COMISIÓN
EUROPEA

Bruselas, 15.9.2022
COM(2022) 454 final

ANNEXES 1 to 6

ANEXOS

de la

PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamrnto (UE) 2019/1020

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

ANEXO I

REQUISITOS ESENCIALES DE CIBERSEGURIDAD

1. REQUISITOS DE SEGURIDAD RELATIVOS A LAS PROPIEDADES DE LOS PRODUCTOS CON ELEMENTOS DIGITALES

1) Los productos con elementos digitales se diseñarán, desarrollarán y producirán de manera que garanticen un nivel adecuado de ciberseguridad sobre la base de los riesgos existentes;

2) Los productos con elementos digitales se entregarán sin ninguna vulnerabilidad conocida que pueda aprovecharse;

3) Sobre la base de la evaluación de riesgos a la que hace referencia el artículo 10, apartado 2, y cuando proceda, los productos con elementos digitales:

   a) se entregarán con una configuración segura por defecto, que incluya la posibilidad de restablecer el producto a su estado original;

   b) garantizarán la protección contra el acceso no autorizado mediante mecanismos de control adecuados, incluidos, entre otros, sistemas de gestión de la autenticación, la identidad o el acceso;

   c) protegerán la confidencialidad de los datos personales o de otro tipo almacenados, transmitidos o tratados de otro modo, mediante, por ejemplo, el cifrado de los datos en reposo o en tránsito pertinentes por medio de los mecanismos más avanzados;

   d) protegerán la integridad de los datos personales o de otro tipo almacenados, transmitidos o tratados de otro modo, los comandos, los programas y la configuración frente a toda manipulación o modificación no autorizada por el usuario, e informarán sobre los casos de corrupción de datos;

   e) tratarán únicamente los datos personales o de otro tipo que sean adecuados, pertinentes y limitados a lo que sea necesario para el uso previsto del producto («minimización de datos»);

   f) protegerán la disponibilidad de funciones esenciales, incluida la resiliencia frente a ataques de denegación de servicio y la mitigación de sus efectos;

   g) minimizarán sus propias repercusiones negativas en la disponibilidad de servicios prestados por otros dispositivos o redes;

   h) estarán diseñados, desarrollados y producidos para limitar las superficies de ataque, incluidas las interfaces externas;

   i) estarán diseñados, desarrollados y producidos para reducir el impacto de un incidente, por medio de mecanismos y técnicas adecuados para paliar el aprovechamiento de las vulnerabilidades;

   j) proporcionarán información relacionada con la seguridad mediante el registro o el seguimiento de la actividad interna pertinente, incluidos el acceso a datos, servicios o funciones y la modificación de estos;

k) garantizarán que las vulnerabilidades puedan subsanarse mediante actualizaciones de seguridad, incluidas, cuando proceda, las actualizaciones automáticas y la notificación de las actualizaciones disponibles a los usuarios.

2. REQUISITOS DE GESTIÓN DE LAS VULNERABILIDADES

Los fabricantes de los productos con elementos digitales:

1) identificarán y documentarán las vulnerabilidades y los componentes presentes en el producto, en particular mediante la elaboración de una nomenclatura de materiales de los programas informáticos en un formato comúnmente utilizado y legible por máquina, que incluya, como mínimo, las dependencias de máximo nivel del producto;

2) por lo que respecta a los riesgos para los productos con elementos digitales, abordarán y subsanarán las vulnerabilidades sin demora, en particular mediante la provisión de actualizaciones de seguridad;

3) llevarán a cabo exámenes y ensayos eficaces y periódicos de la seguridad del producto con elementos digitales;

4) una vez esté disponible una actualización de seguridad, divulgarán información sobre las vulnerabilidades subsanadas, incluidas una descripción de las vulnerabilidades, información que permita a los usuarios identificar el producto con elementos digitales afectado, las repercusiones y la gravedad de las vulnerabilidades e información que ayude a los usuarios a corregir las vulnerabilidades;

5) pondrán en marcha y aplicarán una política de divulgación coordinada de vulnerabilidades;

6) adoptarán medidas para facilitar el intercambio de información sobre posibles vulnerabilidades de su producto con elementos digitales, así como de los componentes de terceros presentes en el producto, en particular proporcionando una dirección de contacto para la notificación de las vulnerabilidades descubiertas en el producto con elementos digitales;

7) preverán mecanismos para distribuir de manera segura las actualizaciones de los productos con elementos digitales, con el fin de garantizar que las vulnerabilidades aprovechables se subsanen o se mitiguen de manera oportuna;

8) garantizarán que, cuando se disponga de parches o actualizaciones de seguridad para hacer frente a los problemas de seguridad detectados, estos se difundan sin demora y de forma gratuita, acompañados de mensajes de aviso que proporcionen a los usuarios la información pertinente, en particular en relación con las posibles medidas que deban adoptarse.

ANEXO II

INFORMACIÓN E INSTRUCCIONES PARA EL USUARIO

Junto al producto con elementos digitales, se especificará, como mínimo:

1. el nombre, nombre comercial registrado o marca registrada, la dirección postal y la dirección de correo electrónico de contacto del fabricante, en el producto o, cuando no sea posible, en su embalaje o en un documento que acompañe al producto;
2. el punto de contacto en el que pueda notificarse y obtenerse información sobre las vulnerabilidades de ciberseguridad del producto;
3. la correcta identificación del tipo, lote, versión o número de serie u otro elemento que permita la identificación del producto, así como las correspondientes instrucciones e información para el usuario;
4. el uso previsto, incluido el entorno de seguridad proporcionado por el fabricante, así como las funcionalidades esenciales del producto e información sobre sus propiedades de seguridad;
5. cualquier circunstancia conocida o previsible, asociada al uso del producto con elementos digitales conforme a su finalidad prevista o a un uso indebido razonablemente previsible, que pueda dar lugar a riesgos de ciberseguridad significativos;
6. si se puede acceder a la nomenclatura de materiales de los programas informáticos y, en su caso, dónde se puede acceder a ella;
7. cuando proceda, la dirección de internet en la que puede accederse a la declaración UE de conformidad;
8. el tipo de apoyo técnico en materia de seguridad ofrecido por el fabricante y hasta cuándo se prestará dicho servicio o, al menos, hasta cuándo está previsto que los usuarios puedan recibir actualizaciones de seguridad;
9. instrucciones detalladas o una dirección de internet en la que se especifiquen dichas instrucciones e información sobre:
    a) las medidas necesarias durante la puesta en servicio inicial y a lo largo de toda la vida del producto para garantizar su uso seguro;
    b) cómo los cambios en el producto pueden afectar a la seguridad de los datos;
    c) cómo pueden instalarse las actualizaciones pertinentes para la seguridad;
    d) cómo realizar la retirada del servicio del producto de forma segura, incluida información sobre cómo pueden eliminarse de forma segura los datos de los usuarios.

ANEXO III

PRODUCTOS CRÍTICOS CON ELEMENTOS DIGITALES

Clase I

1. Programas informáticos de sistemas de gestión de la identidad y programas informáticos de gestión de accesos privilegiados;
2. Navegadores independientes e integrados;
3. Gestores de contraseñas;
4. Programas informáticos que busquen, eliminen o pongan en cuarentena programas maliciosos;
5. Productos con elementos digitales que ejerzan la función de red privada virtual (VPN);
6. Sistemas de gestión de redes;
7. Herramientas de gestión de la configuración de las redes;
8. Sistemas de seguimiento del tráfico de red;
9. Gestión de los recursos de red;
10. Sistemas de gestión de información y eventos de seguridad (SIEM);
11. Gestión de actualizaciones o parches, incluidos los gestores de arranque;
12. Sistemas de gestión de la configuración de aplicaciones;
13. Programas informáticos de acceso o uso compartido a distancia;
14. Programas informáticos de gestión de dispositivos móviles;
15. Interfaces físicas de red;
16. Sistemas operativos no incluidos en la clase II;
17. Cortafuegos, sistemas de detección o prevención de intrusiones no incluidos en la clase II;
18. Encaminadores, módems destinados a la conexión a internet e interruptores, no incluidos en la clase II;
19. Microprocesadores no incluidos en la clase II;
20. Microcontroladores;
21. Circuitos integrados de aplicación específica (ASIC) y matrices de puertas programables *in situ* (FPGA) destinados a ser utilizados por entidades esenciales del tipo contemplado en [el anexo I de la Directiva XXX/XXXX (SRI 2)];
22. Sistemas de control de la automatización industrial no incluidos en la clase II, como controladores lógicos programables, sistemas de control distribuidos, controladores numéricos computerizados para máquinas-herramienta (CNC) y sistemas de control de supervisión y adquisición de datos (SCADA);
23. Internet industrial de las cosas no incluido en la clase II.

Clase II

1. Sistemas operativos para servidores, ordenadores de mesa y dispositivos móviles;
2. Hipervisores y sistemas en tiempo de ejecución de contenedores que permitan la ejecución virtualizada de sistemas operativos y entornos similares;
3. Infraestructuras públicas clave y emisores de certificados digitales;
4. Cortafuegos y sistemas de detección o prevención de intrusiones destinados a un uso industrial;
5. Microprocesadores de uso general;
6. Microprocesadores destinados a su integración en controladores lógicos programables y elementos seguros;
7. Encaminadores, módems destinados a la conexión a internet e interruptores destinados a un uso industrial;
8. Elementos seguros;
9. Módulos de seguridad de los equipos informáticos;
10. Criptoprocesadores seguros;
11. Tarjetas inteligentes, lectores de tarjetas inteligentes y testigos de autenticación;
12. Sistemas de control de la automatización industrial destinados a ser utilizados por entidades esenciales del tipo contemplado en el [anexo I de la Directiva XXX/XXXX (NIS2)], como controladores lógicos programables, sistemas de control distribuidos, controladores numéricos computerizados para máquinas-herramienta (CNC) y sistemas de control de supervisión y adquisición de datos (SCADA);
13. Internet industrial de las cosas destinado a ser utilizado por entidades esenciales del tipo contemplado en [el anexo I de la Directiva XXX/XXXX (SRI 2)];
14. Componentes de sensores y accionadores de robots y controladores de robots;
15. Contadores inteligentes.

ANEXO IV

DECLARACIÓN UE DE CONFORMIDAD

La declaración UE de conformidad a que hace referencia el artículo 20 contendrá toda la información siguiente:

1. El nombre y el tipo del producto con elementos digitales, y toda información adicional que permita su identificación única.
2. El nombre y la dirección del fabricante o de su representante autorizado.
3. La afirmación de que la declaración UE de conformidad se emite bajo la exclusiva responsabilidad del proveedor.
4. El objeto de la declaración (identificación del producto que permita la trazabilidad. Podrá incluir, cuando proceda, una fotografía).
5. La afirmación de que el objeto de la declaración descrito anteriormente es conforme a las normas de armonización de la Unión pertinentes.
6. Referencias a todas las normas armonizadas pertinentes utilizadas o a cualquier otra especificación común o certificación de la ciberseguridad respecto a las cuales se declara la conformidad.
7. En su caso, el nombre y número del organismo notificado, una descripción del procedimiento de evaluación de la conformidad llevado a cabo y la identificación del certificado emitido.
8. Información adicional:

Firmado por y en nombre de: ……

(lugar y fecha de expedición):

(nombre, cargo) (firma):

ANEXO V

CONTENIDO DE LA DOCUMENTACIÓN TÉCNICA

La documentación técnica a que hace referencia el artículo 23 contendrá como mínimo la siguiente información, en función del producto con elementos digitales de que se trate:

1. una descripción general del producto con elementos digitales, incluidas:
   a) su finalidad prevista;
   b) las versiones de los programas informáticos que afecten al cumplimiento de los requisitos esenciales;
   c) cuando el producto con elementos digitales sea un producto consistente en equipos informáticos, fotografías o ilustraciones que muestren las características externas, el marcado y la configuración interna;
   d) la información y las instrucciones para el usuario indicadas en el anexo II;
2. una descripción del diseño, el desarrollo y la producción del producto y de los procesos de gestión de las vulnerabilidades, que incluya:
   a) información completa sobre el diseño y el desarrollo del producto con elementos digitales, incluidos, en su caso, planos y esquemas, o una descripción de la arquitectura del sistema que explique cómo se apoyan o se alimentan mutuamente los componentes de los programas informáticos y cómo se integran en el tratamiento general;
   b) información completa y especificaciones de los procesos de gestión de las vulnerabilidades establecidos por el fabricante, incluida la nomenclatura de materiales de los programas informáticos, la política de divulgación coordinada de vulnerabilidades, pruebas de que se ha facilitado una dirección de contacto para la notificación de vulnerabilidades y una descripción de las soluciones técnicas elegidas para la distribución segura de las actualizaciones;
   c) información completa y especificaciones de los procesos de producción y seguimiento del producto con elementos digitales y la validación de estos procesos;
3. una evaluación de los riesgos de ciberseguridad frente a los cuales se haya diseñado, desarrollado, producido, entregado y mantenido el producto con elementos digitales, tal como se establece en el artículo 10 del presente Reglamento;
4. una lista de las normas armonizadas, aplicadas total o parcialmente, cuyas referencias se hayan publicado en el *Diario Oficial de la Unión Europea*, las especificaciones comunes tal como se definen en el artículo 19 del presente Reglamento o los esquemas de certificación de la ciberseguridad adoptados con arreglo al Reglamento (UE) 2019/881 de conformidad con el artículo 18, apartado 3, y, cuando no se hayan aplicado esas normas armonizadas, especificaciones comunes o esquemas de certificación de la ciberseguridad, la descripción de las soluciones adoptadas para cumplir los requisitos esenciales establecidos en las secciones 1 y 2 del anexo I, junto con una lista de otras especificaciones técnicas pertinentes aplicadas; en caso de normas armonizadas, especificaciones comunes o certificaciones de la ciberseguridad

que se apliquen parcialmente, se especificarán en la documentación técnica las partes que se hayan aplicado;

5. informes de los ensayos realizados para verificar la conformidad del producto y de los procesos de gestión de las vulnerabilidades con los requisitos esenciales aplicables que se establecen en las secciones 1 y 2 del anexo I;

6. una copia de la declaración UE de conformidad;

7. cuando proceda, la nomenclatura de materiales de los programas informáticos, tal como se define en el artículo 3, punto 36, previa solicitud motivada por parte de una autoridad de vigilancia del mercado, siempre que sea necesario para que dicha autoridad pueda comprobar el cumplimiento de los requisitos esenciales establecidos en el anexo I.

ANEXO VI

PROCEDIMIENTOS DE EVALUACIÓN DE LA CONFORMIDAD

Procedimiento de evaluación de la conformidad basado en el control interno (basado en el módulo A)

1. El control interno es el procedimiento de evaluación de la conformidad mediante el cual el fabricante cumple las obligaciones establecidas en los puntos 2, 3 y 4, y garantiza y declara, bajo su exclusiva responsabilidad, que los productos con elementos digitales son conformes con todos los requisitos esenciales establecidos en la sección 1 del anexo I, y que el fabricante cumple los requisitos esenciales establecidos en la sección 2 del anexo I.

2. El fabricante elaborará la documentación técnica descrita en el anexo V.

3. Diseño, desarrollo, producción de los productos con elementos digitales y gestión de las vulnerabilidades

   El fabricante adoptará todas las medidas necesarias para que los procesos de diseño, desarrollo, producción y gestión de las vulnerabilidades, así como el seguimiento de dichos procesos, garanticen la conformidad de los productos con elementos digitales fabricados o desarrollados y de los procesos establecidos por el fabricante con los requisitos esenciales establecidos en las secciones 1 y 2 del anexo I.

4. Marcado de conformidad y declaración de conformidad

4.1. El fabricante colocará el marcado CE en cada producto con elementos digitales que satisfaga los requisitos aplicables del presente Reglamento.

4.2. El fabricante redactará una declaración UE de conformidad por escrito para cada producto con elementos digitales con arreglo al artículo 20 y la mantendrá, junto con la documentación técnica, a disposición de las autoridades nacionales durante un período de diez años después de la introducción en el mercado del producto con elementos digitales. En la declaración UE de conformidad se identificará el producto con elementos digitales para el cual haya sido elaborada. Se facilitará una copia de la declaración CE de conformidad a las autoridades competentes que lo soliciten.

5. Representantes autorizados

   Las obligaciones del fabricante establecidas en el punto 4 podrá cumplirlas, en su nombre y bajo su responsabilidad, su representante autorizado, siempre que estén especificadas en el mandato.

Examen de tipo UE (basado en el módulo B)

1. El examen de tipo UE es la parte de un procedimiento de evaluación de la conformidad mediante la cual un organismo notificado examina el diseño técnico y el desarrollo de un producto y los procesos de gestión de las vulnerabilidades establecidos por el fabricante, y certifica que un producto con elementos digitales cumple los requisitos esenciales establecidos en la sección 1 del anexo I y que el fabricante cumple los requisitos esenciales establecidos en la sección 2 del anexo I.

2. El examen de tipo UE se llevará a cabo mediante una evaluación de la adecuación del diseño técnico y el desarrollo del producto a través del examen de la documentación técnica y las pruebas de apoyo a que se hace referencia en el punto 3, más el examen de las muestras de una o varias partes críticas del producto (combinación del tipo de producción y el tipo de diseño).

3. El fabricante deberá presentar una solicitud de examen de tipo UE a un organismo notificado único de su elección.

La solicitud incluirá:

– El nombre y la dirección del fabricante y, si la solicitud la presenta el representante autorizado, también el nombre y dirección de este.

– Una declaración por escrito de que no se ha presentado la misma solicitud ante ningún otro organismo notificado.

– La documentación técnica, que permitirá evaluar la conformidad del producto con los requisitos esenciales aplicables establecidos en la sección 1 del anexo I, y los procesos de gestión de las vulnerabilidades por parte del fabricante establecidos en la sección 2 del anexo I, e incluirá un análisis y una evaluación adecuados del riesgo o riesgos. Especificará los requisitos aplicables y contemplará, en la medida en que sea pertinente para la evaluación, el diseño, la fabricación y el funcionamiento del producto. Incluirá, cuando proceda, al menos los elementos establecidos en el anexo V.

– Pruebas que acrediten la adecuación de las soluciones técnicas de diseño y desarrollo y de los procesos de gestión de las vulnerabilidades. Estas pruebas mencionarán todos los documentos que se hayan utilizado, en particular, en caso de que las normas armonizadas pertinentes o las especificaciones técnicas no se hayan aplicado íntegramente. Las pruebas incluirán, en caso necesario, los resultados de los ensayos realizados por el laboratorio apropiado del fabricante o por otro laboratorio de ensayo en su nombre y bajo su responsabilidad.

4. El organismo notificado:

4.1. examinará la documentación técnica y las pruebas para evaluar la adecuación del diseño técnico y del desarrollo del producto con los requisitos esenciales establecidos en la sección 1 del anexo I y la adecuación de los procesos de gestión de las vulnerabilidades establecidos por el fabricante con los requisitos esenciales establecidos en la sección 2 del anexo I;

4.2. comprobará que las muestras se han desarrollado o fabricado conforme a la documentación técnica, e identificará los elementos que se han diseñado y desarrollado con arreglo a las disposiciones aplicables de las normas armonizadas o especificaciones técnicas pertinentes, así como los elementos que se han diseñado y desarrollado sin aplicar las disposiciones pertinentes de dichas normas;

4.3. efectuará, o hará que se efectúen, los exámenes y ensayos oportunos para comprobar si, cuando el fabricante haya optado por aplicar las soluciones de las normas armonizadas o especificaciones técnicas pertinentes en relación con los requisitos establecidos en el anexo I, su aplicación ha sido correcta;

4.4. efectuará, o hará que se efectúen, los exámenes y ensayos oportunos para comprobar si, en caso de que no se hayan aplicado las soluciones de las normas armonizadas o

especificaciones técnicas pertinentes en relación con los requisitos establecidos en el anexo I, las soluciones adoptadas por el fabricante cumplen los requisitos esenciales correspondientes;

4.5. acordará con el fabricante el lugar donde se realizarán los exámenes y los ensayos.

5. El organismo notificado elaborará un informe de evaluación que recoja las actividades realizadas de conformidad con el punto 4 y sus resultados. Sin perjuicio de sus obligaciones frente a las autoridades notificantes, el organismo notificado solo dará a conocer el contenido del informe, íntegramente o en parte, con el acuerdo del fabricante.

6. Si el tipo y los procesos de gestión de las vulnerabilidades cumplen los requisitos esenciales establecidos en el anexo I, el organismo notificado expedirá al fabricante un certificado de examen de tipo UE. El certificado incluirá el nombre y la dirección del fabricante, las conclusiones del examen, las condiciones de validez (en su caso) y los datos necesarios para la identificación del tipo aprobado y de los procesos de gestión de las vulnerabilidades. Se podrán adjuntar al certificado uno o varios anexos.

   El certificado y sus anexos contendrán toda la información pertinente que permita evaluar la conformidad de los productos fabricados o desarrollados con el tipo examinado y los procesos de gestión de las vulnerabilidades, y permitir el control en servicio.

   En caso de que el tipo y los procesos de gestión de las vulnerabilidades no cumplan los requisitos esenciales aplicables establecidos en el anexo I, el organismo notificado se negará a expedir un certificado de examen de tipo UE e informará de ello al solicitante, explicando detalladamente su negativa.

7. El organismo notificado se mantendrá informado de los cambios en el estado actual de la técnica generalmente reconocido que indiquen que el tipo aprobado y los procesos de gestión de las vulnerabilidades ya no pueden cumplir los requisitos esenciales establecidos en el anexo I del presente Reglamento, y determinará si tales cambios requieren más investigaciones. En ese caso, el organismo notificado informará al fabricante en consecuencia.

   El fabricante informará al organismo notificado en posesión de la documentación técnica relativa al certificado de examen de tipo UE de todas las modificaciones del tipo aprobado y los procesos de gestión de las vulnerabilidades que puedan afectar a la conformidad con los requisitos esenciales establecidos en el anexo I o las condiciones de validez del certificado. Tales modificaciones requerirán una aprobación adicional en forma de suplemento al certificado original de examen de tipo UE.

8. Cada organismo notificado informará a sus autoridades notificantes sobre los certificados de examen de tipo UE o cualquier añadido o añadidos a ellos que haya expedido o retirado, y, periódicamente o previa solicitud, pondrá a disposición de sus autoridades notificantes la lista de certificados o añadidos que hayan sido rechazados, suspendidos o restringidos de otro modo.

   Cada organismo notificado informará a los demás organismos notificados sobre los certificados de examen de tipo UE o los añadidos a estos certificados que haya rechazado, retirado, suspendido o restringido de otro modo, y, previa solicitud, sobre los certificados o sus añadidos que haya expedido.

La Comisión, los Estados miembros y los demás organismos notificados podrán, previa solicitud, obtener una copia de los certificados de examen de tipo UE o sus suplementos. Previa solicitud, la Comisión y los Estados miembros podrán obtener una copia de la documentación técnica y los resultados de los exámenes efectuados por el organismo notificado. El organismo notificado conservará una copia del certificado de examen de tipo UE, sus anexos y sus añadidos, así como del expediente técnico que incluya la documentación presentada por el fabricante hasta el final de la validez del certificado.

9. El fabricante conservará a disposición de las autoridades nacionales una copia del certificado de examen de tipo UE, sus anexos y sus añadidos, así como la documentación técnica durante un período de diez años después de la introducción del producto en el mercado.

10. El representante autorizado del fabricante podrá presentar la solicitud a que se hace referencia en el punto 3 y cumplir las obligaciones contempladas en los puntos 7 y 9, siempre que estén especificadas en su mandato.

Conformidad con el tipo basada en el control interno de la producción (basada en el módulo C)

1. La conformidad con el tipo basada en el control interno de la producción es la parte del procedimiento de evaluación de la conformidad según la cual el fabricante cumple las obligaciones establecidas en los puntos 2 y 3, y garantiza y declara que los productos en cuestión son conformes con el tipo descrito en el certificado de examen de tipo UE y cumplen los requisitos esenciales establecidos en la sección 1 del anexo I.

2. Producción

2.1. El fabricante tomará todas las medidas necesarias para que la producción y su seguimiento garanticen la conformidad de los productos fabricados con el tipo aprobado descrito en el certificado de examen de tipo UE y con los requisitos esenciales establecidos en la sección 1 del anexo I.

3. Marcado de conformidad y declaración de conformidad

3.1. El fabricante colocará el marcado CE en los productos que sean conformes al tipo descrito en el certificado de examen de tipo UE y satisfagan los requisitos aplicables del instrumento legislativo.

3.2. El fabricante redactará una declaración de conformidad para un modelo de producto y la mantendrá a disposición de las autoridades nacionales durante un período de diez años después de la introducción del producto en el mercado. En la declaración de conformidad se identificará el modelo de producto para el cual ha sido elaborada. Se facilitará una copia de la declaración de conformidad a las autoridades competentes que la soliciten.

4. Representante autorizado

Las obligaciones del fabricante establecidas en el punto 3 podrá cumplirlas su representante autorizado, en su nombre y bajo su responsabilidad, siempre que estén especificadas en su mandato.

Conformidad basada en el aseguramiento de calidad total (basada en el módulo H)

1. La conformidad basada en el aseguramiento de calidad total es el procedimiento de evaluación de la conformidad mediante el cual el fabricante cumple las obligaciones establecidas en los puntos 2 y 5, y garantiza y declara, bajo su exclusiva responsabilidad, que los productos (o las categorías de productos) en cuestión son conformes con los requisitos establecidos en la sección 1 del anexo I y que los procesos de gestión de las vulnerabilidades establecidos por el fabricante cumplen los requisitos establecidos en la sección 2 del anexo I.

2. Diseño, desarrollo, producción de los productos con elementos digitales y gestión de las vulnerabilidades

   El fabricante aplicará un sistema de calidad aprobado, tal como se especifica en el punto 3, para el diseño, el desarrollo y la producción de los productos en cuestión y la gestión de las vulnerabilidades, lo mantendrá operativo a lo largo de todo el ciclo de vida de los productos en cuestión y estará sujeto a la supervisión especificada en el punto 4.

3. Sistema de calidad

3.1. El fabricante presentará una solicitud de evaluación de su sistema de calidad ante el organismo notificado de su elección, para los productos de que se trate.

   La solicitud incluirá:

   – el nombre y la dirección del fabricante y, si la solicitud la presenta el representante autorizado, también el nombre y la dirección de este;

   – la documentación técnica para un modelo de cada categoría de productos que se pretenda fabricar o desarrollar. La documentación técnica incluirá, cuando proceda, al menos los elementos establecidos en el anexo V;

   – la documentación relativa al sistema de calidad; y

   – una declaración por escrito de que no se ha presentado la misma solicitud ante ningún otro organismo notificado.

3.2. El sistema de calidad garantizará la conformidad de los productos con los requisitos esenciales establecidos en la sección 1 del anexo I y la conformidad de los procesos de gestión de las vulnerabilidades establecidos por el fabricante con los requisitos establecidos en la sección 2 del anexo I.

   Todos los elementos, requisitos y disposiciones adoptados por el fabricante deberán reunirse de forma sistemática y ordenada en una documentación compuesta por políticas, procedimientos e instrucciones por escrito. Esta documentación del sistema de calidad permitirá una interpretación coherente de los programas, planes, manuales y registros de calidad.

   En particular, incluirá una descripción adecuada de:

   – los objetivos de calidad, el organigrama y las responsabilidades y competencias del personal de gestión en lo que se refiere al diseño, el desarrollo, la calidad del producto y la gestión de las vulnerabilidades;

   – las especificaciones técnicas de diseño y desarrollo, incluidas las normas que se aplicarán y, en caso de que las normas armonizadas o las especificaciones técnicas pertinentes no se apliquen plenamente, los medios

que se utilizarán para velar por que se cumplan los requisitos esenciales de la sección 1 del anexo I aplicables a los productos;

– las especificaciones de procedimiento, incluidas las normas que se aplicarán y, en caso de que las normas armonizadas o las especificaciones técnicas pertinentes no se apliquen plenamente, los medios que se utilizarán para velar por que se cumplan los requisitos esenciales establecidos en la sección 2 del anexo I aplicables al fabricante,

– las técnicas de control y verificación del diseño y el desarrollo, los procesos y las medidas sistemáticas que se vayan a utilizar en el diseño y el desarrollo de los productos por lo que se refiere a la categoría de productos de que se trate;

– las correspondientes técnicas, procesos y actividades sistemáticas de producción, control de la calidad y aseguramiento de la calidad que se utilizarán;

– los exámenes y los ensayos que se efectuarán antes, durante y después de la producción, y su frecuencia;

– los expedientes de calidad, como los informes de inspección y datos de ensayos, los datos de calibrado, los informes sobre la cualificación del personal implicado, etc.;

– los medios con los que se hace el seguimiento de la consecución del diseño y de la calidad exigidos de los productos y del funcionamiento eficaz del sistema de calidad.

3.3. El organismo notificado evaluará el sistema de calidad para determinar si cumple los requisitos a que se refiere el punto 3.2.

Dará por supuesta la conformidad con dichos requisitos de los elementos del sistema de calidad que cumplan las especificaciones correspondientes de la norma nacional que transponga la norma armonizada o la especificación técnica pertinente.

Además de experiencia en sistemas de gestión de la calidad, el equipo de auditoría tendrá, como mínimo, un miembro con experiencia como evaluador en el campo del producto pertinente y la tecnología del producto en cuestión, así como el conocimiento de los requisitos aplicables del presente Reglamento. La auditoría incluirá una visita de evaluación a las instalaciones del fabricante, siempre que estas existan. El equipo de auditores revisará la documentación técnica mencionada en el punto 3.1, segundo guion, para comprobar si el fabricante es capaz de identificar los requisitos pertinentes del presente Reglamento y de efectuar los exámenes necesarios a fin de garantizar que el producto cumple dichos requisitos.

La decisión se notificará al fabricante o a su representante autorizado.

La notificación incluirá las conclusiones de la auditoría y la decisión de evaluación motivada.

3.4. El fabricante se comprometerá a cumplir las obligaciones que se deriven del sistema de calidad tal como se haya aprobado y a mantenerlo de forma que siga resultando adecuado y eficaz.

3.5. El fabricante mantendrá informado al organismo notificado que haya aprobado el sistema de calidad de cualquier adaptación prevista de dicho sistema.

El organismo notificado evaluará las adaptaciones propuestas y decidirá si el sistema de calidad modificado sigue cumpliendo los requisitos mencionados en el punto 3.2, o si es necesaria una nueva evaluación.

El organismo notificado notificará su decisión al fabricante. La notificación incluirá las conclusiones del examen y la decisión de evaluación motivada.

4. Supervisión bajo la responsabilidad del organismo notificado

4.1. El objetivo de la supervisión es garantizar que el fabricante cumple debidamente las obligaciones que se derivan del sistema de calidad aprobado.

4.2. El fabricante permitirá la entrada del organismo notificado en los locales de diseño, desarrollo, producción, inspección, ensayo y almacenamiento, a efectos de evaluación, y le proporcionará toda la información necesaria, en particular:

– la documentación sobre el sistema de calidad;

– los registros de calidad previstos en la parte del sistema de calidad dedicada al diseño, como los resultados de análisis, cálculos, ensayos, etc.;

– los registros de calidad establecidos en la parte del sistema de calidad dedicada a la fabricación, tales como los informes de inspección, los datos sobre ensayos y calibración, los informes sobre la cualificación del personal afectado, etc.

4.3. El organismo notificado realizará periódicamente auditorías para asegurarse de que el fabricante mantiene y aplica el sistema de calidad y proporcionará un informe de la auditoría al fabricante.

5. Marcado de conformidad y declaración de conformidad

5.1. El fabricante colocará el marcado CE y, bajo la responsabilidad del organismo notificado mencionado en el apartado 3.1, el número de identificación de este último en cada producto que satisfaga los requisitos establecidos en la sección 1 del anexo I del presente Reglamento.

5.2. El fabricante redactará una declaración de conformidad para cada modelo de producto y la mantendrá a disposición de las autoridades nacionales durante un período de diez años después de la introducción del producto en el mercado. En la declaración de conformidad se identificará el modelo de producto para el cual ha sido elaborada.

Se facilitará una copia de la declaración de conformidad a las autoridades competentes que la soliciten.

6. El fabricante mantendrá a disposición de las autoridades nacionales durante un período de diez años después de la introducción del producto en el mercado:

– la documentación técnica a que se refiere el punto 3.1;

– la documentación relativa al sistema de calidad a que se refiere el punto 3.1;

– las adaptaciones a que se refiere el punto 3.5 que hayan sido aprobadas;

– las decisiones y los informes del organismo notificado a que se refieren los puntos 3.5, 4.3 y 4.4.

7. Cada organismo notificado informará a sus autoridades notificantes sobre las aprobaciones de sistemas de calidad expedidas o retiradas, y, periódicamente o previa solicitud, pondrá a disposición de sus autoridades notificantes la lista de

aprobaciones de sistemas de calidad que haya rechazado, suspendido o restringido de otro modo.

Cada organismo notificado informará a los demás organismos notificados sobre las aprobaciones de sistemas de calidad que haya rechazado, suspendido o retirado y, previa solicitud, de las aprobaciones de sistemas de calidad que haya expedido.

8. Representante autorizado

Las obligaciones del fabricante mencionadas en los puntos 3.1, 3.5, 5 y 6 podrá cumplirlas, en su nombre y bajo su responsabilidad, su representante autorizado, siempre que estén especificadas en el mandato.