2025/1550

29.7.2025

REGLAMENTO DE EJECUCIÓN (UE) 2025/1550 DE LA COMISIÓN

de 28 de julio de 2025

por el que se establecen las especificaciones técnicas y otros requisitos del sistema informático descentralizado a que se refiere el Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el 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 ([1]), y en particular su artículo 25, apartado 1, letras a), b), c) y d),

Considerando lo siguiente:

(1) Para establecer el sistema informático descentralizado a que se refiere el Reglamento (UE) 2023/1543, es necesario definir y adoptar especificaciones técnicas, medidas y objetivos para la aplicación de dicho sistema.

(2) De conformidad con el Reglamento (UE) 2023/1543, el sistema informático descentralizado debe estar compuesto por los sistemas informáticos de los Estados miembros y los órganos y organismos de la Unión, así como de puntos de acceso e-CODEX interoperables a través de los cuales están interconectados dichos sistemas informáticos. En consecuencia, las especificaciones técnicas y otros requisitos del sistema informático descentralizado deben reflejar este marco.

(3) Con arreglo al Reglamento (UE) 2023/1543, 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, apartado 3, del Reglamento (UE) 2022/850 del Parlamento Europeo y del Consejo ([2]).

(4) Los Estados miembros podrán optar por utilizar el software de aplicación de referencia desarrollado por la Comisión como sistema de *back-end* en lugar de un sistema informático nacional. A fin de garantizar la interoperabilidad, tanto los sistemas informáticos nacionales como los programas informáticos de aplicación de referencia deben estar sujetos a los mismos requisitos técnicos y especificaciones técnicas establecidos en el presente Reglamento.

(5) Con el fin de mitigar posibles problemas técnicos relacionados con la capacidad y fiabilidad del sistema informático descentralizado, es necesario establecer un umbral para el volumen de pruebas electrónicas transmitidas a través de dicho sistema. Tras el lanzamiento del sistema, debe supervisarse la frecuencia y el volumen de dichas transmisiones, y el umbral debe ajustarse, cuando proceda, para maximizar la eficiencia del sistema.

(6) Con el fin de reforzar la interoperabilidad y la eficiencia del sistema informático descentralizado, el uso de normas adecuadas del ETSI debe ser obligatorio. Debe supervisarse la evolución futura y, en caso necesario, debe considerarse la adopción de normas adicionales del ETSI.

(7) Irlanda está vinculada por el Reglamento (UE) 2023/1543 y, por lo tanto, participa en la adopción del presente Reglamento.

(8) 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 queda vinculada por el presente Reglamento ni sujeta a su aplicación.

([1]) DO L 191 de 28.7.2023, p. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/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).

(9) El Supervisor Europeo de Protección de Datos, a quien se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo ([3]), emitió su dictamen el 25 de junio de 2025.

(10) Las medidas previstas en el presente Reglamento se ajustan al dictamen del Comité establecido por el artículo 26 del Reglamento (UE) 2023/1543.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Especificaciones técnicas del sistema informático descentralizado

En el anexo del presente Reglamento se establecen las especificaciones técnicas y los requisitos técnicos, las medidas y los objetivos del sistema informático descentralizado a que se refiere el artículo 25, apartado 1, del Reglamento (UE) 2023/1543 a efectos de la comunicación contemplada en el artículo 19 de dicho Reglamento.

Artículo 2

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 28 de julio de 2025.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

([3]) 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.° 45/2001 y la Decisión n.° 1247/2002/CE (DO L 295 de 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

ANEXO

ESPECIFICACIONES TÉCNICAS DEL SISTEMA INFORMÁTICO DESCENTRALIZADO

(a que se refiere el artículo 1)

1. Introducción y objeto

En el presente anexo se establecen las especificaciones técnicas, las medidas y los objetivos del sistema informático descentralizado para los procedimientos previstos en el Reglamento (UE) 2023/1543.

Según el Reglamento (UE) 2023/1543, y en particular su artículo 19, el sistema informático descentralizado debe permitir la comunicación escrita entre las autoridades competentes y los establecimientos designados o los representantes legales, entre las autoridades competentes, así como entre las autoridades competentes y los órganos u organismos competentes de la Unión.

2. Definiciones

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»: 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. «Transferencia de estado representacional (REST)»: 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, formularios, documentos y pruebas electrónicas a través del sistema informático descentralizado.

2.8. «API»: una interfaz de programación de aplicaciones basada en una norma común de intercambio de datos, que permite a los proveedores de servicios que utilizan soluciones informáticas a medida para intercambiar información y datos relacionados con las solicitudes de pruebas electrónicas acceder a los sistemas informáticos descentralizados por medios automatizados.

2.9. «Interfaz web»: interfaz de usuario disponible a través de HTTPS en internet, que permite a los proveedores de servicios acceder manualmente al sistema informático descentralizado para comunicarse de forma segura con las autoridades e intercambiar información y datos relacionados con las solicitudes de pruebas electrónicas, sin tener que establecer su propia infraestructura específica.

2.10. «Normas ETSI»: especificaciones técnicas y normas elaboradas por el Instituto Europeo de Normas de Telecomunicaciones (ETSI) para garantizar la interoperabilidad, la seguridad y la eficiencia de las tecnologías de la información y la comunicación. Proporcionan marcos, protocolos y mejores prácticas para una amplia gama de tecnologías, incluidas las redes móviles, las radiocomunicaciones, la ciberseguridad y la infraestructura de internet.

2.11. «Huella *hash*»: salida de longitud fija generada por una función *hash* criptográfica cuando se aplica a una entrada de longitud arbitraria. Una función *hash* criptográfica está diseñada para satisfacer las propiedades de seguridad fundamentales, incluida la resistencia a la preimagen, la resistencia a la segunda preimagen y la resistencia a la colisión, lo que garantiza su solidez frente a los ataques de inversión y colisión.

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

2.13. «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.

2.14. «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.

2.15. «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.

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

2.17. «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. A efectos de la comunicación escrita entre las autoridades competentes de los Estados miembros, entre las autoridades competentes y los establecimientos designados o los representantes legales de los proveedores de servicios, así como entre las autoridades competentes y los órganos u organismos de la Unión, 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 datos. En concreto, 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 consiguiente, para garantizar un intercambio transfronterizo de datos eficaz e interoperable, el sistema informático descentralizado facilitará la comunicación a través del sistema e-CODEX.

3.2. Dado el elevado volumen previsto de pruebas electrónicas que se transmitirán a raíz de una orden de producción europea a través del sistema informático descentralizado, tal como se indica en el artículo 19, apartados 1 y 4, del Reglamento (UE) 2023/1543, que puede dar lugar a limitaciones de capacidad técnica que podrían afectar de forma negativa al sistema informático descentralizado, las pruebas electrónicas se transmitirán a través de este sistema en la medida en que no superen el umbral de 25 megabytes (25 600 kilobytes). La transmisión de pruebas electrónicas que superen dicho umbral se efectuará de conformidad con el artículo 19, apartado 5, de dicho Reglamento.

3.3. Teniendo en cuenta el artículo 19, apartado 6 del Reglamento (UE) 2023/1543, en caso de que una transmisión se efectúe por medios alternativos según lo dispuesto en dicho apartado debido a la imposibilidad de utilizar el sistema informático descentralizado por alguno de los motivos establecidos en el artículo 19, apartado 5, de dicho Reglamento:

3.3.1. Cuando la transmisión se refiera a una comunicación escrita, incluido el intercambio de formularios, entre autoridades competentes y prestadores de servicios en el sentido del artículo 19, apartado 1, del Reglamento (UE) 2023/1543, el emisor de la transmisión registrará la transmisión en su sistema informático nacional que forme parte del sistema informático descentralizado. La información registrada incluirá, como mínimo, un número de referencia del asunto o del expediente, su fecha y hora, el remitente y el destinatario, el nombre del archivo y su tamaño.

3.3.2. Cuando la transmisión se refiera a una comunicación escrita, incluido el intercambio de formularios, entre autoridades competentes, así como a una comunicación escrita con órganos u organismos competentes de la Unión en el sentido del artículo 19, apartado 4, del Reglamento (UE) 2023/1543, el iniciador de la transmisión registrará la transmisión en el sistema informático descentralizado, en particular en su sistema informático nacional o, en su caso, en los sistemas informáticos gestionados por la agencia u organismo competente de la Unión. La información registrada incluirá, como mínimo, un número de referencia del caso o del expediente, la fecha y hora de la transmisión, el remitente y el destinatario, el nombre del archivo y su tamaño.

3.3.3. Cuando las pruebas electrónicas con arreglo a una orden europea de producción se hayan transmitido a través de medios alternativos de comunicación entre los proveedores de servicios y las autoridades competentes del Estado de emisión ([1]), o cuando las pruebas electrónicas se transmitan a través de medios alternativos de la autoridad de ejecución a las autoridades competentes del Estado de emisión con arreglo al procedimiento de ejecución previsto en el artículo 16, apartado 9, del Reglamento (UE) 2023/1543, la persona que inicie la transmisión:

a) Registrará y transmitirá a la autoridad a la que se hayan transmitido o puesto a disposición las pruebas electrónicas la siguiente información como parte de un manifiesto:

1) información sobre el remitente y el destinatario;

2) metadatos que asocien las pruebas electrónicas facilitadas a una o varias órdenes europeas de producción o conservación concretas;

3) la fecha y la hora de la transmisión o la indicación del momento en que las pruebas electrónicas se pusieron a disposición del destinatario;

4) información relativa a los medios de transmisión (por ejemplo, un registro del enlace seguro a través del cual se puso a disposición la prueba electrónica, un justificante de recepción o entrega de los servicios postales, etc. ([2]));

5) el nombre o nombres completos de los archivos de las pruebas electrónicas transmitidas o puestas de otro modo a disposición del destinatario previsto en el Estado de emisión;

6) el tamaño de los datos de las pruebas electrónicas transmitidas o puestas a disposición del destinatario previsto en el Estado de emisión;

7) al menos una huella *hash* de los datos transmitidos o puestos a disposición, y una indicación de los algoritmos *hash* utilizados. Los algoritmos *hash* utilizados para calcular dichos valores resumen deberán ser fuertes desde el punto de vista criptográfico, de uso común y no estar sujetos a debilidades de divulgación pública, como las colisiones (por ejemplo, SHA-512, SHA3-512, BLAKE2 o RIPEMD-160, pero potencialmente uno más fuerte, en función de los avances tecnológicos).

b) Cuando proceda, indicará, como parte del manifiesto mencionado en la letra a) anterior, la fecha y hora hasta la que se podrá seguir accediendo a las pruebas electrónicas. Este plazo proporcionará a la autoridad competente del Estado de emisión un tiempo razonable para recuperar las pruebas electrónicas, que no será inferior a diez días naturales ni superior a cuarenta y cinco días naturales a partir del momento en que se pongan a disposición las pruebas electrónicas. A petición de la autoridad competente del Estado de emisión, el plazo indicado por el originador podrá ampliarse en casos concretos.

c) Podrá hacer constar y transmitir cualquier información u observación adicional pertinente para el caso a la autoridad a la que se hayan transmitido o puesto a disposición las pruebas electrónicas, como parte del manifiesto mencionado en la letra a) anterior.

3.4. Visto el artículo 28 del Reglamento (UE) 2023/1543, los programas informáticos de aplicación de referencia deberán recoger, transmitir o facilitar de otro modo el acceso mediante programación a las estadísticas a que se refiere el apartado 2 de dicho artículo, tanto en formatos de datos estructurados (por ejemplo, XML) como no estructurados (por ejemplo, PDF). De conformidad con el artículo 28, apartado 3, del Reglamento (UE) 2023/1543, cuando estén técnicamente equipados, los portales nacionales ([3]) gestionados por los Estados miembros también podrán transmitir o facilitar estas estadísticas a la Comisión mediante un proceso automatizado. La Comisión publicará orientaciones sobre la estructura de los datos y el método de recogida y comunicación de estas estadísticas.

([1]) Para mayor claridad, las referencias a las autoridades nacionales competentes se entenderán también, *mutatis mutandis*, aplicables a los miembros nacionales de Eurojust, a los fiscales europeos y a los fiscales europeos delegados, en la medida en que estén facultados para desempeñar las mismas funciones en virtud del Derecho de la UE y del Derecho nacional.

([2]) Cabe recordar que, de conformidad con el artículo 19, apartado 5, la transmisión a través de dichos medios de comunicación alternativos deberá cumplir los requisitos de ser rápida, segura y fiable, y permitir al destinatario establecer su autenticidad.

([3]) Por «portales nacionales» deben entenderse los «sistemas informáticos» nacionales que forman parte del sistema informático descentralizado, tal como se define en el artículo 3, apartado 21, del Reglamento (UE) 2023/1543.

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,

b) la comunicación dentro del sistema informático descentralizado entre las autoridades competentes y los órganos y organismos de la Unión,

c) la comunicación entre las autoridades competentes y los proveedores de servicios a través de una API y de la interfaz basada en la web, así como

d) la comunicación con la base de datos de Tribunales.

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, en particular los referenciados por organizaciones europeas de normalización, como ETSI.

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 de pruebas electrónicas utilizarán las normas o léxicos pertinentes que sean necesarios para la correcta validación de los elementos y tipos definidos en este esquema. Se incluyen aquí:

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.

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

4.6. La Comisión definirá las especificaciones de la API común, que los Estados de aplicación pondrán a disposición de los proveedores de servicios como medio de acceso al sistema informático descentralizado. En la medida de lo posible y lo razonable, esta API se basará en ETSI TS 104 144 [«Definición de interfaz para el Reglamento (UE) 2023/1543 relativo a la prueba electrónica para las autoridades nacionales y los proveedores de servicios»].

4.7. 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) 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 (CA) 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 (mensajes, formularios, documentos y pruebas electrónicas) 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 la disponibilidad asegurando el acceso continuo a los servicios y datos, evitando interrupciones debidas a ciberataques o fallos;

e) medidas para garantizar el registro de incidencias de seguridad en consonancia con las recomendaciones internacionales reconocidas en materia de estándares de seguridad informática;

f) 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. 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 adecuadas para garantizar un alto nivel de ciberseguridad.

5.4. 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 sus obligaciones en virtud, respectivamente, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([4]) y de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo ([5]), según proceda.

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

5.6. Teniendo en cuenta su participación en el sistema informático descentralizado, Eurojust y la Fiscalía Europea aplicarán las medidas necesarias para garantizar que sus respectivos sistemas informáticos cumplan los requisitos del Reglamento (UE) 2018/1725 y sus actos constitutivos.

5.7. Los Estados miembros, Eurojust y la Fiscalía Europea 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 que forman parte del sistema informático descentralizado bajo su responsabilidad.

6. **Cifrado de pruebas electrónicas** ([6])

6.1. Sin perjuicio de las medidas de seguridad proporcionadas por el sistema informático descentralizado, al expedir una orden europea de producción las autoridades competentes podrán facilitar de forma adicional un certificado público X.509 específico para el cifrado asimétrico de las pruebas electrónicas.

([4]) 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).

([5]) 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).

([6]) Para evitar dudas, el término «pruebas electrónicas» se limita a la definición que figura en el artículo 3, apartado 8, del Reglamento (UE) 2023/1543.

6.2. La emisión, gestión, verificación y todos los aspectos relacionados de los certificados a los que se hace referencia en el punto 6.1, junto con la correspondiente infraestructura de clave pública, serán responsabilidad exclusiva del Estado emisor.

6.3. Sin perjuicio de futuros avances tecnológicos, los certificados públicos serán compatibles con los algoritmos de cifrado estándar del sector, como RSA (Rivest-Shamir-Adleman) o ECDH (curva elíptica Diffie-Hellman) para ECC (criptografía de curva elíptica).

6.4. Los certificados públicos deberán incluir la extensión adecuada «keyUsage», como «keyEncipherment» o «dataEncipherment» para los certificados basados en RSA, y «keyAgreement» para los certificados basados en ECC. Los certificados se facilitarán en formato PEM (correo con protección de la privacidad) o DER (normas de codificación distinguidas).

6.5. Cuando la autoridad emisora haya facilitado un certificado público X.509, y cuando un proveedor de servicios envíe las pruebas electrónicas presentadas en virtud de una orden europea de entrega, el proveedor, antes de la transmisión de dichos datos a través del sistema informático descentralizado, cifrará las pruebas electrónicas utilizando el certificado público X.509 correspondiente facilitado por el Estado emisor.

6.6. Cuando la autoridad emisora haya facilitado un certificado público X.509, pero la transmisión de pruebas electrónicas cifradas no sea posible por razones técnicas u otras razones justificables, y sin perjuicio de lo dispuesto en el artículo 19, apartado 5, del Reglamento (UE) 2023/1543, el proveedor de servicios podrá transmitir los datos sin cifrado de contenido. En tales casos, el prestador de servicios facilitará una explicación motivada a la autoridad emisora.

7. **Objetivos mínimos de disponibilidad**

7.1. Los Estados miembros, Eurojust y la Fiscalía Europea 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.

7.2. 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.

7.3. 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.

7.4. Los Estados miembros, Eurojust y la Fiscalía Europea notificarán a la Comisión 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.

7.5. Cuando los Estados miembros, Eurojust o la Fiscalía Europea dispongan de períodos fijos regulares de mantenimiento, informarán a la Comisión y a los participantes en el sistema informático descentralizado de las horas y los días en que estén previstos. Sin perjuicio de las obligaciones establecidas en el punto 7.4, en caso de que los componentes del sistema informático descentralizado bajo la responsabilidad de los Estados miembros, Eurojust o la Fiscalía Europea dejen de estar disponibles durante dichos períodos fijos regulares, podrán optar por no notificarlo a la Comisión en cada ocasión.

7.6. En caso de fallo técnico imprevisto de los componentes del sistema informático descentralizado bajo la responsabilidad de los Estados miembros, Eurojust o la Fiscalía Europea, estos informarán sin demora a la Comisión y a los participantes en el sistema informático descentralizado sobre dicho fallo y, si se conoce, sobre el plazo previsto para su recuperación.

7.7. En caso de actividades de mantenimiento o de un fallo técnico inesperado de los componentes del sistema informático descentralizado bajo la responsabilidad de un Estado miembro con repercusiones negativas en la disponibilidad de la API o de la interfaz basada en la web para los proveedores de servicios, el Estado miembro afectado publicará sin demora esta información en un sitio web o la comunicará a los proveedores de servicios que operen en su territorio, sin retrasos injustificados.

7.8. En caso de fallo técnico imprevisto de la base de datos de Tribunales, la Comisión informará sin demora a los Estados miembros, a Eurojust y a la Fiscalía Europea de esta indisponibilidad y, si se conoce, del plazo previsto para su recuperación.

7.9. En caso de perturbación del servicio, los Estados miembros, Eurojust y la Fiscalía Europea 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.

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

8. **Base de datos de Tribunales/autoridades competentes**

8.1. Visto el artículo 19 del Reglamento (UE) 2023/1543, a efectos del funcionamiento del sistema informático descentralizado es esencial establecer una base de datos autorizada sobre los proveedores de servicios y las autoridades competentes.

8.2. La base de datos autorizada sobre las autoridades competentes incluirá la siguiente información en un formato estructurado:

a) a efectos del artículo 19 del Reglamento (UE) 2023/1543, información sobre las autoridades competentes notificadas de conformidad con el artículo 31, apartado 1, letras a) a c), de dicho Reglamento, incluso con respecto a:

1) los miembros nacionales de Eurojust, junto con una indicación de si, con arreglo a la legislación nacional, pueden dictar órdenes europeas de producción y de conservación de conformidad con el artículo 8, apartados 3 y 4, del Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo ([7]);

2) los fiscales europeos delegados y los fiscales europeos, cuando sean notificados por los Estados miembros de conformidad con el artículo 105, apartado 3, del Reglamento (UE) 2017/1939 ([8]) del Consejo como autoridad de emisión competente en el sentido del Reglamento (UE) 2023/1543;

b) cuando proceda, la información necesaria para determinar las zonas geográficas de competencia de las autoridades, u otros criterios pertinentes necesarios para establecer su competencia;

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

8.2.1. La información contemplada en el punto 8.2, letra c) incluirá lo siguiente:

a) información sobre el Estado miembro en el que esté establecido el establecimiento designado del prestador de servicios o en el que resida su representante legal:

1) Estado miembro;

2) autoridad central;

([7]) 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 (DO L 295 de 21.11.2018, p. 138).

([8]) Reglamento (UE) 2017/1939 del Consejo, de 12 de octubre de 2017, por el que se establece una cooperación reforzada para la creación de la Fiscalía Europea (DO L 283 de 31.10.2017, p. 1).

b) información sobre el prestador de servicios:

1) nombre;

2) dirección/establecimiento;

3) el número de registro;

4) forma jurídica;

5) número de teléfono;

6) correo electrónico;

c) información sobre el establecimiento designado/representante legal:

1) tipo de entidad (establecimiento designado/representante legal);

2) nombre;

3) dirección/establecimiento;

4) número de teléfono;

5) correo electrónico;

6) persona/entidad de contacto general;

7) lenguas oficiales aceptadas por el proveedor de servicios/Establecimiento designado/Representante legal;

8) servicios a que se refiere el artículo 2, apartado 1, de la Directiva (UE) 2023/1544 del Parlamento Europeo y del Consejo ([9]) ofrecidos en la Unión;

9) tipo de instrumentos jurídicos de la UE para los que se designa al Establecimiento Designado/ Representante Legal (en situaciones en las que los Estados miembros no participan en todos los instrumentos jurídicos pertinentes de la UE);

10) ámbito territorial de la designación o del nombramiento;

d) autenticación de la información:

1) nombre del representante autorizado;

2) cargo;

3) dirección;

4) número de teléfono;

5) correo electrónico;

6) fecha.

8.2.2. Cuando esté disponible, la información mencionada en el punto 8.2., letra c) podrá incluir:

a) información sobre el prestador de servicios:

1) persona de contacto para consultas sobre las notificaciones (si es distinta del firmante);

2) sitio web;

b) tipos de datos disponibles:

1) para cada servicio afectado:

— tipos de datos disponibles;

— categorías de datos;

— identificadores;

— período de disponibilidad de los datos;

([9]) Directiva (UE) 2023/1544 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, por la que se establecen normas armonizadas para la designación de establecimientos designados y de representantes legales a efectos de recabar pruebas electrónicas en procesos penales (DO L 191 de 28.7.2023, p. 181, ELI: http://data.europa.eu/eli/dir/2023/1544/oj).

2) información adicional sobre los datos;

3) información adicional sobre el servicio (por ejemplo, relaciones de subcontratación);

c) información sobre el establecimiento designado/representante legal:

1) otros proveedores de servicios para los que este establecimiento designado o representante legal está designado;

2) información de contacto para asistencia técnica;

3) contacto de emergencia;

d) información técnica:

1) nombre del punto de contacto técnico;

2) número de teléfono del punto de contacto técnico;

3) correo electrónico del punto de contacto técnico;

4) URL de la API para recuperar información de forma dinámica sobre los tipos de datos;

5) tipo de conexión al sistema informático nacional:

— interfaz web;

— API;

— URL de la API *push* (de transmisión automática).

8.3. Habida cuenta de las necesidades operativas del sistema informático descentralizado:

a) la Comisión será responsable del desarrollo, mantenimiento, funcionamiento y apoyo de la base de datos autorizada;

b) la Comisión posibilitará el acceso a la base de datos autorizada a través de una API puesta a disposición de las autoridades competentes, Eurojust y la Fiscalía Europea a efectos de su participación en el sistema informático descentralizado;

c) los Estados miembros velarán por que la información sobre sus autoridades competentes que figura en el punto 8.2, letras a) y b), en la base de datos autorizada sea completa, exacta y se mantenga actualizada;

d) la base de datos autorizada permitirá a los Estados miembros facilitar y actualizar en ella la información sobre sus proveedores de servicios, y a las autoridades que participen en el sistema informático descentralizado acceder a dicha información mediante programación y recuperarla;

e) los Estados miembros y los proveedores de servicios velarán por que la información que figura en el punto 8.2, letra c), de la base de datos autorizada sea completa, exacta y se mantenga actualizada.