REGLAMENTO DE EJECUCIÓN (UE) 2015/1502 DE LA COMISIÓN

de 8 de septiembre de 2015

sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) 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 el que se deroga la Directiva 1999/93/CE ([1]), y, en particular, su artículo 8, apartado 3,

Considerando lo siguiente:

(1) El artículo 8 del Reglamento (UE) nº 910/2014 establece que un sistema de identificación electrónica notificado en virtud del artículo 9, apartado 1, debe especificar los niveles de seguridad bajo, sustancial y alto de los medios de identificación electrónica expedidos en el marco de ese sistema.

(2) Determinar las especificaciones, las normas y los procedimientos técnicos mínimos es fundamental a fin de garantizar un entendimiento común en cuanto a los detalles de los niveles de seguridad, así como la interoperabilidad al correlacionar los niveles de seguridad nacionales de los sistemas de identificación electrónica notificados con los niveles de seguridad contemplados en el artículo 8, de conformidad con el artículo 12, apartado 4, letra b), del Reglamento (UE) nº 910/2014.

(3) Se ha tenido en cuenta la norma internacional ISO/CEI 29115 en relación con las especificaciones y los procedimientos establecidos en el presente acto de ejecución como norma internacional de principio disponible en el dominio de los niveles de seguridad de los medios de identificación electrónica. No obstante, el contenido del Reglamento (UE) nº 910/2014 difiere de esa norma internacional, en particular por lo que se refiere a los requisitos de prueba y verificación de la identidad, así como a la forma en que se tienen en cuenta las diferencias entre las disposiciones de los Estados miembros en materia de identidad y las herramientas existentes en la UE para el mismo fin. Por lo tanto, el anexo, aunque se basa en esta norma internacional, no debe hacer referencia a ningún contenido específico de la norma ISO/CEI 29115.

(4) El presente Reglamento se ha desarrollado en forma de enfoque basado en los resultados, que es el más apropiado, lo que también se refleja en las definiciones que se utilizan para especificar los términos y conceptos. Estas tienen en cuenta el objetivo del Reglamento (UE) nº 910/2014 en relación con los niveles de seguridad de los medios de identificación electrónica. Por lo tanto, el proyecto piloto a gran escala STORK, incluidas las especificaciones desarrolladas por él, y las definiciones y los conceptos de la norma ISO/CEI 29115 se deben tener en cuenta en la mayor medida posible al establecer las especificaciones y los procedimientos previstos en el presente acto de ejecución.

(5) En función del contexto en el que haya que verificar un aspecto de la prueba de la identidad, las fuentes auténticas pueden adoptar diferentes formas, como registros, documentos y organismos, entre otros. Las fuentes auténticas pueden ser diferentes en los distintos Estados miembros, incluso en un contexto similar.

(6) Los requisitos de prueba y verificación de la identidad deben tener en cuenta los distintos sistemas y prácticas, y garantizar al mismo tiempo una seguridad suficientemente alta con el fin de establecer la confianza necesaria. Por lo tanto, la aceptación de los procedimientos utilizados anteriormente para un fin distinto de la expedición de los medios de identificación electrónica debe estar condicionada a la confirmación de que dichos procedimientos cumplen los requisitos previstos para el correspondiente nivel de seguridad.

([1]) DO L 257 de 28.8.2014, p. 73.

(7) Se suelen emplear ciertos factores de autenticación, como secretos compartidos, dispositivos físicos y atributos físicos. No obstante, se debe fomentar el uso de un mayor número de factores de autenticación, especialmente de las diferentes categorías de factores, para aumentar la seguridad del proceso de autenticación.

(8) El presente Reglamento no debe afectar a los derechos de representación de las personas jurídicas. Sin embargo, el anexo debe contemplar los requisitos relacionados con la vinculación entre los medios de identificación electrónica de las personas físicas y jurídicas.

(9) Debe reconocerse la importancia de los sistemas de gestión de la seguridad de la información y de los servicios, así como también la importancia de utilizar metodologías reconocidas y de aplicar los principios incorporados en normas como las de las series ISO/CEI 27000 e ISO/CEI 20000.

(10) También deben tenerse en cuenta las buenas prácticas en relación con los niveles de seguridad en los Estados miembros.

(11) La certificación de seguridad TI basada en normas internacionales es un importante instrumento para verificar si las características de seguridad de los productos cumplen los requisitos del presente acto de ejecución.

(12) El Comité mencionado en el artículo 48 del Reglamento (UE) nº 910/2014 no ha emitido ningún dictamen en el plazo fijado por su Presidente.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

1. Los niveles de seguridad bajo, sustancial y alto de los medios de identificación electrónica expedidos en el marco de un sistema de identificación electrónica notificado se determinarán con arreglo a las especificaciones y los procedimientos establecidos en el anexo.

2. Las especificaciones y los procedimientos establecidos en el anexo se utilizarán para especificar el nivel de seguridad de los medios de identificación electrónica expedidos en el marco de un sistema de identificación electrónica notificado por medio de la determinación de la fiabilidad y la calidad de los siguientes elementos:

a) inscripción, como se establece en la sección 2.1 del anexo del presente Reglamento, de conformidad con el artículo 8, apartado 3, letra a), del Reglamento (UE) nº 910/2014;

b) gestión de medios de identificación electrónica, como se establece en la sección 2.2 del anexo del presente Reglamento, de conformidad con el artículo 8, apartado 3, letras b) y f), del Reglamento (UE) nº 910/2014;

c) autenticación, como se establece en la sección 2.3 del anexo del presente Reglamento, de conformidad con el artículo 8, apartado 3, letra c), del Reglamento (UE) nº 910/2014;

d) gestión y organización, como se establece en la sección 2.4 del anexo del presente Reglamento, de conformidad con el artículo 8, apartado 3, letras d) y e), del Reglamento (UE) nº 910/2014.

3. Cuando los medios de identificación electrónica expedidos en el marco de un sistema de identificación electrónica notificado cumplen un requisito de un nivel de seguridad superior, se dará por supuesto que cumplen el requisito equivalente de un nivel de seguridad inferior.

4. A menos que se indique lo contrario en la parte pertinente del anexo, todos los elementos enumerados en el anexo para un determinado nivel de seguridad de los medios de identificación electrónica expedidos en el marco de un sistema de identificación electrónica notificado deberán cumplirse para coincidir con el nivel de seguridad reclamado.

Artículo 2

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

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

Hecho en Bruselas, el 8 de septiembre de 2015.

Por la Comisión

El Presidente

Jean-Claude JUNCKER

ANEXO

Especificaciones y procedimientos técnicos de los niveles de calidad bajo, sustancial y alto para medios de identificación electrónica expedidos en el marco de un sistema de identificación electrónica notificado

1. Definiciones aplicables

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

1) «fuente auténtica»: cualquier fuente, independientemente de la forma, en la que se pueda confiar para proporcionar datos, información o pruebas exactos que se puedan utilizar para demostrar la identidad;

2) «factor de autenticación»: un factor confirmado como vinculado a una persona, que se encuentra en alguna de las categorías siguientes:

   a) «factor de autenticación basado en la posesión»: factor de autenticación en el que el sujeto está obligado a demostrar posesión del mismo;

   b) «factor de autenticación basado en el conocimiento»: factor de autenticación en el que el sujeto está obligado a demostrar conocimiento del mismo;

   c) «factor de autenticación inherente»: factor de autenticación que se basa en un atributo físico de una persona física del cual el sujeto está obligado a demostrar su posesión;

3) «autenticación dinámica»: proceso electrónico que utiliza criptografía u otras técnicas para proporcionar un medio de crear a petición una prueba electrónica que demuestre que el sujeto controla o posee los datos de identificación y que cambia con cada autenticación entre el sujeto y el sistema que verifica la identidad del sujeto;

4) «sistema de gestión de la seguridad de la información»: conjunto de procesos y procedimientos diseñados para gestionar a niveles aceptables los riesgos relacionados con la seguridad de la información.

2. Especificaciones y procedimientos técnicos

Los elementos de las especificaciones y los procedimientos técnicos establecidos en el presente anexo se utilizarán para determinar cómo se aplicarán los requisitos y criterios establecidos en el artículo 8 del Reglamento (UE) nº 910/2014 en relación con los medios de identificación electrónica expedidos en el marco de un sistema de identificación electrónica.

2.1. *Inscripción*

2.1.1. Solicitud y registro

Nivel de seguridad	Elementos necesarios
Bajo	1. Asegurarse de que el solicitante conozca los términos y condiciones relacionados con el uso de los medios de identificación electrónica. 2. Asegurarse de que el solicitante conozca las precauciones de seguridad recomendadas relacionadas con los medios de identificación electrónica. 3. Recopilar los datos de identidad pertinentes necesarios para la prueba y verificación de la identidad.
Sustancial	Igual que el nivel bajo.
Alto	Igual que el nivel bajo.

2.1.2. Prueba y verificación de la identidad (persona física)

Nivel de seguridad	Elementos necesarios
Bajo	1. Se puede suponer que la persona está en posesión de pruebas reconocidas por el Estado miembro en el que se realiza la solicitud de los medios de identificación electrónica y que representan la identidad reclamada. 2. Se puede suponer que las pruebas son auténticas o que existen según una fuente auténtica y las pruebas parecen ser válidas. 3. Una fuente auténtica sabe de la existencia de la identidad reclamada y se puede suponer que la persona que reclama la identidad es la misma persona.
Sustancial	Nivel bajo y, además, se debe cumplir una de las alternativas indicadas en los puntos 1 a 4: 1) se ha verificado que la persona está en posesión de pruebas reconocidas por el Estado miembro en el que se realiza la solicitud de los medios de identificación electrónica y que representan la identidad reclamada, así como las pruebas se comprueban para determinar que son auténticas o, según una fuente auténtica, se sabe de su existencia y están relacionadas con una persona real, así como se han tomado medidas para reducir al mínimo el riesgo de que la identidad de la persona no sea la identidad reclamada, teniendo en cuenta, por ejemplo, el riesgo de pruebas perdidas, robadas, suspendidas, revocadas o expiradas; o bien 2) se presenta un documento de identidad durante un proceso de registro en el Estado miembro en el que se ha expedido el documento y el documento está referido a la persona que lo presenta, así como se han tomado medidas para reducir al mínimo el riesgo de que la identidad de la persona no sea la identidad reclamada, teniendo en cuenta, por ejemplo, el riesgo de documentos perdidos, robados, suspendidos, revocados o expirados; o bien 3) cuando los procedimientos utilizados anteriormente por una entidad pública o privada en el mismo Estado miembro para una finalidad distinta de la expedición de medios de identificación electrónica ofrecen una seguridad equivalente a la que proporcionan los establecidos en la sección 2.1.2 para el nivel de seguridad sustancial, no es necesario que la entidad responsable del registro repita esos primeros procedimientos, siempre que dicha seguridad equivalente esté confirmada por un organismo de evaluación de la conformidad de los que se hace referencia en el artículo 2, apartado 13, del Reglamento (CE) nº 765/2008 del Parlamento Europeo y del Consejo [1] o por un organismo equivalente; o bien 4) en los casos en que los medios de identificación se expidan sobre la base de un medio de identificación electrónica notificado válido que tenga el nivel de seguridad sustancial o alto, y teniendo en cuenta los riesgos de que se produzca un cambio en los datos de identificación de la persona, no es necesario repetir los procesos de prueba y verificación de la identidad; cuando los medios de identificación electrónica que sirven de base no se han notificado, el nivel de seguridad sustancial o alto deberá ser confirmado por un organismo de evaluación de la conformidad de los que se hace referencia en el artículo 2, apartado 13, del Reglamento (CE) nº 765/2008 o por un organismo equivalente.

Nivel de seguridad	Elementos necesarios
Alto	Deben cumplirse los requisitos del punto 1 o 2: 1) Nivel sustancial y, además, se debe cumplir una de las alternativas indicadas en las letras a) a c): a) cuando se ha verificado que la persona está en posesión de pruebas de identificación fotográficas o biométricas reconocidas por el Estado miembro en el que se realiza la solicitud de los medios de identificación electrónica y si esas pruebas representan la identidad reclamada, se comprueban las pruebas para determinar que son válidas según una fuente auténtica, así como se identifica al solicitante como la identidad reclamada por medio de la comparación de una o más características físicas de la persona con una fuente auténtica; o bien b) cuando los procedimientos utilizados anteriormente por una entidad pública o privada en el mismo Estado miembro para una finalidad distinta de la expedición de medios de identificación electrónica ofrecen una seguridad equivalente a la que proporcionan los establecidos en la sección 2.1.2 para el nivel de seguridad alto, no es necesario que la entidad responsable del registro repita esos primeros procedimientos, siempre que dicha seguridad equivalente esté confirmada por un organismo de evaluación de la conformidad de los que se hace referencia en el artículo 2, apartado 13, del Reglamento (CE) nº 765/2008 o por un organismo equivalente, así como se toman medidas para demostrar que los resultados de los procedimientos anteriores siguen siendo válidos; o bien c) en los casos en que los medios de identificación se expidan sobre la base de un medio de identificación electrónica notificado válido que tenga el nivel de seguridad alto, y teniendo en cuenta los riesgos de que se produzca un cambio en los datos de identificación de la persona, no es necesario repetir los procesos de prueba y verificación de la identidad; cuando los medios de identificación electrónica que sirven de base no se han notificado, el nivel de seguridad alto deberá ser confirmado por un organismo de evaluación de la conformidad de los que se hace referencia en el artículo 2, apartado 13, del Reglamento (CE) nº 765/2008 o por un organismo equivalente, así como se toman medidas para demostrar que los resultados de este procedimiento anterior de expedición de un medio de identificación electrónica notificado siguen siendo válidos. O BIEN 2) en caso de que el solicitante no presente ninguna prueba de identificación fotográfica o biométrica reconocida, se aplicarán los mismos procedimientos utilizados a escala nacional en el Estado miembro de la entidad responsable del registro para obtener las pruebas de identificación fotográfica o biométrica reconocidas.

([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).

2.1.3. Prueba y verificación de la identidad (persona jurídica)

Nivel de seguridad	Elementos necesarios
Bajo	1. La identidad reclamada de la persona jurídica se demuestra sobre la base de pruebas reconocidas por el Estado miembro en el que se realiza la solicitud para los medios de identificación electrónica.

Nivel de seguridad	Elementos necesarios
	2. Las pruebas parecen ser válidas y se puede suponer que son auténticas o que existen según una fuente auténtica, cuando la inclusión de una persona jurídica en la fuente de autoridad es voluntaria y está regulada por un acuerdo entre la persona jurídica y la fuente auténtica. 3. Una fuente auténtica no tiene constancia de que la persona jurídica esté en un estado que le impediría actuar como esa persona jurídica.
Sustancial	Nivel bajo y, además, se debe cumplir una de las alternativas indicadas en los puntos 1 a 3: 1) La identidad reclamada de la persona jurídica se demuestra sobre la base de pruebas reconocidas por el Estado miembro en el que se realiza la solicitud para los medios de identificación electrónica, incluidos el nombre, la forma jurídica y (si procede) el número de registro de la persona jurídica, así como las pruebas se verifican para determinar si son auténticas o si se sabe de su existencia según una fuente auténtica, cuando la inclusión de la persona jurídica en la fuente auténtica es necesaria para que la persona jurídica opere dentro de su sector, así como se han tomado medidas para reducir al mínimo el riesgo de que la identidad de la persona jurídica no sea la identidad reclamada, teniendo en cuenta, por ejemplo, el riesgo de documentos perdidos, robados, suspendidos, revocados o expirados; o bien 2) cuando los procedimientos utilizados anteriormente por una entidad pública o privada en el mismo Estado miembro para una finalidad distinta de la expedición de medios de identificación electrónica ofrezcan una seguridad equivalente a la que proporcionan los establecidos en la sección 2.1.3 para el nivel de seguridad sustancial, no es necesario que la entidad responsable del registro repita esos primeros procedimientos, siempre que dicha seguridad equivalente esté confirmada por un organismo de evaluación de la conformidad de los que se hace referencia en el artículo 2, apartado 13, del Reglamento (CE) nº 765/2008 o por un organismo equivalente; o bien 3) en los casos en que los medios de identificación se expidan sobre la base de un medio de identificación electrónica notificado válido que tenga el nivel de seguridad sustancial o alto, no es necesario repetir los procesos de prueba y verificación de la identidad; cuando los medios de identificación electrónica que sirven de base no se han notificado, el nivel de seguridad sustancial o alto deberá ser confirmado por un organismo de evaluación de la conformidad de los que se hace referencia en el artículo 2, apartado 13, del Reglamento (CE) nº 765/2008 o por un organismo equivalente.
Alto	Nivel sustancial y, además, se debe cumplir una de las alternativas indicadas en los puntos 1 a 3: 1) la identidad reclamada de la persona jurídica se demuestra sobre la base de pruebas reconocidas por el Estado miembro en el que se realiza la solicitud para los medios de identificación electrónica, incluidos el nombre y la forma jurídica de la persona jurídica y, por lo menos, un identificador único que represente a la persona jurídica utilizado en un contexto nacional, así como las pruebas se comprueban para determinar que son válidas según una fuente auténtica; o bien

Nivel de seguridad	Elementos necesarios
	2) cuando los procedimientos utilizados anteriormente por una entidad pública o privada en el mismo Estado miembro para una finalidad distinta de la expedición de medios de identificación electrónica ofrezcan una seguridad equivalente a la que proporcionan los establecidos en la sección 2.1.3 para el nivel de seguridad alto, no es necesario que la entidad responsable del registro repita esos primeros procedimientos, siempre que dicha seguridad equivalente esté confirmada por un organismo de evaluación de la conformidad de los que se hace referencia en el artículo 2, apartado 13, del Reglamento (CE) nº 765/2008 o por un organismo equivalente, así como se toman medidas para demostrar que los resultados del procedimiento anterior siguen siendo válidos; o bien 3) en los casos en que los medios de identificación se expidan sobre la base de un medio de identificación electrónica notificado válido que tenga el nivel de seguridad alto, no es necesario repetir los procesos de prueba y verificación de la identidad; cuando los medios de identificación electrónica que sirven de base no se han notificado, el nivel de seguridad alto deberá ser confirmado por un organismo de evaluación de la conformidad de los que se hace referencia en el artículo 2, apartado 13, del Reglamento (CE) nº 765/2008 o por un organismo equivalente, así como se toman medidas para demostrar que los resultados de este procedimiento anterior de expedición de un medio de identificación electrónica notificado siguen siendo válidos.

2.1.4. Vinculación entre los medios de identificación electrónica de personas físicas y jurídicas

En su caso, para la vinculación de los medios de identificación electrónica de una persona física y los medios de identificación electrónica de una persona jurídica («vinculación»), se aplican las condiciones siguientes:

1) Deberá ser posible suspender y/o revocar una vinculación. El ciclo de vida de una vinculación (por ejemplo, activación, suspensión, renovación, revocación) se administrará de conformidad con los procedimientos reconocidos a escala nacional.

2) La persona física cuyos medios de identificación electrónica están vinculados a los miembros de identificación electrónica de la persona jurídica podrá delegar el ejercicio de la vinculación en otra persona física sobre la base de los procedimientos reconocidos a nivel nacional. No obstante, la persona física que realiza la delegación seguirá siendo responsable.

3) La vinculación se realizará de la siguiente manera:

Nivel de seguridad	Elementos necesarios
Bajo	1. Se verifica que la prueba de identidad de la persona física que actúa en nombre de la persona jurídica se ha realizado en el nivel bajo o superior. 2. La vinculación se ha establecido sobre la base de los procedimientos reconocidos a escala nacional. 3. Una fuente auténtica no tiene constancia de que la persona física tenga un estado que impida que esa persona actúe en nombre de la persona jurídica.
Sustancial	Punto 3 del nivel bajo, además de lo siguiente: 1. Se verifica que la prueba de identidad de la persona física que actúa en nombre de la persona jurídica se ha realizado en el nivel sustancial o alto.

Nivel de seguridad	Elementos necesarios
	2. La vinculación se ha establecido sobre la base de procedimientos reconocidos a escala nacional, lo que ha dado lugar al registro de la vinculación en una fuente auténtica. 3. La vinculación se ha verificado sobre la base de información proveniente de una fuente auténtica.
Alto	Punto 3 del nivel bajo y punto 2 del nivel sustancial, además de lo siguiente: 1. Se verifica que la prueba de identidad de la persona física que actúa en nombre de la persona jurídica se ha realizado en el nivel alto. 2. La vinculación se ha verificado sobre la base de un identificador único que representa a la persona jurídica utilizado en el contexto nacional; y sobre la base de información que representa de manera exclusiva a la persona física a partir de una fuente auténtica.

2.2. *Gestión de medios de identificación electrónica*

2.2.1. Características y diseño de los medios de identificación electrónica

Nivel de seguridad	Elementos necesarios
Bajo	1. El medio de identificación electrónica utiliza por lo menos un factor de autenticación. 2. El medio de identificación electrónica está diseñado de forma que el emisor toma medidas razonables para asegurarse de que solo se utiliza bajo el control o la posesión de la persona a la que pertenece.
Sustancial	1. El medio de identificación electrónica utiliza por lo menos dos factores de autenticación de distintas categorías. 2. El medio de identificación electrónica está diseñado de forma que se puede suponer que solo se utilizará bajo el control o la posesión de la persona a la que pertenece.
Alto	Nivel sustancial, además de lo siguiente: 1. El medio de identificación electrónica protege contra la duplicación y manipulación, así como contra atacantes con elevado potencial de ataque. 2. El medio de identificación electrónica está diseñado de modo que la persona a la que pertenece lo puede proteger de manera fiable contra la utilización por otros.

2.2.2. Expedición, entrega y activación

Nivel de seguridad	Elementos necesarios
Bajo	Después de la expedición, el medio de identificación electrónica se entrega a través de un mecanismo mediante el cual se puede suponer que solo llega a la persona prevista.
Sustancial	Después de la expedición, el medio de identificación electrónica se entrega a través de un mecanismo mediante el cual se puede suponer que solo se entrega a la persona a la que pertenece.
Alto	El proceso de activación verifica que el medio de identificación electrónica solo se entrega a la persona a la que pertenece.

2.2.3. Suspensión, revocación y reactivación

Nivel de seguridad	Elementos necesarios
Bajo	1. Es posible suspender o revocar un medio de identificación electrónica de manera eficaz y oportuna. 2. Se han tomado medidas para impedir la suspensión, revocación o reactivación no autorizadas. 3. La reactivación se llevará a cabo solo si se siguen cumpliendo los mismos requisitos de seguridad establecidos antes de la suspensión o revocación.
Sustancial	Igual que el nivel bajo.
Alto	Igual que el nivel bajo.

2.2.4. Renovación y sustitución

Nivel de seguridad	Elementos necesarios
Bajo	Teniendo en cuenta los riesgos de un cambio en los datos de identificación de la persona, la renovación o sustitución debe cumplir los mismos requisitos de seguridad que la prueba y verificación de identidad inicial o basarse en un medio de identificación electrónica válido del mismo nivel de seguridad o de un nivel superior.
Sustancial	Igual que el nivel bajo.
Alto	Nivel bajo, además de lo siguiente: Si la renovación o sustitución se basa en un medio de identificación electrónica válido, los datos de identidad se verifican con una fuente auténtica.

2.3. *Autenticación*

Esta sección se centra en las amenazas asociadas al uso del mecanismo de autenticación y enumera los requisitos de cada nivel de seguridad. En esta sección se da por entendido que los controles están en consonancia con los riesgos en el nivel determinado.

2.3.1. Mecanismo de autenticación

La tabla siguiente establece los requisitos por nivel de seguridad con respecto al mecanismo de autenticación, a través del cual la persona física o jurídica utiliza los medios de identificación electrónica para confirmar su identidad a la parte usuaria.

Nivel de seguridad	Elementos necesarios
Bajo	1. La liberación de datos de identificación de la persona va precedida de una verificación fiable del medio de identificación electrónica y su validez. 2. Si se almacenan datos de identificación de la persona como parte del mecanismo de autenticación, dicha información está protegida con el fin de ofrecer protección contra la pérdida y contra cualquier peligro, incluido el análisis fuera de línea. 3. El mecanismo de autenticación aplica controles de seguridad para la verificación de los medios de identificación electrónica, por lo que es muy poco probable que actividades como intentos de adivinación, escucha, reproducción o manipulación de la comunicación por un atacante con potencial de ataque básico mejorado puedan alterar los mecanismos de autenticación.

Nivel de seguridad	Elementos necesarios
Sustancial	Nivel bajo, además de lo siguiente: 1. La liberación de datos de identificación de la persona va precedida de una verificación fiable del medio de identificación electrónica y su validez por medio de una autenticación dinámica. 2. El mecanismo de autenticación aplica controles de seguridad para la verificación de los medios de identificación electrónica, por lo que es muy poco probable que actividades como intentos de adivinación, escucha, reproducción o manipulación de la comunicación por un atacante con potencial de ataque moderado puedan alterar los mecanismos de autenticación.
Alto	Nivel sustancial, además de lo siguiente: El mecanismo de autenticación aplica controles de seguridad para la verificación de los medios de identificación electrónica, por lo que es muy poco probable que actividades como intentos de adivinación, escucha, reproducción o manipulación de la comunicación por un atacante con potencial de ataque alto puedan alterar los mecanismos de autenticación.

2.4. *Gestión y organización*

Todos los participantes que presten un servicio relacionado con la identificación electrónica en un contexto transfronterizo («proveedores») contarán con prácticas y políticas de gestión de la seguridad de la información documentadas, metodologías de gestión de riesgo y otros controles reconocidos para proporcionar garantías a los órganos de control apropiados encargados de los sistemas de identificación electrónica de los respectivos Estados miembros de que se aplican prácticas eficaces. En la sección 2.4, todos los requisitos o elementos deberán entenderse como acordes a los riesgos en el nivel determinado.

2.4.1. Disposiciones generales

Nivel de seguridad	Elementos necesarios
Bajo	1. Los proveedores que presten los servicios operativos objeto del presente Reglamento tienen la condición de autoridad pública o de una entidad jurídica reconocida como tal por la legislación nacional de un Estado miembro, con una organización establecida y en pleno funcionamiento en todas las partes pertinentes para la prestación de los servicios. 2. Los proveedores cumplen los requisitos legales que les incumben en relación con el funcionamiento y la prestación del servicio, incluidos los tipos de información que se pueden solicitar, cómo se realiza la prueba de identidad, qué información se puede conservar y durante cuánto tiempo. 3. Los proveedores están en condiciones de demostrar su capacidad para asumir el riesgo de la responsabilidad por daños y perjuicios, así como que disponen de los recursos financieros suficientes para seguir funcionando y prestar los servicios. 4. Los proveedores son responsables del cumplimiento de cualquiera de los compromisos externalizados a otra entidad, así como del cumplimiento de la política del sistema, como si ellos mismos llevaran a cabo dichas tareas. 5. Los sistemas de identificación electrónica que no se basen en la legislación nacional deberán contar con un plan de cese eficaz. Dicho plan deberá incluir las suspensiones del servicio de manera ordenada o la continuación por otro proveedor, la manera en que se informa a las autoridades competentes y los usuarios finales, así como detalles sobre cómo se deben proteger, conservar y destruir los registros en cumplimiento de la política del sistema.
Sustancial	Igual que el nivel bajo.
Alto	Igual que el nivel bajo.

2.4.2. Avisos publicados e información del usuario

Nivel de seguridad	Elementos necesarios
Bajo	1. Existencia de una definición del servicio publicada que incluya todos los términos, condiciones y tarifas aplicables, incluidas las limitaciones de su uso. La definición del servicio incluirá una política de privacidad. 2. Se deben poner en práctica políticas y procedimientos apropiados con el fin de garantizar que los usuarios del servicio sean informados de manera oportuna y fiable de los cambios que se produzcan en la definición del servicio y en los términos, las condiciones y la política de privacidad aplicables del servicio especificado. 3. Se deben implantar políticas y procedimientos apropiados que proporcionen respuestas completas y correctas a las solicitudes de información.
Sustancial	Igual que el nivel bajo.
Alto	Igual que el nivel bajo.

2.4.3. Gestión de la seguridad de la información

Nivel de seguridad	Elementos necesarios
Bajo	Existe un sistema de gestión de la seguridad de la información eficaz para la gestión y el control de los riesgos para la seguridad de la información.
Sustancial	Nivel bajo, además de lo siguiente: El sistema de gestión de la seguridad de la información satisface normas o principios establecidos para la gestión y el control de los riesgos para la seguridad de la información.
Alto	Igual que el nivel sustancial.

2.4.4. Conservación de información

Nivel de seguridad	Elementos necesarios
Bajo	1. Se debe registrar y mantener la información pertinente mediante un sistema de gestión de registros eficaz, teniendo en cuenta la legislación aplicable y las buenas prácticas en relación con la protección de datos y la conservación de datos. 2. Los registros se deben conservar, en la medida en que lo permita la legislación nacional u otro acuerdo administrativo nacional, y proteger durante el tiempo en que sean necesarios para fines de auditoría y de investigación de las infracciones de seguridad, y retención, tras lo cual los registros se destruirán de manera segura.
Sustancial	Igual que el nivel bajo.
Alto	Igual que el nivel bajo.

2.4.5. Instalaciones y personal

La siguiente tabla representa los requisitos relativos a las instalaciones, el personal y los subcontratistas, en su caso, que desempeñen las funciones reguladas por el presente Reglamento. El cumplimiento de cada uno de los requisitos será proporcional al nivel de riesgo asociado al nivel de seguridad indicado.

Nivel de seguridad	Elementos necesarios
Bajo	1. Existencia de procedimientos que garanticen que el personal y los subcontratistas cuenten con la debida formación, cualificaciones y experiencia en las competencias necesarias para ejecutar las funciones que desempeñan. 2. Dotación de personal y subcontratistas suficientes para el funcionamiento y la asignación de recursos al servicio de manera adecuada según sus políticas y procedimientos. 3. Las instalaciones utilizadas para la prestación del servicio estarán controladas de manera continua y protegidas contra daños causados por fenómenos ambientales, accesos no autorizados y otros factores que puedan afectar a la seguridad del servicio. 4. Las instalaciones utilizadas para la prestación del servicio garantizarán que el acceso a las zonas que tengan o procesen información personal, criptográfica o confidencial se limita al personal o los subcontratistas autorizados.
Sustancial	Igual que el nivel bajo.
Alto	Igual que el nivel bajo.

2.4.6. Controles técnicos

Nivel de seguridad	Elementos necesarios
Bajo	1. Existencia de controles técnicos proporcionales para gestionar los riesgos que puedan afectar a la seguridad de los servicios y que protejan la confidencialidad, integridad y disponibilidad de la información que se procesa. 2. Los canales de comunicación electrónica que se utilizan para intercambiar información personal o confidencial están protegidos contra escucha, manipulación y reproducción. 3. El acceso al material criptográfico confidencial, si se utiliza para expedir medios de identificación electrónica y autenticación, se limita exclusivamente a aquellas funciones y aplicaciones que requieren estrictamente ese acceso. Deberá garantizarse que dicho material no se almacene nunca de manera continua en forma de texto sin formato. 4. Existencia de procedimientos para garantizar el mantenimiento de la seguridad a lo largo del tiempo y que es posible responder a los cambios en los niveles de riesgo, los incidentes y las violaciones de la seguridad. 5. Todos los medios que contienen información personal, criptográfica o confidencial se almacenan, transportan y eliminan de manera segura.
Sustancial	Igual que el nivel bajo, además de lo siguiente: El material criptográfico confidencial, si se utiliza para la expedición de medios de identificación electrónica y autenticación, está protegido contra su manipulación
Alto	Igual que el nivel sustancial.

2.4.7. Cumplimiento y auditoría

Nivel de seguridad	Elementos necesarios
Bajo	Existencia de auditorías internas periódicas cuyo ámbito comprenda todas las partes pertinentes para la prestación de los servicios a fin de garantizar el cumplimiento de las políticas pertinentes.

Nivel de seguridad	Elementos necesarios
Sustancial	Existencia de auditorías internas o externas periódicas e independientes cuyo ámbito comprenda todas las partes pertinentes para la prestación de los servicios a fin de garantizar el cumplimiento de las políticas pertinentes.
Alto	1. Existencia de auditorías externas periódicas e independientes cuyo ámbito comprenda todas las partes pertinentes para la prestación de los servicios a fin de garantizar el cumplimiento de las políticas pertinentes. 2. Cuando un organismo del Estado gestiona directamente un sistema, se auditará de conformidad con el derecho nacional.