COMISIÓN EUROPEA

Bruselas, 4.6.2012
COM(2012) 238 final

2012/0146 (COD)

Propuesta de

REGLAMENTO 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)

{SWD(2012) 135 final}
{SWD(2012) 136 final}

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

La presente exposición de motivos explica una propuesta de marco jurídico destinado a reforzar la confianza en las transacciones electrónicas en el mercado interior.

La creación de confianza en el entorno en línea es esencial para el desarrollo económico. La falta de confianza hace que los consumidores, las empresas y las administraciones duden a la hora de realizar transacciones por vía electrónica y adoptar nuevos servicios.

La *Agenda Digital para Europa*[1] indica qué obstáculos se oponen actualmente al desarrollo digital de Europa y propone medidas legales en relación con la firma electrónica (acción clave nº 3) y el reconocimiento mutuo de la identificación y la autenticación electrónicas (acción clave nº 16), estableciendo así un marco jurídico claro con el fin de eliminar la fragmentación y la ausencia de interoperabilidad, potenciar la ciudadanía digital y prevenir la ciberdelincuencia. Una legislación que garantice el reconocimiento mutuo de la identificación y la autenticación electrónicas en toda la UE, además de la revisión de la Directiva sobre la firma electrónica, es también una medida clave del *Acta del Mercado Único*[2] para la realización del mercado único digital. La *Hoja de Ruta para la Estabilidad y el Crecimiento*[3] subraya el papel clave que para el desarrollo de la economía digital tiene el futuro marco jurídico común para el reconocimiento y la aceptación mutuos de la identificación y la autenticación electrónicas a través de las fronteras.

El marco jurídico propuesto, consistente en un «*Reglamento del Parlamento Europeo y del Consejo relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior*», tiene por objeto hacer posibles unas interacciones electrónicas seguras y sin fisuras entre empresas, ciudadanos y autoridades públicas con el fin de aumentar la eficacia de los servicios en línea públicos y privados, los negocios electrónicos y el comercio electrónico en la UE.

La legislación actual de la UE, a saber, la Directiva 1999/93/CE sobre un «*marco comunitario para la firma electrónica*»[4], incluye esencialmente solo la firma electrónica. No existe ningún marco transfronterizo e intersectorial global de la UE para garantizar la seguridad, fiabilidad y sencillez de las transacciones electrónicas que incluya la identificación, la autenticación y la firma electrónicas.

El objetivo es mejorar la legislación existente y ampliarla incluyendo el reconocimiento y la aceptación mutuos a nivel de la UE de los sistemas de identificación electrónica notificados y otros servicios de confianza electrónicos conexos esenciales.

---

1 COM(2010) 245 de 19.5.2010.
2 COM(2011) 206 final de 13.4.2011.
3 COM (2011) 669 de 12.10.2011.
4 DO L 13 de 19.1.2000, p. 12.

2. RESULTADOS DE LAS CONSULTAS CON LAS PARTES INTERESADAS Y DE LAS EVALUACIONES DE IMPACTO

Esta iniciativa es el resultado de amplias consultas sobre una revisión del actual marco jurídico sobre la firma electrónica en el curso de las cuales la Comisión recogió las reacciones de los Estados miembros, el Parlamento Europeo y otras partes interesadas[5]. La consulta pública en línea se vio complementada por un «Panel de prueba de PYME», a fin de recabar las opiniones y necesidades específicas de las PYME, y otras consultas específicas con partes interesadas[6,7]. La Comisión puso también en marcha una serie de estudios en relación con la identificación, la autenticación y la firma electrónicas y los servicios de confianza conexos (eIAS).

Durante las consultas se puso de manifiesto que una amplia mayoría de interesados coincidía en la necesidad de revisar el marco actual para colmar las lagunas que había dejado la Directiva sobre la firma electrónica. Consideraban que esto respondería mejor a los desafíos planteados por el rápido desarrollo de tecnologías nuevas (en particular el acceso móvil y en línea) y la creciente globalización, manteniendo al mismo tiempo la neutralidad del marco jurídico con respecto a la tecnología.

En consonancia con la política sobre «legislar mejor», la Comisión realizó una evaluación del impacto de las distintas posibilidades de actuación. Se evaluaron tres grupos de opciones políticas examinando, respectivamente, 1) el ámbito de aplicación del nuevo marco, 2) el instrumento jurídico y 3) el nivel de supervisión necesario[8]. La opción política preferida resultó ser la de reforzar la seguridad jurídica, estimular la coordinación de la supervisión nacional, garantizar el reconocimiento y la aceptación mutuos de los regímenes de identificación electrónica e incorporar los servicios de confianza conexos esenciales. La evaluación de impacto concluyó que ello daría lugar a considerables progresos en la seguridad jurídica, la seguridad y la confianza en las transacciones electrónicas transfronterizas, lo que atenuaría la fragmentación del mercado.

---

5 Para más información sobre las consultas, véase http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision

6 Se organizó un seminario de partes interesadas el 10 de marzo de 2011 con representantes de los sectores público y privado y del mundo académico para discutir qué medidas legislativas resultaban necesarias para abordar los retos futuros. Fue un foro interactivo para intercambiar puntos de vista y poner de relieve las diversas posiciones sobre las cuestiones planteadas en la consulta pública. Varias organizaciones enviaron espontáneamente documentos de toma de posición.

7 En particular, la Presidencia polaca de la UE organizó reuniones con los Estados miembros sobre la firma electrónica en Varsovia el 9 de noviembre de 2011 y sobre la identificación electrónica en Poznan el 17 de ese mismo mes. El 25 de enero de 2012, la Comisión convocó un seminario con los Estados miembros para debatir las cuestiones pendientes sobre identificación, autenticación y firma electrónicas.

8 Dentro del primer apartado, se examinaron cuatro opciones: derogar la Directiva sobre la firma electrónica; no modificar la política; incrementar la seguridad jurídica, impulsar la coordinación de la supervisión nacional y garantizar el reconocimiento y la aceptación mutuos de la identificación electrónica en toda la UE; y, por último, ampliar la Directiva incorporando determinados servicios de confianza conexos. En el segundo, se evaluaron los méritos relativos de las posibilidades de regular a través de uno o dos instrumentos, y a través de una Directiva o de un Reglamento. En el tercero, se examinaron las posibilidades ofrecidas por la aplicación de regímenes de supervisión nacionales basados en unos requisitos esenciales comunes frente a un sistema de supervisión basado en la UE. Con ayuda de un grupo que reunía a todas las Direcciones Generales de la Comisión interesadas, se evaluó cada opción política en cuanto a su eficacia para la consecución de los objetivos políticos, su repercusión económica sobre las partes interesadas (y también sobre el presupuesto de las instituciones de la UE), su impacto social y ambiental y su efecto sobre la carga administrativa.

3. ASPECTOS JURÍDICOS DE LA PROPUESTA

3.1 Base jurídica

La presente propuesta se basa en el artículo 114 del TFUE, que se refiere a la adopción de normas a fin de eliminar los obstáculos que dificultan el funcionamiento del mercado interior. Los ciudadanos, las empresas y las administraciones podrán beneficiarse del reconocimiento y la aceptación mutuos de la identificación, la autenticación y la firma electrónicas y otros servicios de confianza a través de las fronteras cuando resulte necesario para el acceso y la realización de procedimientos o transacciones electrónicos.

Se considera que un Reglamento es el instrumento jurídico más apropiado. La aplicabilidad directa de un Reglamento en virtud del artículo 288 del TFUE reducirá la fragmentación jurídica y aportará mayor seguridad jurídica mediante la introducción de un conjunto armonizado de normas básicas que contribuirán al buen funcionamiento del mercado interior.

3.2 Subsidiariedad y proporcionalidad

Para que la acción de la UE esté justificada, debe respetarse el principio de subsidiariedad:

a) Naturaleza transnacional del problema (prueba de necesidad)

La naturaleza transnacional de eIAS exige una acción de la UE. La acción nacional por sí sola no sería suficiente para alcanzar los objetivos y lograr las metas fijadas en la *estrategia Europa 2020*[9]. Recíprocamente, la experiencia ha demostrado que las medidas nacionales han creado barreras *de facto* a la interoperabilidad de la firma electrónica en la UE, y están teniendo actualmente el mismo efecto sobre la identificación electrónica, la autenticación electrónica y los servicios de confianza conexos. Por lo tanto, es necesario que la UE cree un marco que permita abordar la interoperabilidad transfronteriza y mejorar la coordinación de los regímenes nacionales de supervisión. No obstante, la identificación electrónica no se puede abordar en la propuesta de Reglamento del mismo modo genérico que los demás servicios electrónicos de confianza, porque la expedición de medios de identificación constituye una prerrogativa nacional. Por ello, la propuesta se centra exclusivamente en los aspectos transfronterizos de la identificación electrónica.

El Reglamento propuesto crea una situación de igualdad de condiciones para las empresas que prestan servicios de confianza, mientras que las diferencias que existen actualmente entre las legislaciones nacionales generan a menudo inseguridad jurídica y cargas adicionales. La seguridad jurídica aumenta considerablemente al existir unas obligaciones claras de aceptación por los Estados miembros de los servicios de confianza cualificados, lo que constituirá un incentivo adicional para que las empresas salgan al exterior. Por ejemplo, una empresa podrá participar por vía electrónica en una licitación pública puesta en marcha por la administración de otro Estado miembro sin que su firma electrónica quede bloqueada a causa de requisitos nacionales específicos o problemas de interoperabilidad. Del mismo modo, una empresa tendrá la oportunidad de firmar contratos por vía electrónica con una contraparte situada en un Estado miembro diferente sin miedo a que existan distintos requisitos jurídicos para servicios de confianza tales como sellos electrónicos, documentos electrónicos o marcas de tiempo. Por último, podrá entregarse un anuncio de impago de un Estado miembro a otro con la certidumbre de su validez jurídica en ambos Estados miembros. Análogamente, el

[9] Comunicación de la Comisión: Europa 2020. Una estrategia para un crecimiento inteligente, sostenible e integrador, COM(2010) 2020 de 3.3.2010.

comercio en línea será más fiable cuando los compradores dispongan de medios para comprobar que realmente acceden al sitio web del comerciante de su elección, y no a un sitio web que pudiera ser falso.

Unos medios de identificación electrónica mutuamente reconocidos y unas firmas electrónicas aceptadas de manera generalizada facilitarán la prestación transfronteriza de numerosos servicios en el mercado interior y permitirán a las empresas actuar fuera de sus fronteras sin encontrar obstáculos en su interacción con las autoridades públicas. En la práctica, ello supondrá mejoras de eficiencia significativas, tanto para las empresas como para los ciudadanos, a la hora de cumplir con las formalidades administrativas. Por ejemplo, dando a un estudiante la oportunidad de matricularse electrónicamente en una universidad en el extranjero, a un ciudadano la de presentar una declaración fiscal en línea ante otro Estado miembro o a un paciente de acceder a sus datos sanitarios en línea. Si no existen estos medios de identificación electrónica mutuamente reconocidos, un médico no podrá acceder a los datos médicos de los pacientes que necesita para tratarlos y habrán de repetirse pruebas médicas y de laboratorio a las que ya se haya visto sometido el paciente.

b) Valor añadido (prueba de eficacia)

Los objetivos mencionados no se están logrando actualmente en virtud de la coordinación voluntaria entre los Estados miembros, ni es razonablemente probable que esto ocurra en el futuro. Esta situación lleva a la duplicación de esfuerzos, al establecimiento de normas diferentes, a las características transnacionales de los beneficios indirectos generados por las TIC y a la complejidad administrativa que supone establecer tal coordinación a través de acuerdos bilaterales y multilaterales.

Además, la necesidad de superar problemas como a) la ausencia de seguridad jurídica, debida a la heterogeneidad de las disposiciones nacionales que derivan de interpretaciones divergentes de la Directiva sobre la firma electrónica, y b) la falta de interoperabilidad de los sistemas de firma electrónica establecidos a nivel nacional, debida a la aplicación no uniforme de las normas técnicas, exige el tipo de coordinación entre los Estados miembros que puede lograrse más eficazmente a nivel de la UE.

3.3 Exposición detallada de la propuesta

3.3.1 CAPÍTULO I – DISPOSICIONES GENERALES

El artículo 1 define el objeto del Reglamento.

El artículo 2 define el ámbito de aplicación material del Reglamento.

El artículo 3 contiene definiciones de los términos utilizados en el Reglamento. Algunas de las definiciones están tomadas de la Directiva 1999/93/CE, pero otras han sido aclaradas, completadas con elementos adicionales o añadidas.

El artículo 4 determina los principios del mercado interior en lo que se refiere a la aplicación territorial del Reglamento. Se hace mención explícita de que no se impone ninguna restricción a la libre prestación de servicios ni a la libre circulación de productos.

3.3.2 CAPÍTULO II – IDENTIFICACIÓN ELECTRÓNICA

El artículo 5 prevé el reconocimiento y aceptación mutuos de los medios de identificación electrónica incluidos en un régimen notificado a la Comisión en las condiciones establecidas en el Reglamento. La mayoría de los Estados miembros de la UE han introducido algún tipo de régimen de identificación electrónica. Sin embargo, estos sistemas difieren en múltiples aspectos. La ausencia de una base jurídica común que obligue a cada Estado miembro a reconocer y aceptar los medios de identificación electrónica expedidos en otros Estados miembros para acceder a los servicios en línea, junto con la inadecuada interoperabilidad transfronteriza de las identificaciones electrónicas nacionales, crea barreras que impiden a ciudadanos y empresas beneficiarse plenamente del mercado único digital. El reconocimiento y la aceptación mutuos de los medios de identificación electrónica incluidos en un régimen notificado en virtud del Reglamento eliminan estas barreras jurídicas.

El Reglamento no obliga a los Estados miembros a introducir o notificar sistemas de identificación electrónica, sino a reconocer y aceptar las identificaciones electrónicas notificadas en los servicios en línea para acceder a los cuales sea necesaria la identificación electrónica a nivel nacional. El potencial aumento de las economías de escala creadas mediante el uso transfronterizo de medios de identificación electrónica notificados y sistemas de autenticación puede incentivar a los Estados miembros para que notifiquen sus sistemas de identificación electrónica. El artículo 6 establece las cinco condiciones para la notificación de los sistemas de identificación electrónica:

Los Estados miembros pueden notificar los sistemas de identificación electrónica que aceptan en su jurisdicción en los casos en que se requiera la identificación electrónica en un servicio público. Otro requisito es que los correspondientes medios de identificación electrónica sean expedidos por el Estado miembro que notifica un régimen, en su nombre o, al menos, bajo su responsabilidad.

Los Estados miembros deben garantizar un vínculo inequívoco entre los datos de identificación electrónica y la persona de que se trate. Esta obligación no significa que una persona no pueda tener múltiples medios de identificación electrónica, pero todos deberán vincularse con la misma persona.

La fiabilidad de una identificación electrónica depende de la disponibilidad de medios de autenticación (es decir, la posibilidad de verificar la validez de los datos de identificación electrónica). El Reglamento obliga a los Estados miembros notificadores a facilitar la autenticación en línea gratuita ante terceros. La posibilidad de autenticación debe estar disponible interrumpidamente. No se pueden imponer requisitos técnicos específicos, por ejemplo en cuanto a equipos o programas informáticos, a las partes usuarias de dicha autenticación. Esta disposición no es aplicable a los requisitos relativos a los usuarios (titulares) de los medios de identificación electrónica que sean técnicamente necesarios para la utilización de los medios de identificación electrónica, tales como los lectores de tarjetas.

Los Estados miembros deben aceptar la responsabilidad de que el vínculo sea inequívoco (es decir, que los datos de identificación atribuidos a una persona no estén vinculados a ninguna otra) y de la posibilidad de autenticación (es decir, la posibilidad de comprobar la validez de los datos de identificación electrónica). La responsabilidad de los Estados miembros no incluye otros aspectos del proceso de identificación o cualquier transacción que requiera identificación.

El artículo 7 contiene normas sobre la notificación a la Comisión de los sistemas de identificación electrónica.

El artículo 8 tiene por objeto garantizar la interoperabilidad técnica de los sistemas de identificación notificados a través de un enfoque de coordinación, con inclusión de actos delegados.

3.3.3 CAPÍTULO III – SERVICIOS DE CONFIANZA

3.3.3.1 Sección 1 – Disposiciones generales

El artículo 9 establece los principios relativos a la responsabilidad de los proveedores de servicios de confianza tanto cualificados como no cualificados. Se basa en el artículo 6 de la Directiva 1999/93/CE y extiende el derecho a compensación a los daños causados por un proveedor de servicios de confianza negligente que incumple las buenas prácticas de seguridad, lo que desemboca en una violación de la seguridad que tiene un impacto importante sobre el servicio.

El artículo 10 describe el mecanismo para el reconocimiento y aceptación de los servicios de confianza cualificados prestados por un proveedor establecido en un tercer país. Se basa en el artículo 7 de la Directiva 1999/93/CE, pero solo conserva la única opción viable en la práctica, a saber, permitir dicho reconocimiento en virtud de un acuerdo internacional entre la Unión Europea y terceros países u organizaciones internacionales.

El artículo 11 establece los principios de protección y limitación de los datos. Se apoya en el artículo 8 de la Directiva 1999/93/CE.

El artículo 12 trata de la accesibilidad de los servicios de confianza para las personas con discapacidad.

3.3.3.2 Sección 2 – Supervisión

El artículo 13 obliga a los Estados miembros a crear organismos de supervisión, sobre la base del artículo 3, apartado 3, de la Directiva 1999/93/CE, y aclara y amplía su mandato en lo que respecta tanto a los proveedores de servicios de confianza como a los proveedores de servicio de confianza cualificados.

El artículo 14 introduce un mecanismo explícito de asistencia mutua entre los organismos de supervisión de los Estados miembros a fin de facilitar la supervisión transfronteriza de los proveedores de servicios de confianza. Introduce normas sobre las operaciones conjuntas y el derecho de las autoridades de supervisión a participar en estas operaciones.

El artículo 15 introduce la obligación de que los proveedores de servicios de confianza tanto cualificados como no cualificados apliquen las medidas técnicas y organizativas adecuadas para garantizar la seguridad de sus actividades. Además, los organismos de supervisión competentes y otras autoridades pertinentes deberán ser informados de cualquier violación de la seguridad. Si procede, estos informarán a su vez a otros organismos de supervisión de los Estados miembros y, directamente o por mediación del proveedor de servicios de confianza en cuestión, informarán asimismo al público.

El artículo 16 establece las condiciones para la supervisión de los proveedores de servicios de confianza cualificados y de los servicios de confianza cualificados prestados por ellos. Obliga a los proveedores de servicios de confianza cualificados a ser auditados anualmente por un organismo independiente reconocido para confirmar al organismo de supervisión que cumplen las obligaciones establecidas en el Reglamento. Además, el artículo 16, apartado 2,

confiere al organismo de supervisión el derecho a llevar a cabo en cualquier momento auditorías sobre el terreno de los proveedores de servicios de confianza cualificados. También se faculta al organismo de supervisión para impartir instrucciones vinculantes a los proveedores de servicios de confianza cualificados a fin de corregir, de manera proporcionada, cualquier incumplimiento de una obligación que una auditoría de la seguridad haya puesto de manifiesto.

El artículo 17 se refiere a la actividad realizada por el organismo de supervisión a petición de un proveedor de servicios de confianza que desee iniciar un servicio de confianza cualificado.

El artículo 18 prevé el establecimiento de listas de confianza[10] que contengan información sobre los proveedores de servicios de confianza cualificados objeto de supervisión y sobre los servicios cualificados que prestan. Dicha información se pondrá a disposición del público mediante un modelo común, a fin de facilitar su uso automatizado y garantizar un nivel de detalle apropiado.

El artículo 19 establece los requisitos que deben reunir los proveedores de servicios de confianza cualificados a fin de ser reconocidos como tales. Se basa en el anexo II de la Directiva 1999/93/CE.

3.3.3.3 Sección 3 – Firma electrónica

El artículo 20 contiene las normas relativas a los efectos jurídicos de la firma electrónica de una persona física. Amplía y aclara el artículo 5 de la Directiva 1999/93/CE introduciendo una obligación explícita de otorgar a las firmas electrónicas cualificadas los mismos efectos jurídicos que a las firmas manuscritas. Además, los Estados miembros deben garantizar la aceptación transfronteriza de las firmas electrónicas cualificadas, en el contexto de la prestación de servicios públicos, y no deben introducir requisitos adicionales que puedan crear obstáculos a la utilización de tales firmas.

El artículo 21 establece los requisitos de los certificados de firma cualificados. Aclara el anexo I de la Directiva 1999/93/CE y suprime disposiciones que no han funcionado en la práctica (por ejemplo, limitaciones sobre el valor de las transacciones).

El artículo 22 establece los requisitos relativos a los dispositivos de creación de firma electrónica cualificados. Aclara los requisitos relativos a los dispositivos seguros de creación de firmas establecidos en el artículo 3, apartado 5, de la Directiva 1999/93/CE, que deberán considerarse en adelante dispositivos de creación de firmas cualificados con arreglo al presente Reglamento. También deja claro que el alcance de un dispositivo de creación de firmas no tiene por qué limitarse al almacenamiento de datos de creación de firmas. La Comisión podrá crear también una lista de números de referencia de normas relativas a los requisitos de seguridad de los dispositivos.

Basándose en el artículo 3, apartado 4, de la Directiva 1999/93/CE, el artículo 23 introduce el concepto de la certificación de los dispositivos de firma electrónica cualificados para determinar su conformidad con los requisitos de seguridad establecidos en el anexo II. Todos los Estados miembros deben reconocer que estos dispositivos se ajustan a los requisitos cuando un organismo de certificación designado por un Estado miembro lleve a cabo un

[10] La lista de confianza establecida por la Decisión 2009/767/CE de la Comisión, modificada por la Decisión 2010/425/UE de la Comisión, servirá de base para una nueva Decisión de la Comisión sobre las listas de confianza con arreglo al presente Reglamento.

procedimiento de certificación. La Comisión publicará una lista positiva de dichos dispositivos certificados de conformidad con el artículo 24. La Comisión podrá crear también una lista de números de referencia de normas relativas a la evaluación de la seguridad de los productos de tecnología de la información a que se refiere el artículo 23, apartado 1.

El artículo 24 se refiere a la publicación de la lista de dispositivos de creación de firmas electrónicas cualificados por la Comisión tras la notificación de su conformidad por los Estados miembros.

El artículo 25 se apoya en las recomendaciones del anexo IV de la Directiva 1999/93/CE a fin de establecer requisitos vinculantes para la validación de las firmas electrónicas cualificadas con vistas a aumentar la seguridad jurídica de esta validación.

El artículo 26 establece las condiciones de los servicios de validación cualificados.

El artículo 27 establece la condición para la conservación a largo plazo de las firmas electrónicas cualificadas. Esto es posible merced a la utilización de procedimientos y tecnologías capaces de ampliar la fiabilidad de los datos de validación de las firmas electrónicas cualificadas más allá del plazo de su validez tecnológica, cuando a los ciberdelincuentes puede resultarles más fácil falsificarlas.

3.3.3.4 Sección 4 – Sellos electrónicos

El artículo 28 se refiere a los efectos jurídicos de los sellos electrónicos de las personas jurídicas. Se concede una presunción legal específica a los sellos electrónicos cualificados que garantiza la autenticidad e integridad de los documentos electrónicos a los que están vinculados.

El artículo 29 establece los requisitos de los certificados cualificados de sellos electrónicos.

El artículo 30 establece los requisitos de los dispositivos de creación de sellos electrónicos cualificados, así como para la certificación y publicación de la lista.

El artículo 31 establece la condición de validación y conservación de los sellos electrónicos cualificados.

3.3.3.5 Sección 5 – Marca de tiempo electrónica

El artículo 32 se refiere al efecto jurídico de las marcas de tiempo electrónicas. Se concede una presunción legal específica a las marcas de tiempo electrónicas cualificadas con respecto a la certidumbre de la fecha y la hora.

El artículo 33 establece los requisitos de las marcas de tiempo electrónicas cualificadas.

3.3.3.6 Sección 6 – Documentos electrónicos

El artículo 34 establece los efectos jurídicos y las condiciones de aceptación de los documentos electrónicos. Existe una presunción legal específica de autenticidad e integridad de cualquier documento electrónico firmado con una firma electrónica cualificada o que lleve un sello electrónico cualificado. Con respecto a la aceptación de los documentos electrónicos, cuando se exija un documento original o una copia certificada del mismo para la prestación de un servicio público, deberán aceptarse en otros Estados miembros, sin requisitos adicionales,

por lo menos los documentos electrónicos expedidos por las personas competentes para la expedición de los documentos correspondientes y que se consideren originales o copias certificadas de conformidad con la legislación nacional del Estado miembro de origen.

3.3.3.7 Sección 7 – Servicios de entrega electrónica

El artículo 35 dota de efectos jurídicos a los datos enviados o recibidos utilizando un servicio de entrega electrónica. Se garantiza una presunción legal específica en lo que respecta a la integridad de los datos enviados o recibidos y la exactitud de la fecha y hora en que se envían o reciben los datos para los servicios de entrega electrónica cualificados. Asimismo, se garantiza el reconocimiento mutuo de los servicios de entrega electrónica cualificados a nivel de la UE.

El artículo 36 establece los requisitos de los servicios de entrega electrónica cualificados.

3.3.3.8 Sección 8 – Autenticación de sitios web

El objetivo de esta sección es garantizar la autenticidad de un sitio web en lo que se refiere al propietario del sitio.

El artículo 37 establece los requisitos de los certificados cualificados de autenticación de sitios web, que pueden utilizarse para garantizar la autenticidad de un sitio web. El certificado cualificado de autenticación de sitio web proporcionará un conjunto mínimo de información fiable sobre el sitio web y sobre la existencia legal de su propietario.

3.3.4 CAPÍTULO IV – ACTOS DELEGADOS

El artículo 38 contiene las disposiciones estándar relativas al ejercicio de las competencias delegadas en consonancia con el artículo 290 del TFUE (actos delegados). Este artículo autoriza al legislador a delegar en la Comisión las competencias para adoptar actos no legislativos de alcance general que completen o modifiquen determinados elementos no esenciales de un acto legislativo.

3.3.5 CAPÍTULO V – ACTOS DE EJECUCIÓN

El artículo 39 contiene la disposición relativa al procedimiento del comité necesaria para la atribución de competencias de ejecución a la Comisión en los casos en que, de conformidad con el artículo 291 del TFUE, se requieran condiciones uniformes de ejecución de los actos jurídicamente vinculantes de la Unión. Es de aplicación el procedimiento de examen.

3.3.6 CAPÍTULO IV – DISPOSICIONES FINALES

El artículo 40 obliga a la Comisión a evaluar el Reglamento y comunicar sus conclusiones.

El artículo 41 deroga la Directiva 1999/93/CE y prevé una transición fluida de la infraestructura de firma electrónica existente a los nuevos requisitos del Reglamento.

El artículo 42 establece la fecha de entrada en vigor del Reglamento.

4. REPERCUSIONES PRESUPUESTARIAS

Las repercusiones presupuestarias específicas de la propuesta guardan relación con las funciones atribuidas a la Comisión Europea según lo especificado en la ficha financiera legislativa que acompaña a la propuesta.

La propuesta carece de incidencia sobre el gasto operativo.

La ficha financiera legislativa que acompaña a la presente propuesta de Reglamento cubre las repercusiones presupuestarias del propio Reglamento.

2012/0146 (COD)

Propuesta de

REGLAMENTO 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)

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, su artículo 114,

Vista la propuesta de la Comisión Europea,

Previa transmisión de la propuesta de acto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo[11],

Previa consulta al Supervisor Europeo de Protección de Datos[12]

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

(1) La creación de un clima de confianza en el entorno en línea es esencial para el desarrollo económico. La desconfianza hace que los consumidores, las empresas y las administraciones duden a la hora de realizar transacciones por vía electrónica y adoptar nuevos servicios.

(2) El presente Reglamento se propone reforzar la confianza en las transacciones electrónicas en el mercado interior consiguiendo unas interacciones electrónicas seguras y sin fisuras entre las empresas, los ciudadanos y las administraciones públicas e incrementando, en consecuencia, la eficacia de los servicios en línea públicos y privados, los negocios electrónicos y el comercio electrónico en la Unión.

(3) La Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica[13], se refería básicamente a las firmas electrónicas, sin ofrecer un marco global transfronterizo e intersectorial para garantizar unas transacciones electrónicas seguras, fiables y de fácil uso. El presente Reglamento refuerza y amplía el acervo que representa dicha Directiva.

---

11 DO C de , p. .

12 DO C de , p. .

13 DO L 13 de 19.1.2000, p. 12.

(4) La Agenda Digital para Europa de la Comisión[14] señaló que la fragmentación del mercado digital, la falta de interoperabilidad y el incremento de la ciberdelincuencia constituían obstáculos importantes para el ciclo virtuoso de la economía digital. En su informe sobre la ciudadanía de 2010, la Comisión subrayó asimismo la necesidad de resolver los principales problemas que impiden que los ciudadanos europeos disfrutar de los beneficios de un mercado único digital y unos servicios digitales transfronterizos[15].

(5) El Consejo Europeo invitó a la Comisión a crear un mercado único digital para 2015[16] a fin de progresar rápidamente en ámbitos clave de la economía digital y promover un mercado único digital plenamente integrado[17], facilitando el uso transfronterizo de los servicios en línea, con especial atención a la identificación y autenticación electrónicas seguras.

(6) El Consejo invitó a la Comisión a contribuir al mercado único digital creando condiciones apropiadas para el reconocimiento mutuo a través de las fronteras de instrumentos clave tales como la identificación electrónica, los documentos electrónicos, las firmas electrónicas y los servicios de entrega electrónica, así como para unos servicios de administración electrónica interoperables en toda la Unión Europea[18].

(7) El Parlamento Europeo subrayó la importancia de la seguridad de los servicios electrónicos, especialmente de la firma electrónica, y la necesidad de crear una infraestructura de clave pública a nivel paneuropeo, y pidió a la Comisión que estableciese una pasarela de autoridades europeas de validación a fin de garantizar la interoperabilidad transfronteriza de las firmas electrónicas y aumentar la seguridad de las transacciones realizadas a través de Internet[19].

(8) La Directiva 2006/123/CE del Parlamento Europeo y el Consejo, de 12 de diciembre de 2006, relativa a los servicios en el mercado interior[20], exige a los Estados miembros establecer «ventanillas únicas» para garantizar que todos los procedimientos y trámites relativos al acceso a una actividad de servicios y a su ejercicio se puedan realizar fácilmente, a distancia y por vía electrónica, a través de la ventanilla única adecuada y con las autoridades competentes. Ahora bien, muchos servicios en línea accesibles a través de ventanillas únicas exigen la identificación, autenticación y firma electrónicas.

(9) En la mayoría de los casos, los proveedores de servicios de otro Estado miembro no pueden utilizar su identificación electrónica para acceder a tales servicios porque los

---

14 COM(2010) 245 final/2.

15 Informe sobre la ciudadanía de la UE 2010: La eliminación de los obstáculos a los derechos de los ciudadanos de la UE, COM (2010) 603 final, punto 2.2.2, página 13.

16 4/2/2011: EUCO 2/1/11.

17 23/10/2011: EUCO 52/1/11.

18 Conclusiones del Consejo sobre el plan de acción europeo sobre administración electrónica 2011-2015, reunión nº 3093 del Consejo de Transportes, Telecomunicaciones y Energía, Bruselas, 27 de mayo de 2011.

19 Resolución del Parlamento Europeo, de 21 de septiembre de 2010, sobre la plena realización del mercado interior del comercio electrónico, 21.9.10, P7_TA (2010) 0320, y Resolución del Parlamento Europeo, de 15 de junio de 2010, sobre la gobernanza de Internet: los próximos pasos, P7_TA (2010) 0208.

20 DO L 376 de 27.12.2006, p. 36.

regímenes nacionales de identificación electrónica en su país no son reconocidos y aceptados en otros Estados miembros. Esta barrera electrónica excluye a los proveedores de servicios del pleno disfrute de los beneficios del mercado interior. Unos medios de identificación electrónica mutuamente reconocidos y aceptados facilitarán la prestación transfronteriza de numerosos servicios en el mercado interior y permitirán a las empresas actuar fuera de sus fronteras sin encontrar obstáculos en su interacción con las autoridades públicas.

(10) La Directiva 2011/24/UE del Parlamento Europeo y el Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza[21], establece una red de autoridades nacionales encargadas de la sanidad electrónica. A fin de mejorar la seguridad y la continuidad de la asistencia sanitaria transfronteriza, se solicita a esta red que elabore directrices sobre el acceso transfronterizo a los datos y servicios de sanidad electrónica, en particular apoyando *«medidas comunes de identificación y autenticación para facilitar la transferibilidad de los datos en la asistencia sanitaria transfronteriza»*. El reconocimiento y la aceptación mutuos de la identificación y la autenticación electrónicas son esenciales para que la atención sanitaria transfronteriza de los ciudadanos europeos se haga realidad. Cuando una persona se desplaza para ser tratada, sus datos médicos deben ser accesibles en el país que dispense el tratamiento. Para ello es necesario contar con un marco de identificación electrónica sólido, seguro y confiable.

(11) Uno de los objetivos del presente Reglamento es eliminar las barreras existentes para el uso transfronterizo de los medios de identificación electrónica utilizados en los Estados miembros para acceder al menos a los servicios públicos. El presente Reglamento no se propone intervenir en los sistemas de gestión de la identidad electrónica e infraestructuras conexas establecidos en los Estados miembros. Lo que pretende es garantizar que sean posibles la identificación y la autenticación electrónicas seguras para el acceso a los servicios transfronterizos en línea ofrecidos por los Estados miembros.

(12) Los Estados miembros deben seguir siendo libres de utilizar o introducir, a efectos de identificación electrónica, medios de acceder a los servicios en línea. También deben poder decidir si interviene o no el sector privado en la prestación de estos medios. Los Estados miembros no deben estar obligados a notificar sus sistemas de identificación electrónica. Corresponde a los Estados miembros decidir si notifican todos, algunos o ninguno de los sistemas de identificación electrónica utilizados a nivel nacional para el acceso al menos a los servicios públicos en línea o a servicios específicos.

(13) Deben establecerse en el Reglamento ciertas condiciones en relación con qué medios de identificación electrónica tienen que aceptarse y cómo deben notificarse los regímenes. De este modo cada Estado miembro podría adquirir la confianza necesaria en los sistemas de identificación electrónica de los demás y reconocer y aceptar mutuamente los medios de identificación electrónica de sus regímenes notificados. Debe aplicarse el principio de reconocimiento y aceptación mutuos si el Estado miembro notificador cumple las condiciones de notificación y la notificación se ha publicado en el Diario Oficial de la Unión Europea. No obstante, el acceso a estos servicios en línea y su entrega final al solicitante deben estar estrechamente vinculados

[21] DO L 88 de 4.4.2011, p. 45.

al derecho a recibir dichos servicios en las condiciones fijadas por la legislación nacional.

(14) Los Estados miembros deben poder decidir que participe el sector privado en la expedición de medios de identificación electrónica y permitir que dicho sector utilice los medios de identificación electrónica amparados en un régimen notificado a efectos de identificación cuando sea necesario para servicios en línea o transacciones electrónicas. La posibilidad de utilizar estos medios de identificación electrónica permitiría al sector privado recurrir a una identificación y autenticación electrónicas ampliamente utilizadas ya en muchos Estados miembros, al menos para los servicios públicos, y facilitar el acceso de las empresas y los ciudadanos a sus servicios en línea a través de las fronteras. Para facilitar el uso de tales medios de identificación electrónica a través de las fronteras por el sector privado, debe estar disponible la posibilidad de autenticación ofrecida por los Estados miembros para las partes usuarias sin discriminación entre el sector público y el privado.

(15) El uso transfronterizo de medios de identificación electrónica al amparo de un régimen notificado exige que los Estados miembros cooperen para ofrecer la interoperabilidad técnica. Esto excluye cualquier norma técnica nacional específica que exija que las partes no nacionales, por ejemplo, obtengan equipos o programas específicos para verificar y validar la identificación electrónica notificada. Por el contrario, es inevitable imponer requisitos técnicos a los usuarios, derivados de las especificaciones intrínsecas de cualquier dispositivo que se utilice (por ejemplo, las tarjetas inteligentes).

(16) La cooperación de los Estados miembros debe contribuir a la interoperabilidad técnica de los sistemas de identificación electrónica notificados con vistas a fomentar un nivel de confianza y seguridad elevados, adaptados al grado de riesgo. El intercambio de información y el intercambio de las mejores prácticas entre los Estados miembros con miras a su reconocimiento mutuo debe facilitar dicha cooperación.

(17) El presente Reglamento también debe establecer un marco jurídico general para la utilización de los servicios de confianza electrónicos. Sin embargo, no debe crear la obligación general de utilizarlos. En particular, no debe cubrir la prestación de servicios basados en acuerdos voluntarios de Derecho privado. Tampoco debe regular los aspectos relacionados con la celebración y validez de los contratos u otras obligaciones legales cuando existan requisitos de forma establecidos por el Derecho nacional o de la Unión.

(18) Para contribuir al uso transfronterizo general de los servicios de confianza electrónicos, debe ser posible utilizarlos como prueba en procedimientos judiciales en todos los Estados miembros.

(19) Los Estados miembros deben conservar la libertad para definir otros tipos de servicios de confianza, además de los que forman parte de la lista cerrada de servicios de confianza prevista en el presente Reglamento, a efectos de su reconocimiento a nivel nacional como servicios de confianza cualificados.

(20) En razón de la rápida evolución de la tecnología, el presente Reglamento debe adoptar un planteamiento abierto a innovaciones.

(21) El presente Reglamento debe ser neutral en lo que se refiere a la tecnología. Los efectos jurídicos que otorga deben poder lograrse por cualquier medio técnico, siempre que se cumplan los requisitos que en él se estipulan.

(22) Para aumentar la confianza de los ciudadanos en el mercado interior y fomentar el uso de servicios y productos de confianza, deben introducirse los conceptos de servicios de confianza cualificados y de proveedor de servicios de confianza cualificados con miras a indicar los requisitos y obligaciones que garanticen un alto nivel de seguridad de cualquier servicio o producto de confianza cualificado que se preste o utilice.

(23) En consonancia con las obligaciones en virtud de la Convención de las Naciones Unidas sobre los derechos de las personas con discapacidad, que ha entrado en vigor en la UE, las personas con discapacidad deben poder utilizar los servicios de confianza y los productos para el usuario final usados en la prestación de estos servicios en pie de igualdad con los demás consumidores.

(24) Un proveedor de servicios de confianza es un responsable del tratamiento de los datos personales y, por tanto, ha de cumplir las obligaciones previstas en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[22]. En particular, la recogida de datos debe reducirse al mínimo posible teniendo en cuenta la finalidad del servicio prestado.

(25) Los organismos de supervisión deben cooperar e intercambiar información con las autoridades de protección de datos a fin de garantizar la correcta aplicación de la legislación sobre protección de datos por parte de los proveedores de servicios. El intercambio de información debe incluir, en particular, los incidentes en materia de seguridad y las violaciones de los datos personales.

(26) A todos los proveedores de servicios de confianza debe incumbir la aplicación de las buenas prácticas de seguridad adecuadas para los riesgos relacionados con sus actividades a fin de promover la confianza de los usuarios en el mercado único.

(27) Las disposiciones relativas al uso de seudónimos en los certificados no deben impedir a los Estados miembros exigir la identificación de las personas de conformidad con el Derecho nacional o de la Unión.

(28) Todos los Estados miembros deben seguir unos requisitos de supervisión esenciales con el fin de garantizar un nivel de seguridad comparable de los servicios de confianza cualificados. Para facilitar la aplicación coherente de estos requisitos en toda la Unión, los Estados miembros deben adoptar unos procedimientos comparables e intercambiar información sobre sus actividades de supervisión y las mejores prácticas en este campo.

(29) Es esencial la notificación de las violaciones de la seguridad y de las evaluaciones del riesgo para la seguridad con vistas a ofrecer una información adecuada a las partes implicadas en caso de violación de la seguridad o pérdida de la integridad.

(30) Con el fin de permitir a la Comisión y a los Estados miembros evaluar la eficacia de la mecanismo de notificación de violaciones introducido por el presente Reglamento, los

[22] DO L 281 de 23.11.1995, p. 31.

organismos de supervisión deben proporcionar información resumida a la Comisión y a la Agencia Europea de Seguridad de las Redes y de la Información (ENISA).

(31) Para permitir a la Comisión y a los Estados miembros evaluar el impacto del presente Reglamento, debe solicitarse a los organismos de supervisión que faciliten estadísticas sobre la utilización de los servicios de confianza cualificados.

(32) Con el fin de permitir a la Comisión y a los Estados miembros evaluar la eficacia del mecanismo de supervisión reforzada introducido por el presente Reglamento, debe solicitarse a los organismos de supervisión que informen sobre sus actividades. Este elemento sería decisivo para facilitar el intercambio de buenas prácticas entre los organismos de supervisión y garantizaría la verificación de que los requisitos de supervisión esenciales se aplican de forma coherente y eficiente en todos los Estados miembros.

(33) A fin de garantizar la sostenibilidad y durabilidad de los servicios de confianza cualificados y de potenciar la confianza de los usuarios en la continuidad de dichos servicios, los organismos de supervisión deben garantizar que los datos de un proveedor de servicios de confianza cualificado se conservan y mantienen accesibles durante un período de tiempo adecuado incluso en caso de que dicho proveedor deje de existir.

(34) Para facilitar la supervisión de los proveedores de servicios de confianza cualificados, por ejemplo cuando un proveedor preste sus servicios en el territorio de otro Estado miembro y no esté sujeto a supervisión en este, o cuando los ordenadores de un proveedor estén situados en el territorio de un Estado miembro distinto de aquel en el que está establecido, debe crearse un sistema de asistencia mutua entre los organismos de supervisión de los Estados miembros.

(35) Los proveedores de servicios de confianza son responsables del cumplimiento de los requisitos establecidos en el presente Reglamento para la prestación se servicios de confianza, en particular de los servicios de confianza cualificados. Los organismos de supervisión son responsables de supervisar la manera en que los proveedores de servicios de confianza cumplen dichos requisitos.

(36) A in de permitir un proceso de puesta en marcha eficiente, que lleve a la inclusión de los proveedores de servicios de confianza cualificados y de los servicios de confianza cualificados que prestan en listas de confianza, deben fomentarse las interacciones preliminares entre los candidatos a proveedores de servicios de confianza cualificados y el organismo de supervisión competente con vistas a facilitar la diligencia debida que lleve a la prestación de servicios de confianza cualificados.

(37) Las listas de confianza constituyen elementos esenciales para la creación de confianza entre los operadores del mercado, ya que indican la cualificación del proveedor de servicios en el momento de la supervisión, pero no son un requisito previo para alcanzar la cualificación y prestar servicios de confianza cualificados que deriva del respeto de los requisitos contenidos en el presente Reglamento.

(38) Una vez que haya sido objeto de notificación, el organismo del sector público de que se trate no puede rechazar un servicio de confianza cualificado para el cumplimiento de un procedimiento o trámite administrativo por el hecho de no estar incluido en las listas de confianza establecidas por los Estados miembros. A los presentes efectos, por

organismo del sector público debe entenderse cualquier autoridad pública u otra entidad a la que se haya confiado la prestación de servicios de administración electrónica tales como la declaración de impuestos en línea, la solicitud de partidas de nacimiento, la participación en procedimientos de contratación pública electrónica, etc.

(39) Aun cuando es necesario un alto nivel de seguridad para garantizar el reconocimiento mutuo de las firmas electrónicas, en determinados casos, como por ejemplo en el contexto de la Decisión 2009/767/CE de la Comisión, de 16 de octubre de 2009, por la que se adoptan medidas que facilitan el uso de procedimientos por vía electrónica a través de las ventanillas únicas con arreglo a la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior[23], deben aceptarse también las firmas electrónicas que tienen una menor garantía de la seguridad.

(40) Debe ser posible para el firmante confiar a un tercero los dispositivos de creación de firmas electrónicas cualificados, a condición de que se apliquen los procedimientos y mecanismos adecuados para garantizar que el firmante tiene el control exclusivo del uso de sus datos de creación de la firma electrónica y que la utilización del dispositivo cumple los requisitos de la firma cualificada.

(41) Para ofrecer seguridad jurídica sobre la validez de la firma, es esencial detallar qué componentes de una firma electrónica cualificada debe evaluar la parte usuaria que efectúa la validación. Por otra parte, definir los requisitos exigibles a los proveedores de servicios de confianza cualificados que pueden brindar un servicio de validación cualificado a las partes usuarias que no desean o no pueden realizar por sí mismas la validación de las firmas electrónicas cualificadas debe estimular a los sectores privado o público para que inviertan en tales servicios. Ambos elementos deben contribuir a que la validación de la firma electrónica cualificada resulte fácil y cómoda para todas las partes a nivel de la Unión.

(42) Cuando una transacción exija un sello electrónico cualificado de una persona jurídica, debe ser igualmente aceptable una firma electrónica cualificada del representante autorizado de la persona jurídica.

(43) Los sellos electrónicos deben servir como prueba de que un documento electrónico ha sido expedido por una persona jurídica, aportando certeza sobre el origen y la integridad del documento.

(44) El presente Reglamento debe garantizar la conservación a largo plazo de la información, es decir, la validez jurídica de la firma electrónica y los sellos electrónicos durante períodos de tiempo prolongados, garantizando que se puedan validar independientemente de la evolución futura de la tecnología.

(45) Con el fin de potenciar el uso transfronterizo de los documentos electrónicos, el presente Reglamento debe prever los efectos jurídicos de los documentos electrónicos, que deben considerarse equivalentes a los documentos en papel dependiendo de la evaluación del riesgo y siempre que se garanticen su autenticidad e integridad. También es importante para que sigan desarrollándose las transacciones electrónicas transfronterizas en el mercado interior que los documentos electrónicos originales o

[23] DO L 274 de 20.10.2009, p. 36.

las copias certificadas expedidas por los organismos competentes correspondientes en un Estado miembro con arreglo a su Derecho nacional sean aceptadas como tales también en otros Estados miembros. El presente Reglamento no debe afectar al derecho de los Estados miembros a determinar qué constituye un original o una copia a nivel nacional, pero garantiza que estos puedan utilizarse como tales también a través de las fronteras.

(46) Dado que las autoridades competentes en los Estados miembros usan actualmente formatos de firma electrónica avanzada diferentes para firmar electrónicamente sus documentos, es preciso velar por que los Estados miembros puedan soportar técnicamente al menos una serie de formatos de firma electrónica avanzada cuando reciban documentos firmados electrónicamente. Del mismo modo, cuando las autoridades competentes de los Estados miembros utilicen sellos electrónicos avanzados, sería necesario garantizar que soporten al menos una serie de formatos de sello electrónico avanzado.

(47) Además de autenticar el documento expedido por la persona jurídica, los sellos electrónicos pueden utilizarse para autenticar cualquier activo digital de la persona jurídica, por ejemplo, programas informáticos o servidores.

(48) La posibilidad de autenticar sitios web y a sus propietarios haría más difícil la falsificación de sitios web y, en consecuencia, reduciría el fraude.

(49) Para complementar algunos aspectos técnicos concretos del presente Reglamento de manera flexible y rápida, debe delegarse en la Comisión la facultad de adoptar actos de conformidad con el artículo 290 del Tratado de Funcionamiento de la Unión Europea en lo que se refiere a la interoperabilidad de la identificación electrónica; las medidas de seguridad exigidas a los proveedores de servicios de confianza; los organismos independientes reconocidos responsables de auditar a los proveedores de servicios; las listas de confianza; los requisitos relacionados con los niveles de seguridad de las firmas electrónicas; los requisitos de los certificados cualificados de firma electrónica, su validación y su conservación; los organismos responsables de la certificación de los dispositivos de creación de firmas electrónicas cualificadas; y los requisitos relacionados con los niveles de seguridad de los sellos electrónicos y los certificados cualificados de sello electrónico; y la interoperabilidad entre los servicios de entrega. Es especialmente importante que la Comisión celebre las consultas que proceda, incluidas las consultas a expertos, durante sus trabajos de preparación.

(50) Al preparar y elaborar actos delegados, la Comisión debe garantizar que los documentos pertinentes se transmitan al Parlamento Europeo y al Consejo de manera simultánea, oportuna y adecuada.

(51) Con el fin de garantizar unas condiciones uniformes para la aplicación del presente Reglamento, se conferirán competencias de ejecución a la Comisión, en particular, para que especifique los números de referencia de las normas cuya utilización daría la presunción del cumplimiento de determinados requisitos establecidos en el presente Reglamento o definidos en los actos delegados. Estas competencias deben ejercerse de conformidad con el Reglamento (UE) nº 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios

generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión[24].

(52) Por razones de seguridad jurídica y claridad, debe derogarse la Directiva 1999/93/CE.

(53) Para dar seguridad jurídica a los operadores del mercado que ya utilicen certificados reconocidos expedidos de conformidad con la Directiva 1999/93/CE, es necesario prever un período de transición suficiente. También es necesario dotar a la Comisión de los medios necesarios para adoptar los actos de ejecución y los actos delegados con anterioridad a esa fecha.

(54) Dado que los objetivos del presente Reglamento no pueden ser alcanzados de manera suficiente por los Estados miembros y, por consiguiente, puede lograrse mejor, debido a la escala de la acción, a nivel de la Unión, la Unión puede adoptar medidas, de acuerdo con el principio de subsidiariedad consagrado en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad enunciado en dicho artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo, especialmente en lo que se refiere al papel de la Comisión como coordinadora de las actividades nacionales.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Objeto

1. El presente Reglamento establece las reglas de los servicios de identificación electrónica y de confianza electrónica para las transacciones electrónicas con vistas a garantizar el buen funcionamiento del mercado interior.

2. El presente Reglamento establece las condiciones en que los Estados miembros deberán reconocer y aceptar los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica notificado de otro Estado miembro.

3. El presente Reglamento establece un marco jurídico para las firmas electrónicas, los sellos electrónicos, las marcas de tiempo electrónicas, los documentos electrónicos, los servicios de entrega electrónica y la autenticación de sitios web.

4. El presente Reglamento vela por que los servicios y productos de confianza que cumplan sus disposiciones estén autorizados a circular libremente en el mercado interior.

Artículo 2

Ámbito de aplicación

[24] DO L 55 de 28.2.2011, p. 13.

1. El presente Reglamento se aplica a la identificación electrónica facilitada por los Estados miembros, en su nombre o bajo su responsabilidad, y a los proveedores de servicios de confianza establecidos en la Unión.

2. El presente Reglamento no se aplica a la prestación de servicios de confianza electrónicos basados en acuerdos voluntarios de Derecho privado.

3. Tampoco se aplica a los aspectos relacionados con la celebración y validez de los contratos u otras obligaciones legales cuando existan requisitos de forma establecidos por la legislación nacional o de la Unión.

Artículo 3

Definiciones

A efectos del presente Reglamento, se aplicarán las siguientes definiciones:

(1) «identificación electrónica», el proceso de utilizar los datos de identificación de una persona en forma electrónica que representan inequívocamente a una persona física o jurídica;

(2) «medios de identificación electrónica», una unidad material o inmaterial que contiene los datos a que se refiere el punto 1 del presente artículo y que se utiliza para el acceso a servicios en línea según se contempla en el artículo 5;

(3) «sistema de identificación electrónica», un régimen para la identificación electrónica en virtud del cual se expiden medios de identificación electrónica a las personas según se contempla en el punto 1 del presente artículo;

(4) «autenticación», un proceso electrónico que permite la validación de la identificación electrónica de una persona física o jurídica, o del origen y la integridad de un dato electrónico;

(5) «firmante», una persona física que crea una firma electrónica;

(6) «firma electrónica», los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar;

(7) «firma electrónica avanzada», la firma electrónica que cumple los requisitos siguientes:

(a) estar vinculada al firmante de manera única;

(b) permitir la identificación del firmante;

(c) haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo; y

(d) estar vinculada con los datos a que se refiere de modo tal que cualquier modificación ulterior de los mismos sea detectable;

(8) «firma electrónica cualificada», una firma electrónica avanzada que se crea mediante un dispositivo de creación de firmas electrónicas cualificado y que se basa en un certificado cualificado de firma electrónica;

(9) «datos de creación de la firma electrónica», los datos únicos que utiliza el firmante para crear una firma electrónica;

(10) «certificado», una declaración electrónica que vincula los datos de validación de una firma o un sello electrónicos de una persona física o jurídica, respectivamente, con el certificado y confirma esos datos de esa persona;

(11) «certificado cualificado de firma electrónica», una declaración que se utiliza para respaldar las firmas electrónicas, está expedida por un proveedor de servicios de confianza cualificado y cumple los requisitos establecidos en el anexo I;

(12) «servicio de confianza», un servicio electrónico que consiste en la creación, verificación, validación, gestión y conservación de firmas electrónicas, sellos electrónicos, marcas de tiempo electrónicas, documentos electrónicos, servicios de entrega electrónica, autenticación de sitios web y certificados electrónicos, incluidos los certificados de firma electrónica y de sello electrónico;

(13) «servicio de confianza cualificado», un servicio de confianza que cumple los requisitos aplicables previstos en el presente Reglamento;

(14) «proveedor de servicios de confianza», una persona física o jurídica que presta uno o más servicios de confianza;

(15) «proveedor de servicios de confianza cualificado», un proveedor de servicios de confianza que cumple los requisitos establecidos en el presente Reglamento;

(16) «producto», un equipo o programa informático, o los componentes pertinentes de los mismos, destinados a ser utilizados para la prestación de servicios de confianza;

(17) «dispositivo de creación de firmas electrónicas», un equipo o programa informático configurado que se utiliza para crear una firma electrónica;

(18) «dispositivo de creación de firmas electrónicas cualificado», un dispositivo de creación de firmas electrónicas que cumple los requisitos enumerados en el anexo II;

(19) «creador de un sello», una persona física que crea un sello electrónico;

(20) «sello electrónico», datos en forma electrónica anejos a otros datos electrónicos, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de los datos asociados;

(21) «sello electrónico avanzado», un sello electrónico que cumple los requisitos siguientes:

(a) estar vinculado al creador del sello de manera única;

(b) permitir la identificación del creador del sello;

(c) haber sido creado utilizando datos de creación del sello electrónico que el creador del sello puede utilizar para la creación de un sello electrónico, con un alto nivel de confianza, bajo su control exclusivo; y

(d) estar vinculado con los datos a que se refiere de modo tal que cualquier modificación ulterior de los mismos sea detectable;

(22) «sello electrónico cualificado», un sello electrónico avanzado que se crea mediante un dispositivo de creación de sellos electrónicos cualificado y que se basa en un certificado cualificado de sello electrónico;

(23) «datos de creación del sello electrónico», los datos únicos que utiliza el creador del sello electrónico para crearlo;

(24) «certificado cualificado de sello electrónico», una declaración que se utiliza para respaldar un sello electrónico, está expedida por un proveedor de servicios de confianza cualificado y cumple los requisitos establecidos en el anexo III;

(25) «marca de tiempo electrónica», datos en forma electrónica que vinculan otros datos electrónicos con un instante concreto, aportando la prueba de que estos datos existían en ese instante;

(26) «marca de tiempo electrónica cualificada», una marca de tiempo electrónica que cumple los requisitos establecidos en el artículo 33;

(27) «documento electrónico», un documento en cualquier formato electrónico;

(28) «servicio de entrega electrónica», un servicio que permite transmitir datos por medios electrónicos y aporta pruebas relacionadas con la gestión de los datos transmitidos, incluida la prueba del envío o la recepción de los datos, y que protege los datos transmitidos frente a los riesgos de pérdida, robo, deterioro o alteración no autorizada;

(29) «servicio de entrega electrónica cualificado», un servicio de entrega electrónica que cumple los requisitos establecidos en el artículo 36;

(30) «certificado cualificado de autenticación de sitio web», una declaración que permite autenticar un sitio web y vincula el sitio web con la persona a quien ha expedido el certificado un proveedor de servicios de confianza cualificado y que cumple los requisitos establecidos en el anexo IV;

(31) «datos de validación», los datos utilizados para validar una firma electrónica o un sello electrónico.

Artículo 4

Principio del mercado interior

1. No se impondrá restricción alguna a la prestación de servicios de confianza en el territorio de un Estado miembro por un proveedor de servicios de confianza establecido en otro Estado miembro por razones que entren en los ámbitos cubiertos por el presente Reglamento.

2. Se permitirá la libre circulación en el mercado interior de los productos que se ajusten al presente Reglamento.

CAPÍTULO II

IDENTIFICACIÓN ELECTRÓNICA

Artículo 5

Reconocimiento y aceptación mutuos

Cuando sea necesaria una identificación electrónica utilizando un medio de identificación electrónica y una autenticación en virtud de la legislación o la práctica administrativa nacionales para acceder a un servicio en línea, se reconocerá y aceptará a efectos del acceso a dicho servicio todo medio de identificación electrónica expedido en otro Estado miembro que

esté incluido en un régimen que figure en la lista publicada por la Comisión de conformidad con el procedimiento a que se refiere el artículo 7.

Artículo 6

Condiciones de notificación de los sistemas de identificación electrónica

1. Los sistemas de identificación electrónica podrán ser objeto de notificación con arreglo al artículo 7 si se cumple la totalidad de las condiciones siguientes:

(a) los medios de identificación electrónica son expedidos por el Estado miembro notificador, o en su nombre o bajo su responsabilidad;

(b) los medios de identificación electrónica pueden usarse para acceder al menos a los servicios públicos que exigen la identificación electrónica en el Estado miembro notificador;

(c) el Estado miembro notificador garantiza que los datos de identificación de la persona se atribuyen inequívocamente a la persona física o jurídica a la que se refiere el artículo 3, punto 1;

(d) el Estado miembro notificador garantiza que existe una posibilidad de autenticación en línea, en cualquier momento y con carácter gratuito, de manera que cualquier parte usuaria pueda validar los datos de identificación de la persona recibidos en forma electrónica; los Estados miembros no impondrán requisitos técnicos específicos a las partes usuarias establecidas fuera de su territorio que tengan intención de llevar a cabo tal autenticación; en caso de que el sistema de identificación notificado o la posibilidad de autenticación hayan sido violados o parcialmente comprometidos, los Estados miembros suspenderán o revocarán sin demora el sistema de identificación notificado, la posibilidad de autenticación o las partes que estén comprometidas, e informarán a los demás Estados miembros y a la Comisión de conformidad con el artículo 7;

(e) el Estado miembro notificador asume la responsabilidad de:

– i) la atribución inequívoca de los datos de identificación de la persona a que se refiere la letra c), y

– ii) la posibilidad de autenticación especificada en la letra d).

2. La letra e) del apartado 1 se entenderá sin perjuicio de la responsabilidad de las partes en relación con una transacción en la que se utilicen medios de identificación electrónica incluidos en el régimen notificado.

Artículo 7

Notificación

1. Los Estados miembros que notifiquen un sistema de identificación electrónica transmitirán a la Comisión la siguiente información y, sin dilaciones indebidas, cualquier modificación posterior de la misma:

(a) una descripción del sistema de identificación electrónica notificado;

(b) las autoridades responsables del sistema de identificación electrónica notificado;

(c) información sobre quién gestiona el registro de los identificadores de personas inequívocos;

(d) una descripción de la posibilidad de autenticación;

(e) disposiciones relativas a la suspensión o revocación del sistema de identificación notificado, de la posibilidad de autenticación o de las partes que estén comprometidas.

2. Seis meses después de la entrada en vigor del Reglamento, la Comisión publicará en el *Diario Oficial de la Unión Europea* la lista de los sistemas de identificación electrónica notificados de conformidad con el apartado 1 y la información básica al respecto.

3. Si la Comisión recibe una notificación una vez concluido el período a que se refiere el apartado 2, modificará la lista en el plazo de tres meses.

4. La Comisión podrá, mediante actos de ejecución, definir las circunstancias, formatos y procedimientos de la notificación a que se refieren los apartados 1 y 3. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 39, apartado 2.

Artículo 8

Coordinación

1. Los Estados miembros cooperarán a fin de garantizar la interoperabilidad de los medios de identificación electrónica incluidos en un régimen notificado y mejorar su seguridad.

2. La Comisión fijará, mediante actos de ejecución, las modalidades necesarias para facilitar la cooperación entre los Estados miembros a que se refiere el apartado 1, con vistas a fomentar un alto grado de confianza y seguridad que corresponda al nivel de riesgo. Dichos actos de ejecución se referirán, en particular, al intercambio de información, experiencias y buenas prácticas sobre los sistemas de identificación electrónica, la revisión i*nter pares* de los sistemas de identificación electrónica notificados y el examen de la evolución del sector de la identificación electrónica por las autoridades competentes de los Estados miembros. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 39, apartado 2.

3. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 38, referentes a la facilitación de la interoperabilidad transfronteriza de los medios de identificación electrónica mediante el establecimiento de los requisitos técnicos mínimos.

CAPÍTULO III

SERVICIOS DE CONFIANZA

Sección 1

Disposiciones generales

Artículo 9

Responsabilidad

1. Los proveedores de servicios de confianza serán responsables de los perjuicios directos causados a cualquier persona física o jurídica en razón del incumplimiento de las obligaciones establecidas en el artículo 15, apartado 1, a menos que puedan probar que no ha habido negligencia de su parte.

2. Los proveedores de servicios de confianza cualificados serán responsables de los perjuicios directos causados a cualquier persona física o jurídica en razón del incumplimiento de las obligaciones establecidas en el presente Reglamento, en particular en su artículo 19, a menos que puedan probar que no ha habido negligencia de su parte.

Artículo 10

Proveedores de servicios de confianza de terceros países

1. Los servicios de confianza cualificados y los certificados cualificados suministrados por los proveedores de servicios de confianza cualificados establecidos en un tercer país serán aceptados como los servicios de confianza cualificados y los certificados cualificados suministrados por los proveedores de servicios de confianza cualificados establecidos en el territorio de la Unión si los servicios de confianza cualificados o los certificados cualificados originarios del tercer país son reconocidos en virtud de un acuerdo entre la Unión y terceros países u organizaciones internacionales de conformidad con el artículo 218 del TFUE.

2. Con referencia al apartado 1, tales acuerdos garantizarán que los proveedores de servicios de confianza de terceros países u organizaciones internacionales cumplen los requisitos aplicables a los servicios de confianza cualificados y a los certificados cualificados suministrados por los proveedores de servicios de confianza cualificados establecidos en el territorio de la Unión, especialmente en lo que se refiere a la protección de los datos de carácter personal, la seguridad y la supervisión.

Artículo 11

Procesamiento y protección de los datos

1. Cuando procesen datos personales, los proveedores de servicios de confianza y los organismos de supervisión velarán por un procesamiento justo y lícito de conformidad con la Directiva 95/46/CE.

2. Los proveedores de servicios de confianza procesarán los datos personales de conformidad con la Directiva 95/46/CE. El procesamiento estará estrictamente limitado a los datos mínimos necesarios para la expedición y el mantenimiento de un certificado o para la prestación de un servicio de confianza.

3. Los proveedores de servicios de confianza garantizarán la confidencialidad e integridad de los datos relacionados con la persona a la que se presta el servicio de confianza.

4. Sin perjuicio de los efectos jurídicos concedidos a los seudónimos con arreglo al Derecho nacional, los Estados miembros no impedirán que los proveedores de servicios de confianza consignen en los certificados de firma electrónica un seudónimo en lugar del nombre del firmante.

Artículo 12

Accesibilidad para las personas con discapacidad

Los servicios de confianza prestados y los productos para el usuario final utilizados en la prestación de estos servicios deberán ser accesibles para las personas con discapacidad siempre que sea posible.

Sección 2

Supervisión

Artículo 13

Organismo de supervisión

1. Los Estados miembros designarán un organismo adecuado establecido en su territorio o, previo acuerdo mutuo, en otro Estado miembro bajo la responsabilidad del Estado miembro que efectúa la designación. Los organismos de supervisión disfrutarán de todas las competencias de supervisión e investigación necesarias para el ejercicio de sus funciones.

2. El organismo de supervisión será responsable del desempeño de las siguientes tareas:

(a) efectuar un seguimiento los proveedores de servicios de confianza establecidos en el territorio del Estado miembro que lo designa a fin de garantizar que cumplen los requisitos establecidos en el artículo 15;

(b) encargarse de la supervisión de los proveedores de servicios de confianza cualificados establecidos en el territorio del Estado miembro que lo designa y de los servicios de confianza cualificados que prestan con el fin de garantizar que tanto ellos como los servicios de confianza cualificados que prestan cumplan los requisitos aplicables establecidos en el presente Reglamento;

(c) garantizar que la información y los datos pertinentes a que se refiere el artículo 19, apartado 2, letra g), registrados por los proveedores de servicios de confianza cualificados se conservan y permanecen accesibles, una vez que hayan cesado las actividades de un proveedor de servicios de confianza cualificado, durante un período adecuado con vistas a garantizar la continuidad del servicio.

3. Cada organismo de supervisión presentará cada año a la Comisión y a los Estados miembros un informe sobre las actividades de supervisión correspondientes al año civil precedente antes de que finalice el primer trimestre del año siguiente. Dicho informe incluirá, como mínimo:

(a) información sobre sus actividades de supervisión;

(b) un resumen de las notificaciones de violaciones recibidas de los proveedores de servicios de confianza, de conformidad con el artículo 15, apartado 2;

(c) estadísticas sobre el mercado y el uso de los servicios de confianza cualificados, incluida información sobre los propios proveedores de servicio de confianza cualificados, los servicios de confianza cualificados que prestan, los productos que utilizan y la descripción general de sus clientes.

4. Los Estados miembros notificarán a la Comisión y a los demás Estados miembros los nombres y direcciones de sus respectivos organismos de supervisión designados.

5. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 38, en lo que respecta a la definición de los procedimientos aplicables a las tareas mencionadas en el apartado 2.

6. La Comisión podrá, mediante actos de ejecución, definir las circunstancias, formatos y procedimientos relativos al informe a que se refiere el apartado 3. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 39, apartado 2.

Artículo 14

Asistencia mutua

1. Los organismos de supervisión cooperarán con vistas a intercambiar buenas prácticas y facilitarse mutuamente, en el plazo más breve posible, información pertinente y asistencia mutua con el fin de que las actividades pueden realizarse en forma coherente. La asistencia mutua incluirá, en particular, las solicitudes de información y las medidas de supervisión, tales como las peticiones para que se lleven a cabo inspecciones en relación con las auditorías de la seguridad a que se refieren los artículos 15, 16 y 17.

2. El organismo de supervisión al que se haya dirigido una solicitud de asistencia no podrá negarse a atenderla, salvo si:

(a) no es competente para tramitar la solicitud; o

(b) atender la solicitud sería incompatible con el presente Reglamento.

3. Cuando proceda, los organismos de supervisión podrán llevar a cabo investigaciones conjuntas con participación de personal de los organismos de supervisión de otros Estados miembros.

El organismo de supervisión del Estado miembro en el que vaya a tener lugar la investigación, de conformidad con su propia legislación nacional, podrá transferir tareas de investigación al personal del organismo de supervisión asistido. Estas competencias solo podrán ejercerse bajo la autoridad y en presencia de personal del organismo de supervisión anfitrión. El personal del organismo de supervisión asistido estará sujeto a la legislación nacional del organismo de supervisión anfitrión. El organismo de supervisión anfitrión asumirá la responsabilidad por las acciones del personal del organismo de supervisión asistido.

4. La Comisión podrá, mediante actos de ejecución, especificar los formatos y procedimientos de la asistencia mutua prevista en el presente artículo. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 39, apartado 2.

Artículo 15

Requisitos de seguridad aplicables a los proveedores de servicios de confianza

1. Los proveedores de servicios de confianza establecidos en el territorio de la Unión adoptarán las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que prestan. Habida cuenta del estado de la técnica, dichas medidas garantizarán un nivel de seguridad adecuado al grado de riesgo. En particular, se adoptarán medidas para evitar y reducir al mínimo el impacto de los incidentes de seguridad e informar a los interesados de los efectos negativos de cualquier incidente.

Sin perjuicio del artículo 16, apartado 1, cualquier proveedor de servicios de confianza podrá presentar al organismo de supervisión el informe de una auditoría de seguridad realizada por un organismo independiente reconocido a fin de confirmar que se han tomado las medidas de seguridad apropiadas.

2. Los proveedores de servicios de confianza, sin demoras indebidas y cuando sea posible en un plazo de 24 horas tras tener conocimiento de ellas, notificarán al organismo de supervisión competente, al organismo nacional competente en materia de seguridad de la información y a otros terceros pertinentes, tales como las autoridades de protección de datos, cualquier violación de la seguridad o merma de la integridad que tenga un impacto significativo en el servicio de confianza prestado y en los datos personales correspondientes.

Cuando proceda, en particular si una violación de la seguridad o merma de la integridad afecta a dos o más Estados miembros, el organismo de supervisión de que se trate informará al respecto a los organismos de supervisión de los demás Estados miembros y a la Agencia Europea de Seguridad de las Redes y de la Información (ENISA).

El organismo de supervisión de que se trate podrá informar al público o exigir al proveedor de servicios de confianza que lo haga, en caso de considerar que la divulgación de la violación reviste interés público.

3. El organismo de supervisión facilitará a ENISA y a la Comisión una vez al año un resumen de las notificaciones de violaciones recibidas de los proveedores de servicios de confianza.

4. Para la aplicación de los apartados 1 y 2, el organismo de supervisión competente estará facultado para impartir instrucciones vinculantes a los proveedores de servicios de confianza.

5. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 38, a fin de especificar más detalladamente las medidas mencionadas en el apartado 1.

6. La Comisión podrá, mediante actos de ejecución, definir las circunstancias, formatos y procedimientos, incluidos los plazos, aplicables a efectos de los apartados 1 a 3. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 39, apartado 2.

Artículo 16

Supervisión de los proveedores de servicios de confianza cualificados

1. Los proveedores de servicios de confianza cualificados serán auditados por un organismo independiente reconocido una vez al año para confirmar que tanto ellos como los servicios de confianza cualificados que prestan cumplen los requisitos establecidos en el presente Reglamento y presentarán el correspondiente informe de auditoría de seguridad al organismo de supervisión.

2. Sin perjuicio de lo dispuesto en el apartado 1, el organismo de supervisión podrá en cualquier momento, por propia iniciativa o en respuesta a una petición de la Comisión, auditar a los proveedores de servicios de confianza cualificados para confirmar que tanto ellos como los servicios de confianza cualificados que prestan siguen cumpliendo las condiciones establecidas en el presente Reglamento. El organismo de supervisión informará a las autoridades de protección de datos de los resultados de sus auditorías en caso de resultar infringidas las normas sobre protección de datos personales.

3. El organismo de supervisión estará facultado para impartir instrucciones vinculantes a los proveedores de servicios de confianza cualificados a fin de corregir cualquier incumplimiento de los requisitos que figure en el informe de la auditoría de seguridad.

4. Con referencia al apartado 3, en caso de que el proveedor de servicios de confianza cualificado no corrija dicho incumplimiento en el plazo fijado por el organismo de supervisión, perderá su cualificación y será informado por el organismo de supervisión de que se modificará consiguientemente su estado en las listas de confianza a la que se refiere el artículo 18.

5. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 38, relativos a la especificación de las condiciones en las que se reconocerá al organismo independiente que lleve a cabo la auditoría a que se refieren el apartado 1 del presente artículo, el artículo 15, apartado 1, y el artículo 17, apartado 1.

6. La Comisión podrá, mediante actos de ejecución, definir las circunstancias, formatos y procedimientos aplicables a efectos de los apartados 1, 2 y 4. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 39, apartado 2.

Artículo 17

Inicio de un servicio de confianza cualificado

1. Los proveedores de servicios de confianza cualificados notificarán al organismo de supervisión su intención de iniciar la prestación de un servicio de confianza cualificado y le presentarán un informe de auditoría de la seguridad realizado por un organismo independiente reconocido, según lo previsto en el artículo 16, apartado 1. Los proveedores de servicios de confianza cualificados podrán empezar a prestar el servicio de confianza cualificado después de haber presentado al organismo de supervisión la notificación y el informe de auditoría de la seguridad.

2. Una vez remitidos los documentos correspondientes al organismo de supervisión con arreglo al apartado 1, se incluirá a los proveedores de servicios cualificados en las listas de confianza a que se refiere el artículo 18, indicando que se ha presentado la notificación.

3. El organismo de supervisión verificará la conformidad del proveedor de servicios de confianza cualificado y de los servicios de confianza cualificados que presta con los requisitos del Reglamento.

El organismo de supervisión indicará el estado de cualificación de los proveedores de servicios cualificados y de los servicios de confianza cualificados que presta en las listas de confianza después de que la verificación haya concluido positivamente, a más tardar un mes después de efectuada la notificación de conformidad con el apartado 1.

Si la verificación no ha concluido en el plazo de un mes, el organismo de supervisión informará al proveedor de servicios de confianza cualificado especificando los motivos de la demora y el plazo previsto para concluir la verificación.

4. El organismo del sector público de que se trate no podrá rechazar un servicio de confianza cualificado que haya sido objeto de la notificación a que se refiere el apartado 1 para la realización de un procedimiento o trámite administrativo por el hecho de no figurar en las listas a que se refiere el apartado 3.

5. La Comisión podrá, mediante actos de ejecución, definir las circunstancias, formatos y procedimientos a efectos de los apartados 1, 2 y 3. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 39, apartado 2.

Artículo 18

Listas de confianza

1. Cada Estado miembro establecerá, mantendrá y publicará listas de confianza con información relativa a los proveedores de servicios de confianza con respecto a los cuales sea competente, junto con la información relacionada con los servicios de confianza cualificados prestados por ellos.

2. Los Estados miembros establecerán, mantendrán y publicarán, de manera segura, las listas de confianza firmadas o selladas electrónicamente previstas en el apartado 1 en una forma apropiada para el tratamiento automático.

3. Los Estados miembros notificarán a la Comisión, sin retrasos indebidos, información sobre el organismo responsable del establecimiento, mantenimiento y publicación de las listas de confianza nacionales, y detalles relativos al lugar en que se publican dichas listas, los certificados utilizados para firmar o sellar las listas de confianza y cualquier modificación de los mismos.

4. La Comisión pondrá a disposición del público, a través de un canal seguro, la información a que se refiere el apartado 3 en una forma firmada o sellada electrónicamente apropiada para el tratamiento automático.

5. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 38, en lo que respecta a la definición de la información a que se refiere el apartado 1.

6. La Comisión podrá, mediante actos de ejecución, definir las especificaciones técnicas y formatos de las listas de confianza, aplicables a efectos de los apartados 1 a 4. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 39, apartado 2.

Artículo 19

Requisitos para los proveedores de servicios de confianza cualificados

1. Al expedir un certificado cualificado, un proveedor de servicios de confianza cualificado verificará, por los medios apropiados y de acuerdo con el Derecho nacional, la identidad y, si procede, cualquier atributo específico de la persona física o jurídica a la que se expide un certificado cualificado.

Esta información será verificada por el proveedor de servicios cualificado o por un tercero autorizado que actúe bajo la responsabilidad del proveedor de servicios cualificado:

(a) en virtud del aspecto exterior de la persona física o de un representante autorizado de la persona jurídica, o

(b) a distancia, utilizando medios de identificación electrónica dentro de un régimen notificado expedidos de conformidad con la letra a).

2. Los proveedores de servicios de confianza cualificados que prestan servicios de confianza cualificados:

(a) contarán con personal que posea los conocimientos especializados, la experiencia y las cualificaciones necesarios y aplique procedimientos administrativos y de gestión que correspondan a normas europeas o internacionales y hayan recibido una formación adecuada sobre normas de seguridad y de protección de datos personales;

(b) asumirán el riesgo de la responsabilidad por daños y perjuicios contando con recursos financieros suficientes o con pólizas de seguros de responsabilidad adecuadas;

(c) antes de entrar en una relación contractual, informarán a cualquier persona que desee utilizar un servicio de confianza cualificado acerca de las condiciones precisas relativas a la utilización de dicho servicio;

(d) utilizarán sistemas y productos dignos de confianza que estén protegidos contra toda alteración y que garanticen la seguridad y la fiabilidad técnicas de los procesos que sustentan;

(e) utilizarán sistemas dignos de confianza para almacenar los datos que se les faciliten de forma verificable, de modo que:

– estén a disposición del público para su consulta solo cuando se haya obtenido el consentimiento de la persona a la que se han expedido los datos,

– solo personas autorizadas puedan hacer anotaciones y modificaciones,

– pueda comprobarse la autenticidad de la información;

(f) tomarán medidas contra la falsificación y el robo de datos;

(g) registrarán durante un período de tiempo apropiado toda la información pertinente referente a los datos expedidos y recibidos por el proveedor de servicios de confianza cualificado, en particular al objeto de que sirvan de prueba en los procedimientos legales; esta actividad de registro podrá realizarse por medios electrónicos;

(h) contarán con un plan de cesación actualizado para garantizar la continuidad del servicio, de conformidad con las disposiciones del organismo de supervisión con arreglo al artículo 13, apartado 2, letra c);

(i) garantizarán un procesamiento lícito de los datos personales de conformidad con el artículo 11.

3. Los proveedores de servicios de confianza cualificados que expidan certificados cualificados registrarán en su base de datos de certificados la revocación del certificado en un plazo de diez minutos después de haber surtido efecto la revocación.

4. Con respecto a lo dispuesto en el apartado 3, los proveedores de servicios de confianza cualificados que expidan certificados cualificados proporcionará a cualquier parte usuaria información sobre el estado de validez o revocación de los certificados cualificados expedidos por ellos. Esta información deberá estar disponible en cualquier momento al menos por cada certificado en una forma automatizada que sea fiable, gratuita y eficiente.

5. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas para sistemas y productos dignos de confianza. Se presumirá el cumplimiento de los requisitos establecidos en el artículo 19 cuando los sistemas y productos dignos de confianza cumplan dichas normas. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 39, apartado 2. La Comisión publicará estos actos en el *Diario Oficial de la Unión Europea*.

Sección 3

Firma electrónica

Artículo 20

Efectos jurídicos y aceptación de las firmas electrónicas

1. No se denegarán los efectos jurídicos y la admisibilidad como prueba en procedimientos judiciales de una firma electrónica por el mero hecho de ser una firma electrónica.

2. Una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita.

3. Las firmas electrónicas cualificadas serán reconocidas y aceptadas en todos los Estados miembros.

4. Cuando baste una firma electrónica con un nivel de garantía de la seguridad inferior al de la firma electrónica cualificada, en particular para un Estado miembro en relación con el acceso a un servicio en línea ofrecido por un organismo del sector público sobre la base de una

evaluación adecuada de los riesgos inherentes a ese servicio, deberán reconocerse y aceptarse todas las firmas electrónicas cuyo nivel de garantía de la seguridad sea por lo menos el mismo.

5. Los Estados miembros no exigirán para el acceso transfronterizo a un servicio en línea ofrecido por un organismo del sector público una firma electrónica cuyo nivel de garantía de la seguridad sea superior al de una firma electrónica cualificada.

6. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 38, en lo que respecta a la definición de los distintos niveles de seguridad de las firmas electrónicas a que se refiere el apartado 4.

7. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a los niveles de seguridad de la firma electrónica. Se presumirá el cumplimiento del nivel de seguridad definido en un acto delegado adoptado con arreglo al apartado 6 cuando una firma electrónica se ajuste a dichas normas. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 39, apartado 2. La Comisión publicará estos actos en el *Diario Oficial de la Unión Europea*.

Artículo 21

Certificados cualificados de firma electrónica

1. Los certificados cualificados de firma electrónica cumplirán los requisitos establecidos en el anexo I.

2. Los certificados cualificados de firma electrónica no estarán sometidos a ningún requisito obligatorio que exceda de los requisitos establecidos en el anexo I.

3. Si un certificado cualificado de firma electrónica ha sido revocado después de su activación inicial, perderá su validez y no podrá en ninguna circunstancia recuperar su estado renovando su validez.

4. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 38, a fin de especificar más detalladamente los requisitos establecidos en el anexo I.

5. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a los certificados cualificados de firma electrónica. Se presumirá el cumplimiento de los requisitos establecidos en el anexo I cuando un certificado cualificado de firma electrónica se ajuste a dichas normas. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 39, apartado 2. La Comisión publicará estos actos en el *Diario Oficial de la Unión Europea*.

Artículo 22

Requisitos de los dispositivos de creación de firmas electrónicas cualificados

1. Los dispositivos de creación de firmas electrónicas cualificados cumplirán los requisitos establecidos en el anexo II.

2. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a los dispositivos de creación de firmas electrónicas cualificados. Se presumirá el cumplimiento de los requisitos establecidos en el anexo II cuando un dispositivo de creación de firmas electrónicas cualificado se ajuste a dichas normas. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 39, apartado 2. La Comisión publicará estos actos en el *Diario Oficial de la Unión Europea*.

Artículo 23

Certificación de los dispositivos de creación de firmas electrónicas cualificados

1. Los dispositivos de creación de firmas electrónicas cualificados podrán ser certificados por los organismos públicos o privados adecuados designados por los Estados miembros, siempre que hayan sido sometidos a un proceso de evaluación de la seguridad llevado a cabo de conformidad con las normas para la evaluación de la seguridad de los productos de tecnología de la información incluidos en una lista que establecerá la Comisión por medio de actos de ejecución. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 39, apartado 2. La Comisión publicará estos actos en el *Diario Oficial de la Unión Europea*.

2. Los Estados miembros notificarán a la Comisión y a los demás Estados miembros los nombres y direcciones de los organismos públicos o privados designados por ellos a que se refiere el apartado 1.

3. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 38, en lo que respecta al establecimiento de criterios específicos que deben satisfacer los organismos designados a que se refiere el apartado 1.

Artículo 24

Publicación de una lista de dispositivos de creación de firmas electrónicas cualificados certificados

1. Los Estados miembros comunicarán a la Comisión, sin retrasos indebidos, información sobre los dispositivos de creación de firmas electrónicas cualificados que hayan sido certificados por los organismos a que se refiere el artículo 23. También notificarán a la Comisión, sin retrasos indebidos, información sobre los dispositivos de creación de firmas electrónicas que hayan dejado de estar certificados.

2. Sobre la base de la información recibida, la Comisión establecerá, publicará y mantendrá una lista de dispositivos de creación de firmas electrónicas cualificados certificados.

3. La Comisión podrá, mediante actos de ejecución, definir las circunstancias, formatos y procedimientos aplicables a efectos del apartado 1. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 39, apartado 2.

Artículo 25

Requisitos de la validación de las firmas electrónicas cualificadas

1. Una firma electrónica cualificada se considerará válida siempre que pueda establecerse con un elevado nivel de certidumbre que, en el momento de la firma:

(a) el certificado que respalda la firma es un certificado cualificado de firma electrónica que se ajusta a lo dispuesto en el anexo I;

(b) el certificado cualificado requerido es auténtico y válido;

(c) los datos de validación de la firma corresponden a los datos proporcionados a la parte usuaria;

(d) el conjunto de datos que representa inequívocamente al firmante se facilita correctamente a la parte usuaria;

(e) en caso de que se utilice un seudónimo, la utilización del mismo se indica claramente a la parte usuaria;

(f) la firma electrónica se creó mediante un dispositivo de creación de firmas electrónicas cualificado;

(g) la integridad de los datos firmados no se ha visto comprometida;

(h) se han cumplido los requisitos previstos en el artículo 3, punto 7;

(i) el sistema utilizado para validar la firma ofrece a la parte usuaria el resultado correcto del proceso de validación y le permite detectar cualquier problema que afecte a la seguridad.

2. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 38, a fin de especificar más detalladamente los requisitos establecidos en el apartado 1.

3. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a la validación de las firmas electrónicas cualificadas. Se presumirá el cumplimiento de los requisitos establecidos en el apartado 1 cuando la validación de una firma electrónica cualificada se ajuste a dichas normas. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 39, apartado 2. La Comisión publicará estos actos en el *Diario Oficial de la Unión Europea*.

Artículo 26

Servicio de validación cualificado para las firmas electrónicas cualificadas

1. Prestará un servicio de validación cualificado para las firmas electrónicas cualificadas el proveedor de servicios de confianza cualificado que:

(a) realice la validación de conformidad con el artículo 25, apartado 1, y

(b) permita que las partes usuarias reciban el resultado del proceso de validación de una manera automatizada que sea fiable, eficiente y lleve la firma electrónica avanzada o el sello electrónico avanzado del proveedor del servicios de validación cualificado.

2. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas al servicio de validación cualificado a que se refiere el apartado 1. Se presumirá el cumplimiento de los requisitos establecidos en el apartado 1, letra b), cuando el servicio de validación de firmas electrónicas cualificadas se ajuste a dichas normas. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 39, apartado 2. La Comisión publicará estos actos en el *Diario Oficial de la Unión Europea*.

Artículo 27

Conservación de las firmas electrónicas cualificadas

1. Prestará un servicio de conservación de firmas electrónicas cualificado el proveedor de servicios de confianza cualificado que utilice procedimientos y tecnologías capaces de ampliar la fiabilidad de los datos de validación de la firma electrónica cualificada más allá del período de validez tecnológico.

2. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 38, a fin de especificar más detalladamente los requisitos establecidos en el apartado 1.

3. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a la conservación de las firmas electrónicas cualificadas. Se presumirá el cumplimiento de los requisitos establecidos en el apartado 1 cuando los mecanismos de conservación de las firmas electrónicas cualificadas se ajusten a dichas normas. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 39, apartado 2. La Comisión publicará estos actos en el *Diario Oficial de la Unión Europea*.

Sección 4

Sellos electrónicos

Artículo 28

Efectos jurídicos del sello electrónico

1. No se denegarán los efectos jurídicos y la admisibilidad como prueba en procedimientos judiciales de un sello electrónico por el mero hecho de ser un sello electrónico.

2. Un sello electrónico cualificado disfrutará de la presunción legal de garantizar el origen y la integridad de los datos a los que está vinculado.

3. Un sello electrónico cualificado será reconocido y aceptado en todos los Estados miembros.

4. Cuando baste un sello electrónico con un nivel de garantía de la seguridad inferior al del sello electrónico cualificado, en particular para un Estado miembro en relación con el acceso a un servicio en línea ofrecido por un organismo del sector público sobre la base de una evaluación adecuada de los riesgos inherentes a ese servicio, deberán aceptarse todos los sellos electrónicos cuyo nivel de garantía de la seguridad sea al menos equivalente.

5. Los Estados miembros no exigirán para el acceso a un servicio en línea ofrecido por un organismo del sector público un sello electrónico cuyo nivel de garantía de la seguridad sea superior al de un sello electrónico cualificado.

6. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 38, en lo que respecta a la definición de los distintos niveles de garantía de la seguridad de los sellos electrónicos a que se refiere el apartado 4.

7. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a los niveles de garantía de la seguridad de los sellos electrónicos. Se presumirá el cumplimiento del nivel de garantía de la seguridad definido en un acto delegado adoptado con arreglo al apartado 6 cuando un sello electrónico se ajuste a dichas normas. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 39, apartado 2. La Comisión publicará estos actos en el *Diario Oficial de la Unión Europea*.

Artículo 29

Requisitos de los certificados cualificados de sello electrónico

1. Los certificados cualificados de sello electrónico cumplirán los requisitos establecidos en el anexo III.

2. Los certificados cualificados de sello electrónico no estarán sometidos a ningún requisito obligatorio que exceda de los requisitos establecidos en el anexo III.

3. Si un certificado cualificado de sello electrónico ha sido revocado después de su activación inicial, perderá su validez y no podrá en ninguna circunstancia recuperar su estado renovando su validez.

4. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 38, a fin de especificar más detalladamente los requisitos establecidos en el anexo III.

5. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a los certificados cualificados de sello electrónico. Se presumirá el cumplimiento de los requisitos establecidos en el anexo III cuando un certificado cualificado de sello electrónico se ajuste a dichas normas. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 39, apartado 2. La Comisión publicará estos actos en el *Diario Oficial de la Unión Europea*.

Artículo 30

Dispositivos de creación de sellos electrónicos cualificados

1. El artículo 22 se aplicará *mutatis mutandis* a los requisitos de los dispositivos de creación de sellos electrónicos cualificados.

2. El artículo 23 se aplicará *mutatis mutandis* a la certificación de los dispositivos de creación de sellos electrónicos cualificados.

3. El artículo 24 se aplicará *mutatis mutandis* a la publicación de una lista de dispositivos de creación de sellos electrónicos cualificados certificados.

Artículo 31

Validación y conservación de los sellos electrónicos cualificados

Los artículos 25, 26 y 27 se aplicarán *mutatis mutandis* a la validación y conservación de los sellos electrónicos cualificados.

Sección 5

Marca de tiempo electrónica

Artículo 32

Efecto jurídico de las marcas de tiempo electrónicas

1. No se denegarán los efectos jurídicos y la admisibilidad como prueba en procedimientos judiciales de una marca de tiempo electrónica por el mero hecho de estar en forma electrónica.

2. Las marcas de tiempo electrónicas cualificadas disfrutarán de una presunción legal de garantizar la fecha y hora que indican y la integridad de los datos a los que esa fecha y hora están vinculados.

3. Una marca de tiempo electrónica cualificada será reconocida y aceptada en todos los Estados miembros.

Artículo 33

Requisitos de las marcas de tiempo electrónicas cualificadas

1. Una marca de tiempo electrónica cualificada cumplirá los requisitos siguientes:

(a) estar vinculada con exactitud al Tiempo Universal Coordinado (UTC) de forma que se elimine cualquier posibilidad de modificar los datos sin que se detecte;

(b) estar basada en una fuente de información temporal exacta;

(c) haber sido expedida por un proveedor de servicios de confianza cualificado;

(d) haber sido firmada mediante el uso de una firma electrónica avanzada o de un sello electrónico avanzado del proveedor de servicios de confianza cualificado o por cualquier método equivalente.

2. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a la vinculación exacta de la fecha y hora con los datos y una fuente de información temporal exacta. Se presumirá el cumplimiento de los requisitos establecidos en el apartado 1 cuando una vinculación exacta de la fecha y hora con los datos y una fuente de

información temporal exacta se ajuste a dichas normas. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 39, apartado 2. La Comisión publicará estos actos en el *Diario Oficial de la Unión Europea*.

Sección 6

Documentos electrónicos

Artículo 34

Efectos jurídicos y aceptación de los documentos electrónicos

1. Los documentos electrónicos se considerarán equivalente a los documentos en papel y admisibles como prueba en procedimientos judiciales, tomando en consideración su nivel de garantía de autenticidad e integridad.

2. Cualquier documento que lleve una firma electrónica cualificada o un sello electrónico cualificado de la persona competente para expedir el documento en cuestión disfrutará de la presunción legal de su autenticidad e integridad siempre que el documento no contenga ninguna característica dinámica capaz de modificarlo automáticamente.

3. Cuando se exija un documento original o una copia certificada del mismo para la prestación de un servicio en línea ofrecido por un organismo del sector público, deberán aceptarse en otros Estados miembros sin requisitos adicionales por lo menos los documentos electrónicos expedidos por las personas competentes para la expedición de los documentos correspondientes y que se consideren originales o copias certificadas de conformidad con la legislación nacional del Estado miembro que los expide.

4. La Comisión podrá, mediante actos de ejecución, definir los formatos de las firmas o sellos electrónicos que serán aceptados cuando un Estado miembro exija un documento firmado o sellado para la prestación de un servicio en línea ofrecido por un organismo del sector público a que se refiere el apartado 2. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 39, apartado 2.

Sección 7

Servicios de entrega electrónica cualificados

Artículo 35

Efecto jurídico de un servicio de entrega electrónica

1. Los datos enviados o recibidos mediante un servicio de entrega electrónica serán admisibles como prueba en procedimientos judiciales por lo que respecta a la integridad de los datos y la certeza de la fecha y hora en que los datos fueron enviados a un determinado destinatario o recibidos por él.

2. Los datos enviados o recibidos mediante un servicio de entrega electrónica cualificado disfrutarán de la presunción legal de la integridad de los datos y la exactitud de la fecha y hora de envío o recepción de los datos que indica el sistema de entrega electrónica cualificado.

3. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 38, relativos a la especificación de mecanismos para el envío o la recepción de datos mediante el uso de servicios de entrega electrónica, que se emplearán a fin de fomentar la interoperabilidad entre los servicios de entrega electrónica.

Artículo 36

Requisitos de los servicios de entrega electrónica cualificados

1. Los servicios de entrega electrónica cualificados cumplirán los requisitos siguientes:

(a) ser prestados por uno o más proveedores de servicios de confianza cualificados;

(b) permitir la identificación inequívoca del expedidor y, en su caso, del destinatario;

(c) estar protegido el proceso de envío o recepción de datos por una firma electrónica avanzada o un sello electrónico avanzado de un proveedor de servicios de confianza cualificado de tal forma que se impida la posibilidad de que se modifiquen los datos sin que se detecte;

(d) indicar claramente al emisor y al destinatario de los datos cualquier modificación de los datos necesarios a efectos del envío o recepción de los datos;

(e) indicar mediante una marca de tiempo electrónica cualificada la fecha de envío, recepción y eventual modificación de los datos;

(f) en caso de que los datos se transfieren entre dos o más proveedores de servicios de confianza cualificados, se aplicarán los requisitos establecidos en las letras a) a e) a todos los proveedores de servicio de confianza cualificados.

2. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a los procesos de envío y recepción de datos. Se presumirá el cumplimiento de los requisitos establecidos en el apartado 1 cuando el proceso de envío y recepción de datos se ajuste a dichas normas. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 39, apartado 2. La Comisión publicará estos actos en el *Diario Oficial de la Unión Europea*.

Sección 8

Autenticación de sitios web

Artículo 37

Requisitos para los certificados cualificados de autenticación de sitios web

1. Los certificados cualificados de autenticación de sitios web cumplirán los requisitos establecidos en el anexo IV.

2. Los certificados cualificados de autenticación de sitios web serán reconocidos y aceptados en todos los Estados miembros.

3. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 38, a fin de especificar más detalladamente los requisitos establecidos en el anexo IV.

4. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a los certificados cualificados de autenticación de sitios web. Se presumirá el cumplimiento de los requisitos establecidos en el anexo IV cuando un certificado cualificado de autenticación de sitios web se ajuste a dichas normas. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 39, apartado 2. La Comisión publicará estos actos en el *Diario Oficial de la Unión Europea*.

CAPÍTULO IV

ACTOS DELEGADOS

Artículo 38

Ejercicio de la delegación

1. Se faculta a la Comisión para adoptar actos delegados en las condiciones establecidas en el presente artículo.

2. Los poderes para adoptar los actos delegados a que se refieren el artículo 8, apartado 3, el artículo 13, apartado 5, el artículo 15, apartado 5, el artículo 16, apartado 5, el artículo 18, apartado 5, el artículo 20, apartado 6, el artículo 21, apartado 4, el artículo 23, apartado 3, el artículo 25, apartado 2, el artículo 27, apartado 2, el artículo 28, apartado 6, el artículo 29, apartado 4, el artículo 30, apartado 2, el artículo 31, el artículo 35, apartado 3, y el artículo 37, apartado 3, se otorgan a la Comisión por tiempo indefinido a partir de la fecha de entrada en vigor del presente Reglamento.

3. La delegación de poderes a que se refieren el artículo 8, apartado 3, el artículo 13, apartado 5, el artículo 15, apartado 5, el artículo 16, apartado 5, el artículo 18, apartado 5, el artículo 20, apartado 6, el artículo 21, apartado 4, el artículo 23, apartado 3, el artículo 25, apartado 2, el artículo 27, apartado 2, el artículo 28, apartado 6, el artículo 29, apartado 4, el artículo 30, apartado 2, el artículo 31, el artículo 35, apartado 3, y el artículo 37, apartado 3, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto al día siguiente de su publicación en el *Diario Oficial de la Unión Europea* o en una fecha posterior indicada en la misma. No afectará a la validez de los actos delegados que ya estén en vigor.

4. En cuanto la Comisión adopte un acto delegado, lo notificará simultáneamente al Parlamento Europeo y al Consejo.

5. Un acto delegado adoptado de conformidad con el artículo 8, apartado 3, el artículo 13, apartado 5, el artículo 15, apartado 5, el artículo 16, apartado 5, el artículo 18, apartado 5, el artículo 20, apartado 6, el artículo 21, apartado 4, el artículo 23, apartado 3, el artículo 25, apartado 2, el artículo 27, apartado 2, el artículo 28, apartado 6, el artículo 29, apartado 4, el artículo 30, apartado 2, el artículo 31, el artículo 35, apartado 3, y el artículo 37, apartado 3, únicamente entrará en vigor si el Parlamento Europeo o el Consejo no formulan objeciones en un plazo de dos meses desde la notificación del acto al Parlamento Europeo y al Consejo, o si tanto el Parlamento Europeo como el Consejo informan a la Comisión de que no tienen la

intención de formular objeciones. El plazo se prorrogará dos meses a iniciativa del Parlamento Europeo o del Consejo.

CAPÍTULO V

ACTOS DE EJECUCIÓN

Artículo 39

Procedimiento de comité

1. La Comisión estará asistida por un Comité. El comité será conforme a lo dispuesto en el Reglamento (UE) nº 182/2011.

2. En los casos en que se haga referencia al presente apartado, será de aplicación el artículo 5 del Reglamento (UE) nº 182/2011.

CAPÍTULO VI

DISPOSICIONES FINALES

Artículo 40

Informes

La Comisión informará al Parlamento Europeo y al Consejo sobre la aplicación del presente Reglamento. El primer informe se presentará a más tardar cuatro años después de la entrada en vigor del presente Reglamento. Los siguientes informes se presentarán cada cuatro años.

Artículo 41

Derogación

1. Queda derogada la Directiva 1999/93/CE.

2. Las referencias a la Directiva derogada se entenderán hechas al presente Reglamento.

3. Los dispositivos seguros de creación de firma cuya conformidad se haya determinado con arreglo a lo dispuesto en el artículo 3, apartado 4, de la Directiva 1999/93/CE se considerarán dispositivos de creación de firma cualificados con arreglo al presente Reglamento.

4. Los certificados reconocidos expedidos con arreglo a la Directiva 1999/93/CE se considerarán certificados cualificados de firma electrónica en virtud del presente Reglamento hasta su expiración, pero solo durante un plazo máximo de cinco años a partir de la entrada en vigor del presente Reglamento.

Artículo 42

Entrada en vigor

El presente Reglamento entrará en vigor el vigésimo día siguiente al de su publicación en el *Diario Oficial de la Unión Europea*.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*El Presidente*

ANEXO I

Requisitos de los certificados cualificados de firma electrónica

Los certificados cualificados de firma electrónica contendrán:

(a) una indicación, al menos en un formato adecuado para el procesamiento automático, de que el certificado ha sido expedido como certificado cualificado de firma electrónica;

(b) un conjunto de datos que represente inequívocamente al proveedor de servicios de confianza cualificado que expide los certificados cualificados, incluyendo como mínimo el Estado miembro en el que dicho proveedor está establecido y

- para personas jurídicas: el nombre y el número de registro según consten en los registros oficiales,
- para personas físicas: el nombre de la persona;

(c) un conjunto de datos que represente inequívocamente al firmante al que se ha expedido el certificado, incluidos al menos su nombre o un seudónimo, que se identificará como tal;

(d) datos de validación de la firma electrónica que correspondan a los datos de creación de la firma electrónica;

(e) los datos relativos al inicio y final del período de validez del certificado;

(f) el código de identidad del certificado, que debe ser único para el proveedor de servicios de confianza cualificado;

(g) la firma electrónica avanzada o el sello electrónico avanzado del proveedor de servicios de confianza expedidor;

(h) el lugar en que está disponible gratuitamente el certificado que respalda la firma electrónica avanzada o el sello electrónico avanzado a que se hace referencia en la letra g);

(i) la localización de los servicios de estado de validez del certificado que pueden utilizarse para averiguar el estado de validez del certificado cualificado;

(j) cuando los datos de creación de la firma electrónica relacionados con los datos de validación de la firma electrónica se encuentren en un dispositivo de creación de firmas electrónicas cualificado, una indicación adecuada de esto, al menos en una forma apta para el procesamiento automático.

ANEXO II

Requisitos de los dispositivos de creación de firmas cualificados

1. Los dispositivos de creación de firma cualificados garantizarán como mínimo, por medios técnicos y de procedimiento adecuados, que:

(a) esté garantizado el secreto de los datos de creación de la firma electrónica utilizados para la generación de firmas electrónicas;

(b) los datos de creación de la firma electrónica utilizados para la generación de una firma electrónica solo aparezcan una vez;

(c) exista la seguridad razonable de que los datos de creación de la firma electrónica utilizados para la generación de una firma electrónica no pueden ser hallados por deducción y de que la firma está protegida contra la falsificación mediante la tecnología disponible en el momento;

(d) los datos de creación de la firma electrónica utilizados para la generación de una firma electrónica puedan ser protegidos por el firmante legítimo de forma fiable frente a su utilización por otros.

2. Los dispositivos de creación de firmas electrónicas cualificados no alterarán los datos que deben firmarse ni impedirán que dichos datos se muestren al firmante antes de firmar.

3. La generación o la gestión de los datos de creación de la firma electrónica en nombre del firmante correrán a cargo de un proveedor de servicios de confianza cualificado.

4. Los proveedores de servicios de confianza cualificados que gestionen los datos de creación de la firma electrónica en nombre del firmante podrán efectuar una copia de seguridad de los datos de creación de la firma electrónica siempre que se cumplan los siguientes requisitos:

(a) la seguridad de los conjuntos de datos copiados es del mismo nivel que para los conjuntos de datos originales;

(b) el número de conjuntos de datos copiados no supera el mínimo necesario para garantizar la continuidad del servicio.

ANEXO III

Requisitos de los certificados cualificados de sello electrónico

Los certificados cualificados de sello electrónico contendrán:

(a) una indicación, al menos en un formato adecuado para el procesamiento automático, de que el certificado ha sido expedido como certificado cualificado de sello electrónico;

(b) un conjunto de datos que represente inequívocamente al proveedor de servicios de confianza cualificado que expide los certificados cualificados, incluyendo como mínimo el Estado miembro en el que dicho proveedor está establecido y

- para personas jurídicas: el nombre y el número de registro según consten en los registros oficiales,
- para personas físicas: el nombre de la persona;

(c) un conjunto de datos que represente inequívocamente a la persona jurídica a la que se haya expedido el certificado, incluyendo al menos el nombre y el número de registro, tal como se recojan en los registros oficiales;

(d) los datos de validación del sello electrónico que correspondan a los datos de creación del sello electrónico;

(e) los datos relativos al inicio y final del período de validez del certificado;

(f) el código de identidad del certificado, que debe ser único para el proveedor de servicios de confianza cualificado;

(g) la firma electrónica avanzada o el sello electrónico avanzado del proveedor de servicios de confianza expedidor;

(h) el lugar en que está disponible gratuitamente el certificado que respalda la firma electrónica avanzada o el sello electrónico avanzado a que se hace referencia en la letra g);

(i) la localización de los servicios de estado de validez del certificado que pueden utilizarse para averiguar el estado de validez del certificado cualificado;

(j) cuando los datos de creación del sello electrónico relacionados con los datos de validación del sello electrónico se encuentren en un dispositivo de creación de sellos electrónicos cualificado, una indicación adecuada de esto, al menos en una forma apta para el procesamiento automático.

ANEXO IV

Requisitos de los certificados cualificados de autenticación de sitios web

Los certificados cualificados de autenticación de sitios web contendrán:

(a) una indicación, al menos en un formato adecuado para el procesamiento automático, de que el certificado ha sido expedido como certificado cualificado de autenticación de sitios web;

(b) un conjunto de datos que represente inequívocamente al proveedor de servicios de confianza cualificado que expide los certificados cualificados, incluyendo como mínimo el Estado miembro en el que dicho proveedor está establecido y

- para personas jurídicas: el nombre y el número de registro según consten en los registros oficiales,
- para personas físicas: el nombre de la persona;

(c) un conjunto de datos que represente inequívocamente a la persona jurídica a la que se haya expedido el certificado, incluyendo al menos el nombre y el número de registro, tal como se recojan en los registros oficiales;

(d) elementos de la dirección, incluida al menos la ciudad y el Estado miembro, de la persona jurídica a quien se expida el certificado, según figure en los registros oficiales;

(e) el nombre o los nombres de dominio explotados por la persona a la que se expida el certificado;

(f) los datos relativos al inicio y final del período de validez del certificado;

(g) el código de identidad del certificado, que debe ser único para el proveedor de servicios de confianza cualificado;

(h) la firma electrónica avanzada o el sello electrónico avanzado del proveedor de servicios de confianza expedidor;

(i) el lugar en que está disponible gratuitamente el certificado que respalda la firma electrónica avanzada o el sello electrónico avanzado a que se hace referencia en la letra h);

(j) la localización de los servicios de estado de validez del certificado que pueden utilizarse para averiguar el estado de validez del certificado cualificado.

FICHA FINANCIERA LEGISLATIVA

1. MARCO DE LA PROPUESTA/INICIATIVA

En la presente ficha financiera se detallan los requisitos en cuanto a gastos administrativos que comporta la aplicación de la propuesta de Reglamento relativo a *la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior*.

Tras el procedimiento legislativo y el debate para la adopción del Reglamento propuesto por el Parlamento Europeo y el Consejo, la Comisión precisará de doce ETC para preparar los actos delegados y de ejecución conexos, a fin de garantizar la disponibilidad de normas organizativas y técnicas, gestionar la información notificada por los Estados miembros, y en particular mantener la información relacionada con las listas de confianza, sensibilizar a las partes interesadas –en particular los ciudadanos y las PYME– acerca de las ventajas de la utilización de la identificación, autentificación y firma electrónicas y los servicios de confianza conexos (eIAS) e iniciar conversaciones con terceros países con vistas a conseguir la interoperabilidad a nivel mundial en este ámbito.

1.1. Denominación de la propuesta/iniciativa

Propuesta de la Comisión acerca de un Reglamento relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior

1.2. Ámbito(s) político(s) afectado(s) en la estructura GPA/PPA[25]

09 SOCIEDAD DE LA INFORMACIÓN

1.3. Naturaleza de la propuesta/iniciativa

☐ La propuesta/iniciativa se refiere a **una acción nueva**

☐ La propuesta/iniciativa se refiere a **una acción nueva a raíz de un proyecto piloto / una acción preparatoria**[26]

☐ La propuesta/iniciativa se refiere a **la prolongación de una acción existente**

☑ La propuesta/iniciativa se refiere a **una acción reorientada hacia una nueva acción**

1.4. Objetivos

1.4.1. Objetivo(s) estratégico(s) plurianual(es) de la Comisión contemplado(s) en la propuesta/iniciativa

Los objetivos generales de la propuesta son los de las políticas generales de la UE en las que se enmarca, tales como la Estrategia EU 2020. Esta estrategia aspira a

[25] GPA: gestión por actividades. PPA: presupuestación por actividades.

[26] Tal como se contempla en el artículo 49, apartado 6, letra a) o b), del Reglamento financiero.

conseguir que Europa «se convierta en una economía inteligente, sostenible e integradora que disfrute de altos niveles de empleo, de productividad y de cohesión social».

1.4.2. Objetivo(s) específico(s) y actividad(es) GPA/PPA afectada(s)

Potenciar la confianza en las transacciones electrónicas paneuropeas y garantizar el reconocimiento jurídico transfronterizo de la identificación, la autentificación y la firma electrónicas y los servicios de confianza conexos, así como un elevado nivel de protección de los datos y de capacitación de los usuarios en el mercado único (véase la Agenda Digital para Europa, acciones clave 3 y 16).

Actividad(es) GPA/PPA afectada(s)

09 02 - Marco regulador de la Agenda Digital para Europa

1.4.3. Resultado(s) e incidencia esperados

Especifíquense los efectos que la propuesta/iniciativa debería tener sobre los beneficiarios / la población destinataria.

Establecer un entorno normativo claro para los servicios eIAS que impulse la comodidad y confianza de los usuarios en el mundo digital.

1.4.4. Indicadores de resultados e incidencia

Especifíquense los indicadores que permiten realizar el seguimiento de la ejecución de la propuesta/iniciativa.

1. Existencia de proveedores eIAS con actividades en varios Estados miembros de la UE.

2. Grado en que los dispositivos resultan interoperables (por ejemplo, los lectores de tarjetas inteligentes) entre sectores y países.

3. Uso de eIAS por todas las categorías de población.

4. Medida en que utilizan eIAS los usuarios finales para las transacciones nacionales e internacionales (transfronterizas).

5. Grado de armonización en los Estados miembros de la legislación sobre eIAS.

6. Sistemas de identificación electrónica notificados a la Comisión.

7. Servicios accesibles con medios de identificación electrónica notificados en el sector público (p. ej., administración, sanidad, justicia, contratación pública).

8. Servicios accesibles con medios de identificación electrónica notificados en el sector privado (p. ej., banca, comercio, apuestas, acceso a sitios web, servicios de Internet segura).

1.5. Justificación de la propuesta/iniciativa

1.5.1. Necesidad(es) que deben satisfacerse a corto o largo plazo

Las divergencias en la aplicación en cada país de la Directiva sobre la firma electrónica, debidas a diferente interpretación por parte de los Estados miembros, han

creado problemas de interoperabilidad transfronteriza y, por ende, segmentado la situación en la UE y distorsionado el mercado interior. Esta situación va acompañada de una falta de confianza en los sistemas electrónicos que impide que los ciudadanos europeos puedan beneficiarse en el mundo digital del mismo tipo de servicios que en el mundo físico.

1.5.2. Valor añadido de la intervención de la Unión Europea

La acción a nivel de la UE produciría unos beneficios indudables en comparación con la acción a nivel de los Estados miembros. La experiencia ha demostrado ciertamente que las medidas nacionales no solo resultan insuficientes para hacer posibles las transacciones electrónicas a través de las fronteras, sino que, por el contrario, han creado obstáculos a la interoperabilidad de las firmas electrónicas en la UE y están teniendo actualmente el mismo efecto en relación con la identificación y la autenticación electrónicas y los servicios de confianza conexos.

1.5.3. Principales conclusiones extraídas de experiencias similares anteriores

La propuesta se basa en la experiencia adquirida con la Directiva sobre la firma electrónica y los problemas derivados de la transposición y aplicación fragmentadas de dicha Directiva, que han impedido que alcance sus objetivos.

1.5.4. Compatibilidad y posibles sinergias con otros instrumentos pertinentes

Se hace referencia a la Directiva sobre la firma electrónica en varias otras iniciativas de la UE creadas para eliminar los problemas de interoperabilidad y de aceptación y reconocimiento transfronterizos relacionados con determinados tipos de interacciones electrónicas, por ejemplo la Directiva sobre los servicios, las Directivas sobre contratación pública, la Directiva sobre el IVA revisada (facturación electrónica) y el Reglamento sobre la iniciativa ciudadana europea.

Además, la propuesta de Reglamento aportará un marco jurídico favorable a la amplia adopción de los proyectos piloto a gran escala que se han puesto en marcha a nivel de la UE para apoyar el desarrollo de medios de comunicación electrónica interoperables y fiables (entre ellos SPOCS, que respalda la aplicación de la Directiva sobre los servicios; STORK, que apoya el desarrollo y la utilización de identificaciones electrónicas interoperables; PEPPOL, que apoya el desarrollo y la utilización de soluciones de contratación electrónica interoperables; epSOS, que apoya el desarrollo y la utilización de soluciones de sanidad electrónica interoperables; y eCodex, que apoya el desarrollo y la utilización de soluciones de justicia electrónica interoperables).

1.6. Duración e incidencia financiera

☐ Propuesta/iniciativa de **duración limitada**

– ☐ Propuesta/iniciativa en vigor desde [el] [DD/MM]AAAA hasta [el] [DD/MM]AAAA

– ☐ Incidencia financiera desde YYYY hasta YYYY

☑ Propuesta/iniciativa de **duración ilimitada**

1.7. Modo(s) de gestión previsto(s)[27]

☑ **Gestión centralizada directa** a cargo de la Comisión

☐ **Gestión centralizada indirecta** mediante delegación de las tareas de ejecución en:

– ☐ agencias ejecutivas

– ☐ organismos creados por las Comunidades[28]

– ☐ organismos nacionales del sector público / organismos con misión de servicio público

– ☐ personas a quienes se haya encomendado la ejecución de acciones específicas de conformidad con el título V del Tratado de la Unión Europea y que estén identificadas en el acto de base pertinente a efectos de lo dispuesto en el artículo 49 del Reglamento financiero

☐ **Gestión compartida** con los Estados miembros

☐ **Gestión descentralizada** con terceros países

☐ **Gestión conjunta** con organizaciones internacionales (***especifíquense***)

Si se indica más de un modo de gestión, facilítense los detalles en el recuadro de observaciones.

Observaciones

[//]

[27] Las explicaciones sobre los modos de gestión y las referencias al Reglamento financiero pueden consultarse en el sitio BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

[28] Tal como se contemplan en el artículo 185 del Reglamento financiero.

2. MEDIDAS DE GESTIÓN

2.1. Disposiciones en materia de seguimiento e informes

Especifíquense la frecuencia y las condiciones.

La primera evaluación tendrá lugar cuatro años después de la entrada en vigor del Reglamento. Este incluye una cláusula explícita que obliga a la Comisión a presentar informes al Parlamento Europeo y al Consejo sobre su aplicación. Los informes subsiguientes se presentarán cada cuatro años. Se aplicará la metodología de evaluación de la Comisión. Estas evaluaciones se llevarán a cabo con la ayuda de estudios específicos sobre la aplicación de los instrumentos jurídicos, cuestionarios dirigidos a las autoridades nacionales, debates de expertos, seminarios, encuestas del Eurobarómetro, etc.

2.2. Sistema de gestión y de control

2.2.1. Riesgo(s) definido(s)

Se ha llevado a cabo una evaluación de impacto que acompaña a la propuesta de Reglamento. El nuevo instrumento jurídico facilitará el reconocimiento y la aceptación mutuos de la identificación electrónica a través de las fronteras, mejorará el marco actual de la firma electrónica, en particular reforzando la supervisión nacional de los proveedores de servicios de confianza y conferirá efectos jurídicos y reconocimiento a los servicios de confianza conexos. Introduce también el uso de actos delegados y de ejecución como mecanismo para garantizar la flexibilidad frente a la evolución de la tecnología.

2.2.2. Método(s) de control previsto(s)

Los métodos de control existentes aplicados por la Comisión incluirán los créditos suplementarios.

2.3. Medidas de prevención del fraude y de las irregularidades

Especifíquense las medidas de prevención y protección existentes o previstas.

Los métodos de prevención del fraude existentes aplicados por la Comisión cubrirán los créditos suplementarios.

3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

3.1. Rúbrica(s) del marco financiero plurianual y línea(s) presupuestaria(s) de gastos afectada(s)

- Líneas presupuestarias de gasto existentes

En el orden de las rúbricas del marco financiero plurianual y las líneas presupuestarias.

Rúbrica del marco financiero plurianual	Línea presupuestaria	Tipo de **gasto**	Contribución			
	Número [Rúbrica…………...…….]	CD/CND (29)	de países de la AELC[30]	de países candidatos [31]	de terceros países	a efectos de lo dispuesto en el artículo 18.1.a *bis*) del Reglamento financiero
5	09. 01 01 01 Gastos relacionados con personal con empleo activo en la DG Sociedad de la Información y Medios de Comunicación	CND	NO	NO	NO	NO
5	09. 01 02 01 Personal externo	CND	NO	NO	NO	NO

29 CD = créditos disociados / CND = créditos no disociados.

30 AELC: Asociación Europea de Libre Comercio.

31 Países candidatos y, en su caso, países candidatos potenciales de los Balcanes Occidentales.

3.2. Incidencia estimada en los gastos

3.2.1. Resumen de la incidencia estimada en los gastos

Rúbrica del marco financiero plurianual:	**Número**	[Rúbrica 1. **Crecimiento inteligente e integrador** ……..……]

DG: INFSO			Año **2014**	Año **2015**	Año **2016**	Año **2017**	Año 2018	**Año 2019**	**Año 2020**	**TOTAL**
• Créditos de operaciones										
Número de línea presupuestaria – N. A.	Compromisos	(1)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
	Pagos	(2)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
Número de línea presupuestaria -N.A.	Compromisos	(1a)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
	Pagos	(2a)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
Créditos de carácter administrativo financiados mediante la dotación de programas específicos[32]			0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
Número de línea presupuestaria		(3)	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
TOTAL de los créditos para la DG INFSO	Compromisos	=1+1a +3	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**
	Pagos	=2+2a +3	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**	**0.000**

[32] Asistencia técnica y/o administrativa y gastos de apoyo a la ejecución de programas y/o acciones de la UE (antiguas líneas «BA»), investigación indirecta, investigación directa.

Rúbrica del marco financiero plurianual:	**5**	«Gastos administrativos»

En millones EUR (al tercer decimal)

		Año **2014**	Año **2015**	Año **2016**	Año **2017**	Año **2018**	Año **2019**	Año **2020**	**TOTAL**
		DG: INFSO							
• Recursos humanos		1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
• Otros gastos administrativos									
TOTAL DG INFSO	Créditos	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

TOTAL de los créditos para la RÚBRICA 5 del marco financiero plurianual	(Total de los compromisos = Total de los pagos)	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

En millones EUR (al tercer decimal)

		Año **2014**	Año **2015**	Año **2016**	Año **2017**	Year **2018**	Year **2019**	Year **2020**	**TOTAL**
TOTAL de los créditos para las RÚBRICAS 1 a 5 del marco financiero plurianual	Compromisos	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
	Pagos	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

3.2.2. Incidencia estimada en los créditos de operaciones

– ☑ La propuesta/iniciativa no exige la utilización de créditos de operaciones

– ☐ La propuesta/iniciativa exige la utilización de créditos de operaciones, tal como se explica a continuación:

3.2.3. Incidencia estimada en los créditos de carácter administrativo

3.2.3.1. Resumen

– ☐ La propuesta/iniciativa no exige la utilización de créditos administrativos

– ☑ La propuesta/iniciativa exige la utilización de créditos administrativos, tal como se explica a continuación:

En millones EUR (al tercer decimal)

	Año **N 2014**	Año **2015**	Año **2016**	Año **2017**	Año **2018**	Año **2019**	Año **2020**	**TOTAL**
RÚBRICA 5 del marco financiero plurianual								
Recursos humanos	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
Otros gastos administrativos								
Subtotal para la RÚBRICA 5 del marco financiero plurianual	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

Al margen de la RÚBRICA 5[33] del marco financiero plurianual								
Recursos humanos								
Otros gastos de carácter administrativo								
Subtotal al margen de la RÚBRICA 5 del marco financiero plurianual								

TOTAL	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

[33] Asistencia técnica y/o administrativa y gastos de apoyo a la ejecución de programas y/o acciones de la UE (antiguas líneas «BA»), investigación indirecta, investigación directa.

3.2.3.2. Necesidades estimadas de recursos humanos

– ☐ La propuesta/iniciativa no exige la utilización de recursos humanos

– ☑ La propuesta/iniciativa exige la utilización de recursos humanos, tal como se explica a continuación:

Estimación que debe expresarse en valores enteros (o, a lo sumo, con un decimal)

		Año **2014**	Año **2015**	Año **2016**	Año **2017**	Año **2018**	Año **2019**	Año **2020**
• Empleos de plantilla (funcionarios y agentes temporales)								
09 01 01 01 (Sede y Oficinas de Representación de la Comisión)		9	9	9	9	9	9	9
XX 01 01 02 (Delegaciones)								
XX 01 05 01 (Investigación indirecta)								
10 01 05 01 (Investigación directa)								
• Personal externo (en unidades de equivalente a jornada completa, EJC)[34]								
09 01 02 01 (AC, INT, ENCS de la dotación global)		3	3	3	3	3	3	3
XX 01 02 02 (AC, INT, JED, AL y ENCS en las delegaciones)								
XX 01 04 ***yy***[35]	- en la sede[36]							
	- en las delegaciones							
XX 01 05 02 (AC, INT, ENCS - Investigación indirecta)								
10 01 05 02 (AC, INT, ENCS - Investigación directa)								
Otras líneas presupuestarias (especifíquense)								
TOTAL		**12**	**12**	**12**	**12**	**12**	**12**	**12**

Las necesidades en materia de recursos humanos las cubrirá el personal de la DG ya destinado a la gestión de la acción y/o reasignado dentro de la DG, que se complementará en caso necesario con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

Descripción de las tareas que deben llevarse a cabo:

Funcionarios y agentes temporales	Gestionar los procedimientos legislativos para la adopción por el Parlamento Europeo y el Consejo del Reglamento previsto y de los actos delegados o de ejecución conexos. Ámbitos prioritarios:

34 AC = agente contractual; INT = personal de empresas de trabajo temporal («intérimaires»); JED = joven experto en delegación; AL = agente local; ENCS = experto nacional en comisión de servicios.

35 Por debajo del límite de personal externo cargo a créditos de operaciones (antiguas líneas «BA»).

36 Básicamente para los Fondos Estructurales, el Fondo Europeo Agrícola de Desarrollo Rural (Feader) y el Fondo Europeo de Pesca (FEP).

	1. Establecimiento de un nuevo marco legislativo para los servicios de confianza electrónicos 2. Fomento de la adopción de los servicios de confianza electrónicos a través de la sensibilización de los ciudadanos y de las PYME sobre su potencial 3. Seguimiento de la Directiva 1999/93/CE, incluidos los aspectos internacionales 4. Basándose en los proyectos piloto a gran escala, aceleración del logro concreto del objetivo del nuevo marco legislativo.
Personal externo	Ídem según lo indicado anteriormente

3.2.4. Compatibilidad con el marco financiero plurianual vigente

– ☑ La propuesta/iniciativa es compatible con el marco financiero plurianual vigente.

– ☐ La propuesta/iniciativa implicará la reprogramación de la rúbrica correspondiente del marco financiero plurianual.

Explíquese la reprogramación requerida, precisando las líneas presupuestarias afectadas y los importes correspondientes.

– ☐ La propuesta/iniciativa requiere la aplicación del Instrumento de Flexibilidad o la revisión del marco financiero plurianual[37].

Explíquese qué es lo que se requiere, precisando las rúbricas y líneas presupuestarias afectadas y los importes correspondientes.

3.2.5. Contribución de terceros

– ☑ La propuesta/iniciativa no prevé la cofinanciación por terceros

– ☐ La propuesta/iniciativa prevé la cofinanciación que se estima a continuación:

3.3. Incidencia estimada en los ingresos

– ☑ La propuesta/iniciativa no tiene incidencia financiera en los ingresos.

– ☐ La propuesta/iniciativa tiene la incidencia financiera que se indica a continuación:

  – ☐ en los recursos propios

  – ☐ en ingresos diversos

[37] Véanse los puntos 19 y 24 del Acuerdo Interinstitucional.