REGLAMENTO DELEGADO (UE) 2025/885 DE LA COMISIÓN

de 29 de abril de 2025

por el que se completa el Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo en lo que respecta a las normas técnicas de regulación en las que se especifican los mecanismos, sistemas y procedimientos para prevenir, detectar e informar sobre el abuso de mercado, la plantilla que debe utilizarse para notificar la sospecha de abuso de mercado y los procedimientos de coordinación entre las autoridades competentes para la detección y sanción del abuso de mercado

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n.º 1093/2010 y (UE) n.º 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937 ([1]), y en particular su artículo 92, apartado 2, párrafo tercero,

Considerando lo siguiente:

(1) Es necesario establecer los requisitos aplicables a los mecanismos, procedimientos y sistemas que las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional deben implantar para la notificación de órdenes, operaciones y otros aspectos del funcionamiento de la tecnología de registro distribuido (TRD), incluido el mecanismo de consenso, cuando puedan darse circunstancias que indiquen que se ha cometido, se está cometiendo o es probable que se cometa un abuso de mercado. Tales requisitos son fundamentales y deben ayudar a prevenir y detectar el abuso de mercado. Esos requisitos también deben ayudar a garantizar que las notificaciones relativas a sospechas razonables sobre órdenes, operaciones y otros aspectos del funcionamiento de la tecnología de registro distribuido presentadas a las autoridades competentes sean pertinentes, exhaustivas y útiles.

(2) Para garantizar que la prevención y detección del abuso de mercado sea eficaz, deben establecerse sistemas adecuados para el seguimiento de las órdenes, las operaciones y otros aspectos del funcionamiento de la TRD, de conformidad con la escala, el tamaño y la naturaleza de la actividad empresarial de la persona que tramita o ejecuta operaciones a título profesional. Dichos sistemas deben facilitar el análisis humano llevado a cabo por personal debidamente formado, sobre la base de información objetiva a disposición de la entidad informadora. La entidad debe recopilar datos personales adicionales únicamente para garantizar un análisis humano adecuado. A fin de permitir un análisis más profundo de las posibles operaciones con información privilegiada o manipulación del mercado o de los intentos de tales operaciones, los sistemas de seguimiento del abuso de mercado deben ser capaces de generar alertas con arreglo a parámetros especificados. El acceso a dichas alertas debe registrarse para garantizar que solo se utilicen para detectar abusos de mercado. Todo el proceso puede requerir algún nivel de automatización.

(3) Para analizar si los mecanismos, sistemas y procedimientos para prevenir y detectar el abuso de mercado son adecuados, es necesario evaluar el impacto que la persona que tramita o ejecuta operaciones a título profesional podría tener en el mercado. Como parte de dicha evaluación, dichas personas deben valorar si tienen una posición significativa o dominante en cualquier segmento de activos del mercado de criptoactivos, en cuyo caso dichos mecanismos, sistemas y procedimientos deben ser proporcionados a su posición.

(4) La prevención y detección del abuso de mercado requiere un seguimiento continuo de todas las órdenes y operaciones tramitadas o ejecutadas por personas que tramiten o ejecuten operaciones a título profesional, con independencia de que dichas órdenes y operaciones se ejecuten en el registro distribuido («dentro de la cadena») o fuera de este («fuera de la cadena»), incluidas las transferencias de criptoactivos entre cuentas de clientes del mismo proveedor de servicios de criptoactivos.

([1]) DO L 150 de 9.6.2023, p. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj.

(5) Con objeto de facilitar y promover un enfoque y prácticas uniformes en toda la Unión en relación con la prevención, la detección y la sanción de los abusos de mercado, es necesario establecer disposiciones de aplicación para armonizar el contenido, la plantilla y los plazos de la notificación de órdenes, operaciones y otros aspectos del funcionamiento de la TRD sospechosos.

(6) Para compartir recursos, desarrollar y mantener de forma centralizada sistemas de seguimiento y desarrollar conocimientos especializados en el contexto del seguimiento de las órdenes y operaciones sospechosas, las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional deben poder delegar la prevención y detección de dichas órdenes, operaciones y otros aspectos del funcionamiento de la TRD dentro del grupo, o delegar el análisis de datos y la generación de alertas, con sujeción a condiciones adecuadas. Esta delegación no debe impedir a las autoridades competentes evaluar, en cualquier momento, si los mecanismos, sistemas y procedimientos de la persona en la que se hayan delegado las funciones son eficaces para cumplir con la obligación de prevenir y detectar los abusos de mercado. La obligación de informar y la responsabilidad de cumplir el presente Reglamento y el artículo 92 del Reglamento (UE) 2023/1114 deben seguir incumbiendo a la persona que delegue esas funciones.

(7) Los proveedores de servicios de criptoactivos que gestionen una plataforma de negociación deben disponer de normas de negociación adecuadas que contribuyan a prevenir el abuso de mercado. Dichas entidades también deben disponer de sistemas para reproducir el libro de órdenes con el fin de analizar la actividad de negociación.

Una plantilla única y armonizada para la presentación electrónica de una notificación de operaciones y órdenes sospechosas («STOR») facilitaría el intercambio eficiente de información sobre órdenes y operaciones sospechosas entre las autoridades competentes en las investigaciones transfronterizas.

(8) Los campos de información de dicha plantilla STOR, cuando se cumplimenten de forma clara, exhaustiva, objetiva y precisa, deben ayudar a las autoridades competentes a evaluar rápidamente dichas órdenes y operaciones sospechosas y a adoptar las medidas necesarias. Por consiguiente, dicha plantilla debe permitir a las personas que presentan la STOR facilitar la información que las autoridades competentes consideren pertinente sobre órdenes, operaciones u otros aspectos del funcionamiento de la tecnología de registro distribuido sospechosos notificados y explicar los motivos de la sospecha. La plantilla también debe permitir a las personas que presentan la STOR proporcionar datos personales que permitan identificar a las personas implicadas en la actividad sospechosa y asistir a las autoridades competentes en sus investigaciones. Esta información debe proporcionarse desde un principio, de manera que la integridad de la investigación no se vea comprometida por la posible necesidad de una autoridad competente de volver a dirigirse, durante una investigación, a la persona que presentó la STOR. Toda operación de tratamiento de datos personales en virtud del presente Reglamento debe llevarse a cabo de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([2]), 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. En particular, debe respetarse el principio de minimización de datos cuando se recojan datos personales para garantizar el cumplimiento del presente Reglamento.

(9) Para facilitar la presentación de una STOR, la plantilla debe permitir adjuntar los documentos y materiales que se consideren necesarios para apoyar la notificación, también en forma de anexo en el que se enumeren las órdenes u operaciones sospechosas y se detallen sus precios y volúmenes. Además, la plantilla STOR debe permitir la notificación de conductas sospechosas relacionadas con el funcionamiento de la TRD.

(10) Las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional no deben notificar todas las órdenes recibidas o las operaciones realizadas que hayan activado una alerta interna. Un requisito de tal índole sería incompatible con el requisito de apreciar en cada caso si existen motivos razonables de sospecha.

(11) El análisis de las órdenes, operaciones u otros aspectos del funcionamiento de la TRD debe tener en cuenta no solo la información interna de la persona que tramita o ejecuta operaciones con criptoactivos a título profesional, sino toda la información públicamente disponible, incluida la información sobre las operaciones integradas en un sistema de registro público.

([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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(12) Las STOR deben presentarse sin demora a la autoridad competente una vez que se tenga una sospecha razonable de la existencia de un abuso de mercado. El análisis de si una determinada orden u operación ha de considerarse sospechosa debe basarse en hechos y no en especulaciones o presunciones, y debe llevarse a cabo tan rápidamente como sea posible. Retrasar la presentación de una notificación para incorporar nuevas órdenes, operaciones u otros aspectos del funcionamiento de la TRD sospechosos o acumular varias STOR sería irreconciliable con la obligación de actuar sin demora, cuando ya se tenga una sospecha razonable. En cualquier caso, las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional deben evaluar caso por caso si varias órdenes, operaciones u otros aspectos del funcionamiento de la TRD podrían notificarse en una única STOR.

(13) Podrían darse circunstancias en las que se llegue a una sospecha razonable de abuso de mercado algún tiempo después de que tenga lugar la actividad sospechosa, debido a acontecimientos o a información ulteriores. Tal situación no debe ser motivo para no notificar la actividad sospechosa a la autoridad competente. A fin de demostrar el cumplimiento de los requisitos de notificación en esas circunstancias específicas, la persona que presente la STOR debe poder justificar el lapso de tiempo transcurrido entre el momento en que se produjo la actividad sospechosa y la formación de una sospecha razonable de que se está cometiendo, se ha cometido o es probable que se cometa un abuso de mercado.

(14) Para ayudar a las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional en el ejercicio de su criterio a la hora de valorar órdenes u operaciones sospechosas posteriores, estas deben poder recuperar y revisar el análisis de las STOR que hayan presentado, así como de las órdenes, operaciones y conductas relacionadas con el funcionamiento de la TRD sospechosas que se analizaron, pero en relación con los cuales la autoridad competente en cuestión llegó a la conclusión de que los motivos de sospecha no eran razonables.

(15) Para prevenir el abuso de mercado en la mayor medida posible, las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional deben poder perfeccionar sus sistemas de vigilancia y detectar patrones de conducta repetidos que, considerados en conjunto, podrían conducir a una sospecha razonable de abuso de mercado. Por lo tanto, debe exigirse a dichas personas que analicen las órdenes, operaciones, conductas y otros aspectos relacionados con el funcionamiento de la tecnología de registro distribuido sospechosos que no hayan dado lugar a una STOR y que registren dichos análisis. Dichos registros también deben ayudar a dichas personas a demostrar el cumplimiento del artículo 92 del Reglamento (UE) 2023/1114 y deben facilitar el desempeño por parte de las autoridades competentes de sus funciones de supervisión, investigación y control del cumplimiento con arreglo al artículo 92 del Reglamento (UE) 2023/1114.

(16) Teniendo en cuenta que los mercados de criptoactivos son intrínsecamente transfronterizos, es necesario especificar los procedimientos de coordinación entre las autoridades competentes para la detección y sanción del abuso de mercado en caso de situaciones de abuso de mercado transfronterizas. Estos procedimientos de coordinación deben garantizar que no existan investigaciones o actividades de control del cumplimiento contradictorias. En este contexto, las situaciones transfronterizas de abuso de mercado deben incluir los casos en que se lleven a cabo operaciones sospechosas en un Estado miembro en relación con un criptoactivo admitido a negociación en otro Estado miembro y los casos en que el proveedor de servicios de criptoactivos de que se trate opere en más de un Estado miembro.

(17) Es necesario establecer disposiciones para la transmisión de las STOR entre las autoridades competentes. Estos requisitos son fundamentales, a falta de un régimen de notificación sobre las operaciones, para garantizar una supervisión del mercado y un control del cumplimiento eficaces, previniendo al mismo tiempo la transmisión de un flujo masivo de información que no sería útil para la autoridad receptora.

(18) El presente Reglamento se basa en los proyectos de normas técnicas de regulación que la Autoridad Europea de Valores y Mercados (AEVM) ha presentado a la Comisión.

(19) La AEVM ha llevado a cabo consultas públicas abiertas sobre los proyectos de normas técnicas de regulación en que se basa el presente Reglamento, ha analizado los costes y beneficios potenciales conexos y ha recabado el asesoramiento del Grupo de Partes Interesadas del Sector de los Valores y Mercados establecido de conformidad con el artículo 37 del Reglamento (UE) n.º 1095/2010 del Parlamento Europeo y del Consejo ([3]).

([3]) Reglamento (UE) n.º 1095/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Europea de Valores y Mercados), se modifica la Decisión n.º 716/2009/CE y se deroga la Decisión 2009/77/CE de la Comisión (DO L 331 de 15.12.2010, p. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

(20) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725 ([4]), emitió su dictamen el 22 de enero de 2025.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Definiciones

A los efectos del presente Reglamento, se entenderá por:

1. «notificación de operaciones u órdenes sospechosas» («STOR»): la notificación de órdenes u operaciones, incluidas sus cancelaciones o modificaciones, u otros aspectos del funcionamiento de la TRD sospechosos, cuando puedan darse circunstancias que indiquen que se ha cometido, se está cometiendo o es probable que se cometa un abuso de mercado;

2. «medios electrónicos»: los medios de equipo electrónico para el tratamiento (incluida la compresión digital), el almacenamiento y la transmisión de datos, empleando cables, radio, tecnologías ópticas, u otros medios electromagnéticos;

3. «grupo»: un grupo según se define en el artículo 2, punto 11, de la Directiva 2013/34/UE del Parlamento Europeo y del Consejo ([5]);

4. «orden»: cada una de las órdenes, incluidas cada una de las cotizaciones, con independencia de si su objeto es la presentación inicial, la modificación, la actualización o la cancelación de una orden y con independencia de su tipo;

Artículo 2

Requisitos generales

1. Las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional establecerán y mantendrán mecanismos, sistemas y procedimientos que garanticen lo siguiente:

a) un seguimiento eficaz y continuo de todas las órdenes recibidas y transmitidas y de todas las operaciones con criptoactivos ejecutadas, a efectos de prevenir, detectar e identificar las órdenes y operaciones en las que puedan darse circunstancias que indiquen que se ha cometido, se está cometiendo o es probable que se cometa un abuso de mercado;

b) un seguimiento eficaz y continuo de los aspectos del funcionamiento de la TRD, a efectos de detectar e identificar otros aspectos del funcionamiento de la tecnología de registro distribuido, incluido el mecanismo de consenso, cuando puedan darse circunstancias que indiquen que se ha cometido, se está cometiendo o es probable que se cometa un abuso de mercado;

c) la transmisión de STOR a las autoridades competentes de conformidad con los requisitos establecidos en el presente Reglamento y utilizando la plantilla que figura en el anexo.

([4]) Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (Texto pertinente a efectos del EEE) (DO L 295 de 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([5]) Directiva 2013/34/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre los estados financieros anuales, los estados financieros consolidados y otros informes afines de ciertos tipos de empresas, por la que se modifica la Directiva 2006/43/CE del Parlamento Europeo y del Consejo y se derogan las Directivas 78/660/CEE y 83/349/CEE del Consejo (DO L 182 de 29.6.2013, p. 19, ELI: http://data.europa.eu/eli/dir/2013/34/oj).

2. Las obligaciones a que se refiere el apartado 1 se aplicarán a las órdenes, operaciones y otros aspectos del funcionamiento de la TRD que puedan constituir abuso de mercado y se aplicarán con independencia de:

a) la calidad en que actúe la persona que formula la orden o ejecuta la operación;

b) los tipos de clientes de que se trate;

c) si las órdenes se formularon o las operaciones se realizaron dentro o fuera de una plataforma de negociación.

3. Las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional velarán por que los mecanismos, sistemas y procedimientos a que se refiere el apartado 1:

a) sean adecuados y proporcionados con respecto a la escala, dimensión y naturaleza de su actividad;

b) se evalúen periódicamente, al menos mediante una auditoría y una revisión interna anuales, y se actualicen cuando sea necesario;

c) estén claramente documentados por escrito, incluidas sus modificaciones o actualizaciones, a efectos de cumplir lo dispuesto en el presente Reglamento, y velarán por que la información documentada se conserve durante un período de cinco años.

4. Las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional facilitarán a la autoridad competente, previa solicitud, la información sobre la evaluación a que se refiere el apartado 3, incluida la información sobre el nivel de automatización establecido.

Artículo 3

Prevención, seguimiento y detección

1. Los mecanismos, sistemas y procedimientos a que se hace referencia en el artículo 92, apartado 1, del Reglamento (UE) 2023/1114:

a) abarcarán toda la gama de actividades de negociación realizadas por las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional;

b) alertarán de aquellas actividades que requieran un análisis más detallado para detectar posibles abusos de mercado;

c) permitirán a los proveedores de servicios de criptoactivos que gestionen una plataforma de negociación:

   i) analizar, individual y comparativamente, cada operación ejecutada y cada orden formulada, modificada, cancelada o rechazada en los sistemas de la plataforma de negociación;

   ii) prevenir los casos de conductas repetidas observadas en la misma plataforma de negociación;

d) permitir que las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional analicen, individual y comparativamente, cada operación ejecutada y cada orden formulada, modificada, cancelada o rechazada dentro y fuera de una plataforma de negociación, con independencia de que las órdenes y operaciones se realicen o no a través del registro distribuido, y los aspectos del funcionamiento de la TRD que puedan constituir abuso de mercado.

2. Las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional establecerán y mantendrán mecanismos y procedimientos que garanticen un nivel adecuado de análisis humano en la prevención, el seguimiento, la detección y la identificación de las operaciones, las órdenes y los aspectos del funcionamiento de la tecnología de registro distribuido que indiquen que existen o que es probable que existan conductas de abuso de mercado. Las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional recopilarán datos personales adicionales únicamente para garantizar un nivel adecuado de análisis humano.

3. A efectos del artículo 92, apartado 1, del Reglamento (UE) 2023/1114, las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional emplearán sistemas de TIC en la medida adecuada y proporcionada a la escala, el tamaño y la naturaleza de su actividad empresarial.

Los sistemas de TIC a que se refiere el párrafo primero incluirán sistemas de TIC capaces de llevar a cabo de forma diferida la lectura, la reproducción y el análisis de los datos de los libros de órdenes. Dichos sistemas deberán tener capacidad suficiente para operar en un entorno de negociación algorítmica.

A los efectos del párrafo segundo, la negociación algorítmica se refiere a la negociación de criptoactivos en la que un algoritmo informático determina automáticamente los distintos parámetros de las órdenes, incluido si introducir la orden o no, el momento, el precio, la cantidad o cómo va a gestionarse después de su presentación, con limitada o nula intervención humana, no incluyéndose los sistemas que se utilicen únicamente para el envío directo de las órdenes a una o varias plataformas de negociación, para el tratamiento de órdenes que no impliquen la determinación de ningún parámetro de negociación, para la confirmación de órdenes o para el tratamiento posnegociación de las transacciones ejecutadas.

4. Las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional podrán, mediante acuerdo escrito, externalizar a un tercero o delegar en una persona jurídica que forme parte del mismo grupo, tal como se define en el artículo 2, punto 11, de la Directiva 2013/34/UE del Parlamento Europeo y del Consejo ([6]), (en lo sucesivo, «proveedores»), las funciones relacionadas con la prevención, el seguimiento, la detección y la identificación de órdenes, operaciones u otros aspectos del funcionamiento de la TRD que puedan constituir abuso de mercado, incluido el análisis de datos, también de los datos de órdenes y operaciones, y la generación de alertas. Las personas que deleguen o externalicen dichas funciones seguirán siendo plenamente responsables del cumplimiento de todas sus obligaciones en virtud del presente Reglamento y del artículo 92 del Reglamento (UE) 2023/1114. Cuando dichas funciones se externalicen a un tercero, las personas que externalicen dichas funciones deberán cumplir en todo momento los siguientes requisitos:

a) conservar las competencias y los recursos necesarios para:

   i) evaluar la calidad de los servicios prestados y la idoneidad organizativa de los proveedores;

   ii) supervisar los servicios externalizados;

   iii) gestionar de forma continua los riesgos asociados a la externalización de dichas funciones;

b) deben tener acceso directo a toda la información pertinente relativa al análisis de los datos y la generación de alertas.

El acuerdo escrito a que se refiere el párrafo primero describirá los derechos y obligaciones de la persona que delegue o externalice las funciones y los del proveedor. Asimismo, expondrá los motivos por los que la persona que delega o externaliza las funciones podrá resolver el acuerdo.

5. Como parte de los mecanismos, sistemas y procedimientos a que se refieren los apartados 1 y 2, las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional conservarán la información que documente el análisis realizado en relación con las órdenes, operaciones y aspectos del funcionamiento de la TRD que puedan constituir abuso de mercado durante un período de cinco años. Dicha información incluirá el análisis realizado y las razones para presentar o no una STOR. Las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional facilitarán dicha información a la autoridad competente previa solicitud.

([6]) Directiva 2013/34/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre los estados financieros anuales, los estados financieros consolidados y otros informes afines de ciertos tipos de empresas, por la que se modifica la Directiva 2006/43/CE del Parlamento Europeo y del Consejo y se derogan las Directivas 78/660/CEE y 83/349/CEE del Consejo (DO L 182 de 29.6.2013, p. 19, ELI: http://data.europa.eu/eli/dir/2013/34/oj).

Artículo 4

Formación

Las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional organizarán y proporcionarán una formación global y eficaz para el personal que participe en la prevención, el seguimiento, la detección y la identificación de las órdenes, operaciones y otros aspectos del funcionamiento de la TRD que pudieran indicar la existencia de abuso de mercado, incluido el personal que participe en el tratamiento de órdenes y operaciones o que esté a cargo del funcionamiento de la TRD. Dicha formación se llevará a cabo periódicamente y será adecuada y proporcionada en relación con la escala, el tamaño y la naturaleza de la actividad.

Artículo 5

Notificación de órdenes u operaciones sospechosas

1. Las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional establecerán y mantendrán mecanismos, sistemas y procedimientos eficaces que les permitan evaluar, a efectos de la presentación de una STOR, si con referencia a una orden, una operación u otros aspectos de la TRD pudieran darse circunstancias que indicaran que se ha cometido, se está cometiendo o es probable que se cometa abuso de mercado. Dichos mecanismos, sistemas y procedimientos incluirán un nivel adecuado de análisis humano.

2. Las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional notificarán las STOR:

a) utilizando la plantilla STOR que figura en el anexo y cumplimentando los campos de información relativos a las órdenes, operaciones u otros aspectos del funcionamiento de la TRD de manera clara y precisa, con todos los documentos justificativos o anexos;

b) utilizando los medios electrónicos especificados por la autoridad competente.

A efectos del párrafo primero, letra b), la autoridad competente especificará en su sitio web los medios electrónicos que se utilizarán y velará por que dichos medios electrónicos garanticen la exhaustividad, la integridad y la confidencialidad de la información durante la transmisión.

Las STOR a que se refiere el párrafo primero se basarán en hechos y análisis, teniendo en cuenta toda la información de que dispongan las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional.

3. Las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional garantizarán y mantendrán la confidencialidad de la información contenida en la notificación sobre órdenes u operaciones sospechosas y velarán por que la persona respecto de la cual se haya presentado una STOR y todo aquel que no esté obligado a estar al tanto de la presentación de una STOR debido a su función o su puesto en el seno de la persona notificante no sean informados de:

a) la generación de las alertas a que se refiere el artículo 3, apartado 1, letra b);

b) la evaluación que pueda dar lugar a la presentación de una STOR;

c) el hecho de que el informante completará la STOR sin enviar solicitudes de información a la persona con respecto a la cual pueda presentarse la STOR para completar determinados campos;

d) la presentación de una STOR a la autoridad competente, o la intención de presentarla.

Artículo 6

Momento de presentación de las STOR

1. Las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional se asegurarán de disponer de mecanismos, sistemas y procedimientos eficaces para presentar sin demora una STOR, una vez que tengan la sospecha razonable de un abuso de mercado.

2. Los mecanismos, sistemas y procedimientos contemplados en el apartado 1 incluirán la posibilidad de presentar una STOR en relación con operaciones, órdenes u otros aspectos de la TRD que hayan tenido lugar en el pasado, si la sospecha ha surgido a la vista de acontecimientos o informaciones ulteriores. En tales casos, las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional deberán explicar en la STOR el motivo del lapso de tiempo transcurrido entre la presunta infracción y la presentación de la STOR según las circunstancias específicas de cada caso.

3. Las personas que tramiten o ejecuten operaciones con criptoactivos a título profesional deberán presentar a la autoridad competente cualquier otra información pertinente de que tengan conocimiento después de presentar la STOR y facilitarle cualquier información o documento que solicite.

Artículo 7

Intercambio de informes entre autoridades competentes

1. Las autoridades competentes transmitirán las STOR utilizando el formulario para la comunicación de información no solicitada que figura en el anexo IV del Reglamento de Ejecución (UE) 2024/2545 de la Comisión ([7]).

2. La autoridad competente transmisora adjuntará la STOR al formulario a que se refiere el apartado 1, sin necesidad de traducirlo a la lengua de la autoridad competente receptora. La autoridad competente transmisora incluirá cualquier documento adicional facilitado en la STOR, y especificará la base jurídica para la comunicación de la información.

Artículo 8

Procedimientos de coordinación para la detección y sanción de situaciones transfronterizas de abuso de mercado

1. Una autoridad competente que sospeche que se ha producido, que pueda haberse producido o que pueda estarse produciendo un abuso de mercado transfronterizo comunicará el estado de su evaluación preliminar a las demás autoridades competentes afectadas sin demora indebida, incluidas, cuando proceda, las autoridades competentes de las plataformas de negociación en las que el criptoactivo esté admitido a negociación.

Cuando se les informe sobre situaciones transfronterizas de abuso de mercado, las autoridades competentes receptoras compartirán, sin demora indebida, la información sobre cualquier actividad o medida de supervisión en curso o planificada, o, cuando proceda y cuando dicha información esté a disposición de la autoridad competente receptora, sobre una investigación penal en curso sobre el mismo caso.

2. Las autoridades competentes afectadas:

a) se informarán mutuamente de manera periódica de las situaciones transfronterizas de abuso de mercado;

b) se informarán mutuamente de las novedades más significativas relacionadas con situaciones transfronterizas de abuso de mercado;

c) coordinarán sus acciones de supervisión y control del cumplimiento.

([7]) Reglamento de Ejecución (UE) 2024/2545 de la Comisión, de 24 de septiembre de 2024, por el que se establecen normas técnicas de ejecución para la aplicación del Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo en lo que respecta a los formularios, plantillas y procedimientos normalizados para la cooperación y el intercambio de información entre las autoridades competentes (DO L, 2024/2545, 26.11.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2545/oj).

3. Una autoridad competente que haya iniciado formalmente una investigación o una actividad de control del cumplimiento, o, en su caso, que tenga conocimiento de una investigación penal, informará de ello a las demás autoridades competentes afectadas, incluidas, cuando proceda, las autoridades competentes de las plataformas de negociación en las que el criptoactivo esté admitido a negociación. La autoridad competente podrá informar a la AEVM.

4. Las autoridades competentes que hayan iniciado una investigación o una actividad de control del cumplimiento en el contexto de situaciones transfronterizas o que participen en ellas podrán solicitar la coordinación de la AEVM.

5. A efectos del presente artículo, se entenderá por «situaciones transfronterizas de abuso de mercado» cualquiera de las situaciones siguientes:

a) una situación en la que más de una autoridad competente tenga competencia para detectar, investigar o sancionar un posible caso de abuso de mercado,

b) una situación en la que se requiera la cooperación entre dos o más autoridades competentes para detectar, investigar o sancionar un posible caso de abuso de mercado.

Artículo 9

Entrada en vigor

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 29 de abril de 2025.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

ANEXO

Plantilla para la notificación de operaciones u órdenes sospechosas (STOR)

*Téngase en cuenta que **todos** los campos de las secciones 1 a 4 son obligatorios. Cuando no pueda facilitarse información para un campo específico, indique «N/A» y explique brevemente los motivos.*

SECCIÓN 1: IDENTIDAD DE LA ENTIDAD/PERSONA QUE PRESENTA LA STOR

Personas que tramitan o ejecutan operaciones con criptoactivos — especifíquese, en cada caso:

Nombre de la persona física	[Nombre(s) y apellido(s) de la persona física responsable de la presentación de la STOR en la entidad que la presenta].
Cargo que ocupa en la entidad notificante	[Cargo de la persona física responsable de la presentación de la STOR en la entidad que la presenta].
Nombre de la entidad notificante	[Nombre completo de la entidad notificante, y en el caso de las personas jurídicas también: — forma jurídica, según lo establecido en el registro del país con arreglo a cuya legislación se haya constituido, si procede, y — código de identificación como entidad jurídica (código LEI) de conformidad con la norma ISO 17442].
Dirección de la entidad notificante	[Dirección completa (esto es, calle, número, código postal, localidad, estado/provincia) y país].
Calidad en que actúa la entidad con respecto a las órdenes, operaciones o conductas relativas al funcionamiento de la TRD que puedan constituir abuso de mercado	[Descripción de la calidad en que la entidad notificante actuó con respecto a la(s) orden(es), operación(es) o conducta(s) relativas al funcionamiento de la tecnología de registro distribuido que pudieran indicar la existencia de abuso de mercado, por ejemplo, ejecutando órdenes por cuenta de clientes, gestionando una plataforma de negociación...]
Tipo de actividad de negociación (creación de mercado, arbitraje, etc.) y tipo de criptoactivo negociado por la entidad notificante	[Descripción de los posibles acuerdos, circunstancias o relaciones de índole corporativa, contractual u organizativa].
Contacto para la solicitud de información adicional	[Persona de contacto en la entidad notificante a la que solicitar información adicional relativa a la presente notificación (por ejemplo, responsable del cumplimiento) y datos de contacto pertinentes, si no es la persona encargada de presentar la STOR: — nombre(s) y apellido(s), — cargo de la persona de contacto en la entidad notificante, — dirección electrónica profesional, — número de teléfono profesional].
¿Se han comunicado ya los hechos a las autoridades públicas?	Indíquese si los hechos ya se han comunicado a la autoridad pública (y, en ese caso, indique el nombre de la autoridad).

SECCIÓN 2 — OPERACIÓN/ORDEN/CONDUCTA Y OTROS ASPECTOS RELACIONADOS CON EL FUNCIONAMIENTO DE LA TECNOLOGÍA DE REGISTRO DISTRIBUIDO

Descripción del criptoactivo:	Descríbase el criptoactivo objeto de la STOR, especificando: — el nombre completo [incluido el identificador de ficha digital (DTI) de conformidad con la norma ISO 24165-2 o el identificador único equivalente a que se refiere el artículo 15 del Reglamento Delegado (UE) 2025/1140 de la Comisión ([1]) en el que se especifican los registros que deben conservarse de todos los servicios, actividades, órdenes y operaciones de criptoactivos realizados] o la descripción del criptoactivo en ausencia de DTI. Cuando la conducta sospechosa implique un par de criptoactivos, enumere ambos criptoactivos en el par, — el tipo de criptoactivo (ficha referenciada a activos, ficha de dinero electrónico, otros criptoactivos) y, en el caso de las fichas referenciadas a activos y las fichas de dinero electrónico, el valor, derecho o moneda oficial (o combinación de estos) a que se refiere el criptoactivo para mantener un valor estable.
Nombre(s) del (de los) registro(s) distribuido(s):	[Indicar el nombre completo del (de los) registros(s) distribuido(s) en los que se ha observado la conducta sospechosa]
Plataforma de negociación en la que se formuló la orden o se ejecutó la operación	[Especifíquese el nombre y el código de identificación del mercado (MIC) de conformidad con la norma ISO 10383 para identificar la plataforma de negociación en la que se formuló la orden o se ejecutó la operación. Cuando la orden u operación no se haya detectado en una plataforma de negociación, mencione «fuera de una plataforma de negociación» y el código LEI del proveedor de servicios de criptoactivos que haya realizado la operación, cuando proceda].
Lugar (país)	[Nombre completo del país y los dos caracteres del código de país de conformidad con la norma ISO 3166-1]. [Especifíquese: — dónde se formula la orden, — dónde se ejecuta la operación, — dónde tiene lugar la conducta relacionada con el funcionamiento de la tecnología de registro distribuido.]
Descripción de la orden, operación o conducta sospechosa relacionada con el funcionamiento de la TRD	[Descríbanse como mínimo las siguientes características de la(s) orden(es), operación(es) o conducta(s) notificada(s): — fecha(s) y hora(s) de la(s) orden(es), operación(es) o conducta(s). (Las fechas y horas deben notificarse en TUC según el formato de la norma ISO 8601), — número de referencia de la operación o de la orden o comprobación aleatoria de la operación, — fecha y hora de liquidación, — precio de compra/precio de venta, — volumen o cantidad de criptoactivos, — únicamente para las órdenes, tipo de orden (por ejemplo, «compra con límite x EUR»),] [En caso de que existan múltiples órdenes u operaciones que pudieran constituir abuso de mercado, los datos relativos a los precios y volúmenes de las órdenes y operaciones podrán facilitarse a la autoridad competente en un anexo de la STOR].

	— información sobre la cancelación o modificación de la orden, que incluya: — la naturaleza de la modificación (por ejemplo, cambio de precio o de cantidad) e importancia de la modificación, [En caso de que existan múltiples órdenes u operaciones que pudieran constituir operaciones con información privilegiada, manipulación de mercado o intentos de tales operaciones, los datos relativos a los precios y volúmenes de las órdenes y operaciones podrán facilitarse a la autoridad competente en un anexo de la STOR]. — los medios para modificar la orden (por ejemplo, por correo electrónico, por teléfono, etc.). En caso de que se notifique una conducta sospechosa relacionada con el funcionamiento del registro distribuido, facilítense todos los detalles posibles, incluido el impacto que tuvo en la validación de las operaciones y el método utilizado para alterar el funcionamiento de la TRD.
SECCIÓN 3: DESCRIPCIÓN DE LA NATURALEZA DE LA SOSPECHA	
Naturaleza de la sospecha	[Especifíquese el tipo de infracción por el que la(s) orden(es), operación(es) o conducta(s) relacionada(s) con el funcionamiento de la TRD podría(n) constituir abuso de mercado].
Motivos de la sospecha	[Descripción de la actividad (operaciones y órdenes, manera de formular la orden o de ejecutar la operación y características de las órdenes y operaciones que las hacen sospechosas, conductas relativas al funcionamiento de la TRD) y la manera en que el asunto llegó a conocimiento de la persona notificante, precisando los motivos de la sospecha. En el caso de criptoactivos admitidos a negociación o negociados en una plataforma de negociación, una descripción de la naturaleza de la interacción de los libros de órdenes o las operaciones que pudieran constituir abuso de mercado.]
SECCIÓN 4 — IDENTIFICACIÓN DE LA(S) PERSONA(S) RESPONSABLE(S) DE LAS ÓRDENES, OPERACIONES O CONDUCTAS RELACIONADAS CON EL FUNCIONAMIENTO DE LA TECNOLOGÍA DE REGISTRO DISTRIBUIDO QUE PUEDAN CONSTITUIR ABUSO DE MERCADO («PERSONA SOSPECHOSA»)	
Nombre	[En el caso de personas físicas: nombre(s) y apellidos(s)]. [En el caso de personas jurídicas: denominación completa, incluida la forma jurídica, según lo establecido en el registro del país con arreglo a cuya legislación se haya constituido, si procede, y el código de identificación como entidad jurídica (código LEI) de conformidad con la norma ISO 17442].
Número de identificación nacional	[Número y/o texto]. [Cuando el número de identificación nacional no sea aplicable o no se conozca, indíquese la fecha de nacimiento (solo para las personas físicas) en el formato ISO 8601]
Dirección	[Dirección completa (esto es, calle, número, código postal, localidad, estado/provincia) y país].
Información sobre el empleo: — Lugar — Posición	[Información sobre el empleo de la persona sospechosa, a partir de las fuentes de información disponibles a nivel interno en la entidad notificante (por ejemplo, documentación de la cuenta si se trata de un cliente, sistema de información del personal si se trata de un empleado de la entidad notificante)].
Número(s) de cuenta y dirección(es) de monedero(s)	[Número(s) de la(s) cuenta(s) de efectivo, las posibles cuentas conjuntas o poderes notariales sobre la(s) cuenta(s) de la entidad/persona sospechosa. Dirección(es) de monedero(s) implicadas en la transacción o la conducta sospechosas]
Identificador del cliente	[En caso de que la persona sospechosa sea cliente de la entidad notificante.]
Relación con el emisor del criptoactivo de que se trate	[Descripción de los posibles acuerdos, circunstancias o relaciones de índole corporativa, contractual u organizativa].

SECCIÓN 5: INFORMACIÓN ADICIONAL

Otra información pertinente para la notificación, en función de la actividad

[La siguiente lista es indicativa y no exhaustiva. Cuando sea pertinente para la STOR, podrá facilitarse cualquier otra información que la persona notificante considere útil].

— Cargo de la persona sospechosa (por ejemplo, cliente minorista, instituciones).
— Naturaleza de la intervención de la entidad/persona sospechosa (por cuenta propia, por cuenta de un cliente, validador de operaciones en un registro distribuido, otra).
— Cuando la conducta sospechosa se lleve a cabo en una TRD, otra información pertinente podrá incluir:
  — si la operación pasó a través de una cola pública o privada (cifrada) de operaciones (*mempool*) antes de ser validada en la TRD;
  — si la TRD es pública (sin permiso) o privada (con permiso);
  — las posibles interacciones con los contratos inteligentes, incluida la especificación de la dirección del contrato y la función invocada;
— tamaño de la cartera de la entidad/persona sospechosa,
— fecha en la que se inició la relación comercial con el cliente, si la entidad/persona sospechosa es cliente de la persona/entidad notificante,
— tipo de actividad del departamento de negociación, si existe, de la entidad sospechosa,
— patrones de negociación de la entidad/persona sospechosa. A título orientativo, los siguientes son ejemplos de información que puede resultar de utilidad:
  — patrones de negociación de la entidad/persona sospechosa,
  — comparabilidad del tamaño de la orden/operación notificada con el tamaño medio de las órdenes enviadas/operaciones realizadas por la entidad/persona sospechosa durante los últimos doce meses,
  — hábitos de la entidad/persona sospechosa en cuanto a los criptoactivos negociados en los últimos doce meses, en particular, si la orden/operación se refiere a un criptoactivo negociado por la entidad/persona sospechosa el año anterior.
— Otras entidades/personas que se sabe que han participado en las órdenes u operaciones que pudieran constituir abuso de mercado:
  — nombres,
— actividad (por ejemplo, ejecución de órdenes por cuenta de clientes, negociación por cuenta propia, gestión de una plataforma de negociación, validación de operaciones.)

SECCIÓN 6: DOCUMENTACIÓN ADJUNTA

[Lista de anexos y material que se adjuntan a la STOR].

[Ejemplos de dicha documentación: correos electrónicos, grabaciones de conversaciones, registros de órdenes/operaciones, registros de la tecnología de registro distribuido, confirmaciones, informes de intermediarios financieros, poderes notariales y comentarios publicados en los medios, si procede.

En caso de que se incluya en un anexo aparte información detallada sobre las órdenes, operaciones o conductas relativas al funcionamiento de la tecnología de registro distribuido contempladas en la sección 2 de esta plantilla, indíquese el título de ese anexo].

([1]) Reglamento Delegado (UE) 2025/1140 de la Comisión, de 27 de febrero de 2025, por el que se completa el Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo en lo que respecta a las normas técnicas de regulación en las que se especifican los registros que deben conservarse de todos los servicios, actividades, órdenes y operaciones de criptoactivos realizados (DO L, 2025/1140, 10.6.2025, ELI: http://data.europa.eu/eli/reg_del/2025/1140/oj).