REGLAMENTO (UE) Nº 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 23 de julio de 2014

relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE

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 ([1]),

De conformidad con el procedimiento legislativo ordinario ([2]),

Considerando lo siguiente:

(1) La creación de un clima de confianza en el entorno en línea es esencial para el desarrollo económico y social. La desconfianza, en particular debida a la inseguridad jurídica percibida, hace que los consumidores, las empresas y las administraciones públicas 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 proporcionando una base común para lograr interacciones electrónicas seguras entre los ciudadanos, las empresas 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 ([3]) se refiere 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.

(4) La Comunicación de la Comisión de 26 de agosto de 2010 titulada «Una Agenda Digital para Europa» señalaba 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, titulado «La eliminación de los obstáculos a los derechos de los ciudadanos de la UE», la Comisión subrayó asimismo la necesidad de resolver los principales problemas que impiden a los ciudadanos de la Unión disfrutar de los beneficios de un mercado único digital y unos servicios digitales transfronterizos.

(5) En sus conclusiones de 4 de febrero de 2011 y de 23 de octubre de 2011, el Consejo Europeo invitó a la Comisión a crear un mercado único digital para 2015 a fin de progresar rápidamente en ámbitos clave de la economía digital y promover un mercado único digital plenamente integrado facilitando el uso transfronterizo de los servicios en línea, con especial atención a la identificación y autenticación electrónicas seguras.

([1]) DO C 351 de 15.11.2012, p. 73.
([2]) Posición del Parlamento Europeo y del Consejo de 3 de abril de 2014 (no publicada aún en el Diario Oficial) y Decisión del Consejo de 23 de julio de 2014.
([3]) 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 (DO L 13 de 19.1.2000, p. 12).

(6) En sus conclusiones de 27 de mayo de 2011 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.

(7) El Parlamento Europeo, en su Resolución de 21 de septiembre de 2010 sobre la plena realización del mercado interior del comercio electrónico ([1]) 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.

(8) La Directiva 2006/123/CE del Parlamento Europeo y el Consejo ([2]) o 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 ciudadanos de un Estado miembro no pueden utilizar su identificación electrónica para autenticarse en otro Estado miembro porque los sistemas nacionales de identificación electrónica en su país no son reconocidos en otros Estados miembros. Dicha barrera electrónica excluye a los prestadores de servicios del pleno disfrute de los beneficios del mercado interior. Unos medios de identificación electrónica mutuamente reconocidos 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 ([3]) 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 mutuo de la identificación y la autenticación electrónicas es esencial 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) El presente Reglamento debe aplicarse de forma que se cumplan plenamente los principios relativos a la protección de los datos personales establecidos en la Directiva 95/46/CE del Parlamento Europeo y del Consejo ([4]). A tal efecto, visto el principio de reconocimiento mutuo que establece el presente Reglamento, la autenticación a efectos de un servicio en línea debe implicar exclusivamente el tratamiento de los datos identificativos que sean adecuados, pertinentes y no excesivos para la concesión del acceso al servicio en línea de que se trate. Por otra parte, los prestadores de servicios de confianza y el organismo de supervisión deben respetar asimismo los requisitos de confidencialidad y seguridad del tratamiento previstos en la Directiva 95/46/CE.

(12) 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 autenticar al menos en 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.

([1]) DO C 50 de 21.2.2012, p. 1.
([2]) Directiva 2006/123/CE del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006, relativa a los servicios en el mercado interior (DO L 376 de 27.12.2006, p. 36).
([3]) Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza (DO L 88 de 4.4.2011, p. 45).
([4]) 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 (DO L 281 de 23.11.1995, p. 31).

(13) 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 a la Comisión. 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.

(14) Deben establecerse en el presente Reglamento ciertas condiciones en relación con qué medios de identificación electrónica tienen que reconocerse y cómo deben notificarse los sistemas. Esto contribuiría a que cada Estado miembro adquiera la confianza necesaria en los sistemas de identificación electrónica de los demás y a que se reconozcan mutuamente los medios de identificación electrónica de los sistemas notificados. Debe aplicarse el principio de reconocimiento mutuo si el sistema de identificación electrónica del Estado miembro que efectúa la notificación cumple las condiciones de notificación y esta se ha publicado en el *Diario Oficial de la Unión Europea*. Sin embargo, el principio de reconocimiento mutuo debe referirse únicamente a la autenticación a efectos de un servicio en línea. El acceso a estos servicios en línea y su prestación final al solicitante deben estar estrechamente vinculados al derecho a recibir dichos servicios en las condiciones fijadas por la legislación nacional.

(15) La obligación de reconocer los medios de identificación electrónica debe referirse únicamente a los medios cuyo nivel de seguridad de la identidad corresponde a un nivel igual o superior al exigido para el servicio en línea de que se trate. Además, la obligación habrá de aplicarse únicamente cuando el organismo del sector público en cuestión emplee el nivel de seguridad «sustancial» o «alto» en lo tocante al acceso a dicho servicio en línea. Los Estados miembros deberán tener la posibilidad, con arreglo al Derecho de la Unión, de reconocer medios de identificación electrónica con niveles más bajos de certeza de la identidad.

(16) Los niveles de seguridad deben caracterizar el grado de confianza de un medio de identificación electrónica para establecer la identidad de una persona, garantizando así que la persona que afirma poseer una identidad determinada es de hecho la persona a quien se ha atribuido dicha identidad. El nivel de seguridad depende del grado de confianza que aporte este medio de identificación electrónica sobre la identidad pretendida o declarada por una persona, teniendo en cuenta los procedimientos técnicos, (por ejemplo, prueba y verificación de la identidad, autenticación), las actividades de gestión (como la entidad que expide los medios de identificación electrónica, el procedimiento para expedir dichos medios) y los controles aplicados. Como resultado de las actividades la normalización y las actividades internacionales de la financiación de la Unión de proyectos piloto a gran escala, existen varias definiciones y descripciones técnicas de niveles de seguridad. En particular, los proyectos piloto a gran escala STORK e ISO 29115 se refieren, entre otros, a los niveles 2, 3 y 4 que deben tenerse en cuenta en la máxima medida para establecer los requisitos técnicos mínimos, las normas y los procedimientos para los niveles de seguridad bajo, sustancial y alto entendidos en el sentido del presente Reglamento, garantizando al mismo tiempo la aplicación coherente del presente Reglamento, en particular con respecto al nivel de seguridad alto en relación con la acreditación de identidad para la expedición de certificados cualificados. Los requisitos que se establezcan deberán ser tecnológicamente neutros. Debe ser posible cumplir los requisitos de seguridad necesarios mediante diversas tecnologías.

(17) Los Estados miembros deben fomentar que el sector privado utilice voluntariamente los medios de identificación electrónica amparados en un sistema 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 por parte del sector privado de tales medios de identificación electrónica a través de las fronteras, debe estar disponible la posibilidad de autenticación ofrecida por cualquier Estado miembro para las partes usuarias del sector privado establecidas fuera del territorio de dicho Estado miembro en las mismas condiciones aplicadas a las partes usuarias del sector privado establecidas dentro de dicho Estado miembro. Por consiguiente, por lo que respecta a las partes usuarias del sector privado, el Estado miembro que efectúa la notificación podrá definir condiciones de acceso a los medios de autenticación. Dichas condiciones de acceso podrán informar de si en un momento dado los medios de autenticación relacionados con el sistema notificado están disponibles para las partes usuarias del sector privado.

(18) El presente Reglamento establece la responsabilidad del Estado miembro que efectúa la notificación, de la parte que expide los medios de identificación electrónica y de la parte que realiza el procedimiento de autenticación en caso de incumplimiento de las obligaciones pertinentes dispuestas en el mismo. No obstante, el presente Reglamento debe aplicarse en consonancia con las normas nacionales sobre responsabilidad. Por lo tanto, no afectará a dichas normas nacionales, por ejemplo sobre la definición de daños y perjuicios o sobre las normas de procedimiento aplicables, incluida la carga de la prueba.

(19) La seguridad de los sistemas de identificación electrónica es esencial para la confianza en el reconocimiento transfronterizo recíproco de los medios de identificación electrónica. En tal sentido, los Estados miembros deben cooperar en relación con la seguridad y la interoperabilidad de los sistemas de identificación electrónica en el plano de la Unión. Toda vez que los sistemas de identificación electrónica puedan requerir el empleo de equipos o programas informáticos específicos por las partes usuarias a escala nacional, la interoperabilidad transfronteriza exige que los Estados miembros no impongan tales requisitos y los costes asociados a las partes usuarias establecidas fuera de su territorio. En tal caso, se deben debatir y desarrollar soluciones adecuadas dentro del ámbito de aplicación del marco de interoperabilidad. Sin embargo, resultan inevitables los requisitos técnicos derivados de las especificaciones intrínsecas de los medios de identificación electrónica nacionales (por ejemplo tarjetas inteligentes), que pueden afectar a los titulares de esos medios electrónicos.

(20) 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 de las mejores prácticas entre los Estados miembros con miras a su reconocimiento mutuo debe facilitar dicha cooperación.

(21) El presente Reglamento también debe establecer un marco jurídico general para la utilización de los servicios de confianza. Sin embargo, no debe crear la obligación general de utilizarlos ni de instalar un punto de acceso para todos los servicios de confianza existentes. En particular, no debe cubrir la prestación de servicios utilizados exclusivamente dentro de sistemas cerrados entre un conjunto definido de participantes, que no tengan efectos en terceros. Por ejemplo, los sistemas establecidos en empresas o administraciones públicas para gestionar procedimientos internos que hagan uso de servicios de confianza no deben estar sujetos a las obligaciones del presente Reglamento. Únicamente los servicios de confianza prestados al público que tengan efectos en terceros deben cumplir las obligaciones establecidas en el presente Reglamento. Tampoco debe regular el presente Reglamento 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. Por otro lado, no debe afectar a los requisitos nacionales de formato correspondientes a los registros públicos, en particular los registros mercantiles y de la propiedad.

(22) Para contribuir al uso transfronterizo general de los servicios de confianza, debe ser posible utilizarlos como prueba en procedimientos judiciales en todos los Estados miembros. Corresponde al Derecho nacional definir los efectos jurídicos de los servicios de confianza, salvo disposición contraria del presente Reglamento.

(23) En la medida en que el presente Reglamento cree la obligación de reconocer un servicio de confianza, solo podrá no reconocerse tal servicio de confianza cuando el destinatario no pueda leerlo o verificarlo por motivos técnicos sobre los que el destinatario no tenga un control inmediato. No obstante, esta obligación no debe exigir a su vez a un organismo público la obtención del equipo y los programas informáticos necesarios para la legibilidad técnica de todos los servicios de confianza existentes.

(24) Los Estados miembros podrán mantener o introducir disposiciones nacionales, acordes con el Derecho de la Unión, relativas a los servicios de confianza, siempre que tales servicios no estén plenamente armonizados por el presente Reglamento. No obstante, los productos y servicios de confianza que se ajusten al presente Reglamento deben poder circular libremente en el mercado interior.

(25) 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.

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

(27) 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.

(28) Para aumentar en particular la confianza de las pequeñas y medianas empresas y los consumidores 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 prestador cualificado de servicios de confianza 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.

(29) En consonancia con las obligaciones en virtud de la Convención de las Naciones Unidas sobre los Derechos de las Personas con Discapacidad, aprobada por la Decisión 2010/48/CE [1] del Consejo, en particular el artículo 9 de la Convención, 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. Por lo tanto, siempre que sea factible, los servicios de confianza prestados y los productos para el usuario final utilizados en la prestación de estos servicios deben hacerse accesibles para las personas con discapacidad. La evaluación de factibilidad debe incluir, entre otros aspectos, consideraciones técnicas y económicas.

(30) Los Estados miembros deben designar uno o más organismos de supervisión para que lleven a cabo las actividades de supervisión previstas en el presente Reglamento. Asimismo, los Estados miembros deben poder decidir, por mutuo acuerdo con otro Estado miembro, la designación de un organismo de supervisión en el territorio de ese otro Estado miembro.

(31) Los organismos de supervisión deben cooperar con las autoridades de protección de datos, por ejemplo informándoles de los resultados de las auditorías de los prestadores cualificados de servicios de confianza, en caso de resultar infringidas las normas sobre protección de datos de carácter personal. El suministro de información debe incluir, en particular, los incidentes en materia de seguridad y las violaciones de los datos de carácter personal.

(32) A todos los prestadores 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.

(33) 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.

(34) Todos los Estados miembros deben seguir unos requisitos de supervisión esenciales comunes con el fin de garantizar un nivel de seguridad equivalente 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.

(35) Todos los prestadores de servicios de confianza deben estar sometidos a los requisitos del presente Reglamento, en particular en materia de seguridad y responsabilidad, para garantizar la debida diligencia, la transparencia y la rendición de cuentas en relación con sus operaciones y servicios. No obstante, teniendo en cuenta el tipo de servicios prestados por los prestadores de servicios de confianza, es conveniente distinguir, en la medida en que se refiere a estos requisitos, entre prestadores cualificados y no cualificados de servicios de confianza.

(36) El establecimiento de un régimen de supervisión de todos los prestadores de servicios de confianza debe garantizar unas condiciones de igualdad en cuanto a la seguridad y la rendición de cuentas en relación con sus operaciones y servicios, contribuyendo así a la protección de los usuarios y al funcionamiento del mercado interior. Los prestadores no cualificados de servicios de confianza deben estar sujetos a un tipo de supervisión ligera, reactiva y posterior y justificada en función de la naturaleza de sus servicios y operaciones. Por consiguiente, el organismo de supervisión no debe tener la obligación general de supervisar a los prestadores no cualificados de servicios. El organismo de supervisión debe actuar únicamente cuando se le informe (por ejemplo, por parte del propio prestador no cualificado de servicios de confianza, mediante notificación de un usuario o de un socio comercial, o a través de sus propias investigaciones) de que un prestador no cualificado de servicios de confianza no cumple los requisitos del presente Reglamento.

[1] Decisión 2010/48/CE del Consejo, de 26 de noviembre de 2009, relativa a la celebración, por parte de la Comunidad Europea, de la Convención de las Naciones Unidas sobre los Derechos de las Personas con Discapacidad (DO L 23 de 27.1.2010, p. 35).

(37) El presente Reglamento debe establecer la responsabilidad de todos los prestadores de servicios de confianza. Establece, en particular, el régimen de responsabilidad conforme al cual todos los prestadores de servicios de confianza deben responder de los perjuicios ocasionados a cualquier persona física o jurídica con motivo del incumplimiento por su parte de las obligaciones que impone el presente Reglamento. Con objeto de facilitar la evaluación del riesgo financiero que podrían tener que soportar los prestadores de servicios de confianza, o el que deberían cubrir mediante pólizas de seguros, el presente Reglamento permite que los prestadores de servicios de confianza establezcan limitaciones, en determinadas circunstancias, relativas a la utilización de los servicios que prestan y que los exima de responsabilidad por los perjuicios derivados de la utilización de los servicios que superen dichas limitaciones. Debe informarse debidamente a los clientes de estas limitaciones con antelación. Tales limitaciones deben poder ser reconocidas por terceros, por ejemplo mediante la inclusión de información al respecto en las condiciones generales del servicio prestado o por otros medios reconocibles. Con el fin de dar efecto a estos principios, el presente Reglamento debe aplicarse de conformidad con las normas nacionales en materia de responsabilidad. Por lo tanto, el presente Reglamento no afectará a tales normas nacionales, por ejemplo las relativas a la definición de los perjuicios, la intencionalidad, la negligencia o las normas de procedimiento aplicables pertinentes.

(38) 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.

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

(40) 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.

(41) 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 verificar la existencia y la correcta aplicación de las disposiciones relativas a los planes de cese en caso de que los prestadores cualificados de servicios de confianza cesen en sus actividades.

(42) Para facilitar la supervisión de los prestadores cualificados de servicios de confianza, por ejemplo cuando un prestador preste sus servicios en el territorio de otro Estado miembro y no esté sujeto a supervisión en este, o cuando los ordenadores de un prestador 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.

(43) Con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento por parte de los prestadores cualificados de servicios de confianza y de los servicios que prestan, organismos de evaluación de la conformidad deben llevar a cabo evaluaciones de la conformidad, y los prestadores cualificados de servicios de confianza transmitirán los informes de evaluación de la conformidad al organismo de supervisión. Siempre que el organismo de supervisión exija que un prestador cualificado de servicios de confianza presente un informe *ad hoc* de evaluación de la conformidad, el organismo de supervisión debe observar, en particular, el principio de buena administración, incluida la obligación de motivar sus decisiones, así como el principio de proporcionalidad. Por consiguiente, el organismo de supervisión debe justificar debidamente cualquier decisión por la que requiera una evaluación *ad hoc* de la conformidad.

(44) El presente Reglamento tiene por objeto proporcionar un marco coherente con vistas a garantizar un elevado nivel de seguridad y de certidumbre jurídica de los servicios de confianza. En tal sentido, la Comisión, a la hora de examinar la evaluación de la conformidad de los productos y servicios, debe procurar, si procede, establecer sinergias con los sistemas europeos e internacionales pertinentes, como el Reglamento (CE) nº 765/2008 del Parlamento Europeo y el Consejo [1] por el que se establecen los requisitos de acreditación de los organismos de evaluación de la conformidad y vigilancia del mercado de productos.

[1] Reglamento (CE) nº 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) nº 339/93 (DO L 218 de 13.8.2008, p. 30).

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

(46) Las listas de confianza constituyen elementos esenciales para la creación de confianza entre los operadores del mercado, ya que indican la cualificación del prestador de servicios en el momento de la supervisión.

(47) La confianza en los servicios en línea y la conveniencia de estos servicios son fundamentales para que los usuarios los aprovechen plenamente y confíen conscientemente en los servicios electrónicos. Para este fin, debe crearse una etiqueta de confianza «UE» que identifique los servicios de confianza cualificados prestados por prestadores cualificados de servicios de confianza. Esta etiqueta de confianza «UE» para los servicios de confianza cualificados diferenciaría claramente los servicios de confianza cualificados de otros servicios de confianza, contribuyendo así a mejorar la transparencia del mercado. El uso de una etiqueta de confianza «UE» por parte de los prestadores cualificados de servicios de confianza es voluntario y no debe implicar más requisitos que los establecidos en el presente Reglamento.

(48) 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 [1] de la Comisión, deben aceptarse también las firmas electrónicas que tienen una menor garantía de la seguridad.

(49) El presente Reglamento debe establecer el principio de que no se deben denegar los efectos jurídicos de una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla todos los requisitos de la firma electrónica cualificada. Sin embargo, corresponde a las legislaciones nacionales determinar los efectos jurídicos de las firmas electrónicas en los Estados miembros, salvo para los requisitos establecidos en el presente Reglamento según los cuales una firma electrónica cualificada debe tener el efecto jurídico equivalente a una firma manuscrita.

(50) 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.

(51) Debe ser posible para el firmante confiar a un tercero los dispositivos cualificados de creación de firmas electrónicas, 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 electrónica cualificada.

(52) Debido a sus múltiples ventajas económicas, debe desarrollarse la creación de firmas electrónicas a distancia en un entorno de creación de firma electrónica gestionado por un prestador de servicios de confianza en nombre del firmante. Sin embargo, a fin de garantizar que estas firmas electrónicas obtengan el mismo reconocimiento jurídico que las firmas electrónicas creadas en un entorno completamente gestionado por el usuario, los prestadores que ofrezcan servicios de firma electrónica a distancia deben aplicar procedimientos de seguridad de la gestión y administrativos específicos y utilizar sistemas y productos fiables, incluidos canales de comunicación electrónica seguros para garantizar que el entorno de creación de firmas electrónicas es fiable y se utiliza bajo el control exclusivo del firmante. En el caso de una firma electrónica cualificada creada mediante un dispositivo de creación de firmas electrónicas a distancia, se aplicarán los requisitos aplicables a los prestadores cualificados de servicios de confianza contemplados en el presente Reglamento.

[1] 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 (DO L 274 de 20.10.2009, p. 36).

(53) La suspensión de certificados cualificados es una práctica operativa establecida de los prestadores de servicios de confianza en una serie de Estados miembros, distinta de la revocación y que conlleva la pérdida temporal de la validez de un certificado. La seguridad jurídica impone que siempre se indique claramente la suspensión de un certificado. A tal fin, los prestadores de servicios de confianza deben encargarse de indicar claramente la situación del certificado y, si está suspendido, el período preciso durante el cual ha sido suspendido. El presente Reglamento no debe imponer a los prestadores de servicios de confianza ni a los Estados miembros el uso de la suspensión, pero debe establecer normas de transparencia cuando y donde esta práctica sea posible.

(54) La interoperabilidad y el reconocimiento transfronterizos de los certificados cualificados es un requisito previo para el reconocimiento transfronterizo de las firmas electrónicas cualificadas. Por consiguiente, los certificados cualificados no deben estar sometidos a ningún requisito obligatorio que exceda de los requisitos establecidos en el presente Reglamento. No obstante, en el plano nacional debe permitirse la inclusión de atributos específicos, por ejemplo identificadores únicos, en los certificados cualificados, a condición de que tales atributos específicos no comprometan la interoperabilidad y el reconocimiento transfronterizos de los certificados y las firmas electrónicas cualificados.

(55) La certificación de seguridad TI basada en normas internacionales (como ISO 15408 y métodos relacionados de evaluación y acuerdos de reconocimiento mutuo) es un importante instrumento para verificar la seguridad de dispositivos cualificados de creación de firmas electrónicas y debe fomentarse. Con todo, las soluciones y servicios innovadores (como la firma móvil, la firma en nube, etc.) se basan en soluciones técnicas y organizativas de dispositivos cualificados de creación de firmas electrónicas para las que puede no disponerse todavía de normas de seguridad o para las que puede estar en curso la primera certificación de seguridad TI. El nivel de seguridad de dichos dispositivos cualificados de creación de firmas electrónicas debe poder evaluarse mediante procesos alternativos únicamente cuando no se disponga todavía de normas de seguridad o para las que pueda estar en curso la primera certificación de seguridad TI. Dichos procesos deben ser comparables con las normas de certificación de seguridad TI en la medida en que sean equivalentes los niveles de seguridad. Estos procesos podrán facilitarse mediante un examen por homólogos.

(56) En el presente Reglamento se establecen requisitos aplicables a los dispositivos cualificados de creación de firmas electrónicas, a fin de garantizar la funcionalidad de las firmas electrónicas avanzadas. El presente Reglamento no debe regular la totalidad del entorno del sistema en el que operen tales dispositivos. Por consiguiente, el objeto de la certificación de los dispositivos cualificados de creación de firmas debe limitarse a los equipos y programas informáticos empleados para gestionar y proteger los datos de creación de firma creados, almacenados o tratados en el dispositivo de creación de firmas. Tal como se especifica en las normas pertinentes, el alcance de la obligación de certificación debe excluir a las aplicaciones de creación de firmas.

(57) 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, la especificación de los requisitos exigibles a los prestadores cualificados de servicios de confianza 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 y 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.

(58) 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.

(59) 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.

(60) Los prestadores de servicios de confianza que expidan certificados cualificados de sello electrónico deben instaurar las medidas necesarias para poder determinar la identidad de la persona física que representa a la persona jurídica a la que se entregue el certificado cualificado de sello electrónico, cuando se requiera tal identificación a nivel nacional en el contexto de procedimientos judiciales o administrativos.

(61) 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.

(62) Con el fin de garantizar la seguridad de los sellos cualificados de tiempo electrónicos, el presente Reglamento debe requerir el empleo del sello electrónico avanzado o la firma electrónica avanzada, o de otros métodos equivalentes. Cabe esperar que la innovación dé lugar a nuevas tecnologías que garanticen un nivel de seguridad equivalente de los sellos de tiempo. Siempre que se emplee otro método que no sea el sello de tiempo avanzado ni la firma electrónica avanzada, debe corresponder al prestador cualificado de servicios de confianza demostrar, en el informe de evaluación de la conformidad, que dicho método garantiza un nivel de seguridad equivalente y cumple con las obligaciones establecidas en el presente Reglamento.

(63) Los documentos electrónicos son importantes para que sigan desarrollándose las transacciones electrónicas transfronterizas en el mercado interior. El presente Reglamento debe establecer el principio de que no se deben denegar efectos jurídicos a un documento electrónico por el mero hecho de estar en formato electrónico al objeto de garantizar que no se rechazará una transacción electrónica por el mero hecho de que el documento está en formato electrónico.

(64) A la hora de examinar formatos de firmas y sellos electrónicos avanzados, la Comisión debe basarse en los usos, normas y reglamentaciones vigentes, y en particular en la Decisión 2011/130/UE de la Comisión [1].

(65) 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.

(66) Es esencial proporcionar un marco jurídico para facilitar el reconocimiento transfronterizo entre los ordenamientos jurídicos nacionales existentes relacionados con servicios de entrega electrónica certificada. Dicho marco puede abrir, además, nuevas oportunidades de mercados para los prestadores de servicios de confianza de la Unión de ofrecer nuevos servicios paneuropeos de entrega electrónica certificada.

(67) Los servicios de autenticación de sitios web proporcionan un medio por el que puede garantizarse a la persona que visita un sitio web que existe una entidad auténtica y legítima que respalda la existencia del sitio web. Estos servicios contribuyen a crear confianza y fe en la realización de operaciones mercantiles en línea, dado que los usuarios se fiarán de un sitio web que haya sido autenticado. La prestación y la utilización de servicios de autenticación de sitios web son totalmente voluntarias. No obstante, para que la autenticación de sitios web se convierta en un medio de potenciar la confianza, proporcionar al usuario una experiencia mejor y propiciar el crecimiento en el mercado interior, el presente Reglamento debe establecer obligaciones mínimas de seguridad y responsabilidad para los prestadores y los servicios que prestan. A tal efecto, se han tenido en cuenta los resultados de las iniciativas punteras lideradas por el sector (por ejemplo el foro de autoridades de certificación y navegadores-CA/B Forum). Además, el presente Reglamento no debe oponerse a la utilización de otros medios o métodos de autenticación de un sitio web que no estén regulados por el presente Reglamento, ni impedir que prestadores de autenticación de sitios web de terceros países presten sus servicios a clientes situados en la Unión. Ahora bien, los servicios de autenticación de sitios web de un prestador de un tercer país solamente se reconocerán como servicios cualificados de conformidad con el presente Reglamento en caso de que se haya celebrado un acuerdo internacional al respecto entre la Unión y el país de establecimiento del prestador.

(68) De conformidad con las disposiciones del Tratado de Funcionamiento de la Unión Europea (TFUE) en materia de establecimiento, el concepto de «personas jurídicas» permite a los operadores elegir libremente la forma jurídica que consideren adecuada para la realización de sus actividades. Por tanto, las «personas jurídicas» en el sentido del TFUE incluyen todas las entidades constituidas en virtud de la legislación de un Estado miembro, o que se rigen por la misma, independientemente de su forma jurídica.

(69) Se anima a las instituciones, órganos y organismos de la Unión Europea a reconocer la identificación electrónica y los servicios de confianza que contempla el presente Reglamento a efectos de la cooperación administrativa, aprovechando en particular las buenas prácticas existentes y los resultados de los proyectos en curso en los ámbitos previstos por el presente Reglamento.

[1] Decisión 2011/130/UE de la Comisión, de 25 de febrero de 2011, por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes en virtud de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior (DO L 53 de 26.2.2011, p. 66).

(70) 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 TFUE en lo que se refiere a los criterios que deben cumplir los organismos responsables de la certificación de los dispositivos cualificados de creación de firmas electrónicas. Es particularmente importante que la Comisión lleve a cabo las consultas apropiadas durante sus tareas preparatorias, también a nivel de expertos. 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.

(71) Con el fin de garantizar unas condiciones uniformes para la aplicación del presente Reglamento, deben conferirse 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. Estas competencias deben ejercerse de conformidad con el Reglamento (UE) nº 182/2011 del Parlamento Europeo y del Consejo ([1]).

(72) A la hora de adoptar actos delegados o actos de ejecución, la Comisión debe tener debidamente en cuenta las normas y especificaciones técnicas elaboradas por organizaciones y organismos de normalización europeos e internacionales, en particular el Comité Europeo de Normalización (CEN), el Instituto Europeo de Normas de Telecomunicación (ETSI), la Organización Internacional de Normalización (ISO) y la Unión Internacional de Telecomunicaciones (UIT), con vistas a garantizar un elevado nivel de seguridad e interoperabilidad de los servicios de identificación electrónica y de confianza.

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

(74) Para dar seguridad jurídica a los operadores del mercado que ya utilicen certificados reconocidos expedidos a personas físicas de conformidad con la Directiva 1999/93/CE, es necesario prever un período de transición suficiente. De igual modo, han de preverse medidas transitorias para los dispositivos seguros de creación de firmas, cuya conformidad se haya determinado con arreglo a la Directiva 1999/93/CE, así como para los prestadores de servicios de certificación que expidan certificados reconocidos antes del 1 de julio de 2016. Por último, 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.

(75) Las fechas de aplicación que contempla el presente Reglamento no deben impedir que los Estados miembros cumplan las obligaciones que ya tengan a tenor del Derecho de la Unión, en particular de la Directiva 2006/123/CE.

(76) Dado que el objetivo del presente Reglamento no puede ser alcanzado de manera suficiente por los Estados miembros, sino que, debido a la dimensión de la acción, puede lograrse mejor a nivel de la Unión, la Unión puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

(77) El Supervisor Europeo de Protección de Datos fue consultado de conformidad con el artículo 28, apartado 2, del Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo ([2]) y emitió un dictamen el 27 de septiembre de 2012 ([3]).

([1]) 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 (DO L 55 de 28.2.2011, p. 13).

([2]) Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1).

([3]) DO C 28 de 30.1.2013, p. 6.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Objeto

Con el objetivo de garantizar el correcto funcionamiento del mercado interior aspirando al mismo tiempo a un nivel de seguridad adecuado de los medios de identificación electrónica y los servicios de confianza, el presente Reglamento:

a) establece las condiciones en que los Estados miembros deberán reconocer los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica notificado de otro Estado miembro,

b) establece normas para los servicios de confianza, en particular para las transacciones electrónicas, y

c) establece un marco jurídico para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios web.

Artículo 2

Ámbito de aplicación

1. El presente Reglamento se aplica a los sistemas de identificación electrónica notificados por los Estados miembros y a los prestadores de servicios de confianza establecidos en la Unión.

2. El presente Reglamento no se aplica a la prestación de servicios de confianza utilizados exclusivamente dentro de sistemas cerrados resultantes del Derecho nacional o de acuerdos entre un conjunto definido de participantes.

3. El presente Reglamento no afecta al Derecho nacional o de la Unión relacionado con la celebración y validez de los contratos u otras obligaciones legales o de procedimiento relativos a la forma.

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 formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica;

2) «medios de identificación electrónica», una unidad material y/o inmaterial que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea;

3) «datos de identificación de la persona», un conjunto de datos que permite establecer la identidad de una persona física o jurídica, o de una persona física que representa a una persona jurídica;

4) «sistema de identificación electrónica», un régimen para la identificación electrónica en virtud del cual se expiden medios de identificación electrónica a las personas físicas o jurídicas o a una persona física que representa a una persona jurídica;

5) «autenticación», un proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico;

6) «parte usuaria», la persona física o jurídica que confía en la identificación electrónica o el servicio de confianza;

7) «organismo del sector público», las autoridades estatales, regionales o locales, los organismos de Derecho público y las asociaciones formadas por una o varias de estas autoridades o uno o varios de estos organismos de Derecho público, o las entidades privadas mandatarias de al menos una de estas autoridades, organismos o asociaciones para prestar servicios públicos actuando en esa calidad;

8) «organismo de Derecho público», el definido en el artículo 2, apartado 1, punto 4, de la Directiva 2014/24/UE del Parlamento Europeo y del Consejo ([1]);

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

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

11) «firma electrónica avanzada», la firma electrónica que cumple los requisitos contemplados en el artículo 26;

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

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

14) «certificado de firma electrónica», una declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona;

15) «certificado cualificado de firma electrónica», un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I;

16) «servicio de confianza», el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en:

a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o

b) la creación, verificación y validación de certificados para la autenticación de sitios web, o

c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios;

17) «servicio de confianza cualificado», un servicio de confianza que cumple los requisitos aplicables establecidos en el presente Reglamento;

([1]) Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE (DO L 94 de 28.3.2014, p. 65).

18) «organismo de evaluación de conformidad», un organismo definido en el punto 13 del artículo 2 del Reglamento (CE) nº 765/2008 cuya competencia para realizar una evaluación de conformidad de un prestador cualificado de servicios de confianza y de los servicios de confianza cualificados que este presta esté acreditada en virtud de dicho Reglamento;

19) «prestador de servicios de confianza», una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianzas;

20) «prestador cualificado de servicios de confianza», un prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la cualificación;

21) «producto», un equipo o programa informático, o los componentes pertinentes del mismo, destinado a ser utilizado para la prestación de servicios de confianza;

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

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

24) «creador de un sello», una persona jurídica que crea un sello electrónico;

25) «sello electrónico», datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos;

26) «sello electrónico avanzado», un sello electrónico que cumple los requisitos contemplados en el artículo 36;

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

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

29) «certificado de sello electrónico», una declaración electrónica que vincula los datos de validación de un sello con una persona jurídica y confirma el nombre de esa persona;

30) «certificado cualificado de sello electrónico», un certificado de sellos electrónicos que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo III;

31) «dispositivo de creación de sello electrónico», un equipo o programa informático configurado que se utiliza para crear un sello electrónico;

32) «dispositivo cualificado de creación de sello electrónico», un dispositivo de creación de sellos electrónicos que cumple *mutatis mutandis* los requisitos enumerados en el anexo II;

33) «sello de tiempo electrónico», datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante;

34) «sello cualificado de tiempo electrónico», un sello de tiempo electrónico que cumple los requisitos establecidos en el artículo 42;

35) «documento electrónico», todo contenido almacenado en formato electrónico, en particular, texto o registro sonoro, visual o audiovisual;

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

37) «servicio cualificado de entrega electrónica certificada», un servicio de entrega electrónica certificada que cumple los requisitos establecidos en el artículo 44;

38) «certificado de autenticación de sitio web», una declaración que permite autenticar un sitio web y vincula el sitio web con la persona física o jurídica a quien se ha expedido el certificado;

39) «certificado cualificado de autenticación de sitio web», un certificado de autenticación de sitio web expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo IV;

40) «datos de validación», los datos utilizados para validar una firma electrónica o un sello electrónico;

41) «validación», el proceso de verificar y confirmar la validez de una firma o sello electrónicos.

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 prestador 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 y servicios de confianza que se ajusten al presente Reglamento.

Artículo 5

Tratamiento y protección de los datos

1. El tratamiento de los datos personales será conforme a lo dispuesto en la Directiva 95/46/CE.

2. Sin perjuicio de los efectos jurídicos que la legislación nacional contemple para los seudónimos, no se prohibirá su utilización en las transacciones electrónicas.

CAPÍTULO II

IDENTIFICACIÓN ELECTRÓNICA

Artículo 6

Reconocimiento mutuo

1. Cuando sea necesaria una identificación electrónica utilizando un medio de identificación electrónica y una autenticación en virtud de la normativa o la práctica administrativa nacionales para acceder a un servicio prestado en línea por un organismo del sector público en un Estado miembro, se reconocerá en dicho Estado miembro, a efectos de la autenticación transfronteriza en dicho servicio en línea, el medio de identificación electrónica expedido en otro Estado miembro, siempre que:

a) este medio de identificación electrónica haya sido expedido en virtud de un sistema de identificación electrónica incluido en la lista publicada por la Comisión de conformidad con el artículo 9;

b) el nivel de seguridad de este medio de identificación electrónica corresponda a un nivel de seguridad igual o superior al nivel de seguridad requerido por el organismo del sector público para acceder a dicho servicio en línea en el primer Estado miembro, siempre que el nivel de seguridad de dicho medio de identificación electrónica corresponda a un nivel de seguridad sustancial o alto;

c) el organismo público en cuestión utilice un nivel de seguridad sustancial o alto en relación con el acceso a ese servicio en línea.

Este reconocimiento se producirá a más tardar 12 meses después de que la Comisión publique la lista a que se refiere la letra a) del párrafo primero.

2. Un medio de identificación electrónica expedido por un sistema de identificación electrónica incluido en la lista publicada por la Comisión de conformidad con el artículo 9 y que corresponda al nivel de seguridad bajo podrá ser reconocido por los órganos del sector público a efectos de la autenticación transfronteriza del servicio prestado en línea por dichos órganos.

Artículo 7

Condiciones para la notificación de los sistemas de identificación electrónica

Un sistema de identificación electrónica podrá ser objeto de notificación con arreglo al artículo 9, apartado 1, si se cumplen la totalidad de las condiciones siguientes:

a) que los medios de identificación electrónica en virtud del sistema de identificación electrónica hayan sido expedidos:

i) por el Estado miembro que efectúa la notificación,

ii) por mandato del Estado miembro que efectúa la notificación, o

iii) independientemente del Estado miembro que efectúa la notificación y reconocidos por dicho Estado miembro;

b) que los medios de identificación electrónica en virtud del sistema de identificación electrónica puedan usarse para acceder al menos a un servicio prestado por un organismo del sector público que exija la identificación electrónica en el Estado miembro que efectúa la notificación;

c) que tanto el sistema de identificación electrónica como los medios de identificación electrónicos en su virtud expedidos cumplan los requisitos de al menos uno de los niveles de seguridad previstos en el acto de ejecución a que hace referencia el artículo 8, apartado 3;

d) que el Estado miembro que efectúa la notificación garantice que los datos de identificación de la persona que representan en exclusiva a la persona en cuestión se atribuyen de conformidad con las especificaciones técnicas, las normas y los procedimientos del nivel de seguridad pertinente establecido en el acto de ejecución a que se refiere el artículo 8, apartado 3, a la persona física o jurídica a la que se refiere el artículo 3, punto 1, en el momento de expedición de los medios de identificación electrónica previstos en este sistema;

e) que la parte que expide los medios de identificación electrónica previstos en este sistema garantice que los medios de identificación electrónica se atribuyan a la persona a que se refiere la letra d) del presente artículo de conformidad con las especificaciones técnicas, las normas y los procedimientos del nivel de seguridad pertinente establecidos en el acto de ejecución a que se refiere el artículo 8, apartado 3;

f) el Estado miembro que efectúa la notificación garantiza la disponibilidad de la autenticación en línea de manera que cualquier parte usuaria establecida en el territorio de otro Estado miembro pueda confirmar los datos de identificación de la persona recibidos en formato electrónico.

Para las partes usuarias distintas de los organismos del sector público, el Estado miembro que efectúa la notificación podrá definir las condiciones de acceso a esa autenticación. La autenticación transfronteriza deberá ser gratuita cuando se realice en relación con un servicio en línea prestado por un organismo del sector público.

Los Estados miembros no impondrán requisitos técnicos específicos desproporcionados a las partes usuarias que tengan intención de llevar a cabo tal autenticación, cuando esos requisitos impidan u obstaculicen significativamente la interoperabilidad de los sistemas de identificación electrónica notificados;

g) al menos seis meses antes de la notificación a la que se refiere el artículo 9, apartado 1, el Estado miembro que efectúa la notificación presentará a los demás Estados miembros, a efectos de la obligación a que se refiere el artículo 12, apartado 5, una descripción de este sistema, de conformidad con las modalidades de procedimiento establecidas en los actos de ejecución a los que se refiere el artículo 12, apartado 7;

h) el sistema de identificación electrónica cumple los requisitos del acto de ejecución a que se refiere el artículo 12, apartado 8.

Artículo 8

Niveles de seguridad de los sistemas de identificación electrónica

1. Un sistema de identificación electrónica notificado en virtud del artículo 9, apartado 1, deberá especificar los niveles de seguridad bajo, sustancial y alto para los medios de identificación electrónica expedidos en virtud del mismo.

2. Los niveles de seguridad bajo, sustancial y alto cumplirán los siguientes criterios, respectivamente:

a) el nivel de seguridad bajo se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado limitado de confianza en la identidad pretendida o declarada de una persona y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, y cuyo objetivo es reducir el riesgo de uso indebido o alteración de la identidad;

b) el nivel de seguridad sustancial se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado sustancial de confianza en la identidad pretendida o declarada de una persona y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, y cuyo objetivo es reducir sustancialmente el riesgo de uso indebido o alteración de la identidad;

c) el nivel de seguridad alto se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado de confianza en la identidad pretendida o declarada de una persona superior al medio de identificación electrónica con un nivel de seguridad sustancial, y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, cuyo objetivo es evitar el uso indebido o alteración de la identidad.

3. A más tardar el 18 de septiembre de 2015, teniendo en cuenta las normas internacionales pertinentes, y en los términos del apartado 2, la Comisión establecerá, mediante actos de ejecución, las especificaciones técnicas mínimas, las normas y los procedimientos con referencia a los cuales se especificarán los niveles de seguridad bajo, sustancial y alto de los medios de identificación electrónica a efectos del apartado 1.

Estas especificaciones técnicas mínimas, normas y procedimientos se establecerán en referencia a la fiabilidad y la calidad de los siguientes elementos:

a) el procedimiento para demostrar y comprobar la identidad de las personas físicas o jurídicas que solicitan la expedición de los medios de identificación electrónica;

b) el procedimiento para expedir los medios de identificación electrónica solicitados;

c) el mecanismo de autenticación mediante el cual la persona física o jurídica utiliza los medios de identificación electrónica para confirmar su identidad a una parte usuaria;

d) la entidad que expide los medios de identificación electrónica;

e) cualquier otro organismo que intervenga en la solicitud de expedición de los medios de identificación electrónica, y

f) las especificaciones técnicas y de seguridad de los medios de identificación electrónica.

Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

Artículo 9

Notificación

1. El Estado miembro que efectúa la notificación transmitirá a la Comisión la siguiente información y, sin dilaciones indebidas, cualquier modificación posterior de la misma:

a) una descripción del sistema de identificación electrónica, que incluya sus niveles de seguridad y el emisor o emisores de los medios de identificación electrónica en virtud de este sistema;

b) el régimen de supervisión aplicable y la información sobre el régimen de responsabilidades respecto de:

i) la parte que expida los medios de identificación electrónica, y

ii) la parte que utilice el procedimiento de autenticación;

c) la autoridad o autoridades responsables del sistema de identificación electrónica;

d) información sobre la o las entidades que gestionan el registro de los datos únicos de identificación de la persona;

e) una descripción de cómo se cumplen los requisitos de los actos de ejecución a los que se hace referencia en el artículo 12, apartado 8;

f) una descripción de la autenticación a la que se refiere la letra f) del artículo 7;

g) disposiciones relativas a la suspensión o revocación del sistema de identificación electrónica, o autenticación notificados o de las partes interesadas.

2. Un año después de la fecha de aplicación de los actos de ejecución a que hacen referencia el artículo 8, apartado 3, y el artículo 12, apartado 8, 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 del presente artículo y la información básica al respecto.

3. Si la Comisión recibe una notificación una vez haya concluido el período a que se refiere el apartado 2, publicará en el *Diario Oficial de la Unión Europea* las modificaciones de la lista a la que se hace referencia en el apartado 2 en el plazo de dos meses a partir de la fecha de recepción de dicha notificación.

4. Todo Estado miembro podrá presentar a la Comisión la solicitud de suprimir un sistema de identificación electrónica notificado por dicho Estado miembro de la lista a la que se refiere el apartado 2. La Comisión publicará en el *Diario Oficial de la Unión Europea* las modificaciones correspondientes de la lista en el plazo de un mes a partir de la fecha de recepción de la solicitud del Estado miembro.

5. La Comisión podrá, mediante actos de ejecución, definir las circunstancias, formatos y procedimientos relativos a la notificación a que se refiere el apartado 1. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

Artículo 10

Violación de la seguridad

1. En caso de que el sistema de identificación electrónica notificado con arreglo al artículo 9, apartado 1, o la autenticación a que se refiere el artículo 7, letra f), hayan sido violados o puestos parcialmente en peligro de una forma que afecte a la fiabilidad de la autenticación transfronteriza de dicho sistema, el Estado miembro que efectúa la notificación suspenderá o revocará sin dilaciones indebidas dicha autenticación transfronteriza o las partes afectadas, e informará al respecto a los demás Estados miembros y a la Comisión.

2. Cuando se haya subsanado la violación o la puesta en peligro a que se refiere el apartado 1, el Estado miembro que efectúa la notificación restablecerá la autenticación transfronteriza e informará sin dilaciones indebidas a los demás Estados miembros y a la Comisión.

3. Si la violación o la puesta en peligro a que se refiere el apartado 1 no se corrige en un plazo de tres meses a partir de la suspensión o revocación, el Estado miembro que efectúa la notificación comunicará la retirada del sistema de identificación electrónica a los demás Estados miembros y a la Comisión.

La Comisión publicará en el *Diario Oficial de la Unión Europea* las modificaciones correspondientes de la lista a que se refiere el artículo 9, apartado 2, sin dilaciones indebidas.

Artículo 11

Responsabilidad

1. El Estado miembro que efectúa la notificación será responsable de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en caso de incumplimiento de sus obligaciones en virtud de las letras d) y f) del artículo 7 en una transacción transfronteriza.

2. La parte que expida los medios de identificación electrónica será responsable de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en caso de incumplimiento de sus obligaciones en virtud de la letra e) del artículo 7 en una transacción transfronteriza.

3. La parte que realice el procedimiento de autenticación será responsable de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en caso de incumplimiento de sus obligaciones en virtud de la letra f) del artículo 7 en una transacción transfronteriza.

4. Los apartados 1, 2 y 3 se aplicarán con arreglo a las normas nacionales sobre responsabilidad.

5. Los apartados 1, 2 y 3 se entenderán sin perjuicio de la responsabilidad de las partes de acuerdo con la legislación nacional en relación con una transacción en la que se utilicen medios de identificación electrónica incluidos en el sistema de identificación electrónica notificado en virtud del artículo 9, apartado 1.

Artículo 12

Cooperación e interoperabilidad

1. Los sistemas nacionales de identificación electrónica notificados de conformidad con el artículo 9, apartado 1, serán interoperables.

2. A efectos del apartado 1, se establecerá un marco de interoperabilidad.

3. El marco de interoperabilidad debe cumplir los criterios siguientes:

a) aspirar a ser neutro desde un punto de vista tecnológico y no discriminar entre soluciones técnicas nacionales específicas para la identificación electrónica dentro del Estado miembro;

b) ajustarse a las normas internacionales y europeas, siempre que sea posible;

c) facilitar la aplicación del principio de privacidad desde el diseño, y

d) garantizar que los datos personales se procesen con arreglo a la Directiva 95/46/CE.

4. El marco de interoperabilidad consistirá en lo siguiente:

a) una referencia a los requisitos técnicos mínimos relativos a los niveles de seguridad contemplados en el artículo 8;

b) una correlación entre los niveles de seguridad nacionales de los sistemas de identificación electrónica y los niveles de seguridad contemplados en el artículo 8;

c) una referencia a los requisitos técnicos mínimos para la interoperabilidad;

d) una referencia a un conjunto mínimo de datos de identificación de la persona que representan de manera única a una persona física o jurídica, y que está disponible en los sistemas de identificación electrónica;

e) reglas de procedimiento;

f) acuerdos para la resolución de litigios, y

g) normas comunes de seguridad operativa.

5. Los Estados miembros cooperarán con respecto a lo siguiente:

a) la interoperabilidad de los sistemas de identificación electrónica notificados con arreglo al artículo 9, apartado 1, y los sistemas de identificación electrónica que los Estados miembros tienen intención de notificar, y

b) la seguridad de los sistemas de identificación electrónica.

6. La cooperación entre Estados miembros consistirá en:

a) un intercambio de información, experiencia y prácticas idóneas sobre sistemas de identificación electrónica, en particular sobre los requisitos técnicos relacionados con la interoperabilidad y los niveles de seguridad;

b) un intercambio de información, experiencia y prácticas idóneas sobre el trabajo con los niveles de seguridad de los sistemas de identificación electrónica contemplados en el artículo 8;

c) una revisión inter pares de los sistemas de identificación electrónica que entran en el ámbito de aplicación del presente Reglamento, y

d) un examen de las novedades pertinentes en el sector de la identificación electrónica.

7. A más tardar el 18 de marzo de 2015, la Comisión fijará, mediante actos de ejecución, las modalidades de procedimiento necesarias para facilitar la cooperación entre los Estados miembros a que se refieren los apartados 5 y 6, con vistas a fomentar un alto grado de confianza y seguridad que corresponda al nivel de riesgo.

8. A más tardar el 18 de septiembre de 2015, a efectos de establecer condiciones uniformes para la ejecución de los requisitos del apartado 1, la Comisión, sin perjuicio de los criterios establecidos en el apartado 3 y teniendo en cuenta los resultados de la cooperación entre Estados miembros, adoptará actos de ejecución sobre el marco de interoperabilidad tal como se establece en el apartado 4.

9. Los actos de ejecución a que se refieren los apartados 7 y 8 del presente artículo se adoptarán de conformidad con el procedimiento de examen contemplado en el artículo 48, apartado 2.

CAPÍTULO III

SERVICIOS DE CONFIANZA

SECCIÓN 1

Disposiciones generales

Artículo 13

Responsabilidad y carga de la prueba

1. Sin perjuicio de lo dispuesto en el apartado 2, los prestadores de servicios de confianza serán responsables de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en razón del incumplimiento de las obligaciones establecidas en el presente Reglamento.

La carga de la prueba de la intencionalidad o la negligencia de un prestador no cualificado de servicios de confianza corresponderá a la persona física o jurídica que alegue los perjuicios a que se refiere el primer párrafo.

Se presumirá la intencionalidad o la negligencia de un prestador cualificado de servicios de confianza salvo cuando ese prestador cualificado de servicios de confianza demuestre que los perjuicios a que se refiere el párrafo primero se produjeron sin intención ni negligencia por su parte.

2. Cuando un prestador de servicios informe debidamente a sus clientes con antelación sobre las limitaciones de la utilización de los servicios que presta y estas limitaciones sean reconocibles para un tercero, el prestador de servicios de confianza no será responsable de los perjuicios producidos por una utilización de los servicios que vaya más allá de las limitaciones indicadas.

3. Los apartados 1 y 2 se aplicarán con arreglo a las normas nacionales sobre responsabilidad.

Artículo 14

Aspectos internacionales

1. Los servicios de confianza prestados por los prestadores de servicios de confianza establecidos en un tercer país serán reconocidos como legalmente equivalentes a los servicios de confianza cualificados prestados por prestadores cualificados de servicios de confianza establecidos en la Unión si los servicios de confianza originarios del tercer país son reconocidos en virtud de un acuerdo celebrado entre la Unión y el tercer país en cuestión u organizaciones internacionales de conformidad con el artículo 218 del TFUE.

2. Los acuerdos a que se refiere el apartado 1 garantizarán, en particular, que:

a) los prestadores de servicios de confianza de terceros países u organizaciones internacionales con los que se celebren acuerdos y los servicios de confianza que prestan cumplen los requisitos aplicables a los prestadores cualificados de servicios de confianza establecidos en la Unión y a los servicios de confianza cualificados que prestan;

b) los servicios de confianza cualificados prestados por prestadores cualificados de servicios de confianza establecidos en la Unión son reconocidos como legalmente equivalentes a los servicios de confianza prestados por prestadores de servicios en terceros países u organizaciones internacionales con los que se celebran acuerdos.

Artículo 15

Accesibilidad para las personas con discapacidad

Siempre que sea factible, 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.

Artículo 16

Sanciones

Los Estados miembros establecerán normas relativas a las sanciones aplicables a las infracciones del presente Reglamento. Las sanciones previstas serán eficaces, proporcionadas y disuasorias.

SECCIÓN 2

Supervisión

Artículo 17

Organismo de supervisión

1. Los Estados miembros designarán un organismo de supervisión establecido en su territorio o, previo acuerdo mutuo con otro Estado miembro, un organismo de supervisión establecido en otro Estado miembro. Dicho organismo será responsable de las funciones de supervisión en el Estado miembro que efectúa la designación.

Los organismos de supervisión disfrutarán de las competencias necesarias y los recursos adecuados para el ejercicio de sus funciones.

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

3. Las funciones del organismo de supervisión serán las siguientes:

a) supervisar a los prestadores cualificados de servicios de confianza establecidos en el territorio del Estado miembro que lo designa a fin de garantizar, mediante actividades de supervisión previas y posteriores, que dichos prestadores cualificados de servicios de confianza, y los servicios de confianza cualificados prestados por ellos, cumplen los requisitos establecidos en el presente Reglamento;

b) adoptar medidas, en caso necesario, en relación con los prestadores no cualificados de servicios de confianza establecidos en el territorio del Estado miembro que lo designa, mediante actividades de supervisión posteriores, cuando reciba la información de que dichos prestadores no cualificados de servicios de confianza, o los servicios de confianza prestados por ellos, supuestamente no cumplen los requisitos establecidos en el presente Reglamento.

4. Para los fines del apartado 3, y con sujeción a las limitaciones establecidas en el mismo, las funciones del organismo de supervisión incluirá, en particular:

a) cooperar con otros organismos y prestarles asistencia de conformidad con el artículo 18;

b) analizar los informes de evaluación de la conformidad a que se refieren el artículo 20, apartado 1, y el artículo 21, apartado 1;

c) informar a otros organismos de supervisión y al público de la violación de seguridad o la pérdida de integridad, de conformidad con el artículo 19, apartado 2;

d) informar a la Comisión de sus actividades principales de conformidad con el apartado 6 del presente artículo;

e) realizar auditorías o solicitar a un organismo de evaluación de la conformidad que realice una evaluación de la conformidad de prestadores cualificados de servicios de confianza, con arreglo al artículo 20, apartado 2;

f) cooperar con las autoridades de protección de datos, en particular, informándoles, sin demora indebida, de los resultados de las auditorías de los prestadores cualificados de servicios de confianza, en caso de posible infracción de las normas sobre protección de datos personales;

g) conceder la cualificación a los prestadores de servicios de confianza y a los servicios de confianza que prestan, y retirar esta cualificación, con arreglo a los artículos 20 y 21;

h) comunicar al organismo responsable de la lista de confianza a que se refiere el artículo 22, apartado 3, de su decisión de conceder o retirar la cualificación, salvo si dicho organismo es también el organismo de supervisión;

i) verificar la existencia y la correcta aplicación de las disposiciones relativas a los planes de cese en caso de que los prestadores de servicios de confianza cesen sus actividades, con inclusión de la forma en que se hace accesible la información, con arreglo al artículo 24, apartado 2, letra h);

j) requerir que los prestadores de servicios de confianza corrijan cualquier incumplimiento de los requisitos establecidos en el presente Reglamento.

5. Los Estados miembros podrán disponer que el organismo de supervisión establezca, mantenga y actualice una infraestructura de confianza de conformidad con las condiciones establecidas en la legislación nacional.

6. A más tardar el 31 de marzo de cada año, cada organismo de supervisión presentará a la Comisión un informe sobre sus actividades principales del año civil precedente junto con un resumen de las notificaciones de violación recibidas de los prestadores de servicios de confianza, de conformidad con el artículo 19, apartado 2.

7. La Comisión pondrá a disposición de los Estados miembros el informe anual a que se refiere el apartado 6.

8. La Comisión podrá, mediante actos de ejecución, definir los formatos y procedimientos relativos al informe a que se refiere el apartado 6. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

Artículo 18

Asistencia mutua

1. Los organismos de supervisión cooperarán con vistas a intercambiar prácticas idóneas.

Un organismo de supervisión, previa solicitud justificada de otro organismo de supervisión, deberá prestar asistencia a dicho organismo con el fin de que las actividades de los organismos de supervisión pueden realizarse en forma coherente. La asistencia mutua podrá incluir, 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 los informes de evaluación de la conformidad a que se refieren los artículos 20 y 21.

2. El organismo de supervisión al que se haya dirigido una solicitud de asistencia podrá denegar dicha solicitud por alguno de los motivos siguientes:

a) el organismo de supervisión no es competente para prestar la asistencia solicitada;

b) la asistencia solicitada no guarda proporción con las actividades de supervisión del organismo de supervisión realizadas de conformidad con el artículo 17;

c) la prestación de la asistencia solicitada sería incompatible con el presente Reglamento.

3. Cuando proceda, los Estados miembros podrán autorizar a sus respectivos organismos de supervisión para que lleven a cabo investigaciones conjuntas con participación de personal de los organismos de supervisión de otros Estados miembros. Los acuerdos y procedimientos para dichas actividades conjuntas serán aprobadas y establecidas por los Estados miembros de que se trate de conformidad con sus legislaciones nacionales.

Artículo 19

Requisitos de seguridad aplicables a los prestadores de servicios de confianza

1. Los prestadores cualificados y no cualificados de servicios de confianza adoptarán las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que prestan. Habida cuenta de los últimos avances tecnológicos, dichas medidas garantizarán un nivel de seguridad proporcionado 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 cualquiera de tales incidentes.

2. Los prestadores cualificados y no cualificados de servicios de confianza, sin demoras indebidas pero en cualquier caso en un plazo de 24 horas tras tener conocimiento de ellas, notificarán al organismo de supervisión y, en caso pertinente, a otros organismo relevantes como el organismo nacional competente en materia de seguridad de la información, o la autoridad de protección de datos, cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de confianza prestado o en los datos personales correspondientes.

Cuando la violación de seguridad o la pérdida de integridad puedan atentar contra una persona física o jurídica a la que se ha prestado el servicio de confianza, el prestador de servicios de confianza notificará también a la persona física o jurídica, sin demora indebida, la violación de seguridad o la pérdida de integridad.

Cuando proceda, en particular si una violación de la seguridad o pérdida de la integridad afecta a dos o más Estados miembros, el organismo de supervisión notificado informará al respecto a los organismos de supervisión de los demás Estados miembros de que se trate y a la ENISA.

El organismo de supervisión notificado informará al público o exigirá al prestador de servicios de confianza que lo haga, en caso de considerar que la divulgación de la violación de seguridad o la pérdida de integridad reviste interés público.

3. El organismo de supervisión facilitará a la ENISA anualmente un resumen de las notificaciones de violación de la seguridad y pérdida de la integridad recibidas de los prestadores de servicios de confianza.

4. La Comisión podrá, mediante actos de ejecución, establecer:

a) una mayor especificación de las medidas a que se refiere el apartado 1, y

b) la definición de los formatos y procedimientos, incluidos los plazos, aplicables a efectos del apartado 2.

Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

SECCIÓN 3

Servicios de confianza cualificados

Artículo 20

Supervisión de los prestadores cualificados de servicios de confianza

1. Los prestadores cualificados de servicios de confianza serán auditados, al menos cada 24 meses, corriendo con los gastos que ello genere, por un organismo de evaluación de la conformidad. La finalidad de la auditoría será confirmar que tanto los prestadores cualificados de servicios de confianza como los servicios de confianza cualificados que prestan cumplen los requisitos establecidos en el presente Reglamento. Los prestadores cualificados de servicios de confianza enviarán el informe de evaluación de la conformidad correspondiente al organismo de supervisión en el plazo de tres días hábiles tras su recepción.

2. Sin perjuicio de lo dispuesto en el apartado 1, el organismo de supervisión podrá en cualquier momento auditar o solicitar a un organismo de evaluación de la conformidad que realice una evaluación de conformidad de los prestadores cualificados de servicios de confianza, corriendo con los gastos dichos prestadores de servicios de confianza, para confirmar que tanto ellos como los servicios de confianza cualificados que prestan cumplen los requisitos del presente Reglamento. En caso de posible infracción de las normas sobre protección de datos personales, el organismo de supervisión informará a las autoridades de protección de datos de los resultados de sus auditorías.

3. Cuando el organismo de supervisión requiera a un prestador cualificado de servicios de confianza que corrija el incumplimiento de requisitos del presente Reglamento y este prestador no actúe en consecuencia, en su caso, en el plazo fijado por el organismo de supervisión, el organismo de supervisión, teniendo en cuenta en particular el alcance, la duración y las consecuencias de este incumplimiento, podrá retirar la cualificación al prestador o al servicio que este presta e informar al organismo a que se refiere el artículo 22, apartado 3, a efectos de que se actualice la lista de confianza mencionada en el artículo 22, apartado 1. El organismo de supervisión comunicará al prestador cualificado de servicios de confianza la retirada de su cualificación o de la cualificación del servicio de que se trate.

4. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de las siguientes normas:

a) para la acreditación de los organismos de evaluación de la conformidad y para el informe de evaluación de la conformidad a que se refiere el apartado 1;

b) sobre las disposiciones en materia de auditoría con arreglo a las cuales los organismos de evaluación de la conformidad realizarán la evaluación de la conformidad de los prestadores cualificados de servicios de confianza a que se refiere el apartado 1.

Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

Artículo 21

Inicio de un servicio de confianza cualificado

1. Cuando los prestadores de servicios de confianza, sin cualificación, tengan intención de iniciar la prestación de servicios de confianza cualificados, presentarán al organismo de supervisión una notificación de su intención junto con un informe de evaluación de la conformidad expedido por un organismo de evaluación de la conformidad.

2. El organismo de supervisión verificará si el prestador de servicios de confianza y los servicios de confianza que presta cumplen los requisitos establecidos en el presente Reglamento, y en particular, los requisitos establecidos para los prestadores cualificados de servicios de confianza y para los servicios de confianza cualificados que estos prestan.

Si el organismo de supervisión concluye que el prestador de servicios de confianza y los servicios de confianza que este presta cumplen los requisitos a que se refiere el párrafo primero, el organismo de supervisión concederá la cualificación al prestador de servicios de confianza y a los servicios de confianza que este presta y lo comunicará al organismo a que se refiere el artículo 22, apartado 3, a efectos de actualizar las listas de confianza a que se refiere el artículo 22, apartado 1, a más tardar tres meses después de la notificación de conformidad con el apartado 1 del presente artículo.

Si la verificación no ha concluido en el plazo de tres meses, el organismo de supervisión informará al prestador de servicios de confianza especificando los motivos de la demora y el plazo previsto para concluir la verificación.

3. Los prestadores cualificados de servicios de confianza podrán comenzar a prestar el servicio de confianza cualificado una vez que la cualificación haya sido indicada en las listas de confianza a que se refiere el artículo 22, apartado 1.

4. La Comisión podrá, mediante actos de ejecución, definir los formatos y procedimientos a efectos de los apartados 1 y 2. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

Artículo 22

Listas de confianza

1. Cada Estado miembro establecerá, mantendrá y publicará listas de confianza con información relativa a los prestadores cualificados de servicios de confianza con respecto a los cuales sea responsable, 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 a que se refiere 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. A más tardar el 18 de septiembre de 2015 la Comisión, mediante actos de ejecución, especificará la información a que se refiere el apartado 1 y definirá 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 48, apartado 2.

Artículo 23

Etiqueta de confianza «UE» para servicios de confianza cualificados

1. Una vez que la cualificación a que se refiere el artículo 21, apartado 2, párrafo segundo, se haya incluido en la lista de confianza a que se refiere el artículo 22, apartado 1, los prestadores cualificados de los servicios de confianza podrán usar la etiqueta de confianza «UE» para indicar de manera simple, reconocible y clara los servicios de confianza cualificados que prestan.

2. Al utilizar la etiqueta de confianza «UE» para los servicios de confianza cualificados a que se refiere el apartado 1, los prestadores de los servicios de confianza garantizarán que en su sitio web exista un enlace a la lista de confianza pertinente.

3. A más tardar el 1 de julio de 2015 la Comisión, por medio de actos de ejecución, elaborará especificaciones relativas a la forma y en particular la presentación, composición, tamaño y diseño de la etiqueta de confianza «UE» para servicios de confianza cualificados. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

Artículo 24

Requisitos para los prestadores cualificados de servicios de confianza

1. Al expedir un certificado cualificado para un servicio de confianza, un prestador cualificado de servicios de confianza 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.

La información a que se refiere el párrafo primero será verificada por el prestador de servicios de confianza bien directamente o bien por medio de un tercero de conformidad con el Derecho nacional:

a) en presencia de la persona física o de un representante autorizado de la persona jurídica, o

b) a distancia, utilizando medios de identificación electrónica, para los cuales se haya garantizado la presencia de la persona física o de un representante autorizado de la persona jurídica previamente a la expedición del certificado cualificado, y que cumplan los requisitos establecidos con el artículo 8 con respecto a los niveles de seguridad «sustancial» o «alto», o

c) por medio de un certificado de una firma electrónica cualificada o de un sello electrónico cualificado expedido de conformidad con la letra a) o b), o

d) utilizando otros métodos de identificación reconocidos a escala nacional que aporten una seguridad equivalente en términos de fiabilidad a la presencia física. La seguridad equivalente será confirmada por un organismo de evaluación de la conformidad.

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

a) informarán al organismo de supervisión de cualquier cambio en la prestación de servicios de confianza cualificados, y de su intención de cesar tales actividades;

b) contarán con personal y, si procede, con subcontratistas, que posean los conocimientos especializados, la fiabilidad, la experiencia y las cualificaciones necesarios y hayan recibido la formación adecuada en materia de seguridad y normas de protección de datos personales y que apliquen procedimientos administrativos y de gestión que correspondan a normas europeas o internacionales;

c) con respecto al riesgo de la responsabilidad por daños y perjuicios de conformidad con el artículo 13, mantendrán recursos financieros suficientes u obtendrán pólizas de seguros de responsabilidad adecuadas, de conformidad con la legislación nacional;

d) antes de entrar en una relación contractual, informarán, de manera clara y comprensible, a cualquier persona que desee utilizar un servicio de confianza cualificado acerca de las condiciones precisas relativas a la utilización de dicho servicio, incluidas las limitaciones de su utilización;

e) utilizarán sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad y la fiabilidad técnicas de los procesos que sustentan;

f) utilizarán sistemas fiables para almacenar los datos que se les faciliten de forma verificable, de modo que:

i) estén a disposición del público para su recuperación solo cuando se haya obtenido el consentimiento de la persona a la que corresponden los datos,

ii) solo personas autorizadas puedan hacer anotaciones y modificaciones en los datos almacenados,

iii) pueda comprobarse la autenticidad de los datos;

g) tomarán medidas adecuadas contra la falsificación y el robo de datos;

h) registrarán y mantendrán accesible durante un período de tiempo apropiado, incluso cuando hayan cesado las actividades del prestador cualificado de servicios de confianza, toda la información pertinente referente a los datos expedidos y recibidos por el prestador cualificado de servicios de confianza, en particular al objeto de que sirvan de prueba en los procedimientos legales y para garantizar la continuidad del servicio. Esta actividad de registro podrá realizarse por medios electrónicos;

i) contarán con un plan de cese actualizado para garantizar la continuidad del servicio, de conformidad con las disposiciones verificadas por el organismo de supervisión con arreglo al artículo 17, apartado 4, letra i);

j) garantizarán un tratamiento lícito de los datos personales de conformidad con la Directiva 95/46/CE;

k) en caso de los prestadores cualificados de servicios de confianza que expidan certificados cualificados, establecerán y mantendrán actualizada una base de datos de certificados.

3. Cuando los prestadores cualificados de servicios de confianza que expidan certificados cualificados decidan revocar un certificado, registrarán su revocación en su base de datos de certificados y publicarán el estado de revocación del certificado oportunamente y, en todo caso, en un plazo de 24 horas después de la recepción de la solicitud. La revocación será efectiva inmediatamente después de su publicación.

4. Con respecto a lo dispuesto en el apartado 3, los prestadores cualificados de servicios de confianza que expidan certificados cualificados proporcionarán a cualquier parte usuaria información sobre el estado de validez o revocación de los certificados cualificados expedidos por ellos. Esta información deberá estar disponible al menos por cada certificado en cualquier momento y con posterioridad al período de validez del 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 fiables que cumplan con los requisitos establecidos las letras e) y f) del apartado 2 del presente artículo. Se presumirá el cumplimiento de los requisitos establecidos en el presente artículo cuando los sistemas y productos fiables cumplan dichas normas. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

SECCIÓN 4

Firma electrónica

Artículo 25

Efectos jurídicos de las firmas electrónicas

1. No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla los requisitos de la firma electrónica cualificada.

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

3. Una firma electrónica cualificada basada en un certificado cualificado emitido en un Estado miembro será reconocida como una firma electrónica cualificada en todos los demás Estados miembros.

Artículo 26

Requisitos para firmas electrónicas avanzadas

Una firma electrónica avanzada cumplirá 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 firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.

Artículo 27

Firmas electrónicas en servicios públicos

1. Si un Estado miembro requiere una firma electrónica avanzada con el fin de utilizar un servicio en línea ofrecido por un organismo del sector público, o en nombre del mismo, dicho Estado miembro reconocerá las firmas electrónicas avanzadas, las firmas electrónicas avanzadas basadas en un certificado cualificado de firma electrónica y las firmas electrónicas cualificadas por lo menos en los formatos o con los métodos definidos en los actos de ejecución contemplados en el apartado 5.

2. Si un Estado miembro requiere una firma electrónica avanzada basada en un certificado cualificado con el fin de utilizar un servicio en línea ofrecido por un organismo del sector público, o en nombre del mismo, dicho Estado miembro reconocerá las firmas electrónicas avanzadas basadas en un certificado cualificado y las firmas electrónicas cualificadas por lo menos en los formatos o con los métodos definidos en los actos de ejecución contemplados en el apartado 5.

3. Los Estados miembros no exigirán para la utilización transfronteriza de 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.

4. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a firmas electrónicas avanzadas. Se presumirá el cumplimiento de los requisitos de las firmas electrónicas avanzadas mencionadas en los apartados 1 y 2 del presente artículo y en el artículo 26 cuando una firma electrónica avanzada se ajuste a dichas normas. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

5. A más tardar el 18 de septiembre de 2015, y teniendo en cuenta las prácticas, normas y actos jurídicos de la Unión existentes, la Comisión, mediante actos de ejecución, definirá los formatos de referencia de las firmas electrónicas avanzadas o métodos de referencia cuando se utilicen formatos alternativos. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

Artículo 28

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. Los certificados cualificados de firmas electrónicas podrán incluir atributos específicos adicionales no obligatorios. Esos atributos no afectarán a la interoperabilidad y el reconocimiento de las firmas electrónicas cualificadas.

4. Si un certificado cualificado de firma electrónica ha sido revocado después de su activación inicial, perderá su validez desde el momento de su revocación y no podrá en ninguna circunstancia recuperar su estado.

5. Según las condiciones que siguen, los Estados miembros podrán fijar normas nacionales sobre la suspensión temporal de certificados cualificados de firma electrónica:

a) Si un certificado cualificado de firma electrónica ha sido suspendido temporalmente, ese certificado perderá su validez durante el período de suspensión.

b) El período de suspensión se indicará claramente en la base de datos de certificados y el estado de suspensión será visible, durante el período de suspensión, a partir del servicio que proporcione la información sobre el estado del certificado.

6. 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 48, apartado 2.

Artículo 29

Requisitos de los dispositivos cualificados de creación de firmas electrónicas

1. Los dispositivos cualificados de creación de firmas electrónicas 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 cualificados de creación de firmas electrónicas. Se presumirá el cumplimiento de los requisitos establecidos en el anexo II cuando un dispositivo cualificado de creación de firmas electrónicas se ajuste a dichas normas. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

Artículo 30

Certificación de los dispositivos cualificados de creación de firmas electrónicas

1. La conformidad de los dispositivos cualificados de creación de firmas electrónicas con los requisitos que figuran en el anexo II será certificada por los organismos públicos o privados adecuados designados por los Estados miembros.

2. Los Estados miembros notificarán a la Comisión los nombres y direcciones de los organismos públicos o privados a que se refiere el apartado 1. La Comisión pondrá la información a disposición de los Estados miembros.

3. La certificación contemplada en el apartado 1 se basará en los elementos siguientes:

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 la lista que se establecerá de conformidad con el párrafo segundo, o

b) un proceso distinto del proceso contemplado en la letra a), con tal de que ese proceso haga uso de niveles de seguridad equivalentes y que los organismos públicos o privados a los que se refiere el apartado 1 notifiquen ese proceso a la Comisión. Podrá recurrirse a ese proceso únicamente a falta de las normas a que se refiere la letra a) o cuando esté en curso el proceso de evaluación de la seguridad a que se refiere la letra a).

La Comisión establecerá, por medio de actos de ejecución, la lista de las normas para la evaluación de la seguridad de los productos de tecnología de la información a que se refiere la letra a). Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

4. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 47, en lo que respecta al establecimiento de criterios específicos que deben satisfacer los organismos designados a que se refiere el apartado 1 del presente artículo.

Artículo 31

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

1. Los Estados miembros comunicarán a la Comisión, sin retrasos indebidos y no más tarde de un mes después de que haya concluido la certificación, información sobre los dispositivos cualificados de creación de firmas electrónicas que hayan sido certificados por los organismos a que se refiere el artículo 30, apartado 1. También notificarán a la Comisión, sin retrasos indebidos y no más tarde de un mes después de que haya expirado la certificación, 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 cualificados de creación de firmas electrónicas certificados.

3. La Comisión podrá, mediante actos de ejecución, definir los 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 48, apartado 2.

Artículo 32

Requisitos de la validación de las firmas electrónicas cualificadas

1. El proceso de validación de una firma electrónica cualificada confirmará la validez de una firma electrónica cualificada siempre que:

a) el certificado que respalda la firma fuera, en el momento de la firma, un certificado cualificado de firma electrónica que se ajusta al anexo I;

b) el certificado cualificado fuera emitido por un prestador de servicios de confianza y fuera válido en el momento de la firma;

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

d) el conjunto único de datos que representa al firmante en el certificado se facilite correctamente a la parte usuaria;

e) en caso de que se utilice un seudónimo, la utilización del mismo se indique claramente a la parte usuaria en el momento de la firma;

f) la firma electrónica se haya creado mediante un dispositivo cualificado de creación de firmas electrónicas;

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

h) se hayan cumplido los requisitos previstos en el artículo 26, en el momento de la firma.

2. El sistema utilizado para validar la firma electrónica cualificada ofrecerá a la parte usuaria el resultado correcto del proceso de validación y le permitirá detectar cualquier problema que afecte a la seguridad.

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 48, apartado 2.

Artículo 33

Servicio de validación cualificado de firmas electrónicas cualificadas

1. Solo podrá prestar un servicio de validación cualificado de firmas electrónicas cualificadas el prestador cualificado de servicios de confianza que:

a) realice la validación de conformidad con el artículo 32, apartado 1, y

b) permita que las partes usuarias reciban el resultado del proceso de validación de una manera automatizada que sea fiable, eficiente e incluya la firma electrónica avanzada o el sello electrónico avanzado del prestador cualificado de servicio de validación.

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 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 48, apartado 2.

Artículo 34

Servicio cualificado de conservación de firmas electrónicas cualificadas

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

2. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas al servicio cualificado de conservación de firmas electrónicas cualificadas. Se presumirá el cumplimiento de los requisitos establecidos en el apartado 1 cuando los mecanismos del servicio cualificado de conservación de firmas electrónicas cualificadas se ajusten a dichas normas. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

SECCIÓN 5

Sellos electrónicos

Artículo 35

Efectos jurídicos del sello electrónico

1. No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un sello electrónico por el mero hecho de estar en formato electrónico o de no cumplir los requisitos del sello electrónico cualificado.

2. Un sello electrónico cualificado disfrutará de la presunción de integridad de los datos y de la corrección del origen de los datos a los que el sello electrónico cualificado esté vinculado.

3. Un sello electrónico cualificado basado en un certificado cualificado emitido en un Estado miembro será reconocido como un sello electrónico cualificado en todos los demás Estados miembros.

Artículo 36

Requisitos para los sellos electrónicos avanzados

Un sello electrónico avanzado cumplirá 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.

Artículo 37

Sellos electrónicos en servicios públicos

1. Si un Estado miembro requiere un sello electrónico avanzado con el fin de utilizar un servicio en línea ofrecido por un organismo del sector público, o en nombre del mismo, dicho Estado miembro reconocerá los sellos electrónicos avanzados, los sellos electrónicos avanzados basados en un certificado reconocido de sellos electrónicos y los sellos electrónicos cualificados por lo menos en los formatos o con los métodos definidos en los actos de ejecución contemplados en el apartado 5.

2. Si un Estado miembro requiere un sello electrónico avanzado basado en un certificado cualificado con el fin de utilizar un servicio en línea ofrecido por un organismo del sector público, o en nombre del mismo, dicho Estado miembro reconocerá los sellos electrónicos avanzados basados en un certificado cualificado y los sellos electrónicos cualificados por lo menos en los formatos o con los métodos definidos en los actos de ejecución contemplados en el apartado 5.

3. Los Estados miembros no exigirán, para el uso transfronterizo en un servicio en línea ofrecido por un organismo del sector público, un sello electrónico cuyo nivel de seguridad sea superior al de un sello electrónico cualificado.

4. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a los sellos electrónicos avanzados. Se presumirá el cumplimiento de los requisitos de los sellos electrónicos avanzados mencionados en los apartados 1 y 2 del presente artículo y en el artículo 36 cuando un sello electrónico avanzado se ajuste a dichas normas. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

5. A más tardar el 18 de septiembre de 2015, y teniendo en cuenta las prácticas existentes, las normas y actos jurídicos de la Unión, la Comisión adoptará actos de ejecución que definan los formatos de referencia de los sellos electrónicos avanzados o métodos de referencia cuando se utilicen formatos alternativos. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

Artículo 38

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. Los certificados cualificados de sello electrónico podrán incluir atributos específicos adicionales no obligatorios. Esos atributos no afectarán a la interoperabilidad y reconocimiento de los sellos electrónicos cualificados.

4. Si un certificado cualificado de sello electrónico ha sido revocado después de su activación inicial, perderá su validez desde el momento de su revocación y no podrá en ninguna circunstancia recuperar su estado.

5. Según las condiciones expuestas a continuación, los Estados miembros podrán fijar normas nacionales sobre la suspensión temporal de certificados cualificados de sello electrónico:

a) Si un certificado cualificado de sello electrónico ha sido suspendido temporalmente, ese certificado perderá su validez durante el período de suspensión.

b) El período de suspensión se indicará claramente en la base de datos de certificados y el estado de suspensión será visible, durante el período de suspensión, a partir del servicio que proporcione la información sobre el estado del certificado.

6. 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 48, apartado 2.

Artículo 39

Dispositivos cualificados de creación de sello electrónico

1. El artículo 29 se aplicará *mutatis mutandis* a los requisitos de los dispositivos cualificados de creación de sello electrónico.

2. El artículo 30 se aplicará *mutatis mutandis* a la certificación de los dispositivos cualificados de creación de sello electrónico.

3. El artículo 31 se aplicará *mutatis mutandis* a la publicación de una lista de dispositivos cualificados de creación de sello electrónico certificados.

Artículo 40

Validación y conservación de sellos electrónicos cualificados

Los artículos 32, 33 y 34 se aplicarán *mutatis mutandis* a la validación y conservación de los sellos electrónicos cualificados.

SECCIÓN 6

Sello de tiempo electrónico

Artículo 41

Efecto jurídico de los sellos de tiempo electrónicos

1. No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un sello de tiempo electrónico por el mero hecho de estar en formato electrónico o de no cumplir los requisitos de sello cualificado de tiempo electrónico.

2. Los sellos cualificados de tiempo electrónicos disfrutarán de una presunción de exactitud de la fecha y hora que indican y de la integridad de los datos a los que la fecha y hora estén vinculadas.

3. Un sello cualificado de tiempo electrónico emitido en un Estado miembro será reconocido como sello cualificado de tiempo electrónico en todos los Estados miembros.

Artículo 42

Requisitos de los sellos cualificados de tiempo electrónicos

1. Un sello cualificado de tiempo electrónico cumplirá los requisitos siguientes:

a) vincular la fecha y hora con los datos de forma que se elimine razonablemente la posibilidad de modificar los datos sin que se detecte;

b) basarse en una fuente de información temporal vinculada al Tiempo Universal Coordinado, y

c) haber sido firmada mediante el uso de una firma electrónica avanzada o sellada con un sello electrónico avanzado del prestador cualificado de servicios de confianza o por cualquier método equivalente.

2. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a la vinculación de la fecha y hora con los datos y a una fuente de información temporal exacta. Se presumirá el cumplimiento de los requisitos establecidos en el apartado 1 cuando la vinculación de la fecha y hora con los datos y la 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 48, apartado 2.

SECCIÓN 7

Servicio de entrega electrónica certificada

Artículo 43

Efecto jurídico de un servicio de entrega electrónica certificada

1. A los datos enviados y recibidos mediante un servicio de entrega electrónica certificada no se les denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales por el mero hecho de que estén en formato electrónico o no cumplan los requisitos de servicio cualificado de entrega electrónica certificada.

2. Los datos enviados y recibidos mediante un servicio cualificado de entrega electrónica certificada disfrutarán de la presunción de la integridad de los datos, el envío de dichos datos por el remitente identificado, la recepción por el destinatario identificado y la exactitud de la fecha y hora de envío y recepción de los datos que indica el servicio cualificado de entrega electrónica certificada.

Artículo 44

Requisitos de los servicios cualificados de entrega electrónica certificada

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

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

b) asegurar con un alto nivel de fiabilidad la identificación del remitente;

c) garantizar la identificación del destinatario antes de la entrega de los datos;

d) estar protegidos el envío y recepción de datos por una firma electrónica avanzada o un sello electrónico avanzado de un prestador cualificado de servicios de confianza de tal forma que se impida la posibilidad de que se modifiquen los datos sin que se detecte;

e) 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;

f) indicar mediante un sello cualificado de tiempo electrónico la fecha y hora de envío, recepción y eventual modificación de los datos.

En caso de que los datos se transfieran entre dos o más prestadores cualificados de servicios de confianza, se aplicarán los requisitos establecidos en las letras a) a f) a todos los prestadores cualificados de servicios de confianza.

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 48, apartado 2.

SECCIÓN 8

Autenticación de sitios web

Artículo 45

Requisitos de 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. 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 48, apartado 2.

CAPÍTULO IV

DOCUMENTOS ELECTRÓNICOS

Artículo 46

Efectos jurídicos de los documentos electrónicos

No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un documento electrónico por el mero hecho de estar en formato electrónico.

CAPÍTULO V

DELEGACIÓN DE PODERES Y DISPOSICIONES DE EJECUCIÓN

Artículo 47

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 refiere el artículo 30, apartado 4, se otorgarán a la Comisión para un período indefinido a más tardar el 17 de septiembre de 2014.

3. La delegación de poderes a que se refiere el artículo 30, apartado 4, podrá ser revocada en todo momento por el Parlamento Europeo o 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. Los actos delegados adoptados con arreglo al artículo 30, apartado 4, entrarán en vigor únicamente en caso de que ni el Parlamento Europeo ni el Consejo hayan manifestado objeción alguna en un plazo de dos meses a partir de la notificación de dicho acto a ambas instituciones o en caso de que, antes de que expire dicho plazo, el Parlamento Europeo y el Consejo hayan informado a la Comisión de que no manifestarán objeción alguna. El plazo se prorrogará dos meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 48

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 49

Revisión

La Comisión revisará la aplicación del presente Reglamento e informará al Parlamento Europeo y al Consejo a más tardar el 1 de julio de 2020. La Comisión evaluará en particular si es apropiado modificar el ámbito de aplicación del presente Reglamento o sus disposiciones específicas, incluidos el artículo 6, la letra f) del artículo 7 y los artículos 34, 43, 44 y 45, teniendo en cuenta la experiencia adquirida en la aplicación del presente Reglamento, así como la evolución tecnológica, del mercado y jurídica.

El informe mencionado en el párrafo primero irá acompañado, en caso necesario, de propuestas legislativas.

Asimismo, la Comisión presentará un informe al Parlamento Europeo y al Consejo cada cuatro años tras el informe mencionado en el párrafo primero sobre la marcha hacia el logro de los objetivos del presente Reglamento.

Artículo 50

Derogación

1. Queda derogada la Directiva 1999/93/CE con efectos a partir del 1 de julio de 2016.

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

Artículo 51

Medidas transitorias

1. 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 cualificados de creación de firma electrónica con arreglo al presente Reglamento.

2. Los certificados reconocidos expedidos para las personas físicas conforme a la Directiva 1999/93/CE se considerarán certificados cualificados de firma electrónica con arreglo al presente Reglamento hasta que caduquen.

3. Un prestador de servicios de certificación que emita certificados reconocidos conforme a la Directiva 1999/93/CE presentará un informe de evaluación de conformidad al organismo supervisor lo antes posible pero no más tarde del 1 de julio de 2017. Hasta que el prestador de servicios de certificación presente dicho informe de evaluación de conformidad y el organismo supervisor ultime su análisis, el mencionado prestador de servicios de certificación será considerado, según el presente Reglamento, como prestador cualificado de servicios de confianza.

4. Si un prestador de servicios de certificación que emita certificados reconocidos conforme a la Directiva 1999/93/CE no presentara un informe de evaluación de conformidad al organismo supervisor dentro del plazo mencionado en el apartado 3, dicho prestador de servicios de certificación no podrá ser considerado, según el presente Reglamento, como prestador cualificado de servicios de confianza a partir del 2 de julio de 2017.

Artículo 52

Entrada en vigor

1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

2. El presente Reglamento será aplicable a partir del 1 de julio de 2016, a excepción de las disposiciones siguientes:

a) los artículos 8, apartado 3, 9, apartado 5, 12, apartados 2 a 9, 17, apartado 8, 19, apartado 4, 20, apartado 4, 21, apartado 4, 22, apartado 5, 23, apartado, 3, 24, apartado 5, 27, apartados 4 y 5, 28, apartado 6, 29, apartado 2, 30, apartados 3 y 4, 31, apartado 3, 32, apartado 3, 33, apartado 2, 34, apartado 2, 37, apartados 4 y 5, 38, apartado 6, 42, apartado 2, 44, apartado 2, 45, apartado 2, y los artículos 47 y 48 se aplicarán a partir del 17 de septiembre de 2014;

b) el artículo 7, el artículo 8, apartados 1 y 2, los artículos 9, 10, 11 y el artículo 12, apartado 1, se aplicarán a partir de la fecha de aplicación de los actos de ejecución previstos en los artículos 8, apartado 3, y 12, apartado 8;

c) el artículo 6 se aplicará a partir de los tres años de la fecha de aplicación de los actos de ejecución previstos en los artículos 8, apartado 3, y 12, apartado 8.

3. Cuando el sistema de identificación electrónica notificado esté incluido en la lista publicada por la Comisión con arreglo al artículo 9 antes de la fecha mencionada en la letra c) del apartado 2 del presente artículo, el reconocimiento de los medios de identificación electrónica expedidos bajo dicho sistema en virtud del artículo 6 se llevará a cabo a más tardar 12 meses después de la publicación de dicho sistema, pero no antes de la fecha mencionada en la letra c) del apartado 2 del presente artículo.

4. No obstante lo dispuesto en la letra c) del apartado 2 del presente artículo, un Estado miembro podrá decidir que los medios de identificación electrónica con arreglo al sistema de identificación electrónica notificado de conformidad con el artículo 9, apartado 1, por otro Estado miembro se reconozcan en el primer Estado miembro a partir de la fecha de aplicación de los actos de ejecución previstos en los artículos 8, apartado 3, y 12, apartado 8. Los Estados miembros de que se trate se lo comunicarán a la Comisión. La Comisión hará pública esa información.

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

Hecho en Bruselas, el 23 de julio de 2014.

Por el Parlamento	*Por el Consejo*
El Presidente	*El Presidente*
M. SCHULZ	S. GOZI

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 prestador cualificado de servicios de confianza que expide los certificados cualificados, incluyendo como mínimo el Estado miembro en el que dicho prestador está establecido, y

— para personas jurídicas: el nombre y, cuando proceda, el número de registro según consten en los registros oficiales,

— para personas físicas, el nombre de la persona;

c) al menos el nombre del firmante o un seudónimo; si se usara un seudónimo, se indicará claramente;

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 prestador cualificado de servicios de confianza;

g) la firma electrónica avanzada o el sello electrónico avanzado del prestador 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 que pueden utilizarse para consultar el estado de validez del certificado cualificado;

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

ANEXO II

REQUISITOS DE LOS DISPOSITIVOS CUALIFICADOS DE CREACIÓN DE FIRMA ELECTRÓNICA

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

   a) esté garantizada razonablemente la confidencialidad de los datos de creación de firma electrónica utilizados para la creación de firmas electrónicas;

   b) los datos de creación de firma electrónica utilizados para la creación de firma electrónica solo puedan aparecer una vez en la práctica;

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

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

2. Los dispositivos cualificados de creación de firmas electrónicas 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 solo podrán correr a cargo de un prestador cualificado de servicios de confianza.

4. Sin perjuicio de la letra d) del punto 1, los prestadores cualificados de servicios de confianza que gestionen los datos de creación de firma electrónica en nombre del firmante podrán duplicar los datos de creación de firma únicamente con objeto de efectuar una copia de seguridad de los citados datos siempre que se cumplan los siguientes requisitos:

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

   b) el número de conjuntos de datos duplicados 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 prestador cualificado de servicios de confianza que expide los certificados cualificados, incluyendo como mínimo el Estado miembro en el que dicho prestador está establecido, y

— para personas jurídicas: el nombre y, cuando proceda, el número de registro según consten en los registros oficiales,

— para personas físicas, el nombre de la persona;

c) al menos, el nombre del creador del sello y, cuando proceda, 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 prestador cualificado de servicios de confianza;

g) la firma electrónica avanzada o el sello electrónico avanzado del prestador 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 que pueden utilizarse para consultar 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 cualificado de creación de sellos electrónicos, 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 sitio web;

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

— para personas jurídicas: el nombre y, cuando proceda, el número de registro según consten en los registros oficiales,

— para personas físicas, el nombre de la persona;

c) para personas físicas: al menos el nombre de la persona a la que se expida el certificado, o un seudónimo; si se usara un seudónimo, se indicará claramente;

para personas jurídicas: al menos el nombre de la persona jurídica a la que se expida el certificado y, cuando proceda, 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, de la persona física o jurídica a quien se expida el certificado, y, cuando proceda, según figure en los registros oficiales;

e) el nombre o los nombres de dominio explotados por la persona física o jurídica 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 prestador cualificado de servicios de confianza;

h) la firma electrónica avanzada o el sello electrónico avanzado del prestador 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 que pueden utilizarse para consultar el estado de validez del certificado cualificado.