

REGLAMENTO DE EJECUCIÓN (UE) 2022/422 DE LA COMISIÓN
de 14 de marzo de 2022

por el que se establecen las especificaciones técnicas, las medidas y otros requisitos para la implementación del sistema informático descentralizado a que se refiere el Reglamento (UE) 2020/1783 del Parlamento Europeo y del Consejo

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) 2020/1783 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2020, relativo a la cooperación entre los órganos jurisdiccionales de los Estados miembros en el ámbito de la obtención de pruebas en materia civil o mercantil (obtención de pruebas) ⁽¹⁾, y en particular su artículo 25, apartado 1,

Considerando lo siguiente:

- (1) Con el fin de establecer el sistema informático descentralizado para la comunicación y el intercambio de documentos a efectos de la obtención de pruebas, es necesario definir y adoptar especificaciones técnicas, medidas y otros requisitos para la implementación de dicho sistema.
- (2) Existen herramientas de intercambio digital de datos procesales que ni sustituyen a los sistemas informáticos ya establecidos en los Estados miembros, ni requieren modificaciones costosas de dichos sistemas. La herramienta más importante en este sentido es e-CODEX (Sistema de comunicación para la justicia digital mediante intercambio electrónico de datos).
- (3) El sistema informático descentralizado debe estar compuesto por los sistemas finales (*back-end*) de los Estados miembros y los puntos de acceso interoperables, a través de los cuales están interconectados. Los puntos de acceso del sistema informático descentralizado deben basarse en e-CODEX.
- (4) Una vez desarrollado el sistema informático descentralizado, el comité directivo asegurará su funcionamiento y mantenimiento. La Comisión debe crear el comité de dirección en un acto separado.
- (5) 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 ⁽²⁾, emitió su dictamen el 24 de enero de 2022.
- (6) Las medidas previstas en el presente Reglamento se ajustan al dictamen del Comité relativo a la cooperación entre los órganos jurisdiccionales de los Estados miembros en el ámbito de la obtención de pruebas en materia civil o mercantil.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Especificaciones técnicas del sistema informático descentralizado

En el anexo se establecen las especificaciones técnicas, las medidas y otros requisitos para la implementación del sistema informático descentralizado a que se refiere el artículo 25 del Reglamento (UE) 2020/1783.

⁽¹⁾ DO L 405 de 2.12.2020, p. 1.

⁽²⁾ 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).

*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 14 de marzo de 2022.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

ANEXO

Especificaciones técnicas, medidas y otros requisitos del sistema descentralizado a que se refiere el artículo 1**1. Introducción**

El sistema de intercambio en el contexto de la obtención de pruebas es un sistema informático descentralizado basado en e-CODEX que puede llevar a cabo intercambios de documentos y mensajes relacionados con la obtención de pruebas entre los distintos Estados miembros, de conformidad con el Reglamento (UE) 2020/1783. El carácter descentralizado de ese sistema informático permitiría intercambiar datos exclusivamente entre un Estado miembro y otro, sin que ninguna de las instituciones de la Unión intervenga en los intercambios.

2. Definiciones

- 2.1. «Protocolo seguro de transferencia de hipertexto» o «HTTPS»: canales de comunicación cifrada y conexión segura.
- 2.2. «Portal»: la solución de implementación de referencia o la solución nacional conectada al sistema informático descentralizado.
- 2.3. «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 digitales.
- 2.4. «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 digitales.
- 2.5. «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.
- 2.6. «Servicio web»: sistema de *software* diseñado para posibilitar la interacción interoperable entre máquinas en una red; 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.

3. Métodos de comunicación por medios electrónicos

El sistema de intercambio en el contexto de la obtención de pruebas utilizará métodos de comunicación electrónica basados en servicios, como los servicios web u otras infraestructuras de servicios digitales reutilizables a efectos de intercambiar mensajes y documentos.

En concreto, utilizará la infraestructura e-CODEX, que consta de dos componentes principales: el conector y la pasarela.

El conector se encarga de gestionar la comunicación con la solución de implementación de referencia o las soluciones nacionales. Puede procesar el intercambio de mensajes con la pasarela en ambas direcciones, rastrear los mensajes y confirmar su recepción utilizando normas como las pruebas ETSI-REM, validar firmas de documentos profesionales, crear un testigo (*token*) que conserve el resultado de la validación en formato PDF y XML y crear un contenedor utilizando normas como ASIC-S en el cual el contenido profesional de un mensaje está empaquetado y firmado.

La pasarela se encarga del intercambio de mensajes y es agnóstica del contenido del mensaje. Puede enviar y recibir mensajes hacia y desde el conector, validar información de cabecera, identificar el modo de procesamiento correcto, firmar y cifrar mensajes y transferir mensajes a otras pasarelas.

4. **Protocolos de comunicación**

El sistema de intercambio en el contexto de la obtención de pruebas utilizará protocolos de internet seguros, como el HTTPS, para la comunicación de los componentes del portal y del sistema informático descentralizado, así como protocolos de comunicación normalizados, como SOAP, para la transmisión de metadatos y datos estructurados.

En concreto, e-CODEX proporciona una sólida seguridad de la información aprovechando la autenticación y el protocolo criptográfico multicapa más recientes.

5. **Normas de seguridad**

A efectos de la comunicación y difusión de información a través del sistema de intercambio en el contexto de la obtención de pruebas, 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 (HTTPS);
- b) medidas para garantizar la integridad de los datos durante el intercambio de estos;
- c) medidas para garantizar el no repudio del origen del emisor de la información en el sistema de intercambio en el contexto de la obtención de pruebas 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;
- e) medidas para garantizar la autenticación y autorización de todos los usuarios registrados y medidas para verificar la identidad de los sistemas conectados al sistema de intercambio en el contexto de la obtención de pruebas;
- f) el sistema de intercambio en el contexto de la obtención de pruebas se desarrollará de conformidad con el principio de protección de datos desde el diseño y por defecto.

6. **Disponibilidad de los servicios**

- 6.1. El servicio funcionará durante 24 horas todos los días de la semana, con una tasa de disponibilidad del sistema de al menos un 98 %, sin contar el mantenimiento programado.
 - 6.2. Los Estados miembros notificarán a la Comisión las actividades de mantenimiento como sigue:
 - a) con 5 días hábiles de antelación en el caso de los trabajos de mantenimiento que puedan causar una indisponibilidad de hasta 4 horas;
 - b) con 10 días hábiles de antelación en el caso de los trabajos de mantenimiento que puedan causar una indisponibilidad de hasta 12 horas;
 - c) con 30 días hábiles de antelación en el caso de los trabajos de mantenimiento de la infraestructura de la sala de ordenadores que puedan causar una indisponibilidad de hasta 6 días al año.
 - 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. En caso de que los Estados miembros hayan establecido períodos de mantenimiento semanal, informarán a la Comisión de la hora y el día de la semana en que estos estén previstos. Sin perjuicio de las obligaciones establecidas en el punto 6.2, en caso de indisponibilidad de los sistemas de los Estados miembros durante dicho período de mantenimiento, los Estados miembros pueden optar por no informar de ello a la Comisión cada vez que esto ocurra.
 - 6.5. En caso de fallo técnico imprevisto de los sistemas de los Estados miembros, estos informarán a la Comisión sin demora de la indisponibilidad de su sistema, así como, si se conoce, del momento previsto de reanudación del servicio.
 - 6.6. En caso de fallo inesperado de la base de datos de las autoridades competentes, la Comisión informará sin demora a los Estados miembros de la indisponibilidad, así como, si se conoce, del momento previsto de reanudación del servicio.
-