

PLIEGO DE CLÁUSULAS JURÍDICAS PARTICULARES QUE HA DE REGIR EN EL CONTRATO DE SERVICIO DE SISTEMA DE CREACIÓN Y DESARROLLO DE CUADERNOS DE RECOGIDA DE DATOS ELECTRÓNICOS PARA ENSAYOS CLÍNICOS, PARA LA FUNDACIÓN PARA LA INVESTIGACIÓN BIOMÉDICA DEL HOSPITAL UNIVERSITARIO LA PAZ, A ADJUDICAR POR PROCEDIMIENTO ABIERTO MEDIANTE PLURALIDAD DE CRITERIOS. El Proyecto PTC23/00006 ha sido financiado por el Instituto de Salud Carlos III (ISCIII) y cofinanciado por la Unión Europea. Expediente PA 02-2026.

ÍNDICE

1. CARACTERÍSTICAS GENERALES

- 1.1. Objeto del contrato.....
- 1.2. Legislación.....

2. ESPECIFICACIONES TÉCNICAS DEL SUMINISTRO

PLIEGO DE CLÁUSULAS JURÍDICAS PARTICULARES QUE HA DE REGIR EN EL CONTRATO DE SERVICIO DE SISTEMA DE CREACIÓN Y DESARROLLO DE CUADERNOS DE RECOGIDA DE DATOS ELECTRÓNICOS PARA ENSAYOS CLÍNICOS, PARA LA FUNDACIÓN PARA LA INVESTIGACIÓN BIOMÉDICA DEL HOSPITAL UNIVERSITARIO LA PAZ, A ADJUDICAR POR PROCEDIMIENTO ABIERTO MEDIANTE PLURALIDAD DE CRITERIOS. El Proyecto PTC23/00006 ha sido financiado por el Instituto de Salud Carlos III (ISCIII) y cofinanciado por la Unión Europea. Expediente PA 02-2026.

1.- CARACTERÍSTICAS GENERALES

1.1-OBJETO DEL CONTRATO.

El objeto del presente procedimiento es la contratación de los servicios necesarios para la creación de cuadernos de recogida de datos electrónicos (eCRD) a través de una plataforma online con la tecnología más innovadora y con el diseño más intuitivo, para la recogida de datos en cualquier tipo de ensayo clínico, desde pequeños estudios observacionales, hasta grandes y complejos ensayos clínicos, para poder llevar a cabo la gestión y el desarrollo de los ensayos clínicos que se realicen en la Unidad de Investigación Clínica y Ensayos Clínicos del Hospital Universitario La Paz de Madrid.

Dichos servicios deberán respetar los requisitos fijados por la red europea de investigación ECRIN (European Clinical Research Infrastructure Network).

El presente documento tiene por objeto fijar las condiciones técnicas que han de regir el proceso de contratación del servicio a contratar. Dichas condiciones hacen referencia a las características técnicas mínimas que debe contemplar el contrato.

1.2- LEGISLACIÓN.

Los productos presentados a este procedimiento, deberán cumplir la legislación vigente que sea de aplicación.

El contratista deberá respetar el carácter confidencial de aquella información a la que tenga acceso con ocasión de la ejecución del contrato a la que se le hubiese dado el referido carácter en los pliegos o en el contrato, o que por su propia naturaleza deba ser tratada como tal, quedando el contratista sometido a la normativa nacional y europea en materia de protección de datos, siendo ésta una obligación contractual esencial (211.1.f LCSP).

1.3.- DURACIÓN.

El plazo de ejecución del contrato será de DOS (2) años, contando desde el día siguiente de su formalización. Las fechas para la realización de las diferentes operaciones integradas en el Servicio, se concertarán con el adjudicatario.

2. ESPECIFICACIONES TÉCNICAS

Se trata de dar continuidad a una infraestructura con más de 10 años de antigüedad y distribuida geográficamente. Con esta contratación lo que se promueve es la centralización de estos servicios de recogida de datos electrónica dispersos en diferentes puntos del territorio nacional. Se debe dar continuidad a más de 40 ensayos clínicos multicéntricos que ya tienen desarrollados e implementados los eCRDs en producción con la recogida de datos de pacientes reales en marcha sin que ello cause un inconveniente añadido en la inclusión de pacientes en dichos ensayos clínicos. Por lo que el traspaso del sistema actual de eCRD al nuevo sistema debe ser lo más rápido y transparente para los investigadores principales y usuarios del sistema.

Deberán existir dos entornos del sistema, el entorno de desarrollo debe estar aislado y claramente diferenciado del entorno utilizado en producción. Los entornos de desarrollo y producción deben estar aislados entre sí.

El sistema de eCRD a contratar deberá ser un sistema validado, es decir que garantice y documente que el sistema funciona según lo requerido. La validación se producirá cuando el sistema se instale por primera vez, pero si el sistema cambia (se aplican parches, se actualizan, etc.), se debe realizar una nueva validación del sistema. Por lo tanto, la validación será un proceso continuo y se deberán revisar la evaluación de riesgos y la posible revalidación de forma periódica, así como durante los cambios planificados.

Será necesario obtener evidencia de la validación del sistema. Todos los proveedores deberán proporcionar dichas pruebas de validación. La documentación que evidencia la validación será las pruebas de OQ para demostrar que se cumplen los requisitos de la especificación. Y con la validación IQ se demostrará que el software se ha instalado y probado en un entorno específico (servidores web, bases de datos, etc.) garantizando que funciona como se espera.

Los servicios de eCRD a contratar deberán cumplir con los siguientes detalles técnicos, que tendrán que ser demostrados mediante una auditoria específica como último paso antes de la contratación específica de los servicios:

- La ubicación de la infraestructura, tanto los servidores y/o la nube, así como el almacenamiento de las copias de seguridad, deben estar alojados dentro del Espacio Económico Europeo (EEE) y así poder cumplir con los requisitos establecidos en el Reglamento General de Protección de Datos de la UE (RGPD).
- Seguridad de la infraestructura informática: Todos los servidores y equipos relacionados deben estar alojados en una ubicación específica para su servicio. Se debe contar con un sistema de seguridad adecuado y con una política de acceso segura. Los servidores deben

estar alojados en una sala cerrada, con acceso limitado a roles específicos. El sistema debe proporcionar los procedimientos para obtener acceso a la sala, los motivos de acceso y los planes de registro, además de un control de acceso físico.

- **Suministro de energía a la infraestructura informática:** Los servidores y el equipo relacionado deben estar protegidos contra cortes de energía, al menos en la medida en que puedan apagarse de manera ordenada, por ejemplo, mediante una unidad de suministro de energía ininterrumpible (UPS) o mediante una fuente de alimentación alternativa como un generador local para permitir un funcionamiento continuo durante una pérdida de energía prolongada. Estos sistemas de suministro de energía ininterrumpible y cualquier otro equipo utilizado para este propósito también deben probarse periódicamente (según las recomendaciones del fabricante) para garantizar que estén funcionando correctamente.
- **Entorno controlado:** Los servidores requieren condiciones controladas de temperatura y humedad para un funcionamiento óptimo, así que la sala de servidores debe ser capaz de mantener la temperatura dentro de un rango definido aceptable.
- **Alarmas de humo e incendio:** Las salas utilizadas para alojar la infraestructura informática deben estar equipadas con alarmas de humo y de calor, vigiladas 24 horas al día, 7 días a la semana, y probadas periódicamente. Los servidores y el equipo relacionado deben estar protegidos contra incendios. Aunque las alarmas de humo y de calor son habituales, el requisito clave en este caso es que se monitoricen de forma continua y se prueben periódicamente.
- **Fallos del sistema:** Los fallos en cualquier infraestructura informática que se utilice directamente como soporte a la actividad de ensayos clínicos debe disponer del envío automático de alertas al personal responsable. Si la infraestructura informática experimenta algún tipo de fallo, es importante que el personal esté al tanto de esto de manera oportuna. El fallo de una máquina suele ser obvio porque la funcionalidad desaparece de repente, pero también se debe ser consciente de los “fallos silenciosos” que pueden ocurrir en una máquina y que pueden no volverse obvios hasta que pase algún tiempo, cuando esa funcionalidad se necesite con urgencia.
- **Soporte de servidores y recuperación de tiempos de inactividad:** Se debe disponer de mecanismos de soporte de hardware para permitir que el equipo sea reemplazado o reparado según los tiempos planificados para la recuperación ante desastres. La planificación de la continuidad y la respuesta a los problemas deben ser proporcionales al impacto potencial. Se deberá detallar cómo se gestionan las reparaciones y los reemplazos de modo que se puedan lograr los tiempos de respuesta y recuperación especificados para los sistemas mediante planes de continuidad empresarial y recuperación ante desastres.
- **Registros de configuración del servidor:** Deberán estar disponibles registros detallados de las configuraciones del servidor, para una reconstrucción precisa si fuese necesario.

La configuración actual (versión y configuración del sistema operativo, aplicaciones, usuarios, utilidades, etc.) de cada servidor que se utilice directamente para la actividad de ensayos clínicos debe estar documentada. Esto permitiría reconstruir con precisión una máquina al mismo estado si es necesario, y también permite que se realicen trabajos adicionales en un servidor de manera segura, basándose en el conocimiento completo del estado actual de la máquina.

- **Mantenimiento del software del servidor:** Las actualizaciones de software necesarias deben identificarse y aplicarse de manera oportuna pero segura a los sistemas operativos, utilidades y aplicaciones del servidor. Se exige que exista una gestión activa de la aplicación de parches y actualizaciones del servidor, es decir, un conjunto de procedimientos que determinen cómo se hace esto, cuándo y por quién. Aunque puede haber un riesgo en no aplicar parches, ya que estos suelen cerrar las lagunas de seguridad, también existe un riesgo inherente en agregar un parche o actualización a un sistema en funcionamiento. La gestión de parches debe incluir la documentación necesaria para evaluar los riesgos asociados con los parches/actualizaciones y cómo se realizarán los cambios de la manera más segura posible.
- **Firewalls externos:** Se deberá disponer de firewalls externos para bloquear los accesos inadecuados. Sería recomendable realizar pruebas de penetración y monitorizar de forma continua la actividad de tráfico e intentar identificar e investigar cualquier intento de piratería o denegación de servicio.
- **Gestión de inicio de sesión:** El sistema de eCRD debe disponer de una gestión segura de inicio de sesión. Se debe disponer de un método sólido y seguro para autenticar a los usuarios. Por lo general, esto se haría mediante una cuenta de usuario única y una contraseña segura, aunque ahora es común la autenticación biométrica, por ejemplo, la huella dactilar o el reconocimiento facial. Los inicios de sesión deben bloquearse de forma automática después de un período de inactividad determinado, requiriendo una reactivación segura.
- **Continuidad del Negocio:** Se deberá disponer de un Plan de Continuidad del Negocio (BCP) que incluya medidas de Recuperación ante Desastres en respuesta a posibles escenarios de desastre. Se deberán cubrir varios escenarios de desastre, por ejemplo, ciberataque, pérdida de energía en la sala de servidores o robo de equipos. Se deben tener descritas las evaluaciones de los escenarios individuales en cuanto a probabilidad e impacto, y los planes de Recuperación ante Desastres que describan las medidas que se deben tomar para resolver el problema dentro de un marco de tiempo apropiado. Por ejemplo, la pérdida de un disco duro en una matriz RAID con redundancia suficiente podría ser un proceso relativamente relajado en el que se espera que un proveedor de hardware llegue y cambie el disco averiado dentro de las 24 horas; La respuesta a un incendio en una sala de servidores puede requerir una acción más inmediata, como avisar a los servicios de bomberos, reemplazar el equipo dañado, etc. El BCP deberá incluir detalles de los procesos de copia de seguridad y recuperación de datos, específicamente el punto en el que se pueden recuperar los datos y cuánto tiempo se espera que tome esta recuperación. El BCP también deberá cubrir la respuesta a un ciberataque, incluidas las

actividades inmediatas y de seguimiento. Se deben realizar pruebas de respuestas a escenarios de desastre de manera rutinaria, y al menos anualmente. El BCP se considera un documento dinámico y debe actualizarse de forma rutinaria, al menos una vez al año o en función de los cambios en el sistema o el servicio.

- Sistema de copias de seguridad: Las copias de seguridad deberán realizarse utilizando un sistema gestionado, documentado y automático que garantice que los datos nuevos o modificados se guarden en un plazo de 24 horas y que permita verificar que el sistema está funcionando correctamente. La frecuencia de las copias de seguridad no deberá ser inferior a cada 24 horas. Las copias de seguridad diarias se consideran como un mínimo y se deben implementar copias de seguridad más frecuentes. Se deberá asegurar (por ejemplo, enviando informes/copias de registros) de que el proceso de copia de seguridad está funcionando correctamente.
- Almacenamiento de copias de seguridad: El almacenamiento de los medios de copia de seguridad deberá ser suficiente para evitar la pérdida de datos en caso de incendio, ciberataque u otro desastre. Las copias de seguridad no deberán permanecer en la misma ubicación que los datos originales. Se exigirá que se garantice que, si ocurre un desastre a gran escala en uno de los sitios de almacenamiento de datos, esté disponible una copia de los datos.
- Pruebas de recuperación de datos: Las pruebas de los procedimientos de restauración deberán realizarse y documentarse con una frecuencia que refleje los cambios en el sistema. Se deberán tener en cuenta los aspectos prácticos de la restauración, ya sea un archivo individual, una base de datos específica o un servidor completo, y si esta actividad se lleva a cabo en el centro o de forma remota, y también la restauración de los permisos asociados.

Los servicios a contratar deben cumplir con los estándares BPC de la ICH E6 y los principios estadísticos de la ICH E9. El servicio debe estar auditado por auditorías internas y externas. Así como cumplir con los detalles técnicos descritos en el apartado anterior.

Madrid, a 13 de marzo de 2026.

POR EL ÓRGANO DE CONTRATACIÓN,

D. Francisco García Río

Presidente de la Comisión Delegada de la Fundación

CONFORME:
EL ADJUDICATARIO
FECHA Y FIRMA