2024/1942

20.12.2024

REGLAMENTO DE EJECUCIÓN (UE) 2024/1942 DE LA COMISIÓN

de 5 de julio de 2024

por el que se establecen procedimientos comunes y normas detalladas para el acceso a la información electrónica relativa al transporte de mercancías y su tratamiento por parte de las autoridades competentes de conformidad con el Reglamento (UE) 2020/1056 del Parlamento Europeo y del Consejo

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) 2020/1056 del Parlamento Europeo y del Consejo, de 15 de julio de 2020, sobre información electrónica relativa al transporte de mercancías ([1]), y en particular su artículo 8,

Considerando lo siguiente:

(1) El Reglamento (UE) 2020/1056 exige a los Estados miembros que garanticen que todas sus autoridades competentes tengan acceso a la información electrónica relativa al transporte de mercancías («IETM»), en consonancia con procedimientos comunes y normas detalladas, incluidas las especificaciones técnicas comunes y los procedimientos para el tratamiento de información reglamentaria y para la comunicación con los operadores económicos en relación con esa información.

(2) A fin de establecer esos procedimientos comunes y normas, con arreglo al artículo 8 del Reglamento (UE) 2020/1056, la Comisión debe enumerar los principales componentes de las tecnologías de la información y las comunicaciones (TIC) del entorno de intercambio IETM que deben facilitar los Estados miembros, y detallar también las especificaciones funcionales y técnicas de tales componentes.

(3) Para garantizar la flexibilidad a la hora de aplicar esos procedimientos comunes y normas detalladas, los Estados miembros deben poder decidir cómo organizar el suministro de los componentes de TIC, siempre que dichos componentes cumplan las especificaciones funcionales y técnicas correspondientes establecidas en el presente Reglamento de Ejecución. Más concretamente, los Estados miembros pueden decidir establecerlos como componentes separados o integrarlos en un único componente o en varios componentes distintos, cada uno con sus funcionalidades respectivas. También pueden crear componentes múltiples que realicen un mismo conjunto de funcionalidades.

(4) Los Estados miembros deben poder reutilizar los componentes de TIC existentes que ya hayan desarrollado para otros servicios públicos digitales, en la medida en que estos componentes ya ofrezcan, o se adapten para ofrecer, las funcionalidades necesarias con arreglo a las especificaciones establecidas en el presente Reglamento de Ejecución, incluidos los requisitos técnicos, cuando proceda. Los Estados miembros también deben poder optar por establecer, desarrollar y mantener uno o varios de los componentes de TIC previstos en el presente Reglamento conjuntamente con otros Estados miembros.

(5) Cada Estado miembro debe ser responsable de garantizar el mantenimiento y la seguridad de los componentes de TIC que cree o de los que sea responsable, en particular de garantizar la seguridad y confidencialidad de la información tratada en dichos componentes. Si varios Estados miembros deciden crear y gestionar conjuntamente algunos de estos componentes, deben velar por que sus responsabilidades respectivas se establezcan en acuerdos o memorandos de entendimiento adecuados.

(6) Con arreglo al Reglamento (UE) 2020/1056, toda comunicación llevada a cabo dentro del entorno de intercambio IETM debe efectuarse mediante conexiones seguras entre partes debidamente identificadas y autorizadas. Por consiguiente, las especificaciones funcionales y técnicas comunes establecidas en el presente Reglamento de Ejecución deben garantizar que dichos requisitos se cumplan en todas las comunicaciones que tengan lugar entre los participantes en el entorno de intercambio IETM a través de componentes de TIC, también con plataformas IETM.

([1]) DO L 249 de 31.7.2020, p. 33.

(7) Se espera que el número de participantes en el entorno de intercambio IETM sea elevado, tanto a nivel de las autoridades competentes como de los operadores económicos interesados, que serán libres de utilizar las plataformas IETM de su elección. Por lo tanto, sería necesario establecer y mantener un número adecuado de conexiones seguras, autenticadas y autorizadas entre los componentes de TIC del entorno de intercambio IETM. Para reducir los costes asociados a un número tan elevado de conexiones, algunos de los componentes de TIC del entorno de intercambio IETM que establezcan los Estados miembros deben actuar como intermediarios en este intercambio desempeñando una función de pasarela, manteniendo en todo momento un elevado nivel de seguridad y de conformidad con las autorizaciones aplicables.

(8) Dichas pasarelas, o «puertas IETM» (en inglés, «eFTI gates»), deben actuar como intermediarias en el intercambio de información reglamentaria relativa al transporte de mercancías entre los operadores económicos interesados y las autoridades competentes. Las puertas IETM garantizan conexiones seguras y autenticadas con los componentes de TIC que actúan como intermediarios en el acceso de los agentes individuales a nivel de las autoridades competentes de un Estado miembro específico, por una parte, y con las plataformas IETM que contienen los datos a los que tendrían que tener acceso dichos agentes, por otra parte. No deben almacenar ni tratar datos IETM, excepto en el caso de los metadatos conectados al tratamiento de datos IETM, como los identificadores o los registros de operaciones, y solo con fines legítimos, como el encaminamiento, la validación o adaptación de formatos y con fines de seguimiento o estadísticos.

(9) Además, a fin de reducir los costes derivados del establecimiento de conexiones entre las plataformas IETM y las puertas IETM, en particular para los operadores económicos, pero también para las autoridades competentes, tal como se establece en el artículo 8, apartado 2, del Reglamento (UE) 2020/1056, debe exigirse a las plataformas IETM que establezcan y mantengan una conexión segura y autenticada con una única puerta IETM. Dicha puerta IETM debe entonces actuar como intermediaria en la conexión con todas las autoridades competentes de todos los Estados miembros, a través de una red de conexiones seguras y autenticadas entre las distintas puertas IETM.

(10) Habida cuenta del requisito establecido en el artículo 11 del Reglamento (UE) 2020/1056, consistente en que los Estados miembros mantengan una lista actualizada de las plataformas IETM que posean una certificación válida expedida por un organismo de evaluación de la conformidad acreditado en su Estado miembro, esta conexión única de una plataforma IETM con la red de puertas IETM debe establecerse con la puerta IETM del Estado miembro en el que se expidió la certificación de dicha plataforma. Esto facilitaría y haría menos costoso el proceso de verificación de la validez de la certificación de las plataformas IETM, como parte del proceso de garantizar la seguridad y autenticidad de la comunicación con ellas. No obstante, para dar cabida a situaciones en las que ningún organismo de evaluación de la conformidad haya sido acreditado para certificar plataformas IETM en un Estado miembro, las plataformas IETM deben poder establecer su conexión única con la puerta IETM de ese Estado miembro, incluso cuando hayan obtenido la certificación en otros Estados miembros.

(11) Para garantizar un alto nivel de confianza en el entorno de intercambio IETM, los Estados miembros deben seguir siendo responsables de garantizar que todo acceso por parte de sus autoridades competentes al entorno de intercambio IETM esté debidamente identificado, autenticado y autorizado. Los Estados miembros deben garantizar que el acceso de las autoridades competentes a los datos puestos a disposición por los operadores económicos en las plataformas IETM, así como el tratamiento de esos datos, solo se permita tras la debida identificación y autenticación de la identidad de los agentes responsables, así como la debida autorización sobre la base de los derechos de acceso y tratamiento asignados a los agentes, con arreglo a sus respectivas responsabilidades en relación con las disposiciones nacionales y de la UE incluidas en el ámbito de aplicación del Reglamento (UE) 2020/1056. A tal fin, los Estados miembros deben velar por que todas las autoridades competentes establezcan y mantengan registros donde quede constancia actualizada de los derechos de acceso y tratamiento de cada agente responsable, y por que todas las solicitudes de acceso a datos IETM y de tratamiento de estos incluyan referencias a los derechos de acceso y tratamiento del agente responsable de la solicitud. Dichos derechos de acceso y tratamiento deben expresarse como referencias codificadas para minimizar la transferencia de datos personales de los agentes, tal como se definen en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([2]). Los Estados miembros también deben garantizar que sus autoridades competentes adopten todas las medidas necesarias, como pruebas, formaciones y auditorías, para garantizar que sus agentes accedan a los datos y los traten de conformidad con las normas nacionales y de la UE aplicables en materia de protección de datos y confidencialidad comercial.

([2]) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1).

(12) El Reglamento (UE) 2020/1056 exige a los operadores económicos interesados que comuniquen a las autoridades competentes el «enlace único de identificación electrónica» a los datos IETM legibles mecánicamente que se correspondan con la información reglamentaria. Desde el punto de vista procedimental, esta comunicación debe llevarse a cabo de dos maneras, y los componentes de TIC que han de establecer los Estados miembros deben soportar ambos procedimientos. A la hora de solicitar acceso a los datos IETM para llevar a cabo controles de la información reglamentaria, las autoridades competentes deben poder elegir aquel procedimiento que deseen.

(13) En primer lugar, en consonancia con los actuales procedimientos de control de la conformidad en formato papel, los operadores económicos interesados deben poder comunicar directamente a la autoridad competente el enlace único de identificación electrónica durante los controles realizados de forma presencial, ya sea durante la operación de transporte o durante los controles realizados en las instalaciones del operador económico, cuando las disposiciones nacionales o de la UE aplicables prevean la posibilidad de realizar controles una vez finalizadas las operaciones de transporte. Para facilitar el tratamiento por parte de las autoridades competentes, el enlace único de identificación electrónica debe comunicarse en un formato legible mecánicamente, como un código de barras o un código QR, que se muestre en la pantalla de un dispositivo portátil electrónico, como un teléfono móvil o una tableta, o impreso en papel. Las autoridades de los Estados miembros deben poder optar por aceptar que, durante los controles físicos de las operaciones de transporte en curso, el operador económico pueda, con carácter excepcional, comunicar el enlace único de identificación electrónica por correo electrónico u otra aplicación de mensajería electrónica, en situaciones en las que el operador no pueda mostrar directamente el enlace en pantalla o en papel. En el caso de los controles efectuados en las instalaciones de los operadores económicos, cuando el número de operaciones de transporte que deban inspeccionarse sea sustancialmente superior, las autoridades competentes deben poder optar por recibir los enlaces únicos de identificación electrónica por correo electrónico u otra aplicación de mensajería electrónica, a fin de facilitar y optimizar el tratamiento de dichos enlaces. La elección de estos medios de comunicación adicionales debe seguir siendo competencia de las autoridades competentes respectivas.

(14) En segundo lugar, con vistas a un futuro en el que los procesos estarán cada vez más automatizados, los operadores económicos deben comunicar el enlace único de identificación electrónica publicándolo en un repositorio o registro electrónico, junto con determinados identificadores, como la identificación única del medio de transporte, derivados del conjunto de datos IETM asociado a ese enlace único de identificación electrónica. Las autoridades competentes podrían entonces recuperar ese enlace del registro mediante una consulta basada en esos identificadores. Esto permitiría que las autoridades competentes puedan comprobar la información sobre las mercancías transportadas en un camión, tren o gabarra sin pararlos físicamente ni subirse a ellos y, en su caso, aplicar medidas de seguimiento de conformidad con el Derecho nacional. También permitiría a las autoridades competentes obtener de manera más fácil o fiable información sobre las distintas operaciones de transporte realizadas por un medio de transporte determinado, en un período de tiempo determinado, como en el caso de los controles de cabotaje por carretera, en consonancia con las disposiciones del Reglamento (CE) n.º 1072/2009 del Parlamento Europeo y del Consejo ([3]).

(15) Para garantizar la interoperabilidad y la seguridad del intercambio de información entre las puertas IETM establecidas por los distintos Estados miembros, así como entre las puertas IETM y las plataformas IETM, debe utilizarse un conjunto de normas y especificaciones armonizadas para el intercambio de mensajes en el entorno IETM, como la configuración de acuerdos de intercambio de mensajes, procesos de negocio, formatos de datos, identificadores y certificados de seguridad. Los Estados miembros también deben acordar procedimientos seguros para el intercambio de los certificados de seguridad, por ejemplo mediante un sistema personalizado o un protocolo seguro de transferencia de archivos.

(16) A fin de reducir los costes y el tiempo necesario para establecer las puertas IETM y los demás componentes de TIC, los Estados miembros deben basarse, en la medida de lo posible, en normas abiertas mantenidas por organizaciones europeas o internacionales, así como en soluciones reutilizables. Para los formatos de intercambio de mensajes, las normas abiertas aceptadas internacionalmente más utilizadas son XML y JSON. Aunque JSON es un formato más reciente y, en algunos aspectos, más sencillo de aplicar, XML es el formato más común utilizado por los sistemas TIC de las autoridades competentes en la mayoría de los Estados miembros. Por lo tanto, para que los Estados miembros puedan reutilizar las soluciones existentes y reducir así sus costes iniciales de aplicación, todas las comunicaciones entre las puertas IETM y entre dichas puertas y las plataformas IETM deben realizarse utilizando un formato único de intercambio de mensajes, el XML. Del mismo modo, las normas para el intercambio seguro de mensajes mantenidas por la Comisión como parte del componente digital de eDelivery ([4]) y, en particular, el perfil de eDelivery AS4, ofrecen una solución técnica rentable que los Estados miembros ya aplican.

([3]) Reglamento (CE) n.º 1072/2009 del Parlamento Europeo y del Consejo, de 21 de octubre de 2009, por el que se establecen normas comunes de acceso al mercado del transporte internacional de mercancías por carretera (DO L 300 de 14.11.2009, p. 72).

([4]) https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eDelivery.

(17) Al mismo tiempo, los Estados miembros deben poder reutilizar las normas y soluciones de intercambio de mensajes que ya se utilicen en otros servicios públicos digitales para la comunicación entre la puerta IETM y las plataformas IETM establecidas en esos Estados miembros, además de eDelivery. Los requisitos y normas detallados en los que se basen estas soluciones deben ponerse a disposición del público para que los desarrolladores de plataformas IETM interesados puedan aplicarlos, y para que los organismos de evaluación de la conformidad acreditados puedan evaluar si son conformes con las especificaciones.

(18) Del mismo modo, para que los agentes de las autoridades competentes puedan hacer uso de los componentes de TIC que constituyan el punto de acceso, o los «puntos de acceso de la autoridad», al entorno IETM, los Estados miembros deben poder hacer uso de aquellas soluciones electrónicas existentes que garanticen la identificación y autenticación de la identidad de los agentes al acceder a otros servicios públicos digitales nacionales que den acceso a datos personales o comerciales de terceros. Estas soluciones deben basarse, cuando estén disponibles, en los medios de identificación electrónica establecidos en el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo ([5]).

(19) En ese mismo espíritu, los Estados miembros deben poder reutilizar cualquier otro componente de los sistemas de TIC de sus autoridades competentes que desempeñe funciones similares a las especificadas en el presente Reglamento de Ejecución, como los registros de autorizaciones, siempre que se adapten siguiendo los requisitos específicos establecidos en el presente Reglamento de Ejecución.

(20) Para que los agentes de las autoridades competentes puedan utilizar de la manera más fácil posible el entorno de intercambio IETM, y para facilitarles el análisis de los datos IETM puestos a disposición por los operadores económicos en una plataforma IETM, los Estados miembros deben poder adaptar la aplicación de usuario y su interfaz gráfica de usuario a las necesidades de sus agentes. Los Estados miembros también deben poder introducir funcionalidades adicionales soportadas por las aplicaciones de usuario, como el uso de algoritmos inteligentes que puedan pretratar los datos IETM, combinando también información procedente de otras fuentes electrónicas, si así lo desean.

(21) Para que el funcionamiento del entorno IETM sea continuo y fluido, es necesario que se resuelvan rápidamente todos los problemas operativos relacionados con los componentes de TIC establecidos por los Estados miembros. Para contribuir a garantizar esto, los Estados miembros y la Comisión deben establecer una red de apoyo técnico, compuesta por servicios de asistencia específicos a nivel nacional y de la Unión, respectivamente. Esta red debe establecer procedimientos de comunicación claros y garantizar unos períodos mínimos sincronizados de disponibilidad que permitan reaccionar rápidamente ante cualquier posible incidente o interrupción que pudiera afectar al funcionamiento del entorno de intercambio IETM. Estos puntos de contacto de apoyo técnico deben tener las competencias y los recursos humanos y financieros suficientes para poder llevar a cabo sus tareas. Sobre la base de los informes de actividad, los servicios de asistencia técnica podrán publicar información agregada en cuadros de mando específicos del servicio de asistencia. Los períodos mínimos de disponibilidad común de los servicios de asistencia técnica deben revisarse periódicamente a fin de ajustar su actividad y de asignar eficazmente los recursos.

(22) Los componentes de TIC que han de crear los Estados miembros funcionarán como partes integrantes del entorno de intercambio IETM general. Esto significa que el establecimiento y el mantenimiento de esos componentes deben basarse en esfuerzos coordinados, con arreglo a una interpretación armonizada de las especificaciones establecidas en el presente Reglamento. A tal fin, los Estados miembros también deben crear una red de apoyo operativo, en cooperación con la Comisión, en forma de grupo de expertos específico. Para aprovechar los conocimientos especializados y la experiencia adquiridos en el marco del Foro de Transporte y Logística Digitales, esto es, el grupo de expertos creado por la Comisión ([6]) para ayudar en el desarrollo y la ejecución de las actividades y programas de la Unión destinados a la digitalización del sector del transporte y la logística, dicho grupo de expertos debe establecerse como un subgrupo del Foro de Transporte y Logística Digitales.

(23) Para facilitar la labor de aplicación de los Estados miembros y garantizar la aplicación uniforme de estas especificaciones, está previsto complementar el presente Reglamento con documentos de apoyo técnico más detallados y no vinculantes elaborados por la Comisión en cooperación con los Estados miembros en el marco de ese grupo de expertos específico.

([5]) Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (DO L 257 de 28.8.2014, p. 73).

([6]) Decisión C(2018) 5921 de la Comisión, de 13 de septiembre de 2018, por la que se crea el Grupo de Expertos sobre Digitalización del Transporte de Mercancías y la Logística: el Foro de Transporte y Logística Digitales.

(24) Las medidas previstas en el presente Reglamento de Ejecución se ajustan al dictamen del Comité de Facilitación Digital del Transporte y el Comercio.

HA ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Definiciones

A los efectos del presente Reglamento, se entenderá por:

1) «entorno de intercambio IETM»: conjunto de componentes de TIC utilizados para el intercambio de datos de conformidad con el Reglamento (UE) 2020/1056 y los actos delegados y de ejecución adoptados con arreglo a dicho Reglamento;

2) «componente de TIC»: unidad material (equipos informáticos) o inmaterial (programas informáticos) o conjunto de dichas unidades utilizados para realizar funcionalidades específicas que permitan la comunicación electrónica de datos;

3) «agente de la autoridad competente»: persona física facultada para acceder a los requisitos reglamentarios de información a que se refiere el artículo 2, apartado 1, del Reglamento (UE) 2020/1056, así como para tratar tales requisitos, en nombre de una autoridad competente de un Estado miembro;

4) «datos IETM»: los datos correspondientes a la información reglamentaria puestos a disposición por los operadores económicos en una plataforma IETM de conformidad con el Reglamento (UE) 2020/1056;

5) «solicitud de acceso a datos IETM»: solicitud, en nombre de una autoridad competente, para recibir los datos IETM puestos a disposición por los operadores económicos en una plataforma IETM;

6) «comunicación de seguimiento»: comunicación entre las autoridades competentes y los operadores económicos interesados en relación con la información puesta a disposición por los operadores económicos en una plataforma IETM, ocurrida tras el control de conformidad de dicha información por parte de un agente de la autoridad competente en respuesta a una solicitud de acceso a datos IETM. Esta comunicación de seguimiento podrá consistir en una solicitud de los datos IETM que falten, o en información relativa a las medidas de seguimiento adoptadas por la autoridad competente de conformidad con las disposiciones nacionales aplicables;

7) «derechos de acceso»: permisos concedidos a un agente de la autoridad competente para llevar a cabo operaciones en relación con uno o varios subconjuntos de datos IETM;

8) «derechos de tratamiento»: operaciones o conjuntos de operaciones que un agente de la autoridad competente está autorizado a realizar en un subconjunto específico de datos IETM recibido en respuesta a una solicitud de acceso a datos IETM;

9) «medio de identificación electrónica»: unidad material o inmaterial que contiene datos de identificación personal y que se utiliza para la autenticación en servicios en línea;

10) «referencias de identificación»: número de identificación personal o referencia codificada que permite la identificación única de un agente de la autoridad competente;

11) «punto de acceso de las autoridades» (o «AAP», por sus siglas en inglés): componente de TIC o conjunto de componentes de TIC que realiza las funcionalidades establecidas en el artículo 4;

12) «puerta IETM» (en inglés, «eFTI gate»): componente de TIC o conjunto de componentes de TIC que realiza las funcionalidades establecidas en el artículo 6;

13) «puerta solicitante»: puerta IETM que tramita una solicitud de acceso a datos IETM presentada a través de un AAP conectado a dicha puerta IETM o integrado en ella;

14) «puerta receptora»: puerta IETM que tramita una solicitud de acceso a datos IETM recibidos de una puerta solicitante;

15) «eDelivery»: conjunto de especificaciones técnicas y normas para el intercambio electrónico de mensajes desarrolladas por la Comisión en el marco del programa del Mecanismo «Conectar Europa» ([7]) y ampliadas en el marco del programa Europa Digital ([8]);

16) «punto de acceso de eDelivery»: componente de comunicación que forma parte del servicio de transmisión electrónica eDelivery y que se basa en especificaciones y normas técnicas;

17) «descubrimiento estático»: mecanismo que permite que un punto de acceso de eDelivery obtenga los datos de conexión de otro punto de acceso de eDelivery sin recurrir a sistemas de terceros;

18) «descubrimiento dinámico»: mecanismo que permite que un punto de acceso de eDelivery obtenga los datos de conexión de otro punto de acceso de eDelivery buscándolos en un sistema de terceros;

19) «claves de seguridad»: pares de claves de cifrado públicas y privadas, generadas por algoritmos de cifrado, en forma de números muy grandes y con una relación única entre sí;

20) «certificado de seguridad»: documento digital expedido por una autoridad de certificación que se utiliza para establecer un canal seguro de comunicación electrónica entre dos partes; incluye la clave de seguridad pública e información sobre el objeto del certificado;

21) «autoridad de certificación»: entidad que gestiona el ciclo de vida de los certificados digitales, que puede abarcar los procesos de inscripción y los procesos de expedición, entrega, activación, suspensión, revocación, renovación o reactivación de los certificados de seguridad;

22) «aplicación de usuario»: componente de TIC que realiza las funcionalidades establecidas en el artículo 7;

23) «documentos de orientación técnica»: conjunto de documentos técnicos detallados y no vinculantes, elaborados por la Comisión en cooperación con los Estados miembros en el marco del grupo de trabajo a que se refiere el artículo 13.

Artículo 2

Medidas comunes

1. Los Estados miembros velarán por que sus autoridades competentes tengan acceso a los sistemas de TIC que puedan tratar los enlaces únicos de identificación («UIL», por sus siglas en inglés) electrónica comunicados por los operadores económicos con arreglo al artículo 4, apartado 3, del Reglamento (UE) 2020/1056, y que permitan a los agentes de sus autoridades competentes acceder a los datos IETM y tratarlos utilizando cualquiera de los procedimientos siguientes:

a) tratando directamente el UIL, cuando el operador económico lo comunique en un formato legible mecánicamente, mediante su visualización en la pantalla de un dispositivo electrónico o en un soporte físico como el papel, o, cuando la autoridad competente opte por permitir dicha comunicación, también mediante su envío por correo electrónico u otra aplicación de mensajería electrónica;

b) recuperando primero el UIL, según lo haya comunicado el operador económico mediante su publicación en un registro específico, por medio de un identificador único asociado a una operación de transporte.

2. Los Estados miembros velarán por que los sistemas de TIC a que se refiere el apartado 1 ofrezcan al menos las siguientes funcionalidades:

a) identificación debidamente autenticada y debida autorización de los agentes de las autoridades competentes, cada vez que un agente presente una solicitud de acceso a datos IETM;

b) intermediación en las solicitudes de acceso a datos IETM presentadas por los agentes de las autoridades competentes, incluida la recuperación de la información solicitada desde la plataforma o plataformas IETM pertinentes, mediante conexiones seguras a esas plataformas.

([7]) https://digital-strategy.ec.europa.eu/es/activities/cef-digital.
([8]) https://digital-strategy.ec.europa.eu/es/activities/digital-programme.

3. Para llevar a cabo las funcionalidades enumeradas en el apartado 2, dichos sistemas de TIC incluirán, como mínimo, los siguientes componentes:

a) puntos de acceso de las autoridades (AAP);

b) un registro de autorizaciones;

c) puertas IETM;

d) un mecanismo de búsqueda;

e) una aplicación de usuario.

4. Los Estados miembros velarán por que los componentes enumerados en el apartado 3 cumplan los requisitos establecidos en el capítulo II. Los Estados miembros serán responsables de la creación, el alojamiento, el desarrollo, la disponibilidad, el seguimiento, la actualización y el mantenimiento de dichos componentes, así como de la seguridad de la información tratada en ellos. Cuando dos o más Estados miembros creen o desarrollen conjuntamente uno o varios de dichos componentes, serán responsables conjuntamente de su creación, alojamiento, desarrollo, disponibilidad, seguimiento, actualización, mantenimiento y seguridad.

5. Los Estados miembros siguen siendo responsables de garantizar que el acceso de las autoridades competentes a los datos IETM, y el tratamiento de estos, tengan como fin único el comprobar que se cumplen las disposiciones legales nacionales y de la UE aplicables y se lleven a cabo de conformidad con las disposiciones nacionales y de la UE aplicables que establezcan las condiciones para llevar a cabo esos controles de la conformidad, así como con las normas sobre el respeto de la privacidad de los datos personales y la confidencialidad de los datos comerciales.

Artículo 3

Solicitudes de acceso a datos IETM, respuestas y comunicación de seguimiento

1. Los agentes de las autoridades competentes presentarán todas las solicitudes de acceso a los datos IETM a través del componente AAP descrito en el artículo 4, por medio de la aplicación de usuario descrita en el artículo 7.

2. Las solicitudes de acceso a datos IETM contendrán la siguiente información:

a) el UIL de los datos IETM a los que se solicite acceso, o uno o varios identificadores que permitan recuperar el UIL del registro de identificadores descrito en el artículo 11. Esta información la facilitará el agente de la autoridad competente responsable de la solicitud;

b) las referencias a los derechos de acceso del agente de la autoridad competente responsable de la presentación de la solicitud, tal como figuren en el registro de autorizaciones descrito en el artículo 5. Esta información la añadirá automáticamente la aplicación de usuario;

c) el número único de identificación de la solicitud, según haya sido asignado por el AAP. Esta información la añadirá automáticamente la aplicación de usuario.

3. Las respuestas a una solicitud de acceso a datos IETM podrán adoptar una de las formas siguientes:

a) datos IETM transmitidos por una plataforma IETM sobre la base de la información contenida en una solicitud, y los metadatos o identificadores de intercambio de mensajes asociados, necesarios para que las puertas IETM receptoras o los puntos de acceso de las autoridades puedan asociar los datos IETM a la solicitud correspondiente;

b) mensajes de error que contengan especificaciones textuales codificadas o breves del tipo de error cuando la puerta IETM o la plataforma IETM no pueda proporcionar los datos IETM solicitados por razones técnicas o razones relacionadas con procesos de negocio;

c) mensaje en el que se indique que no se dispone de datos, que será emitido por una puerta IETM receptora cuando tramite una solicitud que contenga identificadores y el mecanismo de búsqueda de la puerta detecte que no hay UIL activos vinculados a dichos identificadores en su registro de identificadores;

d) mensaje de «no respuesta», que será transmitido por una puerta IETM o una plataforma IETM cuando dicha puerta o plataforma haya confirmado la recepción de la solicitud pero no haya enviado un mensaje que contenga los datos IETM solicitados en un plazo de sesenta segundos a partir de la confirmación de la recepción.

4. Cuando el agente de la autoridad competente determine que la información puesta a disposición por un operador económico en una plataforma IETM, según se haya obtenido en respuesta a una solicitud de acceso a datos IETM, está incompleta o incumple de otro modo los requisitos reglamentarios de información sobre cuya base se presentó la solicitud, podrá comunicar dichas conclusiones al operador económico presentando una comunicación de seguimiento específica para dicha información. Toda comunicación de seguimiento de este tipo deberá cumplir los requisitos legales nacionales aplicables sobre las medidas de seguimiento de los controles de la conformidad reglamentarios.

5. Cuando se presente una comunicación de seguimiento específica de aquellas a las que se refiere el apartado 4, la autoridad competente también la transmitirá a través del componente AAP, por medio de la aplicación de usuario. Esa comunicación incluirá:

a) la información que debe comunicar la autoridad competente al operador económico, en formato de texto libre, o como documento adjunto;

b) el UIL de los datos IETM y el número único de identificación de la solicitud de acceso a los datos respecto de la que se presenta la comunicación de seguimiento.

CAPÍTULO II

COMPONENTES FUNCIONALES

Artículo 4

Puntos de acceso de las autoridades

1. Los componentes de un AAP permitirán el acceso de los agentes de las autoridades competentes al entorno de intercambio IETM y constituirán el único punto de acceso de los agentes a dicho entorno.

2. Los AAP llevarán a cabo las siguientes funcionalidades:

a) autenticar la identidad de los agentes de las autoridades competentes o garantizar que se autentique la identidad de los agentes de las autoridades competentes;

b) autorizar la solicitud de acceso a datos IETM de los agentes de las autoridades competentes, sobre la base de los derechos de acceso correspondientes almacenados en el registro de autorizaciones, o rechazar la solicitud cuando los agentes de las autoridades competentes no tengan registrados derechos de acceso activos;

c) registrar las solicitudes de acceso a datos IETM que hayan sido autorizadas expidiendo un número único de identificación para cada solicitud, y anotar al menos la siguiente información respecto de cada una de ellas:

   i) referencias de identificación del agente responsable de la presentación de la solicitud,

   ii) el UIL de los datos IETM a los que se solicite acceso, o el identificador o identificadores facilitados por el agente al presentar la solicitud,

   iii) las referencias a los derechos de acceso del agente de la autoridad competente responsable de la presentación de la solicitud, tal como figuren en el registro de autorizaciones,

   iv) la fecha y la hora de presentación de la solicitud;

d) transmitir a la puerta IETM las solicitudes de acceso a datos IETM que hayan sido autorizadas para su tramitación, facilitando la siguiente información:

   i) el número único de identificación de la solicitud,

   ii) el UIL de los datos IETM para los que se solicite acceso, o el identificador o identificadores facilitados por el agente al presentar la solicitud,

   iii) las referencias a los derechos de tratamiento del agente de la autoridad competente responsable de la presentación de la solicitud, tal como figuren en el registro de autorizaciones;

e) recibir las respuestas a las solicitudes transmitidas por la puerta IETM y ponerlas a disposición del agente de la autoridad competente responsable de dicha solicitud a través de la aplicación de usuario;

f) mantener una pista de auditoría de las respuestas recibidas para cada solicitud, registrando al menos la siguiente información:

i) el número único de identificación de la solicitud para la que se recibió la respuesta,

ii) la fecha y la hora en que el AAP recibió la respuesta,

iii) la fecha y la hora en que el AAP remitió la respuesta al agente responsable de la solicitud correspondiente;

g) conservar durante un período de dos años un archivo de las solicitudes de acceso a datos IETM y del registro de respuestas recibidas o, cuando las disposiciones nacionales aplicables relativas a la disponibilidad de pruebas para la aplicación de las disposiciones para las que se requiera acceso a datos IETM prevean un período de tiempo más largo, durante ese período;

h) cuando se presente una comunicación de seguimiento de conformidad con el artículo 3, apartado 4, registrar la comunicación de seguimiento expidiendo un número único de identificación para la comunicación de seguimiento y anotar al menos la siguiente información respecto de dicha comunicación de seguimiento:

i) referencias de identificación del agente responsable de la presentación de la comunicación de seguimiento,

ii) el UIL de los datos IETM y el número único de identificación de la solicitud de acceso a los datos respecto de la que se presentó la comunicación de seguimiento,

iii) la fecha y la hora de presentación de la comunicación de seguimiento,

iv) el contenido de la comunicación de seguimiento;

i) transmitir las comunicaciones de seguimiento a la puerta IETM para su tratamiento, facilitando la siguiente información:

i) el UIL de los datos IETM y el número único de identificación de la solicitud de acceso a los datos respecto de la que se presentó la comunicación de seguimiento,

ii) el contenido de la comunicación de seguimiento.

3. Para ofrecer las funcionalidades establecidas en el apartado 2, el AAP deberá:

a) utilizar medios de identificación electrónica adecuados que permitan una identificación y autenticación fiables de los agentes de las autoridades competentes, o que permitan verificar que la identificación y autenticación de dichos agentes está garantizada por otro componente adecuado de TIC;

b) utilizar un registro de autorizaciones;

c) establecer y mantener una conexión segura con una puerta IETM;

d) permitir una conexión segura con la aplicación de usuario.

4. Los Estados miembros podrán establecer los AAP fuera de la puerta IETM, como parte de los sistemas de TIC de sus autoridades competentes respectivas, o integrándolos en su puerta IETM respectiva.

Artículo 5

Registro de autorizaciones

Los Estados miembros velarán por que los derechos de los agentes de sus autoridades competentes a acceder a datos IETM y tratarlos se inscriban en un registro de autorizaciones y se mantengan actualizados. El registro de autorizaciones incluirá, para cada agente de una autoridad competente, al menos la siguiente información:

a) referencias de identificación únicas del agente;

b) los derechos de acceso del agente correspondiente, expresados como la lista de referencias de los actos jurídicos nacionales y de la Unión que exijan el suministro de información reglamentaria y respecto de los cuales el agente respectivo tenga competencias y, más concretamente, como la lista de los identificadores respectivos de los subconjuntos de datos IETM correspondientes a dichas disposiciones, tal como se establecen en las secciones 3 y 4 del anexo del Reglamento Delegado (UE) 2024/2024 de la Comisión ([9]);

c) los derechos de tratamiento del agente respectivo, expresados como referencias codificadas a las operaciones de tratamiento que el agente tenga derecho a realizar en cada uno de los subconjuntos de datos IETM respectivos, en consonancia con la legislación nacional o de la Unión aplicable que determine las competencias de dicho agente;

d) un registro de los cambios en los derechos de acceso y tratamiento de dicho agente.

Artículo 6

Puertas IETM

1. Las puertas IETM garantizarán, directamente o a través de la conexión con otras puertas IETM, que:

a) las solicitudes de acceso a datos IETM que hayan sido autorizadas se transmitan a la plataforma IETM y contengan la información específica solicitada;

b) para cada solicitud de este tipo, la respuesta recibida de la plataforma IETM correspondiente se transmita a la aplicación de usuario del agente de la autoridad competente responsable de dicha solicitud, ya sea directamente o a través de un AAP, según proceda, y

c) una vez presentada, la comunicación de seguimiento relativa a dicha solicitud se transmita a la plataforma IETM que contenga los datos IETM para los que se haya presentado la solicitud y se haya proporcionado la respuesta.

2. Toda puerta IETM ofrecerá las siguientes funcionalidades:

a) validar la solicitud de acceso a datos IETM y, cuando se haya presentado, la comunicación de seguimiento, de una de las siguientes maneras:

   i) cuando actúe como «puerta solicitante», en los casos en que el AAP se establezca como un componente separado de la puerta IETM, verificando la clave de seguridad del AAP a través del cual se presentó la solicitud o la comunicación de seguimiento,

   ii) cuando actúe como «puerta receptora», verificando la clave de seguridad de la puerta IETM de la que recibió la solicitud o la comunicación de seguimiento,

   iii) cuando falle la validación de la clave de seguridad de la puerta IETM correspondiente, enviando un mensaje de error a la «puerta solicitante», al AAP o al agente de la autoridad competente responsable de la solicitud o de la comunicación de seguimiento, según proceda;

b) tramitar la solicitud de acceso a datos IETM y, cuando se haya presentado, la comunicación de seguimiento, mediante el mecanismo de búsqueda establecido en el artículo 8 y, sobre esa base, remitir la solicitud o la comunicación de seguimiento, según proceda:

   i) a la plataforma IETM o a las puertas IETM correspondientes, cuando actúen como «puerta solicitante»,

   ii) a la plataforma IETM correspondiente, cuando actúe como «puerta solicitante»;

c) mantener una pista de auditoría de todas las solicitudes de acceso a datos IETM o a las comunicaciones de seguimiento que haya tramitado, registrando al menos la siguiente información:

   i) el número único de identificación de la solicitud de acceso a datos IETM o de la comunicación de seguimiento,

   ii) el identificador del AAP o de la puerta IETM solicitante de los que haya recibido dicha solicitud o comunicación de seguimiento,

   iii) la fecha y la hora en que recibió dicha solicitud;

([9]) Reglamento Delegado (UE) 2024/2024 de la Comisión, de 26 de julio de 2024, por el que se completa el Reglamento (UE) 2020/1056 mediante el establecimiento del conjunto de datos comunes IETM y los subconjuntos de datos IETM (DO L, 2024/2024, 20.12.2024, ELI: http://data.europa.eu/eli/reg_del/2024/2024/oj).

d) validar la respuesta recibida a una solicitud que haya tramitado, como sigue:

i) cuando reciba la respuesta directamente de la plataforma IETM, comprobando la clave de seguridad y el estado de certificación de la plataforma IETM sobre la base del registro a que se refiere el apartado 3, letra e),

ii) cuando reciba la respuesta de una «puerta IETM receptora», comprobando la clave de seguridad de dicha puerta IETM sobre la base del registro a que se refiere el apartado 3, letra f),

iii) cuando falle la validación de la clave de seguridad de la puerta IETM o la plataforma IETM correspondiente, enviando el mensaje de error correspondiente a la «puerta solicitante», al AAP o a la aplicación de usuario del agente de la autoridad competente responsable de la solicitud, según proceda;

e) remitir la respuesta recibida a una solicitud que haya tramitado utilizando la misma vía de la solicitud remitida, aunque en secuencia inversa, según proceda:

i) a la «puerta IETM solicitante», o

ii) a la aplicación de usuario del agente de la autoridad competente responsable de dicha solicitud, directamente o a través del AAP;

f) cuando se reciba un acuse de recibo de la solicitud pero no se reciba ninguna otra respuesta en un plazo de sesenta segundos a partir de dicho acuse de recibo, transmitir el mensaje de «no respuesta» a la «puerta solicitante», al AAP o a la aplicación de usuario del agente de la autoridad competente responsable de la solicitud, según proceda;

g) mantener una pista de auditoría de las solicitudes de acceso que haya remitido, registrando al menos la siguiente información:

i) el UIL del conjunto de datos IETM que recibió en respuesta a dicha solicitud,

ii) el número único de identificación de la plataforma IETM o de la «puerta IETM receptora» de la que recibió la respuesta,

iii) la fecha y la hora en que recibió dicha respuesta,

iv) en caso de que no se haya recibido respuesta alguna, una mención a tal efecto;

h) archivar y conservar, a efectos de auditoría, los registros especificados en las letras c) y g) durante un período de dos años o, cuando las disposiciones nacionales relativas a la disponibilidad de pruebas para la aplicación de las disposiciones para las que se requiera acceso a datos IETM prevean un período de tiempo más largo, durante ese período.

3. Para permitir las funcionalidades a que se refiere el apartado 2, toda puerta IETM deberá:

a) utilizar un mecanismo de búsqueda, de conformidad con el artículo 8;

b) establecer y mantener una conexión segura con los AAP que actúen como intermediarios en el acceso al entorno de intercambio IETM por parte de los agentes de las autoridades competentes del Estado miembro que estableció la correspondiente puerta IETM;

c) cuando los AAP se establezcan como componentes integrados de la puerta IETM, establecer y mantener una conexión segura con la aplicación (o aplicaciones) de usuario, según proceda, de los agentes de la autoridad competente del Estado miembro que estableció la puerta IETM correspondiente;

d) cuando los AAP se establezcan como componentes separados de la puerta IETM, establecer y mantener actualizado un registro que contenga los números únicos de identificación y los certificados de seguridad de dichos AAP;

e) establecer y mantener una conexión segura con todas las demás puertas IETM, así como un registro actualizado que contenga los números únicos de identificación y los certificados de seguridad de dichas puertas IETM;

f) establecer y mantener una conexión segura con todas las plataformas IETM que hayan recibido certificación en el Estado miembro o Estados miembros que establecieron la puerta IETM correspondiente, así como un registro actualizado que contenga los números únicos de identificación, las claves de seguridad y el estado de certificación de dichas plataformas IETM;

g) poder utilizar servicios u objetos definidos comúnmente, como la configuración, los códigos de error, las taxonomías o las listas de códigos en el entorno de intercambio IETM, cuando estos servicios u objetos se acuerden en el marco de la red de apoyo operativo a que se refiere el artículo 13.

4. Cuando no exista ningún organismo de evaluación de la conformidad que esté acreditado en un Estado miembro para certificar plataformas IETM con arreglo al artículo 11 del Reglamento (UE) 2020/1056, dicho Estado miembro velará por que su puerta IETM establezca y mantenga la conexión segura y el registro actualizado a que se refiere el apartado 3, letra f), respecto de las plataformas IETM que hayan recibido certificación de organismos de evaluación de la conformidad acreditados en otros Estados miembros. Dicho Estado miembro actuará a petición del operador económico o del proveedor de servicios IETM que explote dicha plataforma, y tras haber solicitado y recibido confirmación del Estado miembro en el que la plataforma IETM recibió la certificación de que no ha recibido ninguna otra solicitud de confirmación para esa misma plataforma IETM de otro Estado miembro. Esto eximirá a la puerta IETM del Estado miembro en el que la plataforma IETM recibió la certificación de la obligación de establecer y mantener una conexión segura con dicha plataforma.

Artículo 7

Aplicación de usuario

1. La aplicación de usuario permitirá a los agentes de las autoridades competentes interactuar con los AAP.

2. La aplicación de usuario ofrecerá al menos las siguientes funcionalidades:

a) generar las solicitudes de acceso a datos IETM, sobre la base de la información facilitada por un agente de la autoridad competente, una vez que este haya sido debidamente identificado, autenticado y autorizado por el AAP;

b) recibir y mostrar al agente de la autoridad competente responsable de la solicitud los datos IETM correspondientes facilitados por las plataformas IETM correspondientes en respuesta a dicha solicitud o los mensajes de «no respuesta» o de error transmitidos por el AAP o la «puerta IETM receptora»;

c) permitir otras operaciones de tratamiento por parte del agente de la autoridad competente responsable de la solicitud de datos IETM recibida, en consonancia con los derechos de tratamiento de dicho agente;

d) cuando las disposiciones nacionales aplicables lo permitan, generar comunicaciones de seguimiento, sobre la base de la información facilitada por un agente de la autoridad competente.

3. Para permitir las funcionalidades a que se refiere el apartado 2, toda aplicación de usuario deberá, como mínimo:

a) proporcionar a los agentes de la autoridad competente una interfaz gráfica de usuario;

b) establecer y mantener una conexión segura con un AAP o una puerta IETM, según proceda;

c) para el tratamiento de datos, utilizar como referencia los subconjuntos de datos correspondientes a las disposiciones de los actos jurídicos nacionales y de la Unión, establecidos por el Reglamento Delegado (UE) 2024/2024, respecto de los cuales los agentes de las autoridades competentes que desarrollaron la aplicación de usuario tienen competencias.

Artículo 8

Mecanismo de búsqueda

1. El mecanismo de búsqueda será un componente integrado en una puerta IETM que, como funcionalidad principal, deberá tratar la información incluida en la solicitud o comunicación de seguimiento, y para ello deberá:

a) recuperar, a partir del UIL de los datos IETM, el identificador de la plataforma IETM que almacena los datos IETM a los que se solicitó el acceso o respecto de los que se presentó la comunicación de seguimiento y, respectivamente, el identificador de la puerta IETM con la que está conectada dicha plataforma;

b) cuando la solicitud de información incluya uno o varios de los identificadores establecidos en el artículo 11, apartado 3, buscar en el registro de identificadores un valor coincidente y

   i) si se encuentra una coincidencia, recuperar el UIL activo o el conjunto de UIL conectados a los identificadores respectivos, para después tratar la información en los UIL respectivos de conformidad con la letra a),

   ii) si no se encuentra ninguna coincidencia, notificarlo a la puerta IETM.

2. Para permitir la funcionalidad a que se refiere el apartado 1, todo mecanismo de búsqueda deberá:

a) mantener un registro de identificadores, de conformidad con el artículo 11;

b) utilizar un registro de editores de metadatos de servicio y un localizador de metadatos de servicio de conformidad con las especificaciones de eDelivery, o un servicio de registro con capacidades similares, para permitir el descubrimiento de las plataformas IETM, sobre la base de la información contenida en la solicitud o en la comunicación de seguimiento.

CAPÍTULO III

ESPECIFICACIONES TÉCNICAS

Artículo 9

Intercambios de mensajes

1. Los Estados miembros velarán por que las puertas IETM que establezcan, así como los AAP y las aplicaciones de usuario de sus autoridades competentes, comuniquen y puedan recibir comunicaciones en un formato normalizado de intercambio de mensajes. Para la comunicación entre las puertas IETM y entre estas y las plataformas IETM, se utilizará el formato XML.

2. Toda comunicación entre puertas IETM tendrá lugar como intercambio de mensajes a través de los puntos de acceso de eDelivery, de conformidad con las especificaciones de intercambio de mensajes de eDelivery, y utilizando el mecanismo de descubrimiento estático de eDelivery.

3. El intercambio de mensajes a través de los puntos de acceso de eDelivery, de conformidad con las especificaciones de intercambio de mensajes de eDelivery, y utilizando el mecanismo de descubrimiento dinámico de eDelivery, también estará habilitado para la comunicación entre las puertas IETM y las plataformas IETM.

4. Cuando un Estado miembro ya haya establecido especificaciones equivalentes, definidas a nivel nacional, para el intercambio seguro de mensajes en los servicios públicos digitales, podrá optar por permitir que la comunicación entre las plataformas IETM y la puerta IETM establecida por ese Estado miembro tenga también lugar sobre la base de dichas especificaciones equivalentes en materia de intercambio de mensajes. En tales casos, los Estados miembros velarán por que dichas especificaciones, debidamente detalladas y actualizadas, estén a disposición del público.

Artículo 10

Certificados de seguridad

1. Los Estados miembros expedirán certificados de seguridad, a través de una autoridad de certificación, a los puntos de acceso de eDelivery integrados en las puertas IETM que hayan establecido, así como a los puntos de acceso de eDelivery o, en su caso, al punto de acceso equivalente de intercambio de mensajes de cada plataforma IETM que haya recibido la certificación de un organismo de evaluación de la conformidad acreditado en su Estado miembro respectivo.

2. Los Estados miembros velarán por que las claves de seguridad privadas del punto de acceso de eDelivery integrado en la puerta (o puertas) IETM se almacenen de forma segura y por que sus correspondientes certificados digitales se expidan de manera segura entre las puertas IETM y entre una puerta IETM y las plataformas IETM conectadas con dicha puerta.

3. Los Estados miembros garantizarán la existencia de mecanismos seguros para recibir, registrar, recuperar y validar las claves públicas o los certificados de seguridad de las plataformas IETM conectadas con su puerta IETM. Cuando un Estado miembro establezca un registro de editores de metadatos de servicio con arreglo a las especificaciones sobre editores de metadatos de servicio de eDelivery, con mecanismos de seguridad adecuados, podrá utilizarse un registro de editores de metadatos de servicio a tal efecto.

Artículo 11

Registro de identificadores

1. El registro de identificadores a que se refiere el artículo 8, apartado 2, letra a), permitirá a los operadores económicos cargar, a través de una plataforma IETM, el UIL de un conjunto de datos IETM junto con los identificadores que permitan la recuperación única de dicho UIL, tal como se indica en el apartado 3. El registro de identificadores permitirá la carga, activación, desactivación o supresión del UIL de un conjunto de datos IETM y de los identificadores respectivos.

2. La composición del UIL permitirá la recuperación del identificador de la puerta IETM, el identificador de la plataforma IETM y el identificador único del conjunto de datos IETM correspondiente a la información reglamentaria puesta a disposición por los operadores económicos en la plataforma IETM correspondiente, donde:

a) el identificador de la puerta IETM estará constituido por un identificador que permita su descubrimiento exclusivo en el entorno IETM;

b) el identificador de la plataforma IETM estará constituido por un identificador que permita su descubrimiento exclusivo en el entorno IETM;

c) la identificación única del conjunto de datos IETM estará constituida por un número único en formato de identificador universal único (UUID, por sus siglas en inglés) asignado automáticamente por la plataforma IETM.

3. Los identificadores que deberá permitir el registro consistirán en:

a) elementos de datos del conjunto de datos IETM correspondientes a la información reglamentaria puesta a disposición por los operadores económicos, tal como se describe en la sección 2 del anexo del Reglamento Delegado (UE) 2024/2024, con los números de identificación siguientes:

   i) eFTI39,

   ii) eFTI188,

   iii) eFTI374,

   iv) eFTI378,

   v) eFTI448,

   vi) eFTI581,

   vii) eFTI578,

   viii) eFTI618,

   ix) eFTI620,

   x) eFTI987,

   xi) eFTI1000;

b) un elemento de datos que indique si se están transportando o no mercancías peligrosas, que presentará las siguientes características: identificador de elemento de datos «eFTI1451»; denominación «Indicador de mercancías peligrosas a bordo», y definición «Indicación de si se transportan o no mercancías peligrosas con arreglo al ADR/ADN/RID. "Sí" significa que las mercancías peligrosas se encuentran a bordo de la unidad de transporte. "No" significa que las mercancías transportadas no figuran en la lista del ADR/ADN/RID de mercancías peligrosas o que las mercancías peligrosas están exentas de los requisitos de información establecidos en los puntos 3.5.6, 5.1.5.4.2, 5.4.1, 5.5.2.4.1 o 5.5.3.7 del ADR/ADN/RID.».

4. El registro de identificadores activará el UIL para ponerlo a disposición para consultas, una vez cargado, y lo desactivará cuando se cargue el identificador a que se refiere el apartado 3, letra a), inciso ii), del presente artículo. Con el fin de permitir los controles con arreglo a las disposiciones del Reglamento (CE) n.º 1072/2009, en el caso de los UIL para los que el identificador previsto en el apartado 3, letra a), inciso vi), del presente artículo tenga el valor «3», correspondiente al «transporte por carretera», el registro de identificadores solo desactivará tales UIL una vez transcurrido el período de tiempo a que se refiere el artículo 8, apartado 2, del Reglamento (CE) n.º 1072/2009. Tras la desactivación, el registro suprimirá el UIL y los identificadores conectados a él.

CAPÍTULO IV

MANTENIMIENTO Y GOBERNANZA

Artículo 12

Red de apoyo técnico

1. Los Estados miembros crearán servicios de asistencia técnica a dos niveles distintos:

a) un servicio de asistencia de «nivel 1», destinado a prestar apoyo técnico a los agentes de las autoridades competentes en caso de que surjan problemas operativos;

b) un servicio de asistencia de «nivel 2», para ofrecer apoyo a:

   i) los servicios de asistencia de «nivel 1» que ofrecen apoyo a los agentes de control,

   ii) los servicios de asistencia de «nivel 1» establecidos por los propietarios de las plataformas IETM para prestar apoyo técnico a los operadores económicos.

2. La Comisión creará un servicio de asistencia de «nivel 3», que deberá:

a) prestar apoyo técnico a los servicios de asistencia de «nivel 2» para resolver problemas operativos relacionados con el funcionamiento del entorno de intercambio IETM general, incluidas las normas, los procedimientos y las especificaciones funcionales y técnicas de ejecución, así como el conjunto de datos comunes y los subconjuntos de datos IETM establecidos en los actos delegados y de ejecución adoptados con arreglo al Reglamento (UE) 2020/1056;

b) actuar como facilitador en los problemas operativos que afecten a dos o más Estados miembros y para los que sea necesaria una coordinación a nivel de la Unión, incluida la interoperabilidad técnica de las puertas IETM y la comunicación entre ellas;

c) interactuar con los servicios de la Comisión que proporcionan programas informáticos específicos o especificaciones de los productos utilizados por el entorno de intercambio IETM, como eDelivery.

3. Los servicios de asistencia técnica de «nivel 1» y «nivel 2» también se pondrán en contacto entre sí para resolver cuestiones de interés común a sus respectivos niveles.

4. La disponibilidad de los servicios de asistencia técnica se sincronizará en toda la Unión para garantizar un período mínimo de disponibilidad común durante los días laborables entre las 10.00 y las 16.00 horas, hora de Europa central (CET/CEST), excepto los días festivos nacionales. Durante los fines de semana y los días festivos nacionales estará disponible un servicio de emergencia, que contará con al menos un miembro del personal de guardia para resolver cuestiones urgentes que afecten gravemente al funcionamiento del entorno de intercambio IETM, ya sea a nivel nacional o de la Unión.

5. Todos los servicios de asistencia técnica utilizarán herramientas de asistencia específicas que permitan la identificación única y el seguimiento de cada solicitud de apoyo técnico, incluso cuando la resolución de una solicitud requiera comunicación entre los servicios de asistencia.

6. Los servicios de asistencia conservarán un registro de todas las solicitudes de asistencia y su historial, y elaborarán informes sobre sus actividades periódicamente.

7. Los Estados miembros se comunicarán mutuamente y comunicarán a la Comisión los datos de contacto de sus respectivos servicios de asistencia de «nivel 2».

8. La fecha de inicio de la disponibilidad de los servicios de asistencia técnica será la fecha a que se refiere el artículo 5, apartado 1, del Reglamento (UE) 2020/1056. La adecuación del período mínimo de disponibilidad común de los servicios de asistencia técnica se evaluará en un plazo de doce meses a partir de esa fecha.

Artículo 13

Red de apoyo operativo

1. Se creará un grupo de trabajo específico como subgrupo del grupo de expertos creado en virtud de la Decisión C(2018) 5921 de la Comisión, con el mandato de garantizar que las operaciones IETM se lleven a cabo con el nivel de calidad requerido.

2. Los miembros del grupo de trabajo nombrados por los Estados miembros actuarán también como «puntos de contacto nacionales IETM».

3. Los miembros del grupo de trabajo cooperarán y se reunirán periódicamente para, entre otras cosas:

a) proporcionar información actualizada sobre el estado operativo del entorno de intercambio IETM;

b) ayudar a los servicios de la Comisión en sus esfuerzos por resolver los problemas técnicos y operativos notificados por los Estados miembros o por el servicio de asistencia de «nivel 3» que requieran coordinación y ayuda operativa a nivel de la Unión;

c) ayudar a la Comisión en la elaboración de documentos de orientación técnica en apoyo de la aplicación del presente Reglamento.

CAPÍTULO V

DISPOSICIONES FINALES

Artículo 14

Entrada en vigor y aplicación

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

Será aplicable a partir de la fecha de entrada en vigor del presente Reglamento.

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

Hecho en Bruselas, el 5 de julio de 2024.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN