

Núm. expediente: [CSE/AH01/1101471032/26/PS](#)

Órgano gestor: Dirección de Sistemas de la Información del Hospital Universitari Vall d'Hebron

**Objeto del contrato:** Servicio auditoría de seguridad de la información y ciberseguridad y el despliegue de infraestructura segura mediante la incorporación de dos nodos en el espacio de datos para el entrenamiento federado en el marco del proyecto VHTeDades del HUVH.

**Tipo:** Servicio

**Procedimiento de adjudicación:** Abierto Simplificado

## PLIEGO DE PRESCRIPCIONES TÉCNICAS

### 1. OBJETO DEL CONTRATO

El presente pliego de prescripciones técnicas contiene la definición de los requerimientos técnicos para la licitación de la realización de una auditoría integral de seguridad de la información y Ciberseguridad del entorno tecnológico del Hospital Universitario Vall d'Hebron, así como el despliegue de infraestructura segura para el entrenamiento federado que permitirá la validar la seguridad de la información del proyecto VHTeDades.

Se incluye dentro del objeto del contrato:

- Licencias necesarias y el soporte anual correspondiente **para la incorporación de los dos nodos en el espacio de datos**
- La instalación, configuración y puesta en marcha de dos nodos en el Espacio de Datos
- La integración de los nodos con el ecosistema tecnológico existente del Proyecto VHTeDades
- Apoyo en el despliegue de un algoritmo de inteligencia artificial para validar el correcto funcionamiento del entorno federado.
- Evaluar el estado actual de la seguridad de la información.
- Identificar vulnerabilidades y riesgos.
- Determinar el grado de cumplimiento normativo.
- Proponer un plan de mejora priorizado y realizable.

### 2. ALCANCE DEL CONTRATO

El alcance del presente contrato comprende el conjunto de actuaciones necesarias para evaluar, definir e implementar el despliegue de infraestructura para el entrenamiento federado y la seguridad de la información:

- Despliegue de infraestructura segura por dos nodos del Espacio de Datos para el entrenamiento federado de forma alineada con los requerimientos de ciberseguridad
- La auditoría de seguridad de la información y ciberseguridad.

## 2.1. La incorporación de dos nodos en el Espacio de Datos VHTeDades

La incorporación de los dos nodos en el Espacio De Datos VHTeDades incluirá, como mínimo las siguientes prestaciones:

- El abastecimiento de las licencias anuales necesarias, con las condiciones de soporte básico suficientes para garantizar el correcto funcionamiento de la solución propuesta que debe permitir validar la seguridad de la información del espacio de datos de extremo a extremo. La instalación, configuración y puesta en marcha de dos nodos, incluyendo todas las tareas técnicas indispensables para que estos nodos queden plenamente operativos dentro del ecosistema del proyecto. Tras la puesta en marcha en la solución, se incluye una bolsa de horas de apoyo de despliegue de 40 horas.
- La incorporación de capacidades avanzadas de análisis y entrenamiento distribuido, que permitan ejecutar procesos de entrenamiento de modelos de inteligencia artificial sin mover los datos de su lugar de origen (entrenamiento federado), garantizando la privacidad, seguridad y protección del dato.
- Los nodos incorporados deben ser totalmente compatibles con lo que se ha desplegado actualmente en el espacio de datos VHTeDades, uTile PET.
- El apoyo necesario para la puesta en marcha de un entorno federado para evaluar las capacidades avanzadas de análisis especificadas en el punto anterior tanto en la entidad que actúa como promotor del espacio de datos y coordinador del entorno federado como los nodos que participan donde los desplegando los nodos clientes. El número de horas incluidas en este soporte es de 60 horas.

## 2.2. Auditoría de seguridad y ciberseguridad

El adjudicatario deberá realizar una auditoría integral que incluya, como mínimo, los siguientes ámbitos:

### 2.2.1 Gobierno y organización

- Modelo organizativo del Hospital
- Modelo de gobierno de la seguridad
- Políticas y procedimientos de seguridad

- Gestión de riesgos
- Gestión de incidentes
- Continuidad de negocio y recuperación de desastres
- Modelo de cumplimiento normativo

### **2.2.2 Sistemas de Tecnologías de la información (IT)**

- Infraestructura local y corporativa
- Redes y segmentación
- Sistemas operativos y servidores
- Sistemas clínicos y corporativos
- Gestión de identidades y accesos
- Monitorización y gestión de eventos
- Gestión de vulnerabilidades
- Seguridad de aplicaciones

### **2.2.3 Equipamiento médico (OT)**

- Identificación y clasificación de activos OT
- Conectividad y dependencias con sistemas IT
- Segmentación IT/OT
- Accesos remotos de proveedores
- Evaluación de riesgos asociados a la seguridad de paciente

La auditoría OT deberá realizarse bajo un enfoque no intrusivo para no afectar a la práctica clínica.

### **2.2.4 Terceros y proveedores**

- Identificación de proveedores críticos
- Evaluación de accesos de terceros
- Análisis de controles contractuales de seguridad
- Evaluación de dependencias externas.

## **3. CARACTERÍSTICAS TÉCNICAS**

### **3.1 La incorporación de dos nodos en el Espacio de Datos VHTeDades**

#### **3.1.1 Requisitos generales de la solución**

La solución tecnológica propuesta deberá garantizar:

- Soberanía del dato, manteniendo su control en origen.

- Interoperabilidad semántica y técnica, conforme a estándares como IDSA, DCAT-AP y HealthDCAT-AP.

- Gobernanza basada en políticas, expresadas mediante ODRL.
- Cumplimiento del marco europeo de uso secundario de datos, incluido el Espacio Europeo de Datos de Salud (EHDS/EEDS).
- Trazabilidad y auditoría completas de los accesos y operaciones.

### 3.1.2 Componentes funcionales de la solución

La solución deberá incluir un conjunto de componentes coordinados que permitan:

- Publicar y descubrir activos de datos y servicios.
- Gestionar identidades y autorizaciones.
- Definir, negociar y ejecutar contratos de datos.
- Orquestar transferencias seguras.
- Habilitar servicios avanzados como entrenamiento federado.

### 3.1.3 Capacidades de entrenamiento federado

La solución deberá incorporar funcionalidades de entrenamiento federado que permitan:

- Entrenar modelos sin mover los datos de su ubicación original.
- Ejecutar entrenamiento local en cada nodo.
- Intercambiar únicamente los parámetros necesarios para la agregación.
- Reducir drásticamente la exposición de datos clínicos.
- Debe ser compatible con la solución actualmente desplegada en VHTeDades.

## 3.2 Auditoría de seguridad y ciberseguridad

### 3.2.1 Auditoría técnica

El adjudicatario deberá realizar auditorías técnicas obligatorias basadas en estándares (NIST, OWASP, CE CVE, CVSS) que incluyan:

#### 3.2.1.1 Análisis de vulnerabilidades

- Escaneo interno y externo
- Identificación de vulnerabilidades en sistemas, redes y servicios.
- Clasificación según cripticidad

#### 3.2.1.2 Test de intrusión (pentest)

El pentest deberá incluir, como mínimo:

- Red interna
- Sistemas expuestos en Internet

- Aplicaciones web
- APIS
- Infraestructura de identidades
- Escenarios de escalada de privilegios Deberán incluirse pruebas manuales y no exclusivamente automatizadas.

#### 3.2.1.3 Auditoría en entorno OT

- Análisis de arquitectura
- Evaluación de segmentación
- Identificación de superficies de ataque
- Técnicas pasivas de análisis

#### 3.2.2 Inventario de activos

El adjudicatario deberá:

- Analizar el inventario IT existente
- Completarlo en caso de carencias
- Elaborar un inventario OT de alto nivel por tipologías.
- Establecer una clasificación de los activos según: o Confidencialidad o Integridad o Disponibilidad o Cripticidad asistencial

#### 3.2.3 Análisis de riesgos

Se realizará un análisis de riesgos basado en

- ISO 31000 • ISO/IEC 27005 que deberá incluir:
- Identificación de amenazas y vulnerabilidades
- Evaluación de impacto (especialmente asistencial)
- Determinación de riesgo inherente y residual
- Controles y salvaguardias
- Priorización de riesgos

#### 3.2.4 Marcos normativos de referencia

La auditoría deberá incluir un análisis de GAPS frente a los siguientes marcos normativos

- Esquema nacional de seguridad (ENS)
- ISO/IE 27001 y 27002
- NIST CSF
- IEC 62443 (por entornos OT)

## 4. METODOLOGÍA

El adjudicatario deberá aplicar una metodología basada en:

- Revisión documental
- Entrevistas con stakeholders
- Talleres de validación
- Análisis técnico

## 5. ENTREGABLES

El adjudicatario final debe presentar como mínimo la siguiente documentación durante el despliegue, en catalán y castellano, y siguiendo el modelo de calidad de soluciones del CTTI que se puede consultar en <https://qualitat.solucions.gencat.cat/>, con el fin de asegurar el correcto funcionamiento y la ejecución adecuada a los casos de uso:

- Toda la documentación que el Hospital considere necesaria durante la ejecución del proyecto
- Toda la documentación necesaria para la memoria y justificación del proyecto ante el órgano responsable de la ayuda.
- Asimismo, será responsabilidad del adjudicatario levantar actas de las reuniones mantenidas durante la ejecución del contrato

En relación con la auditoría, el adjudicatario deberá entregar, como mínimo:

- Documento de definición de alcance
- Documento de análisis de contexto
- Inventario de activos IT
- Inventario de activos OT
- Informe de análisis de riesgos
- Informe de vulnerabilidades
- Informe de pentest
- Informe final de auditoría (ejecutivo y técnico)
- Plan director de Seguridad, deberá incluir:
  - Líneas estratégicas
  - Plan de acciones priorizado
  - Estimación de esfuerzo
  - Plan de ruta temporal

En relación con la incorporación de los dos nodos al Espacio de Datos, el adjudicatario deberá entregar como mínimo:

- Manual de instalación
- Memoria técnica de la incorporación de los nodos
- Evidencia del despliegue y puesta en funcionamiento de los dos nodos
- Documentación de gobernanza y políticas aplicadas incluyendo la trazabilidad y auditoría
- Documentación de manual de usuarios incluyendo lo necesario para la puesta en marcha de una red federada entre el nodo coordinador (HUVH) y los nodos desplegados en el presente pliego.
- Documentación de pruebas e informes de resultados de ejecución de las pruebas.

## 6. VALIDACIÓ

Una vez finalizado el tiempo previsto para el despliegue y funcionamiento de la solución, se realizará una evaluación de la plataforma en términos de rendimiento, integración con todos los componentes, funcionales y unitarias.

Las pruebas a ejecutar deben entregarse con el documento de plan de pruebas siguiendo la metodología del CTTI y el resultado de estas en el informe de resultados de pruebas que será aprobado por el responsable de proyecto por parte del HUVH como una solución válida.

El adjudicatario deberá aportar la documentación necesaria y realizar el traspaso de conocimiento para que el hospital tenga autonomía para ejecutar pruebas de validación de las mitigaciones y correcciones de las vulnerabilidades detectadas.

## 7. FORMACIÓ

El contratista deberá formar el equipo de Sistemas de Información del HUVH y de los centros hospitalarios donde se desplieguen los nodos de conexión al espacio VHTeDades, así como liberar documentación de formación que debe presentarse en diferentes formatos como guías prácticas, vídeos, etc. La formación deberá llevarse a cabo desde el inicio del proyecto, durante el despliegue y al finalizar. La formación debe incluir el traspaso de conocimientos necesarios para la puesta en marcha de la red federada, incluyendo el despliegue de algoritmos de inteligencia artificial en todos los equipos implicados. El equipo de Vall d'Hebron validará que la formación impartida es suficiente para la puesta en marcha y el soporte operativo de la red federada. En caso de que se considere insuficiente, el adjudicatario deberá poner a disposición los medios necesarios para completarla adecuadamente, sin coste adicional para la entidad contratante. La

formación es clave para la correcta ejecución del proyecto y para asumir el soporte por parte de los equipos del HUVH.

## 8. ORGANIZACIÓN DEL PROYECTO

El adjudicatario deberá:

- Designar a un responsable del proyecto
- Definir un plan de proyecto
- Establecer un cronograma y metas
- Proponer un plan de reuniones

## 9. CONDICIONES DE EJECUCIÓN

### Requerimientos de seguridad

La empresa adjudicataria se compromete a tomar todas las medidas técnicas y organizativas a su alcance para garantizar el objetivo de seguridad de la información, que se basa en los tres principios siguientes:

- La **confidencialidad** de la información, asegurando que sólo acceden a ella las personas que han sido autorizadas a hacerlo
- La **integridad de la información**, asegurando que la información y métodos que la procesan son exactos y completos.
- La **disponibilidad** de esta información, asegurando que los usuarios autorizados tienen acceso a estos datos, módulos y aplicaciones cuando lo necesiten.

Asimismo, se compromete a tomar las medidas previstas en la normativa en vigor en materia de seguridad de la información y protección de datos de carácter personal.

El adjudicatario debe cumplir los requisitos establecidos por 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 estos datos (en adelante RGPD)*, por la *Ley Orgánica de datos 3/2018, de 5 de diciembre, de protección de datos personales y de garantía de los derechos digitales (en adelante LOPDGDD)*, y por el *Real Decreto 1720/2007, de 21 de diciembre*, en todo lo que sea de aplicación, y cualquier otra norma relacionada que esté vigente.

### Acceso a datos personales, o de carácter reservado

El adjudicatario tratará los datos personales que acceda como consecuencia de la ejecución de este contrato de conformidad con lo establecido en la normativa vigente en la materia. La



empresa adjudicataria se responsabilizará del uso adecuado de la información que pueda obtenerse con el fin de proteger los datos personales, a lo largo de toda la fase de realización del objeto del contrato y también una vez finalizada sobre la base de las normativas en materia de protección de datos ya mencionadas, así como cualquier otra normativa nacional y de la Unión Europea que sea aplicable.

El incumplimiento de estas obligaciones constituye la infracción tipificada en la LOPDGDD, sin perjuicio de las responsabilidades exigidas ante la jurisdicción ordinaria.

La empresa adjudicataria se compromete a no acceder innecesariamente a aquellos datos a los que tenga acceso por razón de la tarea que tiene encomendada.

Siempre que sea necesario manipular datos se trabajará con datos de pruebas, simuladas o ficticias. Una vez terminado el desarrollo o prueba, se borrarán todos los datos manipulados, tanto si son ficticias como reales.

En caso de que sea necesario acceder a los datos reales, la empresa y sus trabajadores se comprometen a mantener la confidencialidad respecto a la información conocida, a no alterar su contenido y no revelar, comunicar ni poner a disposición de terceros, por ningún medio, escrito, electrónico, verbal o por cualquier otro procedimiento, ninguno de estos datos o parte de ellos o la información que se haya extraído. En este sentido, el adjudicatario formará a sus trabajadores. El adjudicatario asumirá respecto a las finalidades principales que se derivan de esta licitación, el rol de encargado de tratamiento de datos personales en virtud de lo establecido en el artículo 28 del RGPD. En este sentido, será necesaria la firma de un acuerdo de encargado de tratamiento de datos, junto con la firma del contrato.

### **Colaboración en las auditorías periódicas**

La empresa adjudicataria se compromete a facilitar toda la información necesaria para realizar las auditorías periódicas que lleve a cabo el HUVH, así como a aportar sus conocimientos e informaciones con el fin de mejorar los aspectos relacionados con la seguridad y la protección de datos de carácter personal.

Además, no se permitirá impacto en la práctica clínica, todas las actividades tendrán que coordinarse con el hospital y se establecerán ventanas operativas para las diferentes actuaciones que el hospital siempre aprobará.

## **10. REQUISITOS DEL EQUIPO**

Para coordinar las relaciones de trabajo entre el HUVH y el adjudicatario, ambas partes designarán representaciones calificadas técnicamente, las cuales serán los interlocutores

habituales para todas las cuestiones que se susciten en la operativa diaria y resolverán las acciones a realizar y su implementación técnica y administrativa. Específicamente el adjudicatario definirá a un responsable de proyecto y el HUVH definirá a un responsable del contrato.

- Para coordinar las relaciones de trabajo entre HUVH y el Contratista, ambas partes establecen una Comisión de gestión, seguimiento, inspección y control de la prestación del servicio descrito en el presente contrato, que tendrá como principales objetivos de referencia:

- Revisión de los resultados en relación con los niveles de servicio acordados y los objetivos de calidad establecidos.
- Acuerdo y revisión de la conformidad de los requerimientos de protección, confidencialidad y seguridad.
- Acuerdo sobre auditorías periódicas
- Valoración continua de funciones y responsabilidades, áreas de responsabilidad, puntos de interfaz, objetivos del servicio y mejoras de calidad y alcance de la relación contractual.

La Comisión de seguimiento, inspección y control de la prestación del servicio estará formada por un responsable del contrato, por parte del HUVH y por un Director de Proyecto por parte del contratista.

- El Contratista definirá el equipo de trabajo que formará parte del proyecto. El número y características profesionales de los componentes de este equipo será definido por el Contratista, garantizando que será el adecuado para la realización de la prestación. En este aspecto, el HUVH no establece ningún mínimo.

- El HUVH definirá a los interlocutores necesarios para que el Contratista pueda realizar las tareas necesarias.

Además, el equipo deberá disponer de:

- Experiencia en auditorías de seguridad en entornos complejos
- Experiencia en el sector sanitario
- Certificación ISO 27001 Lead Auditor o similar
- Certificaciones de pentest (OSCP, CEH o similares)

## 11. PLAZO DE EJECUCIÓN

El plazo máximo de ejecución es el mercado en las bases de la subvención recibida, a 30 de junio de 2026.

## 12. PRESUPUESTO DE LICITACIÓN

	Preu sense IVA	Preu amb IVA
<b>Total</b>	139.600,00€	168.916,00€

## 13. FACTURACIÓN

Un único pago por importe de 139.600,00 € euros IVA excluido y 168.916,00 € euros IVA incluido.

Barcelona, 27 de abril de 2026

Susanna Aussó Trias

Directora de Sistemas de la Información