

# ANEXO

## Requisitos Técnicos de Ciberseguridad, Interoperabilidad y Conectividad

Dispositivos de Asistencia Implantables (DAIs) y su Ecosistema

El presente Anexo establece los requisitos mínimos de referencia que los licitadores deberán acreditar en su oferta técnica. Los requisitos que aquí se exponen están divididos en dos grupos, los generales de la Dirección General de Salud Digital (en adelante DGSD) y los particulares para este acuerdo marco.

Los requisitos generales son de obligado cumplimiento, y solo la DGSD puede aplicar excepciones siempre que considere que la solución propuesta por el licitador es equivalente y satisfará los objetivos perseguidos. Tanto la solución propuesta como la conformidad de la DGSD deberán quedar documentadas por escrito.

### Requisitos generales de este acuerdo marco.

#### 1. Ciberseguridad y Esquema Nacional de Seguridad (ENS)

Los dispositivos, pasarelas y plataformas que formen parte de la solución deberán alinearse con los principios del Esquema Nacional de Seguridad (ENS), en el nivel que corresponda según la categoría del sistema.

Asimismo, se considera necesario que los proveedores deban estar en condiciones de exhibir la correspondiente Certificación de Conformidad con el Esquema Nacional de Seguridad, aceptándose en su lugar, no obstante, una Declaración de Conformidad con el ENS, únicamente cuando se haya declarado categoría BÁSICA del sistema para el que concurren.

Igualmente, estas condiciones se aplican a los sistemas de información de las entidades del sector privado.

#### 2. Protección de Datos y Privacidad

La solución deberá respetar:

- Reglamento (UE) 2016/679, conocido como Reglamento General de Protección de Datos (RGPD o GDPR)
- Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)

La solución deberá adaptarse a lo dispuesto por la DGSD en cuanto a:

- Definición de roles y responsabilidades, actuando el adjudicatario como encargado del tratamiento.
- Cumplir con los principios de minimización de datos, integridad y confidencialidad.

- Contar con mecanismos adecuados para la obtención y gestión del consentimiento informado cuando sea aplicable.
- Contar con medidas técnicas y organizativas de seguridad aplicadas al tratamiento de datos personales para garantizar un nivel de seguridad adecuado al riesgo.

### **3. Interoperabilidad Técnica y Semántica**

La solución deberá facilitar la interoperabilidad con todas las plataformas indicadas por la DGSD dentro de su ecosistema de aplicaciones corporativas.

La solución deberá poder interoperar mediante los estándares de intercambio de datos sanitarios que determine la DGSD y las normativas de interoperabilidad que estén vigentes en el momento de la licitación. Los estándares y codificaciones mínimos que se requerirán son:

- a) Para el intercambio de información clínica: HL7 v2.x o FHIR R4/R4B.
- b) Para la codificación semántica de observaciones y resultados: LOINC.
- c) Para la codificación de diagnósticos y procedimientos: CIE-10.
- d) Para conceptos y valores: SNOMED CT (edición española).

Independientemente del estándar de intercambio de información clínica que se adopte, el licitador deberá ajustarse a la guía de interoperabilidad vigente publicada por la DGSD en el momento de la licitación, siendo por cuenta del proveedor el desarrollo, implantación y mantenimiento de las integraciones necesarias.

### **Requisitos particulares de este acuerdo marco.**

#### **1. Ciberseguridad y Esquema Nacional de Seguridad (ENS)**

Para esta solución se considerarán:

- Implementación de mecanismos de autenticación mutua y cifrado en las comunicaciones entre dispositivos, pasarelas y plataformas.
- Adopción de configuraciones seguras que eviten el uso de protocolos sin autenticación ni cifrado, especialmente en los canales de telemetría de los DAI's.
- Disponibilidad de documentación técnica que describa la arquitectura de seguridad de la solución ofertada.
- Documentación que acredite la implementación de medidas de seguridad según la categorización del sistema basado en ENS.
- Disponibilidad de documentación de las auditorías de seguridad realizadas en el sistema relacionado.
- Documentación que describa en detalle los roles y tareas relacionadas con los mismos, para valorar los mínimos privilegios necesarios para su correcto desempeño.

#### **2. Ciclo de Vida Seguro del Software y Firmware**

El licitador deberá describir las prácticas de seguridad aplicadas a lo largo del ciclo de vida del software y firmware de la solución. Se valorará que dichas prácticas estén alineadas con guías europeas de referencia y normas aplicables al software electro médico.

Aspectos de referencia que se valorarán:

- Existencia de un proceso documentado de gestión de parches y actualizaciones de seguridad, con plazos orientativos de respuesta ante vulnerabilidades.
- Disponibilidad de una lista de materiales de software (SBOM) o equivalente, que facilite la trazabilidad de componentes.
- Procedimientos de verificación y validación de seguridad integrados en el proceso de desarrollo o integración.

### **3. Interoperabilidad Técnica**

Los datos específicos de DAIs se estructurarán preferentemente conforme al perfil IHE IDCO y la nomenclatura IEEE 11073-10103, o alternativa técnicamente equivalente documentada.

### **4. Conectividad Inalámbrica**

En los casos en que la solución incorpore dispositivos con conectividad inalámbrica (tablets, pasarelas u otros), se deberán cumplir los requisitos aplicables de compatibilidad electromagnética y marcado CE. En particular:

- Los dispositivos BLE que operen en la banda de 2,4 GHz deberán contar con la Declaración CE conforme a la Directiva RED y, cuando aplique, cumplir la norma EN 300 328 v2.2.2.
  - Se aportarán, a requerimiento del contratante, los informes de ensayo de compatibilidad electromagnética (EMC) en entorno sanitario.
  - El licitador indicará si los dispositivos disponen de evaluación de conformidad específica para uso en entornos de atención sanitaria.
-