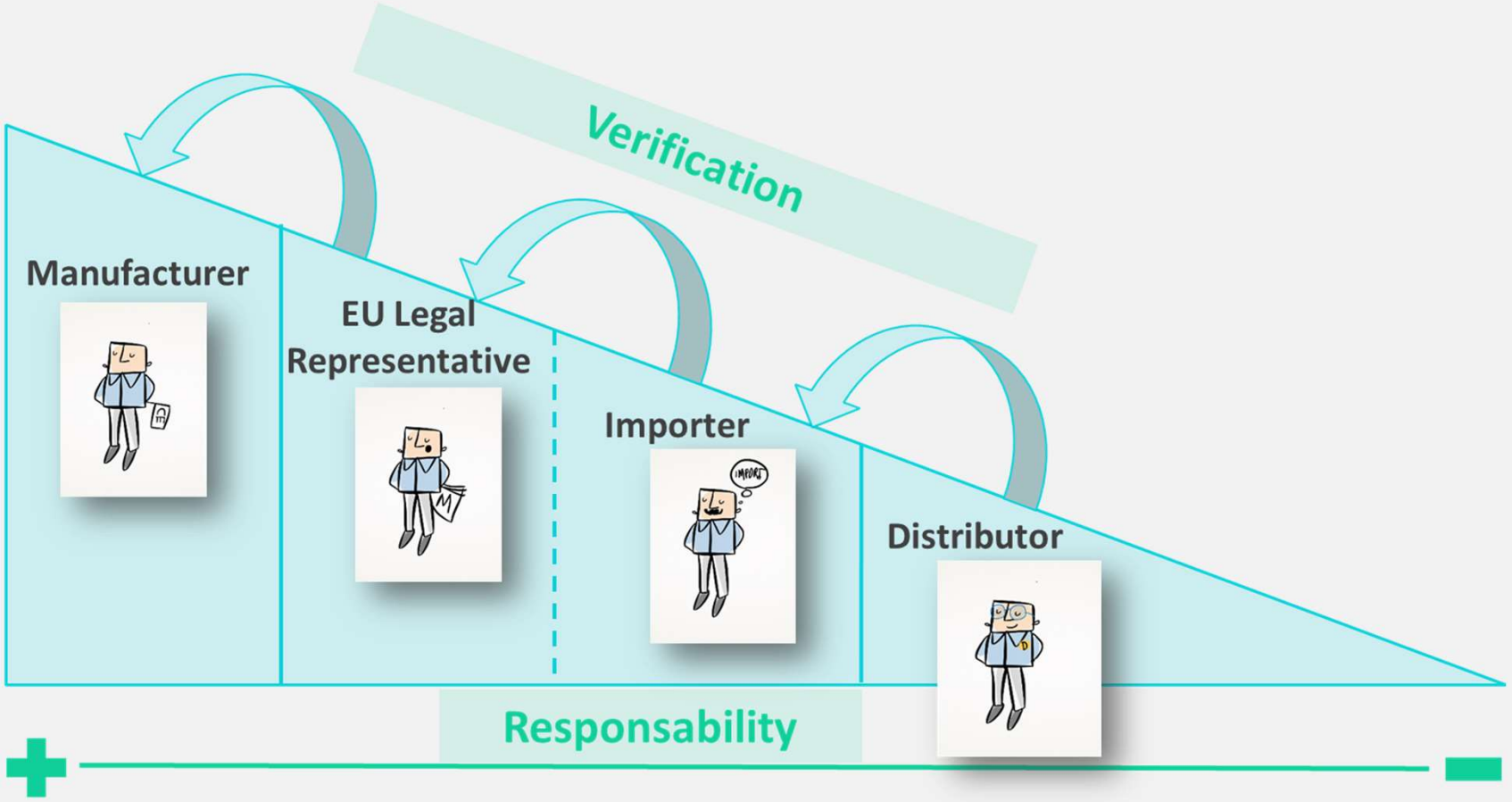
«Monitorização pós-comercialização», todas as atividades desenvolvidas por fabricantes em cooperação com outros operadores económicos no sentido de estabelecer e manter atualizado um procedimento sistemático para **proativamente** recolher e analisar a experiência adquirida com os dispositivos por eles colocados no mercado, disponibilizados no mercado ou que tenham entrado em serviço, a fim de identificar a eventual necessidade de aplicar imediatamente quaisquer ações corretivas ou preventivas que se afigurem necessárias;

- Garantir que os **dispositivos permanecem conformes** com os requisitos dos regulamentos e que os **dados do mundo real são analisados** e considerados, **na melhoria dos dispositivos**, dos processos e da documentação técnica.

- **Proporcional à classe de risco e ao longo do tempo de vida do dispositivo.**

Operadores económicos

Cascata de responsabilidades e verificação retrospetiva da compliance



Active role on Post-market surveillance /Vigilance

Distribuidores
E
Importadores

- ✓ Informa o fabricante de reclamações, incidentes, DM não conforme
- ✓ Informa o fabricante e AC sobre DM com risco grave ou falsificado
- ✓ Cooperar nas ações corretivas
- ✓ Permitir o acesso ou facultar amostras de DM às ACs
- ✓ Rastreabilidade

DOCUMENTAÇÃO PMS
ANEXO III MDR e IVDR

- Sistema
- Documentos :

Procedimentos, <u>Plano</u>, Registos e <u>Relatório</u>

Monitorização pós-comercialização

Monitorização pós-comercialização

TECNOLOGIAS DIGITAIS

- **Recolha <u>proativa</u> da informação sobre a experiência dos utilizadores de dispositivos médicos** (exs: concretos)
  - Compatibilidade
  - Interoperabilidade
  - Tentativas e eventos de acessos não autorizados
  - Vulnerabilidades
  - Incidentes
  - Dificuldades de utilização /usability
  - Componentes de terceiros (hardware ou software)
  - DM AI - monitorizar a interação com outros sistemas AI
  - DM AI - lista detalhada de elementos do plano monitorização pós comercialização previstos no Artigo 72(3) AI Act será publicada

Monitorização pós-comercialização

PARA QUE SERVE?

TECNOLOGIAS DIGITAIS

- ✓ Avaliar a necessidade de **notificação à AC de incidentes graves e não graves**
- ✓ Avaliar a necessidade de **implementação de ações corretivas e preventivas**
- ✓ Avaliar a necessidade **de implementação de ações corretivas de segurança no mercado**
- ✓ Atualizar a **avaliação clínica**
- ✓ Atualizar o **perfil benefício-risco**
- ✓ Atualizar a **conceção, fabrico e instruções de utilização**
- ✓ **Melhorar / corrigir as vulnerabilidades**
- ✓ Atualizar "**Security and Safety Risk Assessment**"
- ✓ **Atualizar a verificação e validação**
- ✓ Atualizar "**Security and Safety Benefit Risk Analisys**"

ATUALIZAR A DOCUMENTAÇÃO TÉCNICA

MDR

«Incidente», qualquer mau funcionamento ou deterioração das características ou do desempenho de um dispositivo disponibilizado no mercado, incluindo erros de utilização devidos a características ergonómicas, bem como qualquer inadequação das informações fornecidas pelo fabricante e qualquer efeito secundário indesejável;

«Incidente grave», qualquer incidente que, direta ou indiretamente, tenha conduzido, possa ter conduzido ou possa vir a conduzir a alguma das seguintes consequências:

a) Morte do doente, do utilizador ou de outra pessoa,

b) Deterioração grave, temporária ou permanente, do estado de saúde de um doente, utilizador ou de outra pessoa,

c) Ameaça grave para a saúde pública.

IMPACTO SAÚDE

CRA

«Quase incidente», um evento que poderia ter posto em causa a **disponibilidade, a autenticidade, a integridade ou a confidencialidade de dados** armazenados, transmitidos ou tratados ou de serviços oferecidos por sistemas de rede e informação ou acessíveis por intermédio destes, que, no entanto, foi possível evitar com êxito ou não se materializou (NIS 2)

«Incidente», um evento que ponha em causa a disponibilidade, a autenticidade, a integridade ou a confidencialidade de dados armazenados, transmitidos ou tratados ou dos serviços oferecidos por sistemas de rede e informação ou acessíveis por intermédio destes (NIS 2)

«Incidente com impacto na segurança de um produto com elementos digitais», um incidente que afeta ou pode afetar negativamente a capacidade de um produto com elementos digitais de proteger a disponibilidade, autenticidade, integridade ou confidencialidade dos dados ou das funções (CRA)

IMPACTO DADOS

DEFINIÇÕES - CRA (CONT.)

- ✓ **«Vulnerabilidade»,** um **ponto fraco, uma suscetibilidade ou uma falha** de um produto com elementos digitais **passível de ser explorado por uma ciberameaça**;

- ✓ **«Vulnerabilidade passível de ser explorada»,** uma vulnerabilidade com potencial para ser efetivamente utilizada por um adversário em condições operacionais práticas;

- ✓ **«Vulnerabilidade ativamente explorada»,** uma vulnerabilidade relativamente à qual existem provas fiáveis da sua exploração num sistema por parte de um agente mal-intencionado sem a autorização do proprietário do sistema.

(...)

VULNERABILIDADES

- ✓ A **complexidade dos softwares, configurações e interdependências** entre softwares contribuem para a existência de vulnerabilidades de cibersegurança
- ✓ Podem ser explorada ou não, mas a sua **existência é suficiente** para a sua descoberta
- ✓ Os **dispositivos devem ser concebidos e fabricados de forma a minimizer os riscos**, e isso implica também a **correção das vulnerabilidades encontradas através da atualização de software ("patches")** mesmo que não estejam diretamente associadas a questões de segurança
- ✓ As vulnerabilidades são uma "porta de entrada" à utilização indevida
- ✓ Os fabricantes devem ter implementadas **Políticas de *Cibersecurity Vulnerabilities Disclosure*** (processos de obter informação das vulnerabilidades, sua avaliação, medidas para mitigação e controlo e informação aos vários stakeholders)

3

VIGILÂNCIA

Infarmed
Autoridade Nacional do Medicamento
e Produtos de Saúde, I.P.

SISTEMA NACIONAL DE VIGILÂNCIA

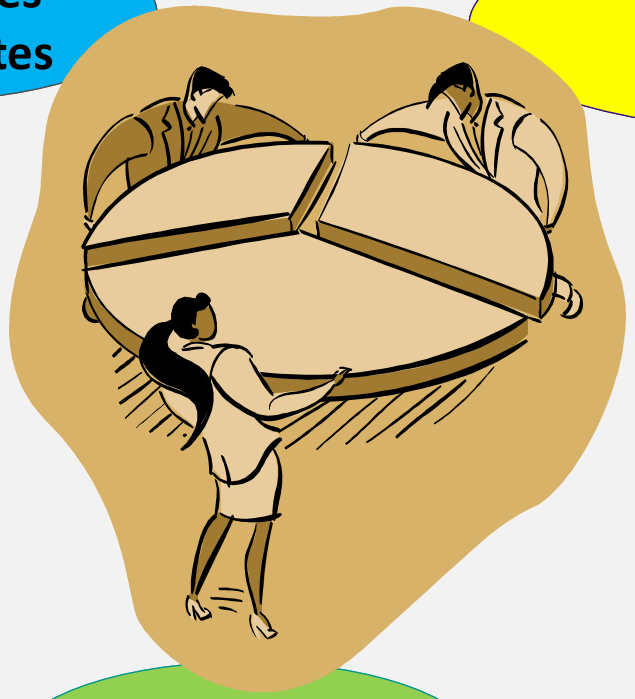
DL 29/2024

- Missão monitorização dos incidentes graves
- Implementação de medidas corretivas de segurança no mercado para evitar a ocorrência de incidentes graves
- Minimização do risco contínua
- Melhoria do conhecimento do perfil de segurança dos dispositivos médicos

INTERVENIENTES – SISTEMA DE VIGILÂNCIA

Autoridades Competentes

Indústria
(fabricantes/ mandatários/importadores/ todos distribuidores)



Utilizadores
(profissionais de saúde, doentes e outros)

Sistema de vigilância fluxo da informação

Utilizadores Profissionais Saúde

NOTIFICAÇÃO de incidente grave

⇩

ANÁLISE → **AC Fabricantes Distribuidores**

Fabricantes (ON, AC se necessário)

⇩

INVESTIGAÇÃO (gestão risco)

⇩

AÇÃO (corretiva/preventiva) → **Fabricantes** (análise pela AC)

FSCA

Fabricantes Distribuidores (AC se necessário)

⇩

DIVULGAÇÃO

(aviso de segurança)

NOTA: As ação corretivas de segurança no mercado (FSCA) são implementadas no mercado para minimizar o risco de ocorrência de incidentes graves (podem ser desencadeadas mesmo antes de ocorrerem incidentes)

Organismo Notificado

INFORMAÇÃO PÓS-MERCADO - GESTÃO DO RISCO

? Problemas nos DMs
Reporte dos utilizadores

Infarmed
Autoridade Nacional do Medicamento e Produtos de Saúde I.P.

Serviços *online*

infoDM
Informação sobre Dispositivos Médicos

Reporte!
Sistema de notificação Incidentes/Denúncias com DM e Efeitos Indesejáveis com Cosméticos

Safety
(segurança do doente)
incidente;
incidente grave

Cibersecurity
(segurança da informação)
vulnerabilidades;
incidentes

! **NOTIFICAÇÃO**

FABRICANTE

- ❑ Avaliar incidentes e vulnerabilidades
- ❑ Adotar medidas: remover DM da net, atualizar o software e/ou outras medidas
- ❑ Comunicação aos utilizadores

- ❖ **Gestão de risco contínua (vulnerability remediation)**
- ❖ **Benefício-risco aceitável**

- ✓ Aumentar a cibersegurança
- ✓ **Minimizar o risco de uma vulnerabilidade associada segurança do doente**

Comunicação aos utilizadores de vulnerabilidades – Aviso de segurança ou outra

A comunicação deve incluir as seguintes informações essenciais:

- ✓ **cronograma** para a resolução da vulnerabilidade (por exemplo, quando a correção estará disponível);
- ✓ **mecanismo de resolução** (por exemplo, como a aplicação da correção ocorrerá);
- ✓ **pontuação da vulnerabilidade**;
- ✓ **índice de explorabilidade** (por exemplo, baixo nível de habilidade) e
- ✓ **método** (por exemplo, remoto) e
- ✓ **medidas provisórias de mitigação de riscos** (por exemplo, quais ações devem ser tomadas, incluindo o uso de controlos compensatórios, enquanto se aguarda a resolução mais permanente).

Profissionais de saúde/Leigos

Vigilância – tipo de notificações à AC pelo fabricante

- Submissão **centralizada** das notificações pelo fabricante – EUDAMED (futuro; mas atualmente e-mail)

  NUR; Nomenclatura DMs; UDI-DI; Nomenclaturas **descrição problema DM, causas, *efeitos na saúde, componentes*;** https://www.imdrf.org/documents/terminologies-categorized-adverse-event-reporting-aer-terms-terminology-and-codes

- Prazos limites **notificação de incidente grave depende da severidade (MIR)** – (art 87º MDR)

  (imediatamente, não mais do que 2, 10, 15 dias de calendário).

- Prazo não definido para **notificação da FSCA** – notificação à AC antes da ação ser tomada, exceto casos de urgência (art 87º MDR).

- **Relatórios periódicos sumários** (previamente acordados) – notificação conjunta de vários incidentes graves semelhantes - causa determinada ou uma FSCA já foi implementada ou incidentes comuns e bem documentados (art 87º MDR).

- **Relatórios de tendência** (art 88º MDR) – aumento estatisticamente significativo na frequência ou severidade de incidentes que não são graves ou de efeitos secundários indesejados esperados – pode ter impacto na relação benefício-risco e que podem constituir riscos inaceitáveis. Fabricante tem de definir como gerir estes incidentes.

VIGILÂNCIA – ARTIGO 87 MDR

COBRE OS ASPECTOS DE CIBERSEGURANÇA? NOTIFICAÇÃO À AUTORIDADE COMPETENTE DOS DMS?

DEPENDE

- SIM
  - ✓Se cumprir a definição de incidente grave
  - ✓Submeter MIR e se necessário relatório FSCA

- NÃO
  - ✓ Caso não cumpra a definição de incidente grave

  Nesta situação as vulnerabilidades e incidentes “security” , bem como as medidas adotadas – Patches (correção de vulnerabilidades)- são geridos e tratados no âmbito do PMS do fabricante e incluídos no PSUR (Periodic Safety Update Report).

RISCO – “SECURITY” E “SAFETY” EXS

Serious incident (Yes/No) SAFETY	Risk Relationship	Device	Security Harm / Security Control	Safety Harm / Safety Control
No	Security risk only.	PACS	Employee stealing data with mobile USB storage on a client pc.	None.
			Implement a User and Usergroup Permission Environment.	Not Applicable.
Yes	Security risk control with a safety impact.	Pacemaker	An unauthorized person is able to fatigue the device by overwhelming the device of requests.	A premature battery depletion may occur.
			Avoid possibility to overwhelming the device.	Not Applicable.

PMS
PSUR

VIGILÂNCIA
MIR e FSCA

ASPECTOS IMPORTANTES PMS E VIGILÂNCIA -TECNOLOGIAS DIGITAIS

- Aspecto da cibersegurança
- Informação para os utilizadores
- Formação dos utilizadores
- Compatibilidade com versões específicas de telemóveis
- Profissional de saúde vs leigo
- Usabilidade
- As Apps e FSCA - garantir que todos os utilizadores leigos têm acesso
- A importância dos dados guardados por estas tecnologias na investigação dos incidentes, principalmente nos leigos
- AI e incidentes graves – maior complexidade

CIBERSEGURANÇA

AO LONGO DO CICLO DE VIDA DO DM

Pre-market activities
Secure Design (Annex I)
Risk management (Annex I)
Establish Risk Control Measures (Annex I)
Validation, Verification, Risk Assessment, Benefit Risk Analysis (Annex I)
Technical Documentation (Annex II and III)
Conformity Assessment (Article 52)
Establish a Post-market Surveillance Plan and Post-market Surveillance System (Article 83 and 84)
Clinical evaluation process (Chapter VI)

Post-market activities
Risk management (Annex I)
Modify Risk Control Measures /Corrective Actions/Patches (Annex I)
Validation, Verification, Risk Assessment, Benefit Risk Analysis (Annex I)
Maintain and update a Post-market Surveillance Plan and Post-market Surveillance System (Article 83 and 84)
Trend Reporting (Article 88)
Analysis of Serious Incidents (Article 89)
Post-Market Surveillance Report (Article 85)
Periodic Safety Update Report (Article 86)
Update Technical Documentation (Annex II and III)
Inform the Electronic System On Vigilance (Article 92)

4

DESAFIOS

Infarmed
Autoridade Nacional do Medicamento
e Produtos de Saúde, I.P.

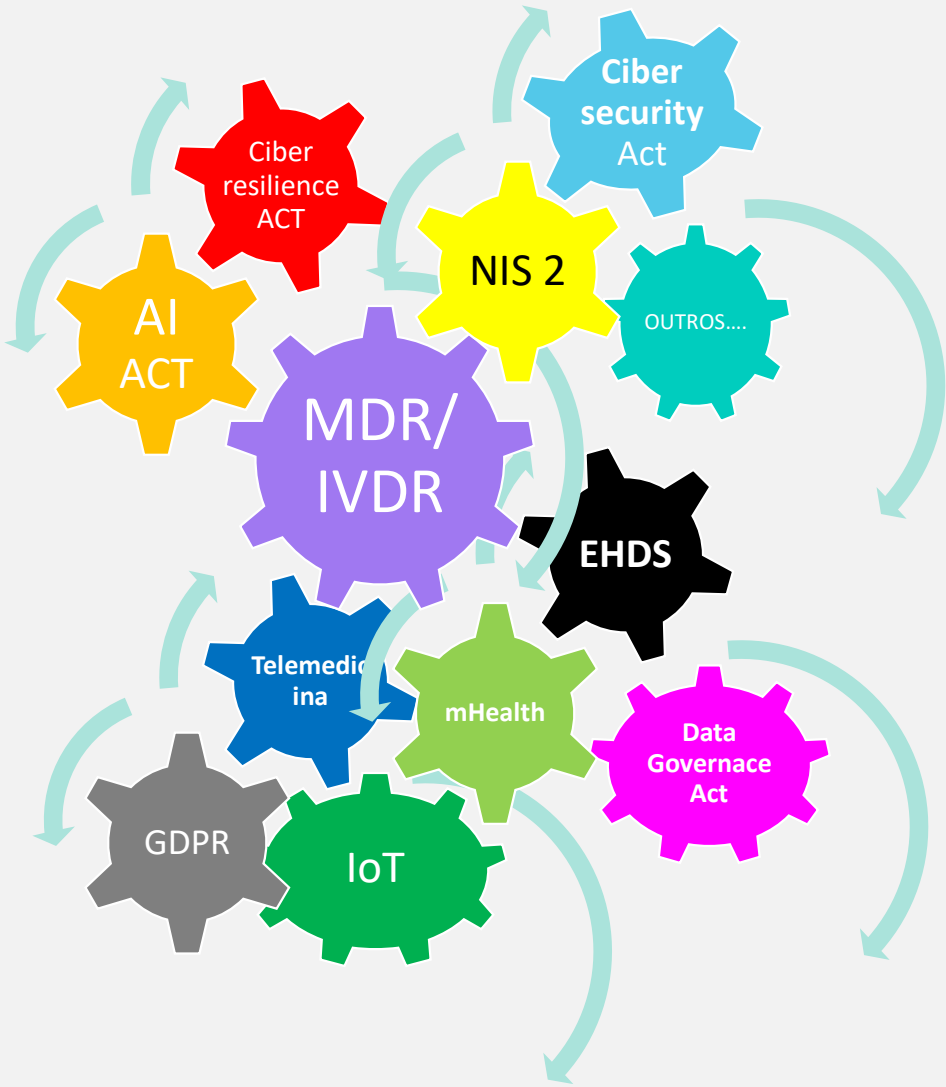
Desafios – Como lidar com big data e PMS

- Because the world has become so connected and everything has become so digitized, there's just an enormous amount of data out there for firms to collect,"
- "From data being shared on personal-use devices to medical devices being linked to a telemetry hub in a hospital setting, to devices that are speaking to doctors directly so they can monitor you remotely – the data is just incredible,"
- "But the problem with having that amount of data out there is, manufacturers aren't necessarily able to get their arms around it and understand what may be going on with their devices, and what may be impacting their performance."

Fonte: *©2017 Lachman Consultant Services, Inc.*
Ricki Chase (ex-FDA Director)

DESAFIOS

Prosseguir com o alinhamento e articulação entre as várias legislações e áreas para Aplicação regulação adequada dos DMs



NOVA PROPOSTA DE ALTERAÇÃO AOS REGULAMENTOS (DEZ 2025)

Cybersecurity (MDR: new Article 87a, Annex I, IVDR: new Article 82a, Annex I)	Serious incidents reported in accordance with the vigilance system established under the MDR or IVDR, which also qualify as actively exploited vulnerabilities and severe incidents as referred to in Regulation (EU) 2024/2847 on cyberresilience, will be made available to the relevant national computer security incident response teams ('CSIRTs') and to the European Union Agency for Cybersecurity (ENISA). In addition, manufacturers will have to report actively exploited vulnerabilities and severe incidents that do not qualify as serious incidents within the meaning of the MDR or IVDR to the CSIRTs and ENISA through Eudamed. In Annex I MDR/IVDR, cybersecurity will be explicitly mentioned in the general safety and performance requirements.

'Article 87a

Reporting of actively exploited vulnerabilities and severe incidents related to devices

1. Without ~~prejudice to the reporting obligations regarding~~ serious incidents and field safety corrective actions set out in Article 87, the manufacturer of a device shall report to the computer security incident response teams ('CSIRTs'), designated as coordinators of the Member States where a device has been made available, and to the European Union Agency for Cybersecurity (ENISA), either of the following:

Anexo I

Section 17.4. is replaced by the following:

'17.4. Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics, IT security measures and cybersecurity, including protection against unauthorised access, necessary to run the software as intended.';

CONCLUINDO…

- A cibersegurança é um aspeto muito importante e específico de alguns dispositivos que tem de ser articulado com a vertente da segurança do doente
- A legislação dos dispositivos médicos no que respeita à gestão do risco assenta no princípio de “**safety” and “security” by design** , sendo a gestão do risco constante deste o pré ao pós mercado, e a demonstração da conformidade continua do cumprimento dos requisitos gerais de segurança e desempenho (que inclui a cibersegurança)
- O processo de **gestão do risco é integrado** “safety” e “security” durante todo o ciclo de vida
- O pós mercado deve **recolher informação e adotar medidas** para minimização do risco na vertente “safety” e “cibersecurity”.
- **Responsabilidade partilhada** de todos os intervenientes fabricante, e outros operadores económicos, utilizadores, reguladores e outros.
- **Partilha de informação**.

PERGUNTAS

Infarmed
Autoridade Nacional do Medicamento
e Produtos de Saúde, I.P.

OBRIGADA

Infarmed
Autoridade Nacional do Medicamento
e Produtos de Saúde, I.P.