

**DECISIÓN DE EJECUCIÓN (UE) 2016/650 DE LA COMISIÓN****de 25 de abril de 2016**

**por la que se fijan las normas para la evaluación de la seguridad de los dispositivos cualificados de creación de firmas y sellos con arreglo al artículo 30, apartado 3, y al artículo 39, apartado 2, del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior**

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE <sup>(1)</sup>, y en particular su artículo 30, apartado 3, y su artículo 39, apartado 2,

Considerando lo siguiente:

- (1) El anexo II del Reglamento (UE) n.º 910/2014 establece los requisitos aplicables a los dispositivos cualificados de creación de firmas electrónicas y a los dispositivos cualificados de creación de sellos electrónicos.
- (2) La labor de elaborar las especificaciones técnicas necesarias para la producción y comercialización de productos que se adecúen al estado actual de la técnica la llevan a cabo las organizaciones competentes en el ámbito de la normalización.
- (3) La ISO/CEI (Organización Internacional de Normalización/Comisión Electrotécnica Internacional) establece los conceptos y principios generales de seguridad de la tecnología de la información y especifica el modelo general de evaluación que debe utilizarse como base para evaluar las propiedades de seguridad de los productos informáticos.
- (4) En el marco del mandato de normalización M/460 otorgado por la Comisión, el Comité Europeo de Normalización (CEN) ha elaborado normas aplicables a los dispositivos cualificados de creación de firmas y sellos electrónicos, cuando los datos de creación de firma electrónica o los datos de creación de sello electrónico se conservan íntegramente, aunque no necesariamente de forma exclusiva, en un entorno gestionado por el usuario. Esas normas se consideran adecuadas para evaluar la conformidad de tales productos con los requisitos pertinentes establecidos en el anexo II del Reglamento (UE) n.º 910/2014.
- (5) El anexo II del Reglamento (UE) n.º 910/2014 establece que solo un prestador cualificado de servicios de confianza puede gestionar datos de creación de firma electrónica en nombre del firmante. Los requisitos de seguridad y sus respectivas especificaciones de certificación difieren cuando el firmante posee físicamente un producto y cuando un prestador cualificado de servicios de confianza actúa en nombre del firmante. Para abordar ambas situaciones y favorecer con el tiempo el desarrollo de productos y criterios de evaluación adaptados a necesidades concretas, el anexo de la presente Decisión debe enumerar normas que abarquen ambas situaciones.
- (6) En el momento de la adopción de la presente Decisión de la Comisión, varios prestadores de servicios de confianza ya ofrecen soluciones para gestionar los datos de creación de firma electrónica en nombre de sus clientes. Las certificaciones de productos se limitan actualmente a los módulos de seguridad de los equipos informáticos certificados con arreglo a diferentes normas, pero todavía no están certificados específicamente con arreglo a los requisitos aplicables a los dispositivos cualificados de creación de sellos y firmas. No obstante, no existen aún normas publicadas, como la norma EN 419 211 (aplicable a la firma electrónica creada en un entorno íntegramente gestionado, aunque no necesariamente de forma exclusiva, por el usuario), para un mercado igualmente importante de productos a distancia certificados. Dado que se están elaborando actualmente las normas que podrían ser adecuadas a tal fin, la Comisión completará la presente Decisión cuando esas normas estén disponibles y se consideren conformes a los requisitos establecidos en el anexo II del Reglamento (UE) n.º 910/2014. Hasta el momento en que se establezca la lista de tales normas, puede utilizarse un proceso alternativo para evaluar la conformidad de esos productos en las condiciones previstas en el artículo 30, apartado 3, letra b), del Reglamento (UE) n.º 910/2014.
- (7) En el anexo figura la norma EN 419 211, que consta de diferentes partes (1 a 6) que abarcan distintas situaciones. Las partes 5 y 6 de dicha norma presentan extensiones relacionadas con el entorno de los

<sup>(1)</sup> DO L 257 de 28.8.2014, p. 73.

dispositivos cualificados de creación de firma, como la comunicación con aplicaciones de creación de firma de confianza. Los fabricantes de productos son libres de aplicar esas extensiones. De conformidad con el considerando 56 del Reglamento (UE) n.º 910/2014, el objeto de la certificación en virtud de los artículos 30 y 39 de dicho Reglamento se limita a proteger los datos de creación de firmas, mientras que las aplicaciones de creación de firmas quedan excluidas del alcance de la certificación.

- (8) A fin de garantizar que las firmas o sellos electrónicos generados por un dispositivo cualificado de creación de firma o sello estén protegidos con seguridad contra la falsificación, como exige el anexo II del Reglamento (UE) n.º 910/2014, una condición indispensable para la seguridad del producto certificado es recurrir a algoritmos criptográficos, longitudes de clave y funciones hash adecuados. Dado que ese aspecto no ha sido armonizado a nivel europeo, los Estados miembros deben cooperar a fin de acordar algoritmos criptográficos, longitudes de clave y funciones hash para su utilización en el ámbito de las firmas y sellos electrónicos.
- (9) La adopción de la presente Decisión deja obsoleta la Decisión 2003/511/CE de la Comisión <sup>(1)</sup>. Procede, por tanto, derogarla.
- (10) Las medidas previstas en la presente Decisión se ajustan al dictamen del Comité a que se refiere el artículo 48 del Reglamento (UE) n.º 910/2014.

HA ADOPTADO LA PRESENTE DECISIÓN:

#### Artículo 1

1. En el anexo de la presente Decisión figuran las normas para la evaluación de la seguridad de productos de tecnología de la información que se aplican a la certificación de dispositivos cualificados de creación de firma electrónica o dispositivos cualificados de creación de sello electrónico de conformidad con el artículo 30, apartado 3, letra a), o con el artículo 39, apartado 2, del Reglamento (UE) n.º 910/2014, cuando los datos de creación de firma electrónica o los datos de creación de sello electrónico se conservan íntegramente, aunque no necesariamente de forma exclusiva, en un entorno gestionado por el usuario.

2. Hasta que la Comisión establezca una lista de normas para la evaluación de la seguridad de los productos de tecnología de la información que se aplican a la certificación de dispositivos cualificados de creación de firmas electrónicas o dispositivos cualificados de creación de sellos electrónicos, cuando un prestador cualificado de servicios de confianza gestione los datos de creación de firma electrónica o los datos de creación del sello electrónico en nombre de un firmante o de un creador de un sello, la certificación de esos productos se basará en un proceso que, de conformidad con el artículo 30, apartado 3, letra b), haga uso de unos niveles de seguridad equivalentes a los exigidos por el artículo 30, apartado 3, letra a), y que sea notificado a la Comisión por el organismo público o privado a que se refiere el artículo 30, apartado 1, del Reglamento (UE) n.º 910/2014.

#### Artículo 2

Queda derogada la Decisión 2003/511/CE.

#### Artículo 3

La presente Decisión entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

Hecho en Bruselas, el 25 de abril de 2016.

Por la Comisión  
El Presidente  
Jean-Claude JUNCKER

---

<sup>(1)</sup> Decisión 2003/511/CE de la Comisión, de 14 de julio de 2003, relativa a la publicación de los números de referencia de las normas que gozan de reconocimiento general para productos de firma electrónica, de conformidad con lo dispuesto en la Directiva 1999/93/CE del Parlamento Europeo y del Consejo (DO L 175 de 15.7.2003, p. 45).

## ANEXO

## LISTA DE NORMAS A QUE SE REFIERE EL ARTÍCULO 1, APARTADO 1

- ISO/IEC 15408 — Information technology — Security techniques — Evaluation criteria for IT security (Tecnología de la información — Técnicas de seguridad — Criterios de evaluación para la seguridad de la TI), Partes 1 a 3 enumeradas a continuación:
    - ISO/IEC 15408-1:2009 — Information technology — Security techniques — Evaluation criteria for IT security — Parte 1. (Tecnología de la información — Técnicas de seguridad — Criterios de evaluación para la seguridad de la TI. Parte 1). ISO, 2009.
    - ISO/IEC 15408-2:2008 — Information technology — Security techniques — Evaluation criteria for IT security — Parte 2. (Tecnología de la información — Técnicas de seguridad — Criterios de evaluación para la seguridad de la TI. Parte 2). ISO, 2008.
    - ISO/IEC 15408-3:2008 Information technology — Security techniques — Evaluation criteria for IT security — Parte 3 (Tecnología de la información — Técnicas de seguridad — Criterios de evaluación para la seguridad de la TI. Parte 3). ISO, 2008.

e

  - ISO/IEC 18045:2008: Information technology — Security techniques — Methodology for IT security evaluation (Tecnología de la información — Técnicas de seguridad — Metodología para la evaluación de la seguridad de la TI).

y

  - EN 419 211 — Protection profiles for secure signature creation device (Perfiles de protección para los dispositivos seguros de creación de firma), Partes 1 a 6 —en su caso— enumeradas a continuación:
    - EN 419211-1:2014 — Protection profiles for secure signature creation device — Part 1: Overview (Perfiles de protección para los dispositivos seguros de creación de firma. Parte 1: Generalidades).
    - EN 419211-2:2013 — Protection profiles for secure signature creation device — Part 2: Device with key generation (Perfil de protección para los dispositivos seguros de creación de firma. Parte 2: Dispositivo con generación de claves).
    - EN 419211-3:2013 — Protection profiles for secure signature creation device — Part 3: Device with key import (Perfil de protección para los dispositivos seguros de creación de firma. Parte 3: Dispositivo con importación de claves).
    - EN 419211-4:2013 — Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application (Perfil de protección para los dispositivos seguros de creación de firma. Parte 4: Extensión para el dispositivo con generación de claves y comunicación confiada con aplicación de generación de certificado).
    - EN 419211-5:2013 — Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application (Perfil de protección para los dispositivos seguros de creación de firma. Parte 5: Dispositivo con generación de claves y comunicación confiada con aplicación de creación de firma).
    - EN 419211-6:2014 — Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted channel to signature creation application (Perfil de protección para los dispositivos seguros de creación de firma. Parte 6: Dispositivo con importación de claves y comunicación confiada con aplicación de creación de firma).
-