

PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HA DE REGIR EL CONTRATO DE SERVICIO PARA EL DISEÑO, EL DESARROLLO, LA IMPLEMENTACIÓN Y EL SOPORTE OPERATIVO DE LA INTRANET DEL PROYECTO AMRI-SYNERGY, A ADJUDICAR POR PROCEDIMIENTO ABIERTO SIMPLIFICADO MEDIANTE PLURALIDAD DE CRITERIOS, PARA LA FUNDACIÓN PARA LA INVESTIGACIÓN BIOMÉDICA DEL HOSPITAL UNIVERSITARIO LA PAZ. EXPEDIENTE. PAS 40-2026. El Proyecto REDES2024-154441 E ha sido financiado por MICIU/AEI /10.13039/501100011033.

ÍNDICE

1. CARACTERÍSTICAS GENERALES

1.1. Objeto del contrato.....	2
1.2. Legislación.....	3
1.3. Duración	3

2. ESPECIFICACIONES TÉCNICAS DEL SERVICIO

2.1. Requerimientos funcionales.....	4
2.2. Descripción de requisitos no funcionales.....	11

PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HA DE REGIR EL CONTRATO DE SERVICIO PARA EL DISEÑO, EL DESARROLLO, LA IMPLEMENTACIÓN Y EL SOPORTE OPERATIVO DE LA INTRANET DEL PROYECTO AMRI-SYNERGY, A ADJUDICAR POR PROCEDIMIENTO ABIERTO SIMPLIFICADO MEDIANTE PLURALIDAD DE CRITERIOS, PARA LA FUNDACIÓN PARA LA INVESTIGACIÓN BIOMÉDICA DEL HOSPITAL UNIVERSITARIO LA PAZ. EXPEDIENTE. PAS 40-2026. El Proyecto REDES2024-154441 E ha sido financiado por MICIU/AEI /10.13039/501100011033.

1.- CARACTERÍSTICAS GENERALES

1.1-OBJETO DEL CONTRATO.

La Fundación para la Investigación Biomédica del Hospital Universitario la Paz (en adelante FIBHULP) tiene por finalidad gestionar programas y proyectos de investigación clínica, y otras actividades conexas en el campo de la Biomedicina, para contribuir a la promoción y protección de la salud de la población y al progreso y mejora del Sistema Sanitario de la Comunidad de Madrid. Dentro de su estructura se encuentra la Unidad de Investigación Clínica (en adelante UIC) de IDIPAZ, la cual no solo pertenece a la Plataforma ISCIII de Soporte para la Investigación Clínica (de aquí en adelante referida como SCReN, por sus siglas en inglés: Spanish Clinical Research Network), sino que actualmente desempeña el rol de Unidad de Coordinación de SCReN, convirtiendo al HU La Paz (y por ende a FIBHULP-IDIPAZ) en el centro coordinador de dicha red/plataforma.

Como parte del programa estratégico para la coordinación de SCReN que se desarrolla desde la UIC, se propone la interacción y colaboración de SCReN con otras estructuras, organizaciones e instituciones nacionales e internacionales en el ámbito de la investigación clínica académica e independiente, mediante el desarrollo conjunto de proyectos y propuestas específicas que facilitan la comunicación, la organización y la sinergias y que devienen en la generación de capacidades e infraestructura a corto, medio y largo plazo. En este marco de actuación se sitúa AMRI Synergy, un proyecto nacional financiado desde la Agencia Estatal de Investigación (en adelante, AEI), referencia REDES2024-154441 E, que pretende facilitar la coordinación y organización de los nodos nacionales de tres de las infraestructuras europeas en salud, BBMRI-ERIC, EATRIS-ERIC y ECRIN-ERIC (siendo SCReN el nodo nacional en este caso) a la hora de abordar proyectos internacionales que puedan requerir servicios multi-infraestructura.

La magnitud y complejidad de este tipo de proyectos hacen necesaria la búsqueda de herramientas y procesos que simplifiquen la solicitud y la gestión de las necesidades y reduzcan la carga administrativa en los flujos de iteración y comunicación entre los usuarios solicitantes (investigadores) y los destinatarios (administradores en los nodos).

El objeto del presente pliego es la contratación de un servicio que incluya el diseño, el desarrollo, la implementación y el soporte operativo (incluyendo evolutivo) de una herramienta tecnológica capaz de responder al objetivo y las necesidades del proyecto AMRI-Synergy, REDES2024-154441 E, personalizada, autónoma y con proyección para los próximos años. Dicha herramienta tecnológica debe constituirse en un entorno seguro y adecuado para habilitar una ventanilla única que posibilite 1) la solicitud de los servicios ofrecidos desde los nodos nacionales de BBMRI-ERIC, EATRIS-ERIC y ECRIN-ERIC en proyectos multi-infraestructura y 2) la gestión eficiente de toda solicitud que se realice a través de la herramienta, garantizando una óptima comunicación para que los actores involucrados puedan compartir la información adecuada en cada caso.

En este pliego se establecerán, por tanto, las condiciones por las cuales se ha de regir la ejecución de los procesos de diseño, desarrollo, implementación y soporte operativo de la herramienta tecnológica, comprendiendo las siguientes actividades:

- Análisis y toma de requisitos con el personal del equipo AMRI Synergy designado para el proyecto.
- Diseño funcional de la solución/ herramienta, que debe incluir 1) un catálogo de servicios vinculables a cada solicitud y 2) un sistema de gestión de roles y accesos que garantice un entorno controlado y seguro de cara a establecer los flujos para la trazabilidad y comunicación efectiva entre el usuario (investigador) y los destinatarios quienes actúan como proveedores de los distintos servicios (nodos).
- Desarrollo *ad hoc* e implementación de la herramienta que durante el primer año se alojará de acuerdo con el registro del dominio y el alojamiento web proporcionado por la empresa adjudicataria. A partir del segundo año, se explorarán las opciones de continuidad, pudiendo valorarse la migración de la infraestructura tecnológica a los servidores de la entidad.
- Generación de informes sencillos sobre la iteración de la solicitud.
- Elaboración de un plan de pruebas para validar que los requisitos son desarrollados correctamente. El plan incluirá pruebas de control de calidad, funcionalidad, usabilidad, compatibilidad con navegadores y dispositivos.

- Validación del desarrollo ajustándose a los requisitos iniciales y al plan de pruebas elaborado previamente.
- Formación para la adecuada administración de la solución/ herramienta.
- Soporte operativo para ejecutar las pruebas, extraer los resultados y realizar los reajustes necesarios y que se proporcionará a lo largo del período de prueba (acompañamiento en la puesta en marcha y soporte inicial durante las primeras semanas) y posteriormente, durante el período de ejecución del contrato.
- Mantenimiento evolutivo durante las primeras semanas, incluyendo una bolsa de horas para la revisión del funcionamiento y los reajustes que puedan precisarse durante el desarrollo y tras la implementación, dando soporte a las dudas y consultas del personal del equipo de proyecto designado como mediador. Dicho mantenimiento incluirá cualquier coste que pudiera derivarse del normal funcionamiento del sistema.
- Entrega de los manuales de uso y el código de la solución/ herramienta.

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 DEL CONTRATO:

- **Duración del contrato:** desde la formalización del contrato por ambas partes y hasta el 30 de abril de 2027.
- **Plazo de ejecución:** el adjudicatario deberá cumplir con los plazos de ejecución establecidos en el Pliego de Prescripciones Técnicas.
- **Procede la prórroga del contrato:** SI. En caso de aprobación de la prórroga del Proyecto de referencia, el contrato podrá ser prorrogado hasta el 30 de abril de 2028.

2. ESPECIFICACIONES TÉCNICAS

PARTE I. REQUISITOS FUNCIONALES

1. DESCRIPCIÓN DE LOS SERVICIOS

Los trabajos a realizar por el adjudicatario quedarán divididos en las siguientes áreas de actividad diferenciada.

1.1 Análisis y toma de requisitos con el personal del equipo AMRI Synergy designado para el proyecto.

Se plantean las siguientes acciones:

- a) Toma de requisitos del objeto, alcance, planificación y requerimientos.
- b) Propuesta de una metodología de trabajo y cronograma.
- c) Estimación de los recursos que son necesarios para dar cabida al proyecto,
- d) Identificación inicial de los riesgos potenciales y propuestas de medidas de mitigación.

1.2 Diseño funcional de la plataforma Arquitectura web

El diseño de la solución/ herramienta debe ser el de una plataforma de base modular y altamente escalable.

La intranet se desarrollará sobre una arquitectura moderna, modular y escalable, concebida para crecer con el proyecto y que sea flexible para posibilitar la expansión progresiva del sistema, Cada funcionalidad se implementará como un módulo independiente, para permitir, desactivar o ampliar capacidades sin necesidad de rediseñar la estructura base, garantizando que cualquier actualización pueda integrarse de manera sencilla y eficiente, sin comprometer la estructura original y evitando procesos adicionales con impacto en tiempos y costes.

Alcance

La intranet debe contemplar:

- 1) **Un mecanismo RBAC de gestión de usuarios, roles y accesos**, basado en un sistema completo de registro y autenticación con soporte para múltiples roles. Este sistema soporta múltiples perfiles y, en función de ellos, habilitará conjuntos de permisos específicos que determinen el acceso a los módulos y al contenido de la solución/ herramienta. Se establecerán, como mínimo, los siguientes roles:
 - a. **Investigador.** Usuario autenticado con permiso para ejecutar operaciones básicas: navegación, generación de solicitudes de servicio, recepción de informes sobre el estado de la solicitud.
 - b. **Coordinador de nodo nacional,** Contiene los permisos del nivel investigador y además, recibe las solicitudes de servicios que involucran a su nodo y decide la iteración de la solicitud para su respuesta, delegando a los correspondientes miembros del equipo en las unidades.
 - c. **Miembro de equipo.** Contiene los permisos del nivel investigador y ofrece respuesta sobre el servicio solicitado. Actualización del informe de solicitud.
 - d. **Administrador.** Control total. El rol/ perfil de administrador podrá crear, editar y desactivar cuentas, así como modificar los permisos de cada usuario de forma individual.

- 2) **Un módulo donde se publique el catálogo de servicios disponibles** dentro de la red del proyecto y ofertados desde los nodos que la integran. El catálogo es dinámico, editable y podrá mantenerse actualizado mediante la incorporación de un sistema de importación de datos, que permitirá incorporar o modificar servicios de forma masiva sin necesidad de edición manual registro a registro (opción también incluida).
- 3) **Un sistema de solicitud de los servicios vinculado al catálogo que incluya las plantillas o los formularios estándar para realizar cada petición y un gestor del flujo de la misma.** Los usuarios pueden realizar solicitudes a través de formularios estructurados y el sistema gestiona el ciclo de vida completo de cada solicitud: creación, asignación, seguimiento de estados y cierre. Se incluirán los siguientes descriptores del estado:
 - a. pendiente: La solicitud se ha completado y ha sido enviada,
 - b. en trámite. La solicitud se ha recibido por todos los nodos involucrados (según selección de servicios del catálogo), pero la revisión no se ha completado y no se ha confirmado como resuelta por los responsables de la revisión.
 - c. resuelta. La solicitud tiene respuesta de todos los nodos involucrados (según solución de servicios del catálogo) y se confirma como resuelta por todos los responsables.

Los responsables reciben notificaciones automáticas en cada actualización del estado.

- 4) **Un registro de toda la actividad generada, accesible para los administradores y que garantice el seguimiento y la trazabilidad.** La plataforma mantendrá un registro completo de la actividad de los usuarios, incluyendo, sin limitarse a solicitudes realizadas, cambios de estado, accesos, modificaciones de contenido y cualquier otra acción relevante. Los administradores podrán consultar este historial en todo momento, mediante filtros por usuario, fecha y tipo de acción, para tener una visión clara y auditable de todo lo que ocurre en la plataforma.
- 5) **Un sistema de generación automática de PDF e informes, con opciones de plantillas personalizadas y de programación para el envío de la información.**

El sistema permitirá generar documentos PDF a partir de las fichas de solicitud, informes de actividad y resúmenes de datos. Los administradores pueden configurar las plantillas de informe y programar envíos periódicos automáticos a los responsables del proyecto.

Aspectos técnicos

Para garantizar su adecuación y funcionalidad, la plataforma debe cumplir con los siguientes requisitos técnicos:

- Diseño adaptativo para garantizar la accesibilidad e interoperabilidad desde distintos tipos de dispositivos: ordenadores de escritorio, tabletas, dispositivos móviles. Se aplicarán técnicas de Adaptive Design que se adapten al contexto de uso.
- Programación de acuerdo con los estándares web recomendados W3C: Desarrollo del Frontend y maquetación: HTML 5, CSS 3, JavaScript (ECMA). Todos los estándares serán validados al final del proyecto sin errores.
- Tecnologías de servidor con un Backend basado en PHP moderno, MySQL para base de datos y Apache para servidor web.

- Interoperable en y compatible con distintos tipos de navegadores: Chrome, Firefox, Edge, Android, IOS, Safari, Opera.
- Estándares de accesibilidad WCAG 2.1 AA. Además, se incluirán contraste adecuado de colores y navegación accesible para lectores de pantalla.
- Optimización de rendimiento para garantizar una carga más rápida y un funcionamiento fluido, mediante la aplicación de buenas prácticas de Web.
- Performance compresión de archivos, caché avanzado, reducción de llamadas al servidor, optimización de imágenes.
- Entorno web seguro, con implementación de protecciones contra ataques comunes y uso de certificados SSL/TLS para encriptación en tránsito.

1.3 Integración y testing

Incluye las siguientes actividades:

Elaboración del plan de pruebas

Se elaborará un plan de pruebas para validar que los requisitos son desarrollados correctamente. El plan incluirá: pruebas de control de calidad, funcionalidad, usabilidad, compatibilidad con navegadores y dispositivos. Se incluye, diseño de la solución tecnológica para adaptativo, perfecto, correctivo y evolutivo.

Teniendo en cuenta que existirán múltiples grupos de usuarios y roles diferenciados, el sistema debe poder delegar ciertas tareas de gestión, permitiendo administrar los niveles de permisos de los diferentes grupos y roles. Se deberá proporcionar, a todos aquellos miembros del equipo de proyecto que sean delegados como administradores, de un acceso total al sistema con una cuenta de administración equiparable a nivel de permisos que las de los desarrolladores de la empresa adjudicataria.

Actividades de Desarrollo

Las actividades del adjudicatario durante las fases de desarrollo de la solución deben encaminarse a garantizar la cobertura funcional, especificaciones técnicas y niveles de calidad, así como, maximizar el carácter estándar de la solución final, con la finalidad de hacerlo fácilmente sostenible.

También se ocupará de aplicar todos los parches de seguridad disponibles, para evitar posibles intentos de acceso no autorizado.

Actividades de Calidad del Software

- a) Implantación en entorno de test o preproducción
- b) Preparación y soporte al acceso de un entorno de test o preproducción, donde se realice el primer test con los usuarios finales de los sistemas.
- c) Se llevarán a cabo las Pruebas de Aceptación en este entorno.

1.4 Formación y puesta en marcha GO LIVE

- a) Implantación en producción y puesta en marcha del sistema.
- b) Formación a los administradores del sistema
- c) Pruebas de Aceptación Finales en este entorno y evolutivo.

2. ENTREGABLES

Se indican los entregables que deberán considerarse con relación a las actividades incluidas en el servicio.

2.1 Análisis y definición de requisitos

Documento detallado con los requisitos funcionales, técnicos y de negocio del proyecto, validado conjuntamente con el equipo del cliente.

2.2 Diseño funcional de la plataforma

Diseño UX/UL: Wireframes y Diseño Visual

Proceso unificado que abarca desde los wireframes de baja fidelidad hasta el diseño visual definitivo. Se incluirán diagramas de navegación, especificación de flujos de procesos y el diseño gráfico profesional alineado con la identidad corporativa de la Plataforma ISCIII SCReN, con definición de paleta decolores, tipografía y guías de estilo.

Frontend (Maquetación HTML/CSS/JS)

Plantillas HTML responsivas, hoja de estilos CSS, y componentes JavaScript interactivos, todos validados con estándares web.

Backend y Base de Datos

Programación completa del servidor, APIs REST, lógica de negocio, y modelo de base de datos.

2.3 Integración y testing

Tests exhaustivos de control de calidad, funcionalidad, usabilidad, compatibilidad con navegadores y dispositivos.

El adjudicatario deberá entregar obligatoriamente un informe/auditoría de validación de accesibilidad y código antes de la puesta en marcha.

2.4 Formación y puesta en marcha (GO LIVE)

Formación

Sesiones de formación para los administradores de la intranet, orientadas a la gestión de usuarios, contenidos y configuración de los módulos principales.

Puesta en marcha (GO LIVE)

Seguimiento completo durante la puesta en producción y soporte inicial durante las primeras semanas.

3. PLANIFICACIÓN

Se deberá establecer una planificación del proyecto por fases, con relación a las actividades incluidas en el servicio y los entregables que se definan para el proyecto.

3.1 Fase 1: Análisis y Diseño

Reuniones de clarificación de requisitos, análisis detallado, wireframes y diseño visual inicial.

3.2 Fase 2: Desarrollo del Backend

Programación del servidor, base de datos, APIs, sistemas de autenticación y lógica de negocio.

3.3 Fase 3: Desarrollo del Frontend

Maquetación HTML/CSS, componentes JavaScript, integración con backend.

3.4 Fase 4: Testing y Optimización

Tests de funcionalidad, compatibilidad, seguridad, optimización de rendimiento, fixes de bugs.

3.5 Fase 5: Formación y Puesta en marcha

Formación a los administradores, go-live y soporte inicial. PARTE II. REQUISITOS NO FUNCIONALES

4. SEGUIMIENTO DEL CONTRATO.

Una vez adjudicado el contrato será obligación de la empresa adjudicataria informar a este órgano quien será la persona que asumirá el rol de coordinador técnico o responsable del contrato por parte de la empresa. Con el objeto de garantizar la correcta ejecución del contrato se establecerá un comité de proyecto constituido por el responsable del contrato por parte de la FIBHULP, el coordinador técnico o responsable del contrato de la empresa, y todo el personal que por sus perfiles técnicos o funcionales se estimen necesarios para la correcta ejecución de los trabajos.

5. REUNIÓN DE LANZAMIENTO DEL PROYECTO DE DESARROLLO

Una vez adjudicado el contrato la empresa adjudicataria presentará en esta reunión de lanzamiento cuya fecha será fijada por la FIBHULP la siguiente documentación:

- Plan detallado de actividades del proyecto. Dicho plan deberá ser un desarrollo pormenorizado del plan presentando en la oferta. Se deberán indicar los hitos del proyecto, todos los entregables que se deben suministrar (tanto documentación como código) y los recursos empleados por parte de la empresa. Los equipos técnicos de la FIBHULP y la empresa adjudicataria revisarán el plan presentado y en caso de detectar cambios significativos respecto a la información suministrada inicialmente durante el proceso de contratación, las conclusiones del análisis serán sometidas a consideración a fin de revisar, analizar y alcanzar una solución técnica de común acuerdo entre las partes. En caso de discrepancias prevalecerán los criterios de la FIBHULP.
- Política de Seguridad. En los términos indicados en el apartado Documento de Seguridad.
- Documento de Seguridad. Este documento debe de contener la información requerida en el apartado Personas usuarias de sistemas de información en la parte adjudicataria.
- Documentación del plan de calidad. Dicho plan deberá ser un desarrollo pormenorizado del plan presentando en la oferta. La FIBHULP podrá solicitar tantas modificaciones como considere de forma que se ajuste a los requisitos de estándares de calidad de este organismo.

6. REUNIONES DE SEGUIMIENTO

Se establecerá un calendario adecuado para el seguimiento de las actividades del proyecto AMRI Synergy incluidas en el servicio, teniendo lugar como mínimo de forma mensual, desde la fecha de firma del contrato hasta la finalización del mismo. Dichas reuniones seguirán el procedimiento establecido por la FIBHULP.

7. METODOLOGÍA DEL TRABAJO

Se aplicará la metodología de trabajo definida por equipo del proyecto AMRI Synergy y se hará un seguimiento de tareas por parte de la FIBHULP. La documentación relativa a la planificación, desarrollo, implementación y soporte operativo del proyecto será realizada por el adjudicatario.

8. GESTIÓN DE LA SEGURIDAD EN LA PRESTACIÓN DEL SERVICIO

El adjudicatario deberá cumplir la normativa legal aplicable en materia de seguridad en el marco de los servicios prestados. Con carácter general deberá prestarse especial atención al cumplimiento de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, el Reglamento General de Protección de Datos (UE) 2016/679, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. Respecto a la gestión, administración y operación de los sistemas de información y de los datos a que se tenga acceso, en el marco de los trabajos del presente contrato, se deberán cumplir los requisitos de seguridad recogidos en este clausulado en todas las infraestructuras, servicios y sistemas del adjudicatario que den servicio a la FIBHULP. El adjudicatario estará obligado a la realización y al mantenimiento de los registros de evidencias del cumplimiento, durante al menos todo el periodo de ejecución del contrato, de las actividades relacionadas a continuación:

- a) Definir, implementar y mantener una política de seguridad de la información coherente y con el mismo nivel de exigencia, al menos, que la de la FIBHULP.
- b) Implementar, según corresponda, los análisis, ingeniería y salvaguardas de seguridad con objeto de proteger los datos, infraestructuras, servicios y sistemas de información, mediante la ejecución de los controles que den respuesta a los requisitos especificados en este clausulado; todo ello integrado en una gestión de análisis y gestión del riesgo.
- c) Extender lo especificado en el punto anterior a los posibles contratos o relaciones con terceros vinculados a sistemas de información, productos y servicios que estén relacionados con la prestación del servicio objeto del contrato.
- d) En la fase de diseño funcional de los desarrollos que puedan ser objeto del contrato se realizará un estudio previo de su naturaleza y las medidas de seguridad que requieran de conformidad con la naturaleza de la información y el servicio que soportan y los requisitos de la distinta normativa que les aplique. Esta especificación de requisitos de seguridad se documentará conforme a lo establecido en los estándares al respecto de la materia.

A continuación, se establecen las condiciones y medidas en materia de seguridad que el adjudicatario deberá implantar y mantener para la prestación del servicio. Estas

condiciones y medidas se considerarán como de obligado cumplimiento y con carácter de mínimos, teniendo en cuenta que el adjudicatario podrá implantar adicionalmente otros que considere adecuados o necesarios a lo largo de la ejecución del contrato. En todo caso, se estará a lo dispuesto en los estándares de seguridad de la FIBHULP. Asimismo, la FIBHULP podrá modificar esta relación de requisitos mínimos en el marco de los mecanismos que se fijen con el adjudicatario para gestionar cambios en el alcance y las condiciones del servicio prestado, comunicando dicha variación al adjudicatario, quién estará obligado a adecuar sus sistemas a la modificación.

i. Documentación de seguridad El adjudicatario deberá entregar los siguientes documentos, que deberán estar permanentemente actualizados y a disposición de la FIBHULP en cualquier momento de la ejecución del contrato:

- **Política de Seguridad.** Documento de alto nivel basado en la Política de Seguridad de la Información de la FIBHULP que defina lo que significa la “Seguridad de la Información” en la organización, y aplicable al servicio prestado. El documento deberá estar accesible por todos los miembros de la organización que intervengan en la prestación del servicio y redactado de forma sencilla, precisa y comprensible.
- **Documento de Seguridad,** coherente con los documentos de seguridad y de normativa que exige el RGPD 671/2016 y 3/2010 respectivamente, en lo que corresponda a cada uno, donde se encuentre la normativa de seguridad que recoja todas las medidas de seguridad propuestas, la forma de su cumplimiento y las responsabilidades asociadas, con indicación expresa de la identidad del Responsable de Seguridad del Servicio (en la parte adjudicataria).

ii. Personas usuarias de sistemas de información en la parte adjudicataria. Las personas usuarias de los sistemas de información relacionados con el objeto del servicio deberán 1) haber firmado la cláusula compromiso de cumplimiento, secreto y confidencialidad, que se entregará al inicio del proyecto y 2) estar identificadas y autorizadas por el adjudicatario antes de efectuar cualquier uso de los sistemas mediante el correspondiente procedimiento que incluya los procesos de identificación, autenticación y autorización. Se tendrán en cuenta para el Documento de Seguridad.

- **Correspondencia y relación de los perfiles y las funciones asociadas al servicio prestado** para la FIBHULP, así como las personas asociadas a dichos perfiles que pudieran tener acceso a información de la entidad, y el tipo de información a la que pudieran tener acceso, ya sea datos de carácter personal, de administración electrónica u otro tipo.
- **La relación de usuarios con privilegios de administración de los sistemas de información de la FIBHULP** (asociados a posibles tareas habituales o puntuales de mantenimiento, explotación de sistemas o cualquier otra que pudiera implicar el acceso a datos del entorno de producción de los sistemas de información de la entidad), si se diera la circunstancia.
- **El registro de la acreditación del conocimiento y compromiso de la cláusula de seguridad de este pliego por parte de todos los usuarios**, así como la renuncia expresa de los derechos de propiedad intelectual que les

podrían corresponder. Las obligaciones subsistirán aún después de finalizar la relación contractual. El contratista se compromete a formar e informar a su personal en las obligaciones que se derivan de estas cláusulas y de la normativa que se menciona, para lo cual programará las acciones formativas necesarias. Las relaciones de usuarios mencionadas deberán estar permanentemente actualizadas durante la prestación del servicio.

iii. Medidas de seguridad y compromisos del adjudicatario en materia de seguridad de los servicios de administración electrónica. El adjudicatario asumirá el cumplimiento de lo establecido en el Esquema Nacional de Seguridad (Real Decreto 3/2010, de 8 enero - ENS) en lo referido a la adopción de medidas de seguridad de los servicios prestados. Para lo cual, deberá cumplir con lo establecido en la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, 13 por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad siendo el sistema objeto del contrato de categoría Alta en las siguientes dimensiones Disponibilidad=M, Integridad=M, Confidencialidad = A, Autenticidad = M y Trazabilidad = M. El adjudicatario deberá observar los estándares que se deriven de la normativa de seguridad de la información de la FIBHULP. Entre ellos, pero sin descartar el resto contemplado en la citada normativa, estarán los siguientes:

- El adjudicatario deberá realizar las acciones necesarias para concienciar regularmente al personal interviniente en la prestación del servicio acerca de su papel y responsabilidad para que la seguridad del sistema y de los servicios prestados alcance los niveles exigidos.
- Se formará regularmente al personal interviniente en la prestación del servicio en aquellas materias que requieran para el desempeño de sus funciones, en cuanto al servicio prestado.
- Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos en el ENS, se aplicarán las medidas de seguridad indicadas en su Anexo II, ya sean pertenecientes al marco organizativo, operacional o de protección.
- El Documento de Seguridad del adjudicatario reflejará, además de lo estipulado con carácter general, la relación de las medidas de seguridad y la forma en la que se procederá al cumplimiento en materia de seguridad en los sistemas de información de administración electrónica en el transcurso del desarrollo de los trabajos.

iv Medidas de seguridad y compromisos del adjudicatario en el caso de acceso remoto a infraestructuras de la FIBHULP. La información asociada a los accesos a infraestructuras de producción de la FIBHULP que alberguen datos o información bajo responsabilidad de esta entidad durante el periodo de ejecución de los servicios y del periodo de garantía de los mismos deberá estar a disposición de la FIBHULP, y contemplará las acciones de realizadas por cada usuario, el motivo, la solicitud y autorización de la FIBHULP, el mecanismo utilizado, así como todos los datos referidos a los dispositivos y mecanismos utilizados. Además, se deberán cumplir las siguientes medidas de seguridad:

- No se habilitarán ni utilizarán las funciones de las aplicaciones o sistemas operativos que permitan guardar o recordar las credenciales de acceso de forma automática.
 - Las infraestructuras del adjudicatario que se utilicen para dar cumplimiento al objeto del contrato y que deban acceder a la red corporativa de la FIBHULP deberán estar aisladas lógicamente y físicamente, de forma que dichas infraestructuras se utilicen de forma exclusiva para la prestación de los servicios, debiéndose asegurar que no existen conexiones directas entre cualquier otra red distinta de la habilitada para la prestación del servicio y cualquier red de la FIBHULP a la que se acceda en virtud del contrato, ya sea una red pública (ej. Internet) o privada, exceptuándose las conexiones autorizadas requeridas para la prestación del servicio.
 - Entre cada red, subred o servicio de comunicaciones se implantarán cortafuegos (firewalls), que deberán estar configurados con la política del menor privilegio, bloqueando o denegando cualquier tipo de tráfico no autorizado o innecesario para la prestación del servicio. De la misma forma se permitirán únicamente los puertos, protocolos o servicios autorizados por la FIBHULP. Cualquier puerto, protocolo o servicio no especificado como autorizado se denegará por defecto. Los accesos a Internet se efectuarán obligatoriamente a través de proxies con sistema de identificación de su uso o mediante algún mecanismo que permita llevar una trazabilidad de dichos accesos.
 - El uso del correo electrónico deberá contar con filtro antivirus debidamente actualizado periódicamente.
 - No se compartirán las cuentas de correo asignadas de forma personal, ni se podrá desviar de forma automática el correo electrónico profesional a cuentas particulares. El adjudicatario deberá tener definido un Plan de Contingencia que ofrezca respuesta a emergencias, operaciones de respaldo y restauración y otras eventualidades, que, al menos, garantice la correcta operación y entrega de los servicios según los niveles de servicio especificados en el apartado correspondiente. Se implementarán salvaguardas para detectar o minimizar la modificación o destrucción no autorizada de datos. Se mantendrá y ejecutará una política de respaldo automático de datos, verificación y restauración (en su caso).
 - La información que deba suprimirse deberá destruirse de tal forma que sea imposible su recuperación.
 - Se incluirá un sistema de protección antivirus, actualizado periódicamente y de forma automática, y que deberá utilizarse sobre cualquier fichero, soporte y software antes de que cualquiera de éstos resida o se instale en los sistemas de información. La frecuencia de actualización será como mínimo semanal.
- v Restricciones generales. En el marco de la ejecución del contrato, y respecto a la información y a los sistemas de información, las siguientes actividades están específicamente prohibidas:
- Acceder a dependencias o hacer uso de equipamiento de la FIBHULP (teléfono, ordenadores, impresoras, dispositivos de digitalización, material fungible, etc.) de cualquier naturaleza cuando no se disponga de autorización expresa para ello.

- El personal del adjudicatario tendrá terminantemente prohibido el acceso a cualquier información o documentación de la FIBHULP, en especial, los datos de carácter personal sin la autorización expresa de ésta para ello.
- La utilización de los sistemas de información para la realización de actividades ilícitas o no autorizadas, como la comunicación, distribución o cesión de datos, medios u otros contenidos a los que se tenga acceso en virtud de la ejecución de los trabajos y, especialmente, los que estén protegidos por disposiciones de carácter legislativo o normativo.
- La instalación no autorizada de software, modificación de la configuración o conexión a redes.
- La modificación no autorizada del sistema de información o del software instalado, el uso del sistema distinto al de su propósito.
- La sobrecarga, prueba, o desactivación de los mecanismos de seguridad y las redes, así como la monitorización de redes o teclados.
- La reubicación física y los cambios de configuración de los sistemas de información o de sus redes de comunicación.
- La instalación de dispositivos o sistemas ajenos al desarrollo del contrato sin autorización previa, tales como dispositivos USB, soportes externos, ordenadores portátiles, puntos de acceso inalámbricos o PDA's.
- La posesión, distribución, cesión, revelación o alteración de cualquier información sin el consentimiento expreso del propietario de la misma.
- Compartir cuentas e identificadores personales (incluyendo contraseñas y PINs) o permitir el uso de mecanismos de acceso, sean locales o remotos a usuarios no autorizados.
- Inutilizar o suprimir cualquier elemento de seguridad o protección o la información que generen.

vi Auditoría de la seguridad y trazabilidad de los servicios

El adjudicatario adquirirá el compromiso de ser auditado por personal autorizado por la FIBHULP en cualquier momento en el desarrollo de los trabajos, con el fin de verificar la seguridad implementada, comprobando que se cumplen las recomendaciones de protección y las medidas de seguridad de la distinta normativa, en función de las condiciones de aplicación en cada caso.

Asimismo, y en el marco de la ejecución de los trabajos, y con el fin de garantizar la seguridad de la información manejada, la FIBHULP se reserva la capacidad de monitorizar la actividad de los sistemas, por lo que se informará a los usuarios de este aspecto.

La auditoría se basará en la existencia de evidencias que permitan sustentar objetivamente el cumplimiento en cuanto a 1) el registro de incidencias, 2) la documentación de los procedimientos, y 3) el examen del personal afectado: conocimiento y praxis de las medidas que le afectan

9. CALIDAD DE LOS TRABAJOS

Durante la ejecución del contrato, el personal de FIBHULP podrá supervisar la correcta ejecución de la prestación, y en su caso, instar al adjudicatario a que adopte las acciones

correctoras necesarias. Para ello, el adjudicatario deberá permitir el acceso a sus instalaciones donde se estén llevando a cabo los trabajos y facilitar la documentación y la realización de cualquier acción dirigida a constatar el grado de avance y/o la calidad en la ejecución de los contratos. FIBHULP, podrá establecer controles de calidad y acciones de aseguramiento de la calidad de la actividad desarrollada en las entregas de desarrollos de software antes de su paso al entorno de producción, conforme a las políticas y estándares definidos y a través de los procedimientos y herramientas implantados. Son objeto de seguimiento de FIBHULP las siguientes tareas con su documentación asociada:

- a) Validación del estilo de codificación (uniforme, claro y ajustado a estándares).
- b) Pruebas unitarias y de regresión automatizadas que permitan validar el correcto funcionamiento de la solución.
- c) Pruebas funcionales automatizadas para verificar que el producto entregado cumple con los requisitos y necesidades establecidos, mediante el uso de herramientas que permitan la grabación y almacenamiento de pruebas de usuario para posteriores pruebas de regresión y para su ejecución y certificación en distintos entornos.
- d) Pruebas de rendimiento para el aseguramiento de que el software cumple con las cargas de trabajo previstas.
- e) Monitorización técnica de aplicaciones, para obtener información del funcionamiento y consumo de recursos de la aplicación en el tiempo y detectar las causas de los errores una vez producidos. Pruebas de seguridad automatizadas, como la explotación de vulnerabilidades típicas de las aplicaciones Web, y verificación de checklists asociadas a la normativa de desarrollo seguro de software basadas en guías de estándares y metodologías Open Source Security Testing Methodology Manual (OSSTMM), Open Web Application Security Project (OWASP), o equivalentes.

10. CONFIDENCIALIDAD

La empresa adjudicataria y el personal encargado de la realización de las tareas guardará secreto profesional sobre todas las informaciones, documentos y asuntos a los que tenga acceso o conocimiento durante la vigencia del contrato, estando obligado a no hacer públicos o enajenar cuantos datos conozcan como consecuencia o con ocasión de su ejecución, incluso después de finalizar el plazo contractual.

Esta obligación no se limita al tiempo de ejecución del correspondiente contrato al que está asociado el proyecto indicado, sino que deberá ser respetada aun después de su cumplimiento o resolución.

Cualquier información, fuese cual fuere su naturaleza (bien técnica, comercial, financiera, operacional o de otro tipo), en cualquier forma o soporte (ya sea verbal, escrita, grabada o de cualquier otro tipo), que pudiera ser facilitada por la FIBHULP o cualquier tercero que tenga relaciones contractuales con la FIBHULP, en relación con el objeto del presente pliego, será considerada como “información confidencial”, incluyéndose en esta categoría aquella información que fuese generada a partir de la información confidencial.

La empresa adjudicataria y el personal encargado de la realización de las tareas (en adelante el Equipo del Proyecto) se obligan a:

Guardar la información confidencial, bien sea escrita, grabada o en cualquier otro soporte, separada de cualquier otra información de la que pudiera disponer el Equipo del Proyecto.

Utilizar o transmitir la información confidencial exclusivamente para los fines del objeto del contrato.

No realizar copia de la información confidencial sin el previo consentimiento escrito de la FIBHULP, excepto aquellas copias que sean necesitadas por el Equipo del Proyecto para su estudio interno.

Restringir el acceso a la información confidencial únicamente a aquellas personas que necesiten conocerla para los fines del objeto del contrato, y asegurarse de que dichas personas conocen las obligaciones que les resultan aplicables en virtud de lo establecido en el presente documento.

No facilitar información confidencial a tercero alguno sin el previo consentimiento escrito de la FIBHULP y asegurarse de que, en caso de haber obtenido dicha autorización, dicho tercero firma un compromiso de confidencialidad en términos equivalentes a los del presente documento.

Cualquier publicidad o información a los medios de comunicación referida a la simple existencia del contrato o su contenido, deberá ser previamente aprobada por escrito por la A.

El Equipo del Proyecto procederá a destruir o a devolver a la FIBHULP toda la información (confidencial o no) a la finalización del objeto del contrato referido, bien sea escrita, grabada o en cualquier otro soporte que se pudiera encontrar recogida.

La empresa contratista formará e informará de estas obligaciones al personal que participe en el desarrollo del contrato, asumiendo, en caso contrario, las responsabilidades que pudieran derivarse por su incumplimiento.

11. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El adjudicatario deberá cumplir todas las medidas aplicables al tratamiento de la información en el Real Decreto 3/2010, de 8 de enero de 2010, sobre 19 el Esquema Nacional de Seguridad, así como el Reglamento General de Protección de Datos (RGPD), de aplicación en el tratamiento de datos personales. El contratista, una vez adjudicado el contrato, tendrá la consideración de encargado del tratamiento de los datos personales a los que tenga acceso con motivo de la prestación del servicio, quedando obligados, responsable y encargado, al cumplimiento de lo dispuesto en la normativa de protección de datos personales. En todo caso, el adjudicatario deberá respetar la normativa vigente en materia de protección de datos quedando obligado a lo establecido en el 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 esos datos. Asimismo, el adjudicatario deberá cumplir explícitamente sobre Gestión de la Seguridad en la Prestación del Servicio y en concreto:

- a) la obligación de mantener la finalidad para la cual se ceden los datos
- b) la obligación de someterse a la normativa nacional y de la Unión europea en materia de protección de datos personales
- c) la obligación de la empresa adjudicataria de presentar una declaración en la que se ponga de manifiesto dónde van a estar ubicados los servidores y desde dónde se van a prestar los servicios asociados a los mismos
- d) La obligación de comunicar cualquier cambio que se produzca, a lo largo de la vida del contrato, de la información facilitada en la declaración a que se refiere la letra c) anterior
- e) La obligación de los licitadores de indicar en su oferta, si tienen previsto subcontratar los servidores o los

servicios asociados a los mismos, el nombre o el perfil empresarial, definido por referencia a las condiciones de solvencia profesional o técnica, de los subcontratistas a los que vaya a encomendar su realización. Las obligaciones indicadas en las letras anteriores tienen el carácter de esenciales a los efectos previstos en la letra f) del artículo 223 del 20 TRLCSP. El contratista asume la total responsabilidad de las obligaciones anteriores en materia de protección de datos personales respecto a la ejecución del contrato que, en su caso, puedan efectuar los subcontratistas. La efectividad de la adjudicación queda condicionada a la presentación de la declaración a la que se refiere la letra c) por parte del adjudicatario. No podrá iniciarse la ejecución del contrato basado en tanto el organismo interesado no constata que la declaración efectuada por el contratista cumple la normativa en materia de protección de datos personales. Con carácter previo al inicio de la ejecución del contrato, la empresa adjudicataria y el organismo interesado deben firmar un modelo de acuerdo/ declaración responsable en el que se indique el tratamiento a efectuar de los datos personales, la identificación de la información afectada, las obligaciones del responsable de los datos, así como la ubicación de los servidores y las prestaciones asociadas al presente contrato basado.

12. PENALIZACIONES

No conformidad en la entrega de documentación

Se considerará como "no conformidad" en la entrega de documentación de proyecto acordada tanto en la reunión de lanzamiento como en las diferentes reuniones, así como informes de actividad, informes de seguimiento del servicio, y cualquier otra información que el adjudicatario entregue a la FIBHULP, los siguientes supuestos:

- a) Cualquier error, errata u omisión en la información entregada a la FIBHULP que suponga una desviación significativa, a criterio del mismo, de la información real respecto de la reflejada en la documentación entregada.
- b) El retraso en la entrega de cualquier documentación requerida por la FIBHULP bajo demanda, transcurridos 2 días naturales desde la fecha límite de entrega de dicha documentación La FIBHULP ejecutará las siguientes penalizaciones, por cada "no conformidad" en la entrega de documentación detectada durante el periodo de evaluación del indicador.

Número de "no conformidades" Penalización

Entre 2 y 5	1%
Entre 6 y 10	2%
Entre 11 y 15	2,5%
Más de 15	— 3%

Esta penalización se podrá acumular a criterio de la FIBHULP a otras penalizaciones no pudiendo superarse el total acumulado el 15% del total del importe del contrato.

No conformidad en el cumplimiento de las acciones acordadas.

Por necesidades del servicio y bajo el alcance del presente contrato, la FIBHULP podrá establecer alguna acción acordada en las reuniones de seguimiento como BAJO PENALIZACIÓN. Dicha categorización se establecerá de forma justificada y con la suficiente antelación, al menos, en la reunión de seguimiento anterior. Dicha acción acordada BAJO PENALIZACIÓN se categorizará a su vez como CRÍTICA y NO CRÍTICA. La FIBHULP aplicará las siguientes penalizaciones sobre el importe de la factura de la fase del proyecto en que se encuentre.

Tiempo de retraso desde la fecha de finalización de la tarea acordada BAJO PENALIZACIÓN CRÍTICA

Penalización

Entre 2 y 7 días 2%

Entre 8 y 15 días 5%

Entre 16 y 20 días 7,5%

Más de 20 días 9%

Tiempo de retraso desde la fecha de finalización de la tarea acordada BAJO PENALIZACIÓN NO CRÍTICA □ Penalización

Entre 2 y 7 días 1%

Entre 8 y 15 días 2%

Entre 16 y 20 días 3%

Más de 20 días 6%

Esta penalización se podrá acumular a criterio de la FIBHULP a otras penalizaciones no pudiendo superarse el total acumulado el 15% del total del importe del contrato.

13. MEDIOS TÉCNICOS

Los medios técnicos utilizados por el adjudicatario seguirán en todo momento la política de seguridad de este FIBHULP. El adjudicatario deberá aportar las infraestructuras informáticas, espacios y medios técnicos necesarios para la prestación del servicio y para poder integrarse en caso necesario en las herramientas y flujos de trabajo de FIBHULP desde la localización desde la que preste sus servicios (hardware, líneas de comunicaciones, dispositivos, herramientas para el servicio con sus correspondientes licencias, entornos de desarrollo, etc.). El adjudicatario equipará a las personas prestadoras del servicio con todos los medios técnicos necesarios para dicha prestación, incluidos los motivados por desplazamientos a los centros correspondientes (vehículos, dietas, portátil, licencias para el entorno de desarrollo, ofimáticas y las necesarias para la elaboración de los entregables, teléfono móvil, etc.)

Madrid, a 14 de agosto 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