Conselho da
União Europeia

Bruxelas, 16 de setembro de 2022
(OR. en)

12429/22
ADD 1

Dossiê interinstitucional:
2022/0272(COD)

CYBER 298
JAI 1181
DATAPROTECT 254
TELECOM 369
MI 665
CSC 388
CSCI 133
CODEC 1310
IA 133

NOTA DE ENVIO

de:	Secretária-geral da Comissão Europeia, com a assinatura de Martine DEPREZ, diretora
data de receção:	15 de setembro de 2022
para:	Secretariado-Geral do Conselho
n.° doc. Com.:	COM(2022) 454 final - ANEXOS 1 a 6
Assunto:	ANEXOS da PROPOSTA DE REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera o Regulamento (UE) 2019/1020

Envia-se em anexo, à atenção das delegações, o documento COM(2022) 454 final - ANEXOS 1 a 6.

Anexo: COM(2022) 454 final - ANEXOS 1 a 6

COMISSÃO
EUROPEIA

Bruxelas, 15.9.2022
COM(2022) 454 final

ANNEXES 1 to 6

ANEXOS

da

PROPOSTA DE REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera o Regulamento (UE) 2019/1020

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

ANEXO I

REQUISITOS ESSENCIAIS DE CIBERSEGURANÇA

1. REQUISITOS DE SEGURANÇA RELATIVOS ÀS PROPRIEDADES DOS PRODUTOS COM ELEMENTOS DIGITAIS

(1) Os produtos com elementos digitais devem ser concebidos, desenvolvidos e produzidos de modo a garantir um nível adequado de cibersegurança com base nos riscos;

(2) Os produtos com elementos digitais devem ser entregues sem nenhuma vulnerabilidade conhecida passível de ser explorada;

(3) Com base na avaliação dos riscos referida no artigo 10.º, n.º 2, e se for caso disso, os produtos com elementos digitais devem:

(a) Ser entregues com uma configuração segura por defeito, incluindo a possibilidade de restaurar o produto para o seu estado original;

(b) Assegurar a proteção contra o acesso não autorizado através de mecanismos de controlo adequados, incluindo, nomeadamente, sistemas de autenticação, identidade ou gestão de acessos;

(c) Proteger a confidencialidade dos dados armazenados, transmitidos ou tratados de outra forma, sejam eles pessoais ou de outra natureza, por exemplo através da cifragem de dados inativos ou em trânsito pertinentes por mecanismos de ponta;

(d) Proteger a integridade dos dados armazenados, transmitidos ou tratados de outra forma, sejam eles pessoais ou de outra natureza, dos comandos, dos programas e da configuração contra qualquer manipulação ou modificação não autorizada pelo utilizador, bem como comunicar informações sobre as corrupções;

(e) Tratar apenas dados, pessoais ou de outra natureza, que sejam adequados, pertinentes e limitados ao que é necessário para a utilização prevista do produto («minimização de dados»);

(f) Proteger a disponibilidade de funções essenciais, incluindo a resiliência a ataques de negação de serviço e a atenuação dos seus efeitos;

(g) Minimizar o seu próprio impacto negativo na disponibilidade de serviços prestados por outros dispositivos ou redes;

(h) Ser concebidos, desenvolvidos e produzidos de forma a limitar superfícies de ataque, incluindo interfaces externas;

(i) Ser concebidos, desenvolvidos e produzidos de forma a reduzir o impacto de incidentes, utilizando mecanismos e técnicas adequados de atenuação da exploração;

(j) Facultar informações relacionadas com a segurança através do registo e/ou controlo da atividade interna pertinente, incluindo o acesso ou a alteração de dados, serviços ou funções;

(k) Assegurar a possibilidade de resolver as vulnerabilidades através de atualizações de segurança, incluindo, se for caso disso, através de atualizações automáticas e da notificação aos utilizadores das atualizações disponíveis.

2. REQUISITOS DE TRATAMENTO DE VULNERABILIDADES

Os fabricantes dos produtos com elementos digitais devem:

(1) Identificar e documentar vulnerabilidades e componentes existentes no produto, nomeadamente elaborando uma lista de materiais do *software* num formato de uso corrente e legível por máquina que abranja, pelo menos, as dependências de nível superior do produto;

(2) Em relação aos riscos que os produtos com elementos digitais enfrentam, resolver e corrigir, sem demora, as vulnerabilidades, nomeadamente disponibilizando atualizações de segurança;

(3) Efetuar ensaios e análises eficazes e regulares da segurança do produto com elementos digitais;

(4) Uma vez disponibilizada uma atualização de segurança, divulgar publicamente informações sobre as vulnerabilidades corrigidas, incluindo uma descrição das mesmas, informações que permitam aos utilizadores identificar o produto com elementos digitais afetado, os impactos das vulnerabilidades, a sua gravidade e informações que ajudem os utilizadores a corrigir as vulnerabilidades;

(5) Definir e aplicar uma política de divulgação coordenada de vulnerabilidades;

(6) Tomar medidas para facilitar a partilha de informações sobre potenciais vulnerabilidades no seu produto com elementos digitais, bem como em componentes de terceiros incluídos nesse produto, nomeadamente facultando um endereço de contacto para a comunicação das vulnerabilidades detetadas no produto com elementos digitais;

(7) Prever mecanismos para distribuir de forma segura as atualizações de produtos com elementos digitais, a fim de assegurar a correção ou atenuação das vulnerabilidades passíveis de serem exploradas em tempo útil;

(8) Assegurar que as atualizações corretivas de segurança ou outras atualizações disponíveis para resolver problemas de segurança identificados sejam distribuídas sem demora e de forma gratuita, juntamente com orientações que facultem aos utilizadores informações pertinentes, nomeadamente sobre as eventuais medidas a tomar.

ANEXO II

INFORMAÇÕES E INSTRUÇÕES DESTINADAS AO UTILIZADOR

No mínimo, devem ser fornecidas com o produto com elementos digitais as seguintes indicações:

1. O nome, nome comercial registado ou marca registada do fabricante, bem como o seu endereço postal e endereço de correio eletrónico de contacto, apostos no produto ou, se tal não for possível, na embalagem ou num documento que o acompanhe;

2. O ponto de contacto por meio do qual se pode comunicar e receber informações sobre vulnerabilidades de cibersegurança do produto;

3. A identificação correta do tipo, lote, versão ou número de série ou outros elementos que permitam a identificação do produto e as respetivas instruções e informações destinadas ao utilizador;

4. A utilização prevista, incluindo o ambiente de segurança proporcionado pelo fabricante, bem como as funcionalidades essenciais do produto e informações sobre as propriedades de segurança;

5. Qualquer circunstância conhecida ou previsível, relacionada com a utilização do produto com elementos digitais de acordo com a sua finalidade prevista ou em condições de utilização indevida razoavelmente previsível que possam dar origem a riscos de cibersegurança significativos;

6. Se é possível aceder à lista de materiais do *software* e, se for caso disso, onde se pode fazê-lo;

7. Se for caso disso, o endereço Internet que permite aceder à declaração de conformidade UE;

8. O tipo de apoio técnico no domínio da segurança que o fabricante oferece e até quando será prestado ou, no mínimo, até quando os utilizadores podem esperar receber atualizações de segurança;

9. Instruções pormenorizadas ou um endereço Internet que remeta para tais instruções pormenorizadas e informações sobre:

   (a) As medidas a tomar quando o produto é posto em funcionamento pela primeira vez e ao longo de toda a sua vida útil de modo a garantir uma utilização segura do mesmo;

   (b) Como as alterações do produto podem afetar a segurança dos dados;

   (c) Como podem ser instaladas atualizações relevantes em termos de segurança;

   (d) A desativação segura do produto, incluindo informações sobre como se pode remover de forma segura os dados dos utilizadores.

ANEXO III

PRODUTOS CRÍTICOS COM ELEMENTOS DIGITAIS

Classe I

1. *Software* de sistemas de gestão de identidade e *software* de gestão de acesso privilegiado;
2. Navegadores autónomos e incorporados;
3. Gestores de senhas;
4. *Software* de pesquisa, remoção ou colocação em quarentena de *software* malicioso;
5. Produtos com elementos digitais com a função de rede privada virtual (VPN);
6. Sistemas de gestão de rede;
7. Ferramentas de gestão da configuração da rede;
8. Sistemas de monitorização do tráfego na rede;
9. Gestão de recursos de rede;
10. Sistemas de gestão de informações e eventos de segurança (SIEM);
11. Gestão de atualizações/atualizações corretivas, incluindo gestores de arranque;
12. Sistemas de gestão da configuração de aplicações;
13. *Software* de acesso remoto/partilha à distância;
14. *Software* de gestão de dispositivos móveis;
15. Interfaces físicas da rede;
16. Sistemas operativos não abrangidos pela classe II;
17. Barreiras de segurança, sistemas de deteção e/ou prevenção de intrusões não abrangidos pela classe II;
18. Encaminhadores, *modems* para ligação à Internet e comutadores não abrangidos pela classe II;
19. Microprocessadores não abrangidos pela classe II;
20. Microcontroladores;
21. Circuitos integrados de aplicação específica (ASIC) e redes de portas lógicas programáveis (FPGA) destinados a serem utilizados por entidades essenciais do tipo referido no [anexo I da Diretiva XXX/XXXX (SRI 2)];

22. Sistemas de controlo da automação industrial (IACS) não abrangidos pela classe II, tais como controladores lógicos programáveis (PLC), sistemas de controlo distribuído (DCS), controladores numéricos computorizados (CNC) para máquinas-ferramentas e sistemas de supervisão, controlo e aquisição de dados (SCADA);

23. Internet das coisas industrial não abrangida pela classe II.

Classe II

1. Sistemas operativos para servidores, computadores de secretária e dispositivos móveis;

2. Hipervisores e sistemas *container runtime* que permitam a execução virtualizada de sistemas operativos e ambientes semelhantes;

3. Infraestruturas de chaves públicas e emitentes de certificados digitais;

4. Barreiras de segurança, sistemas de deteção e/ou prevenção de intrusões destinados a utilização industrial;

5. Microprocessadores de uso geral;

6. Microprocessadores destinados a integração em controladores lógicos programáveis e em elementos seguros;

7. Encaminhadores, *modems* para ligação à Internet e comutadores destinados a utilização industrial;

8. Elementos seguros;

9. Módulos de segurança físicos (HSM);

10. Criptoprocessadores seguros;

11. Cartões inteligentes, leitores de cartões inteligentes e dispositivos de autenticação;

12. Sistemas de controlo da automação industrial (IACS) destinados a serem utilizados por entidades essenciais do tipo referido no [anexo I da Diretiva XXX/XXXX (SRI 2)], tais como controladores lógicos programáveis (PLC), sistemas de controlo distribuído (DCS), controladores numéricos computorizados (CNC) para máquinas-ferramentas e sistemas de supervisão, controlo e aquisição de dados (SCADA);

13. Dispositivos da Internet das coisas industrial destinados a serem utilizados por entidades essenciais do tipo referido no [anexo I da Diretiva XXX/XXXX (SRI 2)];

14. Componentes de sensores e acionadores de robôs e controladores de robôs;

15. Contadores inteligentes.

ANEXO IV

DECLARAÇÃO DE CONFORMIDADE UE

A declaração de conformidade UE referida no artigo 20.º deve conter todas as seguintes informações:

1. Nome e tipo do produto com elementos digitais, bem como quaisquer informações complementares que permitam a sua identificação única;

2. Nome e endereço do fabricante ou do respetivo mandatário;

3. Menção de que a declaração de conformidade UE é emitida sob a exclusiva responsabilidade do fornecedor;

4. Objeto da declaração (identificação do produto que permita rastreá-lo, podendo incluir uma fotografia, se for caso disso);

5. Menção de que o objeto da declaração acima mencionado está em conformidade com a legislação de harmonização da União aplicável;

6. Referências a quaisquer normas harmonizadas pertinentes aplicadas ou a quaisquer outras especificações comuns ou certificações da cibersegurança em relação às quais é declarada a conformidade;

7. Se for caso disso, nome e número do organismo notificado, descrição do procedimento de avaliação da conformidade efetuado e identificação do certificado emitido;

8. Informações complementares:

Assinado em nome de: ……

(local e data de emissão):

(nome, cargo) (assinatura):

ANEXO V

TEOR DA DOCUMENTAÇÃO TÉCNICA

A documentação técnica referida no artigo 23.º deve incluir, pelo menos, as informações indicadas a seguir, consoante aplicável ao produto com elementos digitais em causa:

1. Uma descrição geral do produto com elementos digitais, incluindo:

   (a) A sua finalidade prevista;

   (b) Versões do *software* suscetíveis de afetar a conformidade com os requisitos essenciais;

   (c) Se o produto com elementos digitais for um produto de *hardware*, fotografias ou ilustrações que mostrem as características externas, a marcação e a disposição interna;

   (d) Informações e instruções destinadas aos utilizadores, conforme consta do anexo II;

2. Uma descrição da conceção, do desenvolvimento, da produção do produto e dos processos de tratamento de vulnerabilidades, incluindo:

   (a) Informações completas sobre a conceção e o desenvolvimento do produto com elementos digitais, incluindo, se for caso disso, ilustrações e esquemas e/ou uma descrição da arquitetura do sistema que explique de que forma os componentes de *software* se apoiam ou se alimentam mutuamente e se integram no processamento global;

   (b) Informações e especificações completas sobre os processos de tratamento de vulnerabilidades aplicados pelo fabricante, incluindo a lista de materiais do *software*, a política de divulgação coordenada de vulnerabilidades, comprovativos da disponibilização de um endereço de contacto para a comunicação de vulnerabilidades e uma descrição das soluções técnicas escolhidas para a distribuição segura de atualizações;

   (c) Informações e especificações completas sobre os processos de produção e controlo do produto com elementos digitais e a validação desses processos;

3. Uma avaliação dos riscos de cibersegurança tidos em conta na conceção, no desenvolvimento, na produção, na entrega e na manutenção do produto com elementos digitais, em conformidade com o artigo 10.º do presente regulamento;

4. Uma lista das normas harmonizadas aplicadas total ou parcialmente, cujas referências tenham sido publicadas no *Jornal Oficial da União Europeia*, das especificações comuns previstas no artigo 19.º do presente regulamento ou dos sistemas de certificação da cibersegurança aplicados ao abrigo do Regulamento (UE) 2019/881, nos termos do artigo 18.º, n.º 3, e, nos casos em que essas normas harmonizadas, especificações comuns ou sistemas de certificação da cibersegurança

não tenham sido aplicados, uma descrição das soluções adotadas para dar cumprimento aos requisitos essenciais estabelecidos no anexo I, secções 1 e 2, incluindo uma lista de outras especificações técnicas pertinentes aplicadas. Em caso de aplicação parcial das normas harmonizadas, das especificações comuns ou dos sistemas de certificação da cibersegurança, a documentação técnica deve especificar as partes que foram aplicadas;

5. Relatórios dos ensaios realizados para verificar a conformidade do produto e dos processos de tratamento de vulnerabilidades com os requisitos essenciais aplicáveis estabelecidos no anexo I, secções 1 e 2;

6. Uma cópia da declaração de conformidade UE;

7. Se for caso disso, a lista de materiais do *software*, na aceção do artigo 3.º, ponto 36, na sequência de um pedido fundamentado de uma autoridade de fiscalização do mercado, desde que tal seja necessário para que a referida autoridade possa verificar a conformidade com os requisitos essenciais estabelecidos no anexo I.

ANEXO VI

PROCEDIMENTOS DE AVALIAÇÃO DA CONFORMIDADE

Procedimento de avaliação da conformidade baseado no controlo interno (com base no módulo A)

1. O controlo interno é o procedimento de avaliação da conformidade mediante o qual o fabricante cumpre as obrigações estabelecidas nos pontos 2, 3 e 4 e garante e declara, sob a sua exclusiva responsabilidade, que os produtos com elementos digitais cumprem todos os requisitos essenciais constantes do anexo I, secção 1, e que o fabricante cumpre os requisitos essenciais estabelecidos no anexo I, secção 2.

2. O fabricante deve elaborar a documentação técnica descrita no anexo V.

3. Conceção, desenvolvimento, produção e tratamento de vulnerabilidades de produtos com elementos digitais

   O fabricante deve tomar todas as medidas necessárias para que os processos de conceção, desenvolvimento, produção e tratamento de vulnerabilidades, bem como o respetivo controlo, assegurem a conformidade dos produtos com elementos digitais fabricados ou desenvolvidos e dos processos aplicados pelo fabricante com os requisitos essenciais previstos no anexo I, secções 1 e 2.

4. Marcação de conformidade e declaração de conformidade

4.1. O fabricante deve apor a marcação CE em cada produto com elementos digitais que cumpra os requisitos aplicáveis do presente regulamento.

4.2. O fabricante deve elaborar uma declaração de conformidade UE escrita para cada produto com elementos digitais nos termos do artigo 20.º e mantê-la, juntamente com a documentação técnica, à disposição das autoridades nacionais, por um período de dez anos a contar da data de colocação no mercado do produto com elementos digitais. A declaração de conformidade UE deve identificar o produto com elementos digitais para o qual foi elaborada. Deve ser fornecida cópia da declaração de conformidade UE às autoridades competentes, a seu pedido.

5. Mandatários

   As obrigações do fabricante enunciadas no ponto 4 podem ser cumpridas, em seu nome e sob a sua responsabilidade, pelo seu mandatário, desde que se encontrem especificadas no mandato.

Exame UE de tipo (com base no módulo B)

1. O exame UE de tipo é a parte do procedimento de avaliação da conformidade em que um organismo notificado examina o projeto técnico e o desenvolvimento de um produto, bem como os processos de tratamento de vulnerabilidades aplicados pelo fabricante, e certifica que um produto com elementos digitais cumpre os requisitos essenciais estabelecidos no anexo I, secção 1, e que o fabricante cumpre os requisitos essenciais estabelecidos no anexo I, secção 2.

– O exame UE de tipo deve ser realizado através da avaliação da adequação do projeto técnico e do desenvolvimento do produto mediante análise da documentação técnica e dos elementos de prova referidos no ponto 3, bem como do exame de amostras de uma ou mais partes críticas do produto (combinação de tipo de produção e tipo de projeto).

2. O fabricante deve apresentar o pedido de exame UE de tipo a um único organismo notificado da sua escolha.

O pedido deve incluir os seguintes elementos:

– o nome e o endereço do fabricante e, se for apresentado pelo mandatário, o nome e o endereço deste último,

– uma declaração por escrito indicando que o mesmo pedido não foi apresentado a nenhum outro organismo notificado,

– a documentação técnica, que deve permitir avaliar a conformidade do produto com os requisitos essenciais aplicáveis constantes do anexo I, secção 1, e os processos de tratamento de vulnerabilidades do fabricante constantes do anexo I, secção 2, e deve incluir uma análise e uma avaliação adequadas do(s) risco(s). A documentação técnica deve especificar os requisitos aplicáveis e abranger, se tal for pertinente para efeitos de avaliação, a conceção, o fabrico e o funcionamento do produto. A documentação técnica deve conter, se for caso disso, pelo menos os elementos previstos no anexo V,

– os elementos de prova da adequação das soluções de projeto técnico e desenvolvimento e dos processos de tratamento de vulnerabilidades. Esses elementos devem fazer menção aos documentos utilizados, designadamente nos casos em que não foram integralmente aplicadas as normas harmonizadas e/ou as especificações técnicas pertinentes. Os elementos de prova devem incluir, se necessário, os resultados dos ensaios realizados pelo laboratório competente do fabricante ou por qualquer outro laboratório de ensaios em nome e sob a responsabilidade do fabricante.

3. O organismo notificado deve:

3.1. Examinar a documentação técnica e os elementos de prova para avaliar a adequação do projeto técnico e do desenvolvimento do produto aos requisitos essenciais constantes do anexo I, secção 1, e a adequação dos processos de tratamento de vulnerabilidades aplicados pelo fabricante aos requisitos essenciais estabelecidos no anexo I, secção 2;

3.2. Verificar se a amostra ou amostras foram desenvolvidas ou fabricadas em conformidade com a documentação técnica e identificar os elementos concebidos e desenvolvidos de acordo com as disposições aplicáveis das normas harmonizadas e/ou especificações técnicas pertinentes, bem como os elementos cuja conceção e desenvolvimento não se baseiem nas disposições pertinentes dessas normas;

3.3. Realizar, ou mandar realizar, os exames e os ensaios adequados para verificar se, caso o fabricante tenha optado pelas soluções constantes das normas harmonizadas e/ou especificações técnicas pertinentes para os requisitos previstos no anexo I, essas soluções foram corretamente aplicadas;

3.4. Realizar, ou mandar realizar, os exames e ensaios necessários para verificar se, caso as soluções constantes das normas harmonizadas e/ou especificações técnicas pertinentes para os requisitos previstos no anexo I não tenham sido aplicadas, as soluções adotadas pelo fabricante cumprem os requisitos essenciais correspondentes;

3.5. Acordar com o fabricante o local de realização dos exames e dos ensaios.

4. O organismo notificado deve elaborar um relatório de avaliação que indique as atividades desenvolvidas de acordo com o ponto 4 e os respetivos resultados. Sem prejuízo das suas obrigações para com as autoridades notificadoras, o organismo notificado só pode divulgar, no todo ou em parte, o conteúdo desse relatório com o acordo do fabricante.

5. Se o tipo e os processos de tratamento de vulnerabilidades cumprirem os requisitos essenciais constantes do anexo I, o organismo notificado deve remeter ao fabricante um certificado de exame UE de tipo. O certificado deve conter o nome e o endereço do fabricante, as conclusões do exame, as condições (se as houver) da sua validade e os dados necessários à identificação do tipo aprovado e dos processos de tratamento de vulnerabilidades. O certificado pode ser acompanhado de um ou mais anexos.

   O certificado e os seus anexos devem conter todas as informações necessárias para permitir a avaliação da conformidade dos produtos fabricados ou desenvolvidos com o tipo e os processos de tratamento de vulnerabilidades examinados e para permitir o controlo em serviço.

   Nos casos em que o tipo e os processos de tratamento de vulnerabilidades não cumpram os requisitos essenciais aplicáveis constantes do anexo I, o organismo notificado deve recusar emitir um certificado de exame UE de tipo e deve informar o requerente desse facto, fundamentando pormenorizadamente as razões da sua recusa.

6. O organismo notificado deve manter-se a par das alterações do estado da técnica geralmente reconhecido que indiquem que o tipo aprovado e os processos de tratamento de vulnerabilidades podem ter deixado de cumprir os requisitos essenciais aplicáveis constantes do anexo I do presente regulamento e deve determinar se tais alterações requerem exames complementares. Em caso afirmativo, o organismo notificado deve informar o fabricante desse facto.

   O fabricante deve informar o organismo notificado que possui a documentação técnica relativa ao certificado de exame UE de tipo de todas as modificações do tipo aprovado e dos processos de tratamento de vulnerabilidades que possam afetar a conformidade com os requisitos essenciais constantes do anexo I ou as condições de

validade do certificado. Tais modificações devem ser objeto de aprovação complementar, na forma de aditamento ao certificado original de exame UE de tipo.

7. O organismo notificado deve informar as autoridades notificadoras dos certificados de exame UE de tipo e/ou respetivos aditamentos que emitiu ou retirou e fornecer-lhes periodicamente, ou mediante pedido, a lista dos certificados e/ou respetivos aditamentos recusados, suspensos ou objeto de restrições.

   Cada organismo notificado deve informar os outros organismos notificados dos certificados de exame UE de tipo e/ou respetivos aditamentos que tenha recusado, retirado, suspendido ou submetido a quaisquer outras restrições e, mediante pedido, dos certificados que tenha emitido e/ou dos aditamentos que tenha introduzido nos mesmos.

   A Comissão, os Estados-Membros e os outros organismos notificados podem, mediante pedido, obter cópia dos certificados de exame UE de tipo e/ou dos respetivos aditamentos. Mediante pedido, a Comissão e os Estados- Membros podem obter cópia da documentação técnica e dos resultados dos exames efetuados pelo organismo notificado. O organismo notificado deve conservar uma cópia do certificado de exame UE de tipo e dos respetivos anexos e aditamentos, assim como do processo técnico, incluindo a documentação apresentada pelo fabricante, até ao termo da validade do certificado.

8. O fabricante deve manter à disposição das autoridades nacionais uma cópia do certificado de exame UE de tipo e dos respetivos anexos e aditamentos, assim como da documentação técnica, por um período de dez anos a contar da data de colocação do produto no mercado.

9. O mandatário do fabricante pode apresentar o pedido referido no ponto 3 e cumprir as obrigações previstas nos pontos 7 e 9, desde que se encontrem especificadas no mandato.

Conformidade com o tipo baseada no controlo interno da produção (com base no módulo C)

1. A conformidade com o tipo baseada no controlo interno da produção é a parte do procedimento de avaliação da conformidade mediante a qual o fabricante cumpre as obrigações estabelecidas nos pontos 2 e 3 e garante e declara que os produtos em causa estão em conformidade com o tipo descrito no certificado de exame UE de tipo e satisfazem os requisitos essenciais constantes do anexo I, secção 1.

2. Produção

2.1. O fabricante deve tomar todas as medidas necessárias para que a produção e o respetivo controlo garantam a conformidade dos produtos fabricados com o tipo aprovado descrito no certificado de exame UE de tipo e com os requisitos essenciais constantes do anexo I, secção 1.

3. Marcação de conformidade e declaração de conformidade

3.1. O fabricante deve apor a marcação CE em cada produto que esteja em conformidade com o tipo descrito no certificado de exame UE de tipo e que cumpra os requisitos aplicáveis do instrumento legislativo.

3.2. O fabricante deve elaborar uma declaração de conformidade escrita para cada modelo de produto e mantê-la à disposição das autoridades nacionais, por um período de dez anos a contar da data de colocação do produto no mercado. A declaração de conformidade deve identificar o modelo de produto para o qual foi elaborada. Deve ser fornecida às autoridades competentes, a pedido destas, uma cópia da declaração de conformidade.

4. Mandatário

As obrigações do fabricante enunciadas no ponto 3 podem ser cumpridas, em seu nome e sob a sua responsabilidade, pelo seu mandatário, desde que se encontrem especificadas no mandato.

Conformidade baseada na garantia de qualidade total (com base no módulo H)

1. A conformidade baseada na garantia de qualidade total é o procedimento de avaliação da conformidade mediante o qual o fabricante cumpre as obrigações estabelecidas nos pontos 2 e 5 e garante e declara, sob a sua exclusiva responsabilidade, que os produtos (ou as categorias de produtos) em causa cumprem os requisitos essenciais constantes do anexo I, secção 1, e que os processos de tratamento de vulnerabilidades por si aplicados cumprem os requisitos estabelecidos no anexo I, secção 2.

2. Conceção, desenvolvimento, produção e tratamento de vulnerabilidades de produtos com elementos digitais

O fabricante deve aplicar um sistema de qualidade aprovado, nos termos do ponto 3, para a conceção, o desenvolvimento e a produção dos produtos em causa e para o tratamento de vulnerabilidades, deve manter a sua eficácia durante todo o ciclo de vida dos produtos em causa e fica sujeito à fiscalização prevista no ponto 4.

3. Sistema de qualidade

3.1. O fabricante deve apresentar um pedido de avaliação do seu sistema de qualidade para os produtos em causa a um organismo notificado da sua escolha.

O pedido deve incluir os seguintes elementos:

– o nome e o endereço do fabricante e, se for apresentado pelo mandatário, o nome e o endereço deste último,

– a documentação técnica para um modelo de cada categoria de produtos que se pretende fabricar ou desenvolver. A documentação técnica deve conter, no mínimo, se aplicável, os elementos previstos no anexo V,

– a documentação relativa ao sistema de qualidade, e

– uma declaração escrita indicando que o mesmo pedido não foi apresentado a nenhum outro organismo notificado.

3.2. O sistema de qualidade deve assegurar a conformidade dos produtos com os requisitos essenciais constantes do anexo I, secção 1, e a conformidade dos processos de tratamento de vulnerabilidades aplicados pelo fabricante com os requisitos estabelecidos no anexo I, secção 2.

Todos os elementos, requisitos e disposições adotados pelo fabricante devem ser documentados de modo sistemático e ordenado, sob a forma de políticas, procedimentos e instruções escritas. A documentação relativa ao sistema de qualidade deve permitir uma interpretação coerente dos programas, planos, manuais e registos de qualidade.

Em especial, deve conter uma descrição adequada do seguinte:

– objetivos de qualidade e estrutura organizativa, responsabilidades e competências dos órgãos de gestão no que diz respeito à conceção, ao desenvolvimento, à qualidade do produto e ao tratamento de vulnerabilidades,

– especificações do projeto técnico e do desenvolvimento, incluindo as normas que serão aplicadas e, se as normas harmonizadas e/ou as especificações técnicas pertinentes não forem integralmente aplicadas, os meios a utilizar para assegurar o cumprimento dos requisitos essenciais constantes do anexo I, secção 1, aplicáveis aos produtos,

– especificações processuais, incluindo as normas que serão aplicadas e, se as normas harmonizadas e/ou as especificações técnicas pertinentes não forem integralmente aplicadas, os meios a utilizar para assegurar o cumprimento dos requisitos essenciais constantes do anexo I, secção 2, aplicáveis ao fabricante,

– o controlo da conceção e do desenvolvimento, bem como as técnicas, os processos e as ações sistemáticas de verificação da conceção e do desenvolvimento a adotar ao conceber e desenvolver os produtos pertencentes à categoria abrangida,

– as técnicas, processos e ações sistemáticas de produção, controlo da qualidade e garantia da qualidade a aplicar correspondentes,

– exames e ensaios a executar antes, durante e após a produção, e a frequência com que serão realizados,

– os registos de qualidade, como relatórios de inspeções e dados dos ensaios, dados de calibração, relatórios de qualificação do pessoal envolvido, etc.,

– meios que permitam controlar a obtenção da qualidade exigida ao nível da conceção e do produto, bem como a eficácia do funcionamento do sistema de qualidade.

3.3. O organismo notificado deve avaliar o sistema de qualidade para determinar se este satisfaz os requisitos referidos no ponto 3.2.

O organismo notificado deve presumir que são conformes com esses requisitos os elementos do sistema de qualidade que cumpram as especificações correspondentes da norma nacional que transpõe a norma harmonizada e/ou as especificações técnicas aplicáveis.

Para além de experiência em sistemas de gestão da qualidade, o grupo de auditores deve incluir pelo menos um membro com experiência como assessor no domínio pertinente do produto e na tecnologia do produto em causa e com conhecimento dos requisitos aplicáveis do presente regulamento. A auditoria deve incluir uma visita de avaliação às instalações do fabricante, no caso de estas existirem. O grupo de auditores deve analisar a documentação técnica referida no ponto 3.1, segundo travessão, para verificar a capacidade de o fabricante identificar os requisitos aplicáveis do presente regulamento e realizar os exames necessários, com vista a assegurar a conformidade do produto com esses requisitos.

A decisão deve ser notificada ao fabricante ou ao respetivo mandatário.

A notificação deve conter as conclusões da auditoria e a decisão de avaliação fundamentada.

3.4. O fabricante compromete-se a cumprir as obrigações decorrentes do sistema de qualidade aprovado e a assegurar que permanece adequado e eficaz.

3.5. O fabricante mantém informado o organismo notificado que tiver aprovado o sistema de qualidade de qualquer alteração planeada para o referido sistema.

O organismo notificado deve avaliar as alterações propostas e decidir se o sistema da qualidade alterado continua a satisfazer os requisitos referidos no ponto 3.2 ou se é necessária uma reavaliação.

O organismo notificado deve notificar o fabricante da sua decisão. A notificação deve conter as conclusões do exame e a decisão de avaliação fundamentada.

4. Fiscalização sob a responsabilidade do organismo notificado

4.1. O objetivo da fiscalização é garantir que o fabricante cumpre devidamente as obrigações decorrentes do sistema de qualidade aprovado.

4.2. O fabricante deve permitir o acesso do organismo notificado, para fins de avaliação, aos locais de conceção, desenvolvimento, produção, inspeção, ensaio e armazenamento, e facultar-lhe todas as informações necessárias, em especial:

– a documentação relativa ao sistema de qualidade,

– os registos de qualidade previstos na parte do sistema de qualidade dedicada à conceção, tais como resultados de análises, cálculos, ensaios, etc.,

– os registos de qualidade previstos na parte do sistema de qualidade dedicada ao fabrico, tais como relatórios de inspeções, dados dos ensaios e de calibração, relatórios de qualificação do pessoal envolvido, etc.

4.3. O organismo notificado deve efetuar auditorias periódicas para se certificar de que o fabricante mantém e aplica o sistema de qualidade e deve fornecer-lhe os relatórios dessas auditorias.

5. Marcação de conformidade e declaração de conformidade

5.1. O fabricante deve apor a marcação CE e, sob a responsabilidade do organismo notificado referido no ponto 3.1, o número de identificação deste último em cada produto que cumpra os requisitos constantes do anexo I, secção 1 do presente regulamento.

5.2. O fabricante deve elaborar uma declaração de conformidade escrita para cada modelo de produto e mantê-la à disposição das autoridades nacionais, por um período de dez anos a contar da data de colocação do produto no mercado. A declaração de conformidade deve identificar o modelo de produto para o qual foi elaborada.

Deve ser fornecida às autoridades competentes, a pedido destas, uma cópia da declaração de conformidade.

6. O fabricante deve manter à disposição das autoridades nacionais, durante um período não inferior a dez anos a contar da data de colocação do produto no mercado:

– a documentação técnica referida no ponto 3.1,

– a documentação relativa ao sistema de qualidade referida no ponto 3.1,

– a alteração, aprovada, a que se refere o ponto 3.5,

– as decisões e os relatórios do organismo notificado a que se referem os pontos 3.5, 4.3 e 4.4.

7. Cada organismo notificado deve informar as suas autoridades notificadoras das aprovações de sistemas de qualidade concedidas ou retiradas e, periodicamente ou mediante pedido, deve disponibilizar a essas autoridades a lista das aprovações de sistemas de qualidade que tenha recusado, suspendido ou submetido a quaisquer outras restrições.

Cada organismo notificado deve informar os outros organismos notificados das aprovações de sistemas de qualidade que tenha recusado, suspendido, retirado e, se lhe for pedido, das aprovações que tenha concedido a sistemas de qualidade.

8. Mandatário

As obrigações do fabricante enunciadas nos pontos 3.1, 3.5, 5 e 6 podem ser cumpridas, em seu nome e sob a sua responsabilidade, pelo respetivo mandatário, desde que se encontrem especificadas no mandato.