2025/2447

5.12.2025

REGLAMENTO DE EJECUCIÓN (UE) 2025/2447 DE LA COMISIÓN

de 4 de diciembre de 2025

por el que se establecen disposiciones de aplicación del Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo en lo que respecta a las especificaciones técnicas, las medidas y otros requisitos para el establecimiento y la utilización del sistema informático descentralizado para el tratamiento y la comunicación seguros de información

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, sobre la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust) y por el que se sustituye y deroga la Decisión 2002/187/JAI del Consejo ([1]), y en particular su artículo 22 *bis*, apartado 3, y su artículo 22 *ter*, apartado 1, letras a), b), c) y d),

Considerando lo siguiente:

(1) El Reglamento (UE) 2018/1727 establece el marco para la nueva infraestructura digital interna de Eurojust y el establecimiento de un sistema descentralizado de comunicación digital segura entre las autoridades nacionales competentes de los Estados miembros y Eurojust.

(2) La comunicación digital segura se llevará a cabo a través del sistema informático descentralizado. A fin de establecer el sistema informático descentralizado, es necesario proponer especificaciones técnicas que definan los métodos de comunicación y los protocolos de comunicación, las medidas técnicas que garanticen las normas mínimas de seguridad de la información, y los objetivos mínimos de disponibilidad y en materia de seguridad para la implantación de dicho sistema.

(3) De conformidad con el artículo 22 *bis*, apartado 1, del Reglamento (UE) 2018/1727, el sistema informático descentralizado debe estar compuesto por los sistemas informáticos de los Estados miembros y Eurojust, así como por puntos de acceso e-CODEX interoperables a través de los cuales están interconectados dichos sistemas informáticos. Las especificaciones técnicas y otros requisitos del sistema informático descentralizado establecidos en el presente Reglamento deben tener en cuenta dicho marco.

(4) Los puntos de acceso del sistema informático descentralizado deben basarse en puntos de acceso e-CODEX autorizados, tal como se definen en el artículo 3, punto 3, del Reglamento (UE) 2022/850 del Parlamento Europeo y del Consejo ([2]).

(5) La implantación del sistema informático descentralizado se enmarca en un sistema informático descentralizado más amplio basado en e-CODEX, denominado «Sistema de Intercambio Digital en el Ámbito de la Justicia» (o «JUDEX», por su acrónimo en inglés). Por lo tanto, es preciso un intercambio efectivo de información sobre los cambios que se produzcan de tipo horizontal.

(6) Con arreglo a lo dispuesto en el artículo 22 *bis*, apartado 4, del Reglamento (UE) 2018/1727, los Estados miembros y Eurojust podrán decidir utilizar el programa informático de aplicación de referencia desarrollado por la Comisión como sistema dorsal (*back-end*) en lugar de un sistema informático nacional. A fin de garantizar la interoperabilidad, tanto los sistemas informáticos nacionales como el programa informático de aplicación de referencia deben estar sujetos a los mismos requisitos y especificaciones técnicas.

(7) Los datos relativos a delitos de terrorismo y a casos graves de delincuencia organizada deben transmitirse de manera estructurada para mejorar la calidad y la pertinencia de la información, así como para garantizar que la información pueda integrarse con mayor eficiencia en el sistema de gestión de casos de Eurojust y cotejarse mejor con la información ya archivada en dicho sistema. Procede definir el formato y las normas técnicas para la transmisión de los datos dactiloscópicos y las fotografías que pueden transmitirse a Eurojust con el fin de identificar a personas objeto de procesos penales relacionados con delitos de terrorismo.

([1]) DO L 295 de 21.11.2018, p. 138, ELI: http://data.europa.eu/eli/reg/2018/1727/oj.

([2]) Reglamento (UE) 2022/850 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a un sistema informatizado para el intercambio electrónico transfronterizo de datos en el ámbito de la cooperación judicial en materia civil y penal (sistema e-CODEX), y por el que se modifica el Reglamento (UE) 2018/1726 (DO L 150 de 1.6.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(8) Eurojust facilita y apoya la emisión y ejecución de solicitudes de cooperación judicial, incluidas las solicitudes y decisiones basadas en instrumentos que den efecto al principio de reconocimiento mutuo. Las autoridades nacionales competentes deben poder solicitar la asistencia y coordinación de Eurojust a través del sistema informático descentralizado.

(9) A fin de garantizar la eficiencia y la coherencia, es importante que las especificaciones técnicas que se establezcan en virtud del Reglamento (UE) 2018/1727 sean compatibles con las especificaciones técnicas establecidas conforme a lo dispuesto en los Reglamentos (UE) 2023/2844 ([3]), (UE) 2023/1543 ([4]) y (UE) 2024/3011 ([5]) del Parlamento Europeo y del Consejo, así como con futuras medidas de digitalización pertinentes para el mandato de Eurojust de apoyar a las autoridades nacionales competentes.

(10) Cualquier otra comunicación entre Eurojust y las autoridades nacionales competentes, como la comunicación de información sobre los resultados del tratamiento de información, incluida la existencia de vínculos con casos ya archivados en el sistema de gestión de casos de conformidad con el artículo 22 del Reglamento (UE) 2018/1727 cuando Eurojust actúe por iniciativa propia, o de información transmitida a Eurojust con el fin de preservar, analizar y almacenar pruebas relacionadas con el genocidio, los crímenes contra la humanidad, los crímenes de guerra y las infracciones penales conexas, de conformidad con el artículo 4, apartado 1, letra j), de dicho Reglamento, también debe poder realizarse a través del sistema informático descentralizado.

(11) Para garantizar que el presente Reglamento tenga en cuenta sus necesidades operativas, se ha consultado a Eurojust de conformidad con el artículo 22 *bis*, apartado 3, del Reglamento (UE) 2018/1727.

(12) De conformidad con el artículo 4 del Protocolo n.º 21 sobre la posición del Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, Irlanda ha notificado, mediante carta de 9 de septiembre de 2019, su deseo de aceptar y vincularse por el Reglamento (UE) 2018/1727. La Decisión (UE) 2019/2006 de la Comisión ([6]) confirmó su participación. El Reglamento (UE) 2023/2131 del Parlamento Europeo y del Consejo ([7]) modificó el Reglamento (UE) 2018/1727 para permitir el establecimiento de canales de comunicación digital seguros entre Eurojust y las autoridades nacionales competentes y proporciona la base jurídica del presente Reglamento. Habida cuenta de que Irlanda no notificó su deseo de participar en la adopción y aplicación del Reglamento (UE) 2023/2131 ni ha notificado su deseo de aceptar dicho Reglamento y de quedar vinculada por él, Irlanda, de conformidad con los artículos 1 y 2 y el artículo 4 *bis*, apartado 1, del Protocolo n.º 21, no está vinculada por el Reglamento (UE) 2023/2131 ni está sujeta a su aplicación. Irlanda no participa, por lo tanto, en la adopción del presente Reglamento.

(13) De conformidad con los artículos 1 y 2 del Protocolo n.º 22 sobre la posición de Dinamarca, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, Dinamarca no participó en la adopción del Reglamento (UE) 2018/1727. Dinamarca no está por lo tanto obligada por el presente Reglamento ni está sujeta a su aplicación.

([3]) Reglamento (UE) 2023/2844 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre la digitalización de la cooperación judicial y del acceso a la justicia en asuntos transfronterizos civiles, mercantiles y penales, y por el que se modifican determinados actos jurídicos en el ámbito de la cooperación judicial (DO L, 2023/2844, 27.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2844/oj).

([4]) Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales (DO L 191 de 28.7.2023, p. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

([5]) Reglamento (UE) 2024/3011 del Parlamento Europeo y del Consejo, de 27 de noviembre de 2024, relativo a la remisión de causas en materia penal (DO L, 2024/3011, 18.12.2024, ELI: http://data.europa.eu/eli/reg/2024/3011/oj).

([6]) Decisión (UE) 2019/2006 de la Comisión, de 29 de noviembre de 2019, relativa a la participación de Irlanda en el Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo sobre la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust) (DO L 310 de 2.12.2019, p. 59, ELI:http://data.europa.eu/eli/dec/2019/2006/oj).

([7]) Reglamento (UE) 2023/2131 del Parlamento Europeo y del Consejo, de 4 de octubre de 2023, por el que se modifican el Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo y la Decisión 2005/671/JAI del Consejo en lo que respecta al intercambio de información digital en casos de terrorismo (DO L, 2023/2131, 11.10.2023, ELI: http://data.europa.eu/eli/reg/2023/2131/oj).

(14) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo ([8]), emitió su dictamen el 21 de octubre de 2025.

(15) Las medidas previstas en el presente Reglamento se ajustan al dictamen del Comité establecido por el artículo 22 *quater* del Reglamento (UE) 2018/1727.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Especificaciones técnicas del sistema informático descentralizado

Las especificaciones técnicas, las medidas y los objetivos del sistema informático descentralizado a que se refiere el artículo 22 *ter*, apartado 1, letras a), b), c) y d), del Reglamento (UE) 2018/1727 serán los que figuran en el anexo I del presente Reglamento.

Artículo 2

Especificaciones de procesamiento digital

Las especificaciones de procesamiento digital aplicables a la comunicación electrónica a través del sistema informático descentralizado a que se refiere el artículo 22 *bis*, apartado 3, del Reglamento (UE) 2018/1727 serán las que figuran en el anexo II del presente Reglamento.

Artículo 3

Especificaciones técnicas para la transmisión de impresiones dactilares y fotografías

Las especificaciones técnicas y el formato para la transmisión de impresiones dactilares y fotografías a que se refiere el artículo 22 *bis*, apartado 3, del Reglamento (UE) 2018/1727 serán los que figuran en el anexo III del presente Reglamento.

Artículo 4

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 los Estados miembros de conformidad con los Tratados.

Hecho en Bruselas, el 4 de diciembre de 2025.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

([8]) 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 (DO L 295 de 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

ANEXO I

ESPECIFICACIONES TÉCNICAS, MEDIDAS Y OBJETIVOS DEL SISTEMA INFORMÁTICO DESCENTRALIZADO

1. **Introducción y objeto**

En el presente anexo se establecen las especificaciones técnicas, las medidas y los objetivos del sistema informático descentralizado para el intercambio de información previsto en el Reglamento (UE) 2018/1727.

El carácter descentralizado del sistema informático permite que las autoridades nacionales competentes y Eurojust intercambien datos directamente y de forma segura.

2. **Definiciones**

A los efectos del presente anexo, se entenderá por:

2.1. «Protocolo seguro de transferencia de hipertexto» o «HTTPS»: canales de comunicación cifrada y conexión segura.

2.2. «No repudio del origen»: medidas que certifican la integridad y el origen de los datos, con métodos tales como la certificación digital, las infraestructuras de clave pública y las firmas electrónicas y sellos electrónicos.

2.3. «No repudio de la recepción»: medidas que certifican al originador que el destinatario previsto ha recibido los datos, con métodos tales como la certificación digital, las infraestructuras de clave pública y las firmas electrónicas y sellos electrónicos.

2.4. «SOAP» (Protocolo Simple de Acceso a Objetos): según las normas del Consorcio World Wide Web, especificación de protocolo de mensajería para el intercambio de información estructurada al implementar servicios web en redes informáticas.

2.5. «REST» (Transferencia de Estado Representacional): estilo de arquitectura de software para diseñar aplicaciones en red, que se basa en un modelo de comunicación cliente-servidor sin estado y utiliza métodos normalizados para realizar operaciones sobre recursos, que suelen representarse en formatos estructurados.

2.6. «Servicio web»: sistema de *software* diseñado para posibilitar la interacción interoperable entre máquinas en una red y que cuenta con una interfaz descrita en un formato procesable mediante sistemas informáticos.

2.7. «Intercambio de datos»: el intercambio de mensajes y documentos a través del sistema informático descentralizado.

2.8. «e-CODEX»: el sistema e-CODEX definido en el artículo 3, punto 1, del Reglamento (UE) 2022/850.

2.9. «Léxico de referencia de la UE para la justicia digital»: el léxico de referencia de la UE para justicia digital definido en el punto 4 del anexo del Reglamento (UE) 2022/850.

2.10. «ebMS»: el servicio de mensajería ebXML, que es un protocolo de mensajería desarrollado en el marco de OASIS que permite el intercambio seguro, fiable e interoperable de documentos comerciales electrónicos mediante SOAP, apoyando la integración de empresa a empresa a través de diversos sistemas.

2.11. «AS4»: las siglas de Applicability Statement 4 [Declaración de Aplicabilidad 4], una norma OASIS que define un perfil de ebMS 3.0; simplifica la mensajería segura e interoperable entre empresas mediante el uso de estándares abiertos como SOAP y WS-Security.

2.12. «Objetivo de tiempo de recuperación»: el tiempo máximo aceptable para restablecer el servicio tras un incidente.

2.13. «Objetivo de punto de recuperación»: cantidad máxima aceptable de pérdida de datos en caso de fallo.

3. **Métodos de comunicación por medios electrónicos**

3.1. El sistema informático descentralizado utilizará métodos de comunicación basados en servicios, como servicios web u otros componentes reutilizables y soluciones de *software* a efectos de intercambio de mensajes y documentos.

3.2. En concreto, el sistema informático descentralizado implicará la comunicación a través de puntos de acceso e-CODEX, tal como se establece en el artículo 5, apartado 2, del Reglamento (UE) 2022/850. Por lo tanto, para garantizar un intercambio transfronterizo de datos eficaz e interoperable, el sistema informático descentralizado ha de ser compatible con la comunicación a través del sistema e-CODEX.

4. **Protocolos de comunicación**

4.1. El sistema informático descentralizado utilizará protocolos de Internet seguros para:

a) la comunicación dentro del sistema informático descentralizado entre las autoridades competentes y Eurojust;

b) la comunicación con la base de datos de tribunales/autoridades competentes a que se refiere el punto 7.1.

4.2. Para la definición y la transmisión de metadatos y datos estructurados, los componentes del sistema informático descentralizado se basarán en normas y protocolos industriales exhaustivos y ampliamente aceptados, como SOAP y REST.

4.3. Para los protocolos de transporte y mensajería, el sistema informático descentralizado se basará en protocolos seguros basados en normas, tales como:

a) perfil AS4 para el intercambio transfronterizo de datos, que garantice una mensajería segura y fiable con cifrado y no repudio;

b) API HTTPS/RESTful para la comunicación compatible con los formatos JSON y XML;

c) SOAP para interacciones de alta fiabilidad, incorporando WS-Security para autenticación y cifrado.

4.4. A efectos de un intercambio de datos fluido e interoperable, los protocolos de comunicación utilizados por el sistema informático descentralizado deberán cumplir las normas de interoperabilidad pertinentes.

4.5. Cuando proceda, los esquemas XML utilizarán las normas o léxicos pertinentes que sean necesarios para la correcta validación de los elementos y tipos definidos en este esquema. Dichas normas o léxicos podrán incluir:

a) léxico de referencia de la UE para la justicia digital;

b) tipos de datos no cualificados;

c) una lista de códigos de lenguas de la Unión Europea.

4.6. Por lo que respecta a los protocolos de seguridad y autenticación, el sistema informático descentralizado se basará en protocolos basados en normas tales como:

a) TLS (seguridad de la capa de transporte) para la comunicación cifrada y autenticada a través de redes, compatible con la autenticación mutua mediante certificados digitales X.509;

b) OAuth/OpenID Connect (OIDC) para la autenticación y autorización seguras;

c) PKI (infraestructura de clave pública) y firmas digitales para el intercambio seguro de claves y la verificación de la integridad de los mensajes, utilizando certificados digitales (X.509) emitidos por autoridades de certificación de confianza.

5. **Objetivos de seguridad de la información y medidas técnicas pertinentes**

5.1. A efectos del intercambio de información a través del sistema informático descentralizado, entre las medidas técnicas destinadas a garantizar los estándares mínimos en materia de seguridad informática deberán figurar:

a) medidas para garantizar la confidencialidad de la información mediante, entre otras cosas, la utilización de canales seguros de comunicación;

b) medidas para garantizar la integridad de los datos en reposo y en tránsito;

c) medidas para garantizar el no repudio del origen del emisor de la información en el sistema informático descentralizado y el no repudio de la recepción de información;

d) medidas para garantizar el registro de incidencias de seguridad en consonancia con las recomendaciones internacionales reconocidas en materia de estándares de seguridad informática ([1]);

e) medidas para garantizar la autenticación y autorización del usuario y medidas para verificar la identidad de los sistemas conectados al sistema informático descentralizado.

5.2. Los componentes del sistema informático descentralizado garantizarán la seguridad de la comunicación y la transmisión de datos, mediante el uso de cifrado, infraestructura de clave pública con certificados digitales para la autenticación y el intercambio seguro de claves, y protocolos de mensajería segura como AS4 (ebMS), API RESTful y SOAP para mantener la confidencialidad e integridad de los mensajes.

5.3. Cuando se emplee TLS en el contexto del sistema informático descentralizado, se utilizará la última versión estable del protocolo o, en su defecto, una versión sin vulnerabilidades de seguridad conocidas. Solo se permitirán longitudes de clave que garanticen un nivel adecuado de seguridad criptográfica, y no se utilizarán conjuntos de cifrado obsoletos o de los que se tenga constancia que son inseguros.

5.4. En la medida de lo posible, los certificados digitales PKI utilizados a efectos del funcionamiento del sistema informático descentralizado serán expedidos por autoridades de certificación reconocidas como prestadores cualificados de servicios de confianza de conformidad con el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo ([2]). Se aplicarán medidas para garantizar que dichos certificados se utilicen únicamente para los fines previstos, al nivel de confianza requerido y de conformidad con los requisitos aplicables del Reglamento (UE) n.º 910/2014.

5.5. Los componentes del sistema informático descentralizado se desarrollarán de conformidad con el principio de protección de datos desde el diseño y por defecto, y se aplicarán las medidas administrativas, organizativas y técnicas apropiadas para garantizar un alto nivel de ciberseguridad.

5.6. La Comisión diseñará, desarrollará y mantendrá el programa informático de aplicación de referencia de conformidad con los requisitos y principios de protección de datos establecidos en el Reglamento (UE) 2018/1725. El programa informático de aplicación de referencia facilitado por la Comisión permitirá a los Estados miembros cumplir las obligaciones que les imponen, respectivamente, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([3]) y la Directiva (UE) 2016/680, según proceda.

([1]) Sin perjuicio del registro a efectos de seguridad, los mecanismos de registro empleados por los componentes del sistema informático descentralizado permitirán, según proceda, garantizar el cumplimiento de los requisitos establecidos en el artículo 88 del Reglamento (UE) 2018/1725 y, en su caso, en el artículo 25 de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO L 119 de 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

([2]) 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, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([3]) 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).

5.7. Los Estados miembros que utilicen un sistema de *back-end* nacional distinto del programa informático de aplicación de referencia aplicarán las medidas necesarias para garantizar que aquel cumple los requisitos del Reglamento (UE) 2016/679 y de la Directiva (UE) 2016/680, según proceda.

5.8. Eurojust aplicará las medidas necesarias para garantizar que su sistema de *back-end*, o una instancia del programa informático de aplicación de referencia que despliegue, cumpla los requisitos de los Reglamentos (UE) 2018/1725 y (UE) 2018/1727.

5.9. Los Estados miembros y Eurojust establecerán mecanismos sólidos de detección de amenazas y respuesta a incidentes para garantizar la identificación, mitigación y recuperación oportunas de los incidentes de seguridad, de conformidad con sus políticas pertinentes, para los sistemas informáticos bajo su responsabilidad que forman parte del sistema informático descentralizado.

6. **Objetivos mínimos de disponibilidad**

6.1. Eurojust y los Estados miembros garantizarán una disponibilidad de veinticuatro horas al día, siete días a la semana, de los componentes del sistema informático descentralizado bajo su responsabilidad, con un objetivo de tasa de disponibilidad técnica de al menos el 98 % del año, sin contar el mantenimiento programado.

6.2. La Comisión garantizará la disponibilidad de la base de datos de tribunales veinticuatro horas al día, siete días a la semana, con un objetivo de disponibilidad técnica superior al 99 % del año, sin contar el mantenimiento programado.

6.3. En la medida de lo posible, durante los días laborables, las operaciones de mantenimiento se planificarán entre las 20.00 y las 7.00 horas CET.

6.4. Los Estados miembros notificarán a la Comisión, a Eurojust y a los demás Estados miembros las actividades de mantenimiento del siguiente modo:

a) con cinco días hábiles de antelación en el caso de los trabajos de mantenimiento que puedan causar una indisponibilidad de hasta cuatro horas;

b) con diez días hábiles de antelación en el caso de las labores de mantenimiento que puedan causar una indisponibilidad de entre cuatro y doce horas;

c) con treinta días hábiles de antelación en el caso de los trabajos de mantenimiento que puedan causar una indisponibilidad de más de doce horas.

6.5. Cuando los Estados miembros dispongan de ventanas fijas regulares de mantenimiento, informarán a la Comisión, a Eurojust y a los demás Estados miembros de las horas y los días en que estén previstos. Sin perjuicio de las obligaciones establecidas en la frase primera, si los componentes del sistema informático descentralizado bajo la responsabilidad de los Estados miembros dejan de estar disponibles durante dichas ventanas fijas regulares, los Estados miembros podrán optar por no notificarlo a la Comisión en cada ocasión.

6.6. En caso de fallo técnico imprevisto de un componente del sistema informático descentralizado bajo la responsabilidad de los Estados miembros, estos informarán sin demora a la Comisión y a los demás Estados miembros del fallo y, si se conoce, del plazo previsto para su recuperación.

6.7. Eurojust notificará a la Comisión y a los Estados miembros las actividades de mantenimiento del siguiente modo:

a) con cinco días hábiles de antelación en el caso de los trabajos de mantenimiento que puedan causar una indisponibilidad de hasta cuatro horas;

b) con diez días hábiles de antelación en el caso de las labores de mantenimiento que puedan causar una indisponibilidad de entre cuatro y doce horas;

c) con treinta días hábiles de antelación en el caso de los trabajos de mantenimiento que puedan causar una indisponibilidad de más de doce horas.

6.8. Cuando Eurojust disponga de ventanas fijas regulares de mantenimiento, informará a la Comisión y a los Estados miembros de las horas y los días en que estén previstas. Sin perjuicio de las obligaciones establecidas en la frase primera, si los componentes del sistema informático descentralizado bajo la responsabilidad de Eurojust dejan de estar disponibles durante dichas ventanas fijas regulares, Eurojust podrá optar por no notificarlo a la Comisión en cada ocasión.

6.9. En caso de fallo técnico imprevisto de un componente del sistema informático descentralizado bajo la responsabilidad de Eurojust, Eurojust informará sin demora a la Comisión y a los Estados miembros del fallo y, si se conoce, del plazo previsto para su recuperación.

6.10. En caso de fallo técnico imprevisto de la base de datos de tribunales/autoridades competentes, la Comisión informará sin demora a Eurojust y a los Estados miembros de esta indisponibilidad y, si se conoce, del plazo previsto para su recuperación.

6.11. En caso de perturbación del servicio, los Estados miembros y Eurojust garantizarán la rápida recuperación del servicio y la pérdida mínima de datos, de conformidad con el objetivo de tiempo de recuperación y el objetivo de punto de recuperación.

6.12. Los Estados miembros y Eurojust aplicarán las medidas oportunas para alcanzar los objetivos de disponibilidad anteriormente expuestos y establecerán procedimientos para responder eficazmente a los incidentes.

7. **Base de datos de tribunales/autoridades competentes**

7.1. De conformidad con el artículo 22 *bis* del Reglamento (UE) 2018/1727, el sistema informático descentralizado permitirá la comunicación electrónica entre las autoridades nacionales competentes y Eurojust. Teniendo en cuenta las obligaciones de intercambio de información entre las autoridades nacionales competentes y Eurojust en virtud de los artículos 21, 21 *bis* y 22, pero también el papel de Eurojust a la hora de facilitar y apoyar la emisión y ejecución de cualquier solicitud de asistencia legal mutua o reconocimiento mutuo de conformidad con el artículo 8, apartado 1, del Reglamento (UE) 2018/1727, las autoridades competentes implicadas deben ser claramente identificables cuando utilicen el sistema informático descentralizado. Por lo tanto, es esencial establecer una base de datos autorizada de la información de dichas autoridades a efectos del sistema informático descentralizado.

7.2. La base de datos de tribunales/autoridades competentes incluirá la siguiente información en un formato estructurado:

a) a efectos del artículo 8, apartados 1, 3 y 4, y de los artículos 21, 21 *bis* y 22 del Reglamento (UE) 2018/1727, información sobre las autoridades nacionales competentes, incluidos los corresponsales nacionales, tal como se establece en el artículo 20 de dicho Reglamento, así como sobre los miembros nacionales de conformidad con el artículo 7 ([4]) de dicho Reglamento;

b) cuando proceda, la información necesaria para determinar los ámbitos geográficos o material de competencia de las autoridades, u otros criterios pertinentes necesarios para establecer su competencia;

c) información necesaria para el correcto encaminamiento técnico de los mensajes dentro del sistema informático descentralizado.

7.3. La Comisión será responsable del desarrollo, mantenimiento, funcionamiento y apoyo de la base de datos de tribunales/autoridades competentes.

7.4. La base de datos de tribunales/autoridades competentes permitirá que los Estados miembros y Eurojust actualicen la información contenida en ella, y que las autoridades nacionales competentes y los miembros nacionales participantes en el sistema informático descentralizado accedan mediante programas a dicha información y la recuperen.

7.5. El acceso a la base de datos de tribunales/autoridades competentes será posible a través de un protocolo de comunicación común, con independencia de que las autoridades competentes conectadas al sistema informático descentralizado utilicen un sistema nacional de *back-end* o hayan desplegado el programa informático de aplicación de referencia.

7.6. Los Estados miembros velarán por que la información contemplada en el punto 7.2 sobre sus autoridades competentes que conste en la base de datos de tribunales/autoridades competentes sea completa y exacta y esté actualizada.

([4]) Esto se entiende sin perjuicio de la delegación de poderes del miembro nacional en su adjunto, en otros miembros del personal de la oficina nacional o en personal autorizado de Eurojust.

ANEXO II

ESPECIFICACIONES DE PROCESAMIENTO DIGITAL

El artículo 3, punto 9, del Reglamento (UE) 2022/850 define «especificación de procesamiento digital» como «las especificaciones técnicas para los modelos de proceso de negocio y los esquemas de datos que establecen la estructura electrónica de los datos intercambiados mediante el sistema e-CODEX».

El presente anexo establece las especificaciones técnicas para los modelos de proceso de negocio y las especificaciones técnicas de los esquemas de datos.

1. **Especificaciones técnicas para los modelos de proceso de negocio con arreglo al Reglamento (UE) 2018/1727**

Las especificaciones técnicas para los modelos de proceso de negocio se recogen en los puntos 1.1 a 1.5. Definen los aspectos clave necesarios para permitir la comunicación electrónica a efectos del Reglamento (UE) 2018/1727 a través del sistema informático descentralizado.

El sistema informático descentralizado únicamente permitirá el intercambio de información entre las autoridades nacionales competentes de un Estado miembro y el miembro nacional de dicho Estado miembro.

1.1. *Intercambio de información relacionada con el Registro Judicial Antiterrorista europeo [artículo 21 bis del Reglamento (UE) 2018/1727]*

1.1.1. Transmisión del modelo de datos del Registro Judicial Antiterrorista europeo:

La autoridad nacional competente transmite al miembro nacional datos sobre los procedimientos por terrorismo destinados al Registro Judicial Antiterrorista europeo.

1.1.2. Recepción del modelo de datos del Registro Judicial Antiterrorista europeo:

El miembro nacional recibe los datos del Registro Judicial Antiterrorista europeo.

1.1.3. Modelo de solicitud de consentimiento:

El miembro nacional solicita el consentimiento de su autoridad nacional competente.

1.1.4. Recepción del modelo de solicitud de consentimiento:

La autoridad nacional competente recibe la solicitud de consentimiento.

1.1.5. Envío de la respuesta al modelo de solicitud de consentimiento:

La autoridad nacional competente envía una respuesta a la solicitud de consentimiento.

1.1.6. Recepción de la respuesta al modelo de solicitud de consentimiento:

El miembro nacional recibe la respuesta a la solicitud de consentimiento.

1.1.7. Modelo para informar sobre un vínculo:

El miembro nacional informa a la autoridad nacional competente sobre el vínculo con otro caso.

1.1.8. Actualización del modelo de datos del Registro Judicial Antiterrorista europeo:

La autoridad nacional competente transmite los datos que requieran actualización o supresión a su respectivo miembro nacional.

1.1.9. Recepción del modelo de datos del Registro Judicial Antiterrorista europeo actualizado:

El miembro nacional recibe los datos del Registro Judicial Antiterrorista europeo que requieren actualización o supresión.

1.2. *Intercambio de información relacionada con delitos graves [artículo 21 del Reglamento (UE) 2018/1727]*

1.2.1. Transmisión del modelo de datos sobre delitos transfronterizos graves:

La autoridad nacional competente transmite a Eurojust datos sobre delitos transfronterizos graves.

1.2.2. Recepción del modelo de datos sobre delitos transfronterizos graves:

El miembro nacional recibe los datos sobre delitos transfronterizos graves.

1.2.3. Modelo de solicitud de consentimiento:

El miembro nacional solicita el consentimiento de su autoridad nacional competente.

1.2.4. Recepción del modelo de solicitud de consentimiento:

La autoridad nacional competente recibe la solicitud de consentimiento.

1.2.5. Envío de la respuesta al modelo de solicitud de consentimiento:

La autoridad nacional competente envía una respuesta a la solicitud de consentimiento.

1.2.6. Recepción de la respuesta al modelo de solicitud de consentimiento:

El miembro nacional recibe la respuesta a la solicitud de consentimiento.

1.2.7. Modelo para informar sobre un vínculo:

El miembro nacional informa a la autoridad nacional competente sobre el vínculo con otro caso.

1.2.8. Actualización del modelo de datos sobre delitos transfronterizos graves:

La autoridad nacional competente transmite los datos que requieran actualización o supresión a su respectivo miembro nacional.

1.2.9. Recepción del modelo de datos sobre delitos transfronterizos graves actualizado:

El miembro nacional recibe los datos sobre delitos transfronterizos graves que requieren actualización o supresión.

1.3. *Intercambio de información general*

1.3.1. Envío del modelo de información:

El miembro nacional envía información a la autoridad nacional competente o viceversa.

1.3.2. Recepción del modelo de información:

La autoridad nacional competente o el miembro nacional recibe la información.

1.3.3. Respuesta al modelo de información:

La autoridad nacional competente responde a la información remitida por el miembro nacional o viceversa.

1.3.4. Recepción del modelo de respuesta:

El miembro nacional recibe la respuesta de la autoridad nacional competente.

1.3.5. Envío del modelo de información:

La autoridad nacional competente envía información al miembro nacional.

1.3.6. Recepción del modelo de información:

El miembro nacional recibe la información.

1.3.7. Respuesta al modelo de información:

El miembro nacional responde a la información remitida por la autoridad nacional competente.

1.3.8. Recepción del modelo de respuesta:

La autoridad nacional competente recibe la respuesta del miembro nacional.

1.4. *Función de facilitación y apoyo [artículo 8, apartado 1, del Reglamento (UE) 2018/1727]*

Nota: Cuando los modelos de facilitación y apoyo descritos en el punto 1.5 impliquen el intercambio de formularios preceptivos establecidos por actos jurídicos de la Unión en el ámbito de la cooperación judicial en materia penal, los modelos utilizarán, cuando estén disponibles, las representaciones de datos estructurados pertinentes y los esquemas XML desarrollados para dichos actos, por ejemplo, los establecidos a efectos de la aplicación del Reglamento (UE) 2023/2844 u otros instrumentos pertinentes.

1.5. *Modelo de solicitud de facilitación o apoyo:*

1.5.1. Transmisión del modelo de solicitud de facilitación o apoyo:

La autoridad nacional competente transmite una solicitud de facilitación o de apoyo a su respectivo miembro nacional.

1.5.2. Recepción del modelo de solicitud de facilitación o apoyo:

El miembro nacional recibe la solicitud de facilitación o de apoyo y la transmite al miembro nacional del Estado miembro requerido fuera de JUDEX.

1.5.3. Transmisión del modelo de solicitud de facilitación o de apoyo a la autoridad nacional competente:

El miembro nacional del Estado miembro requerido envía la solicitud a su autoridad nacional competente respectiva.

1.5.4. Recepción del modelo de solicitud de facilitación o apoyo:

La autoridad nacional competente recibe la solicitud de facilitación o apoyo.

1.5.5. Envío de la respuesta al modelo de solicitud de facilitación o apoyo:

La autoridad nacional competente envía una respuesta a la solicitud o información relativa a ella al miembro nacional del Estado miembro requerido.

1.5.6. Recepción de la respuesta al modelo de solicitud de facilitación o apoyo:

El miembro nacional recibe la respuesta a la solicitud de facilitación o apoyo de la autoridad nacional competente, o información relativa a dicha solicitud, y la comparte con el miembro nacional del Estado miembro solicitante fuera de JUDEX.

1.5.7. Respuesta al modelo de solicitud de facilitación o apoyo:

El miembro nacional del Estado miembro solicitante responde a la solicitud de facilitación o apoyo de la autoridad nacional competente o comparte la información relativa a dicha solicitud.

1.5.8. Recepción del modelo de respuesta:

La autoridad nacional competente recibe la respuesta o la información relativa a la solicitud de facilitación o apoyo.

2. **Especificaciones técnicas para los esquemas de datos**

Las especificaciones técnicas que deben servir de base para el desarrollo de las definiciones de esquemas XML (XSD) para la digitalización del Reglamento (UE) 2018/1727 se establecen en los puntos 2.1 y 2.2 del presente anexo. Estas especificaciones definen los componentes clave, así como cualquier otra información, con el fin de proporcionar una descripción completa de la producción de estos esquemas.

La descripción tiene vocación genérica, lo que permite modificar y ampliar las XSD producidas sin que sea necesario introducir cambios significativos en estas especificaciones.

Las especificaciones se aplicarán a la presentación preceptiva de los esquemas anexos al Reglamento (UE) 2018/1727, a cualquier mensaje predefinido o a cualquier mensaje de texto libre utilizado en los intercambios en virtud de dicho Reglamento.

2.1. *Consideraciones generales*

Para todos los esquemas que deban facilitarse, se aplicarán las siguientes disposiciones:

2.1.1. Versiones

Se incluirá un atributo de versión que facilite la gestión de las versiones del esquema y permita actualizarlo en futuras iteraciones según los requisitos de negocio. El atributo de versión indicará si la nueva versión es compatible con las versiones anteriores al introducir nuevas características o mejoras.

2.1.2. Metadatos y declaración del esquema

— Cuando proceda, el esquema utilizará las normas o léxicos pertinentes, requeridos por e-CODEX para proporcionar interoperabilidad, que sean necesarios para la correcta validación de los elementos y tipos definidos en este esquema. Esto puede incluir:

  — léxico de referencia de la UE para la justicia digital

  — tipos de datos no cualificados

  — una lista de códigos de lenguas de la Unión Europea

— Asimismo, cuando proceda, los esquemas podrán incorporar las normas ETSI pertinentes para hacer uso de sus definiciones.

2.1.3. Anotaciones y documentación

— **Anotaciones**: normalmente, cada elemento del esquema irá acompañado de anotaciones. Las anotaciones proporcionan información legible por el ser humano sobre el elemento en la que a menudo se define su finalidad o uso de manera clara y concisa.

2.1.4. Uso y adaptabilidad

El esquema se ajustará a las normas establecidas en las letras a) a d):

a) **Estructura modular**: cada sección se diseñará con una funcionalidad específica y podrá reutilizarse o adaptarse de forma independiente. Esto hará que el esquema sea fácil de personalizar para diferentes casos de uso.

b) **Extensibilidad**: el esquema se diseñará de modo que puedan incluirse nuevos elementos o atributos si en el futuro se necesita información adicional. Para ello, se utilizarán elementos y secuencias opcionales que puedan extenderse sin romper las implementaciones existentes.

c) **Estructura adaptable**: el esquema se diseñará de manera que permita añadir o modificar elementos o tipos de datos según sea necesario. La estructura del esquema se adaptará a los cambios en los requisitos sin necesidad de rediseños importantes.

d) **Elementos opcionales**: los elementos de un esquema pueden marcarse como opcionales, es decir, pueden incluirse u omitirse en función de circunstancias específicas.

El esquema estará diseñado para permitir la recogida de datos estructurados para solicitudes específicas.

2.1.5. Modificaciones

El diseño del esquema se caracterizará por la flexibilidad, la modularidad y la facilidad de adaptación. Los tipos complejos y los elementos opcionales se incorporarán al diseño de tal manera que pueda abordar escenarios diversos y, al mismo tiempo, seguir siendo fácil de modificar y ampliar.

2.2. *Intercambio de datos estructurados*

Los datos estructurados a que se refieren los puntos 2.2.1 y 2.2.2 se facilitarán de conformidad con el artículo 22 *bis*, apartado 3, del Reglamento (UE) 2018/1727. El esquema también permitirá indicar los conjuntos de datos que se eliminarán en futuras actualizaciones.

2.2.1. Datos del Registro Judicial Antiterrorista europeo

Las siguientes especificaciones técnicas del esquema de datos establecen un marco estructurado para crear el esquema en formato XML.

a) Sección de primer nivel

Esta sección de primer nivel corresponde a la información establecida en el anexo III del Reglamento (UE) 2018/1727, es decir, la información destinada al Registro Judicial Antiterrorista europeo.

b) Estructura del mensaje

La estructura de los datos del Registro Judicial Antiterrorista europeo consistirá en una secuencia de elementos e incluirá, como mínimo, los siguientes:

i) información para la identificación de personas físicas:

— apellido(s),

— nombre,

— alias, en su caso,

— fecha de nacimiento,

— lugar de nacimiento (ciudad y país),

— nacionalidad(es),

— documento de identificación (tipo y número del documento),

— sexo,

— lugar de residencia;

ii) información para la identificación de personas jurídicas:

— razón social,

— forma jurídica,

— lugar de la sede central;

iii) información para la identificación de personas tanto físicas como jurídicas:

— número(s) de teléfono,

— correo(s) electrónico(s),

— datos de cuentas en bancos o en otras entidades financieras,

— condición en el proceso;

iv) información sobre el delito:

— información sobre las personas jurídicas implicadas en la preparación o comisión de un delito de terrorismo,

— calificación jurídica del delito con arreglo al Derecho nacional,

— forma de delincuencia grave aplicable de la lista a que se refiere el anexo I,

— pertenencia a un grupo terrorista (si la hubiera),

— tipología de terrorismo (como, por ejemplo, yihadista, separatista, de izquierda o de derecha),

— breve exposición del caso;

v) información sobre el procedimiento nacional:

— estado del procedimiento,

— fiscalía competente,

— número del expediente,

— fecha de inicio del procedimiento judicial formal,

— vínculos con otros casos pertinentes;

vi) campo de información adicional (texto libre);

vii) código de autorización previa.

2.2.2. Datos transmitidos de conformidad con el artículo 21 del Reglamento (UE) 2018/1727

a) Artículo 21, apartado 4, del Reglamento (UE) 2018/1727, sobre la creación de equipos conjuntos de investigación (ECI)

i) Sección de primer nivel

Esta sección de primer nivel corresponde a la información a que se refiere el artículo 21, apartado 4, del Reglamento (UE) 2018/1727 sobre la creación de ECI.

ii) Estructura del mensaje

La estructura de los datos consistirá en una secuencia de elementos e incluirá, como mínimo, los siguientes:

— Autoridad judicial nacional encargada del proceso penal

— Número de referencia nacional del proceso penal

— Estado del proceso penal

— Infracciones penales investigadas

— Otros países implicados en el caso

— ¿El caso ya cuenta con el apoyo de Eurojust?

— En caso afirmativo, ¿cuál es el número de identificación del caso de Eurojust?

— En caso negativo, ¿se trata de una solicitud de ayuda?

— ¿El caso cuenta con el apoyo de Europol?

— En caso afirmativo, ¿grupo de trabajo operativo o Aplicación de la Red de Intercambio Seguro de Información (SIENA)?

— Acuerdo ECI:

— Países implicados

— Partes en el ECI (autoridades nacionales encargadas de las investigaciones)

— Número de referencia nacional del proceso penal objeto del ECI

— Fecha de firma

— Duración

— Infracciones penales investigadas

— Breve exposición del caso

— Principales sospechosos en el proceso penal cubierto por el ECI (nombre, apellidos, fecha y lugar de nacimiento y posiblemente otras categorías de datos pertinentes y necesarias conforme al anexo II)

— Resultados del trabajo de los ECI:

— Dificultades/retrasos a la hora de:

— crear el ECI

— solicitar o poner en común pruebas en el seno del ECI

— acordar o aplicar una estrategia común de enjuiciamiento

— Admisibilidad/inadmisibilidad/evaluación de las pruebas del ECI en los procesos nacionales

— Resultado del proceso judicial (enjuiciamientos que han prosperado y que no han prosperado, y condenas/absoluciones)

iii) Código de autorización previa

b) Artículo 21, apartado 5, del Reglamento (UE) 2018/1727, sobre casos graves complejos

i) Sección de primer nivel

Esta sección de alto nivel corresponde a la información a que se refiere el artículo 21, apartado 5, del Reglamento Eurojust, es decir, casos graves y complejos.

ii) Estructura del mensaje

La estructura de los datos consistirá en una secuencia de elementos e incluirá, como mínimo, los siguientes:

— Autoridad judicial nacional encargada del proceso penal

— Número de referencia nacional del proceso penal

— Estado del proceso penal

— Infracciones penales investigadas

— Otros países implicados en el caso

— ¿El caso ya cuenta con el apoyo de Eurojust?

— En caso afirmativo, ¿cuál es el número de identificación del caso de Eurojust?

— En caso negativo, ¿se trata de una solicitud de ayuda?

— ¿El caso cuenta con el apoyo de Europol?

— En caso afirmativo, ¿grupo de trabajo operativo o SIENA?

— Forma de delincuencia grave aplicable

— Participación de una red de delincuencia organizada

— De carácter mafioso

— Red transnacional de delincuencia organizada

— Repercusiones a escala de la UE

— Principales sospechosos en el proceso penal (nombre, apellidos, fecha y lugar de nacimiento y posiblemente otras categorías de datos pertinentes y necesarias conforme al anexo II)

— Breve exposición del caso

— Otros países implicados

— Países con los que ya se ha iniciado la cooperación

— Autoridades competentes implicadas en otro país

— Instrumentos de cooperación judicial utilizados

— Número de solicitudes enviadas/recibidas

— Existencia de investigaciones vinculadas

— Países con los que se va a activar la cooperación/países posiblemente afectados

— Tipo de cooperación necesaria (por ejemplo, extradición, obtención de pruebas, otro tipo de cooperación)

— Existencia de investigaciones vinculadas

iii) Código de autorización previa

c) Artículo 21, apartado 6, letra a), del Reglamento (UE) 2018/1727, sobre conflictos de jurisdicción

i) Sección de primer nivel

Esta sección de primer nivel corresponde a la información a que se refiere el artículo 21, apartado 6, letra a), del Reglamento (UE) 2018/1727, es decir, los conflictos de jurisdicción

ii) Estructura del mensaje

La estructura de los datos consistirá en una secuencia de elementos e incluirá, como mínimo, los siguientes:

— Autoridad judicial nacional encargada del proceso penal

— Número de referencia nacional del proceso penal

— Estado del proceso penal (por ejemplo, investigación, instrucción, juicio)

— Infracciones penales investigadas

— Otros países implicados en el caso

— ¿El caso ya cuenta con el apoyo de Eurojust?

— En caso afirmativo, ¿cuál es el número de identificación del caso de Eurojust?

— En caso negativo, ¿se trata de una solicitud de ayuda?

— ¿El caso cuenta con el apoyo de Europol?

— En caso afirmativo, ¿grupo de trabajo operativo o SIENA?

— Otros países implicados

— Autoridades nacionales competentes del otro país, si se conocen

— Número de referencia nacional del proceso penal en otro país

— Fase del proceso en otro país, si se conoce

— Conflicto positivo o negativo

— Conflicto real o potencial

— Actividades de coordinación ya emprendidas [por ejemplo, consultas en virtud de la Decisión marco 2009/948/JAI del Consejo ([1])]

— Breve exposición del caso

— Principales sospechosos comunes (nombre, apellidos, fecha y lugar de nacimiento y posiblemente otras categorías de datos pertinentes y necesarias conforme al anexo II)

iii) Código de autorización previa

d) Artículo 21, apartado 6, letra b), sobre entregas vigiladas

i) Sección de primer nivel

Esta sección de primer nivel corresponde a la información a que se refiere el artículo 21, apartado 6, letra b), del Reglamento (UE) 2018/1727: entregas vigiladas

ii) Estructura del mensaje

La estructura de los datos consistirá en una secuencia de elementos e incluirá, como mínimo, los siguientes:

— Autoridad judicial nacional encargada del proceso penal

— Número de referencia nacional del proceso penal

— Estado del proceso penal (por ejemplo, investigación, instrucción, juicio)

— Infracciones penales investigadas

— Otros países implicados en el caso

— ¿El caso ya cuenta con el apoyo de Eurojust?

— En caso afirmativo, ¿cuál es el número de identificación del caso de Eurojust?

— En caso negativo, ¿se trata de una solicitud de ayuda?

— ¿El caso cuenta con el apoyo de Europol?

— En caso afirmativo, ¿grupo de trabajo operativo o SIENA?

— Otros países implicados

— País de origen/tránsito/destino

— Autoridades nacionales competentes de otros países

— Existencia de investigaciones vinculadas en otros países

([1]) Decisión marco 2009/948/JAI del Consejo, de 30 de noviembre de 2009, sobre la prevención y resolución de conflictos de ejercicio de jurisdicción en los procesos penales (DO L 328 de 15.12.2009, p. 42, ELI: http://data.europa.eu/eli/dec_framw/2009/948/oj).

— Tipo de mercancías entregadas (por ejemplo, drogas y tipo/dinero/armas/cigarrillos/otros)

— Situación de la entrega vigilada (por ejemplo, prevista, en curso, finalizada)

— Resultado de la entrega vigilada, si ya se ha ejecutado

— Instrumento de cooperación judicial utilizado

— Principales sospechosos comunes (nombre, apellidos, fecha y lugar de nacimiento y posiblemente otras categorías de datos pertinentes y necesarias conforme al anexo II)

iii) Código de autorización previa

e) Artículo 21, apartado 6, letra c), del Reglamento (UE) 2018/1727, sobre problemas reiterados con instrumentos de cooperación judicial

i) Sección de primer nivel

Esta sección de primer nivel corresponde a la información a que se refiere el artículo 21, apartado 6, letra c), del Reglamento (UE) 2018/1727: problemas reiterados con instrumentos de cooperación judicial

ii) Estructura del mensaje

La estructura de los datos consistirá en una secuencia de elementos e incluirá, como mínimo, los siguientes:

— Autoridad judicial nacional encargada del proceso penal

— Número de referencia nacional del proceso penal

— Estado del proceso penal (por ejemplo, investigación, instrucción, juicio)

— Infracciones penales investigadas

— Otros países implicados en el caso

— ¿El caso ya cuenta con el apoyo de Eurojust?

— En caso afirmativo, ¿cuál es el número de identificación del caso de Eurojust?

— En caso negativo, ¿se trata de una solicitud de ayuda?

— ¿El caso cuenta con el apoyo de Europol?

— En caso afirmativo, ¿grupo de trabajo operativo o SIENA?

— Otros países implicados

— Autoridades nacionales competentes, si se conocen

— En calidad de autoridad de emisión o de ejecución

— Instrumento de cooperación judicial en cuestión (por ejemplo, ODE, OEI, embargo y decomiso)

— Solicitud específica en cuestión (es decir, qué medida de investigación, qué tipo de embargo, ODE para la ejecución de la pena o para el enjuiciamiento)

— Denegación o dificultad reiterada

— En caso de denegación, ¿qué motivo específico se invoca?

— Breve descripción del problema

— Otras autoridades nacionales afectadas por el mismo problema, en su caso

iii) Código de autorización previa

2.3. *Códigos de autorización previa*

Cuando se intercambien datos con Eurojust a través de JUDEX, las autoridades nacionales competentes indicarán, mediante códigos de autorización previa, el tratamiento ulterior, el acceso y la transferencia de datos tras la identificación de un vínculo. Los códigos de autorización previa indicarán si la información relacionada con el vínculo puede compartirse con otras autoridades nacionales competentes, otros órganos y organismos de la Unión, terceros países u organizaciones internacionales, y en qué medida.

2.4. *Mensajes predefinidos*

Los mensajes predefinidos son representaciones de intercambios establecidos por el Reglamento (UE) 2018/1727, pero para los que no se dispuso ninguna forma específica en el acto jurídico. Sus tipos y número se determinan durante el análisis institucional y técnico.

Las definiciones de esquemas XLM (XSD) para los mensajes predefinidos se diseñarán para garantizar la coherencia, la estructura y el cumplimiento de las necesidades institucionales.

Se aplicará lo siguiente a dichos esquemas.

a) la sección de primer nivel de este esquema se nombrará de acuerdo con el tipo de mensaje específico que se esté definiendo;

b) los campos necesarios para el tipo de mensaje específico se añadirán y definirán dentro de esta estructura, garantizando una representación adecuada de los elementos de datos.

2.5. *Mensajes de texto libre*

Los mensajes de texto libre son representaciones de intercambios que permiten contenidos no estructurados o parcialmente estructurados, lo que ofrece flexibilidad al tiempo que se siguen cumpliendo los requisitos reglamentarios e institucionales. Las XSD para los mensajes de texto libre estarán diseñadas de manera que garanticen la coherencia y el formato adecuado.

Se aplicará lo siguiente a dichos esquemas.

a) la sección de primer nivel del esquema se nombrará de acuerdo con el tipo específico de mensajes de texto libre que se esté definiendo;

b) el esquema definirá la estructura necesaria para el mensaje de texto libre, permitiendo al mismo tiempo un orden adecuado de los elementos según sea necesario;

c) los campos necesarios para el tipo específico de mensaje de texto libre se añadirán y definirán dentro de esta estructura, garantizando una representación adecuada de los elementos de datos.

ANEXO III

ESPECIFICACIONES TÉCNICAS DE LAS IMPRESIONES DACTILARES Y LAS FOTOGRAFÍAS

Los mensajes intercambiados a través del sistema informático descentralizado podrán ir acompañados de documentos adjuntos, incluidos archivos del National Institute of Standards and Technology (Instituto Nacional de Normalización y Tecnologías, NIST) que contengan impresiones dactilares y fotografías, de conformidad con las especificaciones técnicas establecidas en los puntos 1 y 2.

1. **Impresiones dactilares**

Las impresiones dactilares que puedan compartirse con Eurojust con el fin de identificar de forma fiable a las personas objeto de procesos penales relacionados con delitos de terrorismo cumplirán las siguientes condiciones:

a) que las impresiones dactilares se faciliten en un archivo que contenga imágenes digitales de impresiones dactilares (el archivo NIST de impresiones dactilares) y se presenten de conformidad con la norma ANSI/NIST-ITL 1-2011 Actualización 2015 (o una versión más reciente);

b) que el archivo NIST de impresiones dactilares conste de hasta diez impresiones dactilares individuales: rodadas, planas o ambas;

c) que todas las impresiones dactilares estén etiquetadas;

d) que las impresiones dactilares se tomen mediante su escaneo en vivo o su entintado e impresión en papel, siempre que las impresiones dactilares en papel se hayan escaneado en la resolución requerida y con la misma calidad;

e) que el archivo NIST de impresiones dactilares permita la inclusión de información complementaria, como las condiciones de registro de las impresiones dactilares y el método utilizado para la obtención de imágenes individuales de impresiones dactilares;

f) que las impresiones dactilares tengan una resolución nominal de 500 o 1 000 píxeles por pulgada ([1]) (con una desviación aceptable de ± 10 píxeles por pulgada) con 256 niveles de gris;

g) El algoritmo de compresión de impresiones dactilares que se utilizará debe seguir las recomendaciones del National Institute of Standards and Technology («NIST») (Instituto Nacional de Normalización y Tecnologías). Los datos dactiloscópicos con una resolución de 500 píxeles por pulgada se comprimen utilizando el algoritmo WSQ (ISO/IEC 19794-5:2005). Los datos dactiloscópicos con una resolución de 1 000 píxeles por pulgada se comprimen utilizando la norma JPEG 2000 de compresión de imágenes (ISO/IEC 15444-1) y su sistema de codificación. El objetivo de la relación de compresión es de 15:1.

2. **Fotografías**

Las fotografías que puedan compartirse con Eurojust con el fin de identificar de forma fiable a las personas objeto de procesos penales relacionados con delitos de terrorismo cumplirán las siguientes condiciones:

a) que se facilite solo una imagen facial en un archivo fotográfico (el archivo NIST de fotografía) y se presente de conformidad con la norma ANSI/NIST-ITL 1-2011 Actualización 2015 o cualquier versión más reciente disponible;

b) que las fotografías sean en escala de grises, en color o en la parte del espectro cercana al infrarrojo;

c) que la calidad de las fotografías se base en los requisitos de imagen de la norma ISO/IEC 19794-5:2011 para las imágenes frontales, o cualquier versión más reciente disponible;

d) que el archivo NIST de fotografía permita incluir información complementaria, en particular la fecha en que se tomó la imagen;

([1]) Píxeles por pulgada.

e) que las fotografías, en modo vertical, tengan una resolución mínima de 600 píxeles por 800 píxeles y máxima de 1 200 píxeles por 1 600 píxeles;

f) que la cara ocupe un espacio dentro de la fotografía que garantice un mínimo de 120 píxeles entre el centro de cada ojo;

g) que el algoritmo de compresión de las fotografías utilizado siga las recomendaciones del National Institute of Standards and Technology («NIST») (Instituto Nacional de Normalización y Tecnologías). Las fotografías se comprimirán una sola vez con el sistema de codificación y la norma de compresión de imágenes JPEG (ISO/IEC 10918) o JPEG 2000 (ISO/IEC 15444), con una relación máxima permitida de compresión de imágenes de 20:1.