

Este documento se ha obtenido directamente del original, que contenía todas las firmas auténticas, y se han ocultado los datos personales y los códigos que permitían acceder al original.

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA EL DISEÑO, IMPLEMENTACIÓN, PUESTA EN MARCHA Y DINAMIZACIÓN DE UN CENTRO DEMOSTRADOR PARA EXPERIMENTACIÓN EN CIBERSEGURIDAD DEL SECTOR SALUD, EN EL ÁMBITO DEL PROGRAMA RETECH (Redes Territoriales de Especialización Tecnológica) Y EN EL MARCO DEL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA - FINANCIADO POR LA UNIÓN EUROPEA – NEXT GENERATION EU.

1	INTRODUCCIÓN	2
2	OBJETO DEL CONTRATO.....	4
3	LOTE 1 – IDENTIFICACIÓN DEL ESTADO DE LA CIBERSEGURIDAD, CREACIÓN DE UN CONJUNTO DE CASOS DE USO, DESPLIEGUE DE UN ENTORNO TECNOLÓGICO Y DEFINICIÓN DE UN CATÁLOGO DE SERVICIOS	5
3.1	LOTE 1 ACTUACIÓN 1 ESTADO DE LA CIBERSEGURIDAD Y DEFINICIÓN DE LOS CASOS DE USO 5	
3.1.1	ESTADO DE LA CIBERSEGURIDAD.....	6
3.1.2	CASOS DE USO	8
3.2	LOTE 1 ACTUACIÓN 2 DESPLIEGUE DE UN ENTORNO TECNOLÓGICO.....	10
3.2.1	ACTUACIÓN 2 ETAPA 1. DISEÑO INICIAL.....	11
3.2.1.1	Espacios mínimos disponibles en el Centro Demostrador	11
3.2.1.2	Herramientas de gestión mínimas del Centro Demostrador.....	12
3.2.2	ACTUACIÓN 2 ETAPA 2. DESPLIEGUE, CONFIGURACIÓN Y PUESTA EN MARCHA	16
3.2.3	ACTUACIÓN 2 ETAPA 3. GESTIÓN Y EXPLOTACIÓN	17
3.3	LOTE 1 ACTUACIÓN 3. DEFINICIÓN Y DISEÑO DE UN CATÁLOGO DE SERVICIOS.....	19
3.4	LOTE 1 ACTUACIÓN 4. TRANSFERENCIA DEL SERVICIO	25
3.5	LOTE 1 EQUIPO DE TRABAJO	26
4	LOTE 2 COMUNICACIÓN Y DIFUSIÓN	29
4.1	LOTE 2 ACTIVIDADES	29
4.2	LOTE 2 EQUIPO DE TRABAJO	31
5	CUMPLIMIENTO NORMATIVO DE AMBOS LOTES.....	32
5.1	PRINCIPIO DNSH (ARTÍCULO 5 ORDEN HFP/1030/2021)	32
5.2	ETIQUETADO VERDE Y ETIQUETADO DIGITAL (ARTÍCULO 4 ORDEN HFP/1030/2021)	32
5.3	PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL	33
5.4	SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN	33
5.5	COMUNICACIÓN Y PUBLICIDAD	34

1 INTRODUCCIÓN

De acuerdo con el Decreto 261/2023, de 29 de noviembre, del Consejo de Gobierno, por el que se establece la estructura orgánica de la Consejería de Digitalización, a esta le corresponden, entre otras, las siguientes competencias, incluida la ciberseguridad, en los respectivos ámbitos materiales:

- El fomento y coordinación de la transformación digital de la Comunidad de Madrid, así como de la sociedad de la información y el conocimiento.
- La planificación y dirección de las acciones de impulso de la economía digital de las empresas en la Comunidad de Madrid, sin perjuicio de las competencias de otras consejerías.
- El impulso y apoyo a las empresas, así como el desarrollo de programas para facilitar su transformación digital, en el uso de las tecnologías y en la promoción de la capacitación digital en el tejido empresarial, sin perjuicio de las competencias de otras consejerías.
- La promoción del desarrollo del sector digital en la Comunidad de Madrid, sin perjuicio de las competencias de otras consejerías.
- La promoción y apoyo al desarrollo de la sociedad digital para los ciudadanos.
- La coordinación y ejecución de las políticas de impulso de la sociedad de la información, contribuyendo a la reducción de la brecha digital.
- El apoyo a las Entidades Locales en todo lo referente a la modernización, innovación y proceso de transformación digital, sin perjuicio de las competencias de otros centros directivos, impulsando el desarrollo de los servicios y gobierno digitales, fomentando el uso de plataformas comunes y la reutilización de activos digitales, en colaboración con la consejería competente en materia de Administración Local.

La ciberseguridad aplicada al sector sanitario se ha convertido en una cuestión de la máxima relevancia. El proceso de transformación digital que está experimentando el sector hace que los servicios clínicos y hospitalarios dependan fuertemente de las infraestructuras digitales.

La automatización está alcanzando no solo a los servicios de gestión del paciente y a otros servicios de soporte (logística, contabilidad y finanzas, compras, etc.) si no que afecta también a los equipos clínicos y de laboratorio. Los dispositivos médicos conectados están transformando la forma en que funciona el sector, tanto dentro de los centros sanitarios como entre los diferentes actores de la industria de la salud.

Sin embargo, el aumento de los flujos de información dentro y fuera de los hospitales y las clínicas, conlleva riesgos importantes que necesitan ser abordados.

Algunos de los riesgos comprenden daños a la seguridad del paciente o pérdida de información personal, que pueden ser causados por acciones maliciosas, por errores humanos, del sistema o de terceros, y por fenómenos naturales. A medida que la superficie de ataque aumenta con la introducción de nuevos dispositivos conectados, la probabilidad y el posible impacto de los ataques crece exponencialmente.

Es clave por tanto el impulso a la ciberseguridad en el sector salud, mejorando el posicionamiento y la especialización inteligente de las empresas, incentivando la innovación, la formación y la concienciación con soluciones.

El Programa de Redes Territoriales de Especialización Tecnológica (en adelante RETECH) constituye uno de los nuevos ejes transversales de la Agenda España Digital 2026 y está alineado con dos de las principales metas de la Agenda, como son, liderar la transformación digital de manera inclusiva y sostenible y focalizar los esfuerzos de digitalización en sectores económicos clave. El objetivo del Programa RETECH es impulsar redes territoriales de especialización tecnológica, articulando proyectos regionales que se orienten a la transformación y especialización digital, asegurando la coordinación, la colaboración y la complementariedad.

Los proyectos RETECH Ciber, cofinanciados con presupuesto del Plan de Recuperación, Transformación y Resiliencia del INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA (INCIBE), se instrumentalizan a través de la firma de convenios de colaboración.

Los convenios firmados en el marco del programa RETECH contribuyen a la consecución del Componente 15.17 Ciberseguridad: Fortalecimiento de las capacidades de Ciberseguridad de ciudadanos, pymes y profesionales; impulso del ecosistema del sector. En concreto, RETECH se engloba en la puesta en marcha del Programa de Impulso a la Industria de la Ciberseguridad Nacional y de sus acciones conexas, actuando sobre aspectos claves de la industria como: Impulsar la industria nacional de ciberseguridad para el surgimiento, crecimiento y desarrollo de empresas en este sector; Formar y desarrollar talentos especializados en el campo de la ciberseguridad y fomentar las acciones de internacionalización en el ámbito de la ciberseguridad.

En particular, los convenios vinculados al programa RETECH contribuyen a la consecución de los hitos CID 245 y CID 453 (continuación del CID 245). Además, contribuyen de igual manera al CID 248 cuando finalice el proyecto y se justifique la finalización de la ejecución de las actividades recogidas en cada uno de los convenios:

- **Hito CID 245:** Puesta en marcha del Programa de Impulso a la Industria de la Ciberseguridad Nacional, del Programa Global de Innovación en Seguridad y de las acciones conexas. Descripción: Puesta en marcha del Programa de Impulso a la Industria de la Ciberseguridad Nacional y del Programa Global de Innovación en Seguridad y de otras acciones conexas (con la adjudicación de un presupuesto total de 311 000 000 EUR), que incide en aspectos clave de esta industria, tales como: - el impulso de la industria de ciberseguridad nacional con vistas al surgimiento, el crecimiento y el desarrollo de nuevas empresas en este sector; - el desarrollo de y servicios de elevado valor añadido en el ámbito de la ciberseguridad; - la formación y capacitación de personas con talento especializadas en el ámbito de la ciberseguridad; - las acciones de internacionalización en el ámbito de la ciberseguridad; - la implantación de un centro demostrador para el desarrollo de infraestructura de ciberseguridad y la creación de nuevos servicios de ciberseguridad, incluidos laboratorios de ensayo y simuladores de ciberataques; - el desarrollo de certificaciones para la etiqueta de ciberseguridad.
- **Hito CID 453:** Puesta en marcha del Programa de Impulso a la Industria de la Ciberseguridad Nacional, del Programa Global de Innovación en Seguridad y de las

acciones conexas. Descripción: Continuación del Hito 245 del despliegue del Programa de Impulso a la Industria de la Ciberseguridad Nacional y del Programa Global de Innovación en Seguridad y de otras acciones conexas (con la adjudicación de un presupuesto de 107.000.000 de euros, además de los 311.000.000 de euros del Hito 245, es decir, una adjudicación total de 418.000.000 de euros), que incide en aspectos clave de esta industria, tales como: - el impulso de la industria de ciberseguridad nacional con vistas al surgimiento, el crecimiento y el desarrollo de nuevas empresas en este sector; - el desarrollo de soluciones y servicios de elevado valor añadido en el ámbito de la ciberseguridad; - la formación y capacitación de personas con talento especializadas en el ámbito de la ciberseguridad; - las acciones de internacionalización en el ámbito de la ciberseguridad; - la implantación de un centro demostrador para el desarrollo de infraestructura de ciberseguridad y la creación de nuevos servicios de ciberseguridad, incluidos laboratorios de ensayo y simuladores de ciberataques; - el desarrollo de certificaciones para la etiqueta de ciberseguridad.

- **Hito CID 248:** Finalización de los proyectos del programa de impulso a la industria de la Ciberseguridad nacional, del programa global de innovación en seguridad y de las acciones conexas. Descripción: finalización de los proyectos incluidos en el Programa de Impulso a la Industria de la Ciberseguridad Nacional y el Programa Global de Innovación en Seguridad, y otras acciones conexas en los siguientes ámbitos (adjudicados en el Hito 245 y en el Hito 453): - el impulso de la industria de ciberseguridad nacional con vistas al surgimiento, el crecimiento y el desarrollo de nuevas empresas en este sector; - el desarrollo de soluciones y servicios de elevado valor añadido en el ámbito de la ciberseguridad; - la formación y capacitación de personas con talento especializadas en el ámbito de la ciberseguridad; - las acciones de internacionalización en el ámbito de la ciberseguridad; - la implantación de un centro demostrador para el desarrollo de infraestructura de ciberseguridad y la creación de nuevos servicios de ciberseguridad, incluidos laboratorios de ensayo y simuladores de ciberataques; - el desarrollo de certificaciones para la etiqueta de ciberseguridad.

La Comunidad de Madrid presenta el PROYECTO RESEDA EN EL SECTOR SALUD (en adelante “Proyecto RESEDA”), con temática de Ciberseguridad, y alineado con la Agenda España Digital 2026 y el Plan de Recuperación, Transformación y Resiliencia.

El 29 de mayo de 2024 se firmó el Convenio de colaboración en el ámbito de la convocatoria RETECH entre la Comunidad de Madrid y la S.M.E. INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA M.P., S.A. (INCIBE). La firma de dicho Convenio tiene por objeto desarrollar y ejecutar el PROYECTO RESEDA, por la Comunidad de Madrid e INCIBE, alineándose así con la Agenda España Digital 2026 y contribuyendo a la consecución del Componente 15.I7 del Plan de Recuperación, Transformación y Resiliencia.

2 OBJETO DEL CONTRATO

La presente licitación se encuadra en el marco del Plan de Recuperación, Transformación y Resiliencia (PRTR), contribuyendo a la consecución del Componente C15.I7 Ciberseguridad: Fortalecimiento de las capacidades de Ciberseguridad de ciudadanos, pymes y profesionales; impulso del ecosistema del sector.

De acuerdo con lo establecido en el art. 99.3 de la LCSP, se ha considerado oportuno la división del objeto de licitación en 2 lotes, pudiendo cada empresa licitadora presentarse a uno o a la totalidad de lotes que la conforman.

El objeto del contrato y los lotes que lo conforman son los siguientes:

- **Lote 1 – CENTRO DEMOSTRADOR**

Diseño y puesta en marcha de un centro demostrador de ciberseguridad en el ámbito del sector sanitario. Incluye las siguientes actuaciones:

- El licitador realizará una identificación del estado de la ciberseguridad en la región de la Comunidad de Madrid, con especial foco en el sector salud, desarrollando 15 de casos de uso para abordar los principales retos y problemas relacionados con la protección de la información, los servicios, los equipos y sistemas de Smart Health. La identificación del estado de la ciberseguridad y los casos de uso serán presentados en la oferta para su posterior aprobación por parte de la Dirección General de Estrategia Digital.
- Despliegue de un entorno tecnológico que permita reproducir de la forma más realista y fiel posible, los casos diseñados en la actuación anterior, y aporte las facilidades necesarias para explotar de forma presencial o remota los servicios que se van a ir desplegando en la actuación siguiente:
- Definición y diseño de un catálogo de servicios que aporte valor a todas las partes interesadas, organizaciones sanitarias públicas y privadas, empresas especializadas, emprendedores, profesionales y personas interesadas en adquirir conocimientos para entrar en el mercado profesional de la ciberseguridad.

- **Lote 2 – PLAN DE DIFUSIÓN.**

En paralelo a las actuaciones del Lote 1 se llevarán a cabo acciones de divulgación que permitan poner el proyecto en conocimiento de la ciudadanía, de las empresas y las instituciones.

3 LOTE 1 – IDENTIFICACIÓN DEL ESTADO DE LA CIBERSEGURIDAD, CREACIÓN DE UN CONJUNTO DE CASOS DE USO, DESPLIEGUE DE UN ENTORNO TECNOLÓGICO Y DEFINICIÓN DE UN CATÁLOGO DE SERVICIOS

3.1 LOTE 1 ACTUACIÓN 1 ESTADO DE LA CIBERSEGURIDAD Y DEFINICIÓN DE LOS CASOS DE USO

Identificación del estado de la ciberseguridad en la región de la Comunidad de Madrid, con especial foco en el sector salud, y creación de 15 de casos de uso para abordar los principales retos y problemas relacionados con la protección de la información, los servicios, los equipos y sistemas de Smart Health.

3.1.1 ESTADO DE LA CIBERSEGURIDAD

El adjudicatario procederá a realizar una identificación del estado de la ciberseguridad en la región de la Comunidad de Madrid incluyendo un apartado específico para el sector salud que permita determinar los principales retos y problemas existentes.

Para ello realizará un análisis exhaustivo de los centros de salud, pymes y otros actores relevantes en este sector. Esto implica evaluar las medidas de ciberseguridad existentes, identificar posibles vulnerabilidades y determinar los principales retos y problemas en materia de ciberseguridad. Además, se llevará a cabo la identificación de todos los actores relevantes en el sector de la ciberseguridad en salud, incluyendo empresas, organizaciones gubernamentales, profesionales de la salud y otros actores clave que puedan influir en la seguridad de la información en este ámbito.

Las actividades por realizar en esta actuación, como mínimo, serán las siguientes:

- Realizar un análisis cuantitativo y cualitativo de las características, dimensionamiento, magnitudes económicas, infraestructuras y servicios de la ciberseguridad en el sector en la Comunidad de Madrid.
- Analizar el entorno competitivo del ecosistema de ciberseguridad, así como las tendencias advertidas a nivel global, llevando a cabo una identificación de las ventajas competitivas de las diferentes soluciones.
- En cada solución identificada en los diferentes casos de uso (actuales y futuros), se analizarán los competidores más directos, su propuesta de valor y una comparativa de sus fortalezas y debilidades en el mercado.
- Identificación de ineficiencias en la gestión de la información y alternativas para la unificación de la información.
- Realizar un análisis sintético sobre aspectos del entorno social, económico, político, administrativo, cultural, tecnológico, etc., que pueden influir en el desarrollo del ecosistema ciber en la Comunidad de Madrid.
- Identificación y análisis de todos los agentes relevantes en materia de ciberseguridad en la Comunidad de Madrid (AA.PP., empresas públicas, entidades, consorcios y mancomunidades, patronatos, agrupaciones empresariales, principales empresas, etc.), elaborando una ficha de cada uno de ellos y determinando aspectos tales como conocimiento de cada agente, influencia, nivel de apoyo necesario de cada agente para el cumplimiento de los objetivos del proyecto, etapa del proyecto en la que se verá afectado, canal de comunicación más eficiente, actuaciones que pudieran realizar para reforzar el proyecto, etc.
- Analizar los canales de distribución comercial y promocional con los que operan los agentes del sector.
- Identificación de tendencias actuales en ámbitos geográficos de similar naturaleza, si bien no es excluyente optar por otros ámbitos territoriales (grandes ciudades, nivel autonómico o nacional), teniendo en consideración la oferta, la demanda, la comercialización y la gestión.
- Se realizará un diagnóstico global a nivel Regional, nacional e internacional de las grandes líneas del sector de la ciberseguridad, que se plasmará en los correspondientes análisis DAFO (Debilidades, Amenazas, Fortalezas y Oportunidades) y subsiguiente

análisis CAME (Corregir, Afrontar, Mantener y Explotar). Igualmente, y a los dos niveles descritos, se hará una primera valoración de los principales productos y servicios del sector, confrontando de forma matricial su nivel de interés y su nivel de competitividad. Por último, se efectuará un análisis de la situación actual de las áreas de interés identificadas y los productos enmarcados en éstas, estructurados del siguiente modo:

- Oferta de equipamientos y servicios en ciberseguridad.
- Accesibilidad y las infraestructuras existentes o previstas.
- Recursos de atracción de talento en ciberseguridad y su singularidad.
- Grado de concienciación en el sector, incluyendo las empresas y/o marcas más conocidas.
- Capacidad de organización actual o potencial.
- Definición de los principios que deben tenerse en cuenta en la definición de un modelo integral de ciberseguridad en el territorio. A través de un modelo colaborativo que comprenda organizaciones que formen parte de la demanda (hospitales, clínicas, laboratorios, tanto públicos como privados), oferentes de tecnología (gran, mediana y pequeña empresa de ciberseguridad), universidades y centros de investigación aplicada.
- Definición del modelo objetivo de mejora del ecosistema de la ciberseguridad en la Comunidad de Madrid basado en la tecnología, conforme a los resultados del diagnóstico. Este modelo deberá contar con:
 - Definición de los atributos necesarios para impulsar el sector de la ciberseguridad en la Comunidad de Madrid.
 - Definir y proponer las tecnológicas, casos de uso, modelos, prototipados necesarios para impulsar nuevos modelos de negocio, que permitan agregar valor y posicionamiento competitivo del sector y por consiguiente, de las empresas participantes:
 - Definición a alto nivel de las tecnológicas identificadas.
 - Sistemas de calidad a aplicar en el marco del proyecto.
 - Nuevos Modelos de comercialización.
 - Mecanismos de transferencia de capacidades y conocimiento que permita el correcto desarrollo de modelos de gestión adaptados a cada caso de uso
 - Definir los elementos aceleradores del ecosistema de ciberseguridad en la Comunidad de Madrid, que permitan una mejor comercialización, una imagen integrada y con ello un mejor posicionamiento del sector.
- Definición del modelo de relación de las empresas con el centro demostrador para la mejora de los servicios de ciberseguridad de las empresas, definiendo las herramientas y procedimientos necesarios para instrumentalizar la colaboración.
- Definición de los mecanismos de intercambio de información
- Realizar una propuesta de actuaciones concretas que cumplan las siguientes características:
 - Acciones alineadas con los productos identificados como prioritarios en la fase de Diagnóstico.
 - Iniciativas que se consideren como actividades complementarias necesarias o aconsejables para el fortalecimiento o mejor desarrollo de determinadas

actuaciones concretas, como pueden ser medidas de sensibilización y difusión, capacitación o la creación de contenidos específicos.

- Otras relacionadas con alianzas estratégicas.
- Definir un sistema de indicadores clave que permita el adecuado seguimiento de las medidas propuestas, así como la medición de la mejora e impulso del ecosistema de ciberseguridad en la Comunidad de Madrid en términos de rendimiento y sostenibilidad.

3.1.2 CASOS DE USO

Se entiende por caso de uso la definición de un escenario específico en el que se describe cómo un sistema, servicio o proceso debe responder a una amenaza o incidente de seguridad. Estos casos de uso son esenciales para planificar, implementar y mejorar las estrategias de ciberseguridad, ya que ayudan a anticipar y gestionar los riesgos de manera efectiva.

Partiendo de esta identificación el adjudicatario creará 15 casos de uso que aborden de manera realista los principales retos y problemas relacionados con la protección de la información, los servicios, los equipos y sistemas de los llamados Smart Health, es decir, aquellos que se basan en procesos optimizados y automatizados desplegados en un entorno TIC de activos interconectados, particularmente basados en Internet de las cosas (IoT), para mejorar los procedimientos de atención al paciente existentes e introducir nuevas capacidades.

Cada caso de uso deberá documentarse con una ficha técnica, que actuará a modo de resumen ejecutivo del caso, que contendrá al menos los siguientes apartados, independientemente de la documentación propia particular de cada caso, que deberá adjuntarse en su integridad a la documentación de cada caso de uso:

Ficha Resumen de caso de uso (50 páginas máximo)		
Apartado	Descripción	Extensión orientativa
Título del caso	Se intentará, en la medida de lo posible, dar a cada caso un nombre, lo más comercial e intuitivo posible, que identifique de forma amigable la esencia del caso que se pretende demostrar.	
1.- Ficha Técnica Resumen Ejecutivo		
1.2. Objeto	Se describirá de manera resumida el objetivo que se pretende conseguir con el caso de uso, utilizando un lenguaje amigable que puede ser entendido por las empresas y actores del ecosistema al que irá dirigido.	1 página

1.3. Explicación del caso	Se realizará una exposición detallada del caso indicando la situación de partida, los actores implicados, la problemática que se pretende resolver, las implicaciones, los riesgos y amenazas del mismo, así como las actuaciones que se pretenden llegar a cabo y los resultados esperados.	2 páginas
1.4. Elementos a analizar que conforman el caso	Se llevará a cabo una identificación y definición de los elementos más importantes que conforman el caso, así como una descripción y catalogación de los mismos como punto de partida para analizar el caso.	2 páginas
1.5. Fuentes de datos, tecnología, hardware y software implicado	Se analiza de forma exhaustiva el software y hardware que pudiera ser utilizado en todo el proceso, así como las fuentes de datos del caso de uso, sus características, propiedad intelectual, modelos de explotación, calidad, origen, volúmenes, transformaciones, etc.	4 páginas
1.6. Equipos específicos necesarios	Deberán especificarse los equipos específicos necesarios para cada caso de uso detallando cómo pueden ser vulnerables a ciberataques.	4 páginas
1.7. Barreras y riesgos	Deberán detallarse las barreras y riesgos que el caso de uso plantea indicando la forma de mitigarlas	4 páginas
1.8. Metodologías empleadas en el caso	Se realizará una explicación detallada de las metodologías utilizadas, describiendo de forma exhaustivamente su aplicación práctica en el caso de uso concreto.	4 páginas
1.9. Descripción de las técnicas y algoritmos utilizados en el caso	Se realizará una explicación detallada sobre las técnicas y algoritmos utilizados en el caso, tanto para analizar el caso de uso como para resolverlo, describiendo de forma pormenorizada las técnicas y algoritmos utilizadas y su aplicación práctica en el caso de uso concreto.	4 páginas
1.10. Soluciones propuestas al caso de uso	Se realizará una explicación detallada sobre las soluciones propuestas al caso de uso, detallando en qué consisten desde el punto	5-10 páginas

	de vista funcional, tecnológico, jurídico, económico, de organización empresarial, etc y la viabilidad de su aplicación práctica.	
1.11. Resultados obtenidos	Se deberá detallar con claridad los resultados obtenidos del caso de uso y las implicaciones del mismos en toda la cadena de valor del ecosistema de ciberseguridad en la Comunidad de Madrid	3 páginas
1.12. Coste Económico	Estimaciones económicas de cada uno de los elementos que están implicados en el caso y comparaciones de soluciones y alternativas de mercado y su coste efectivo	3 páginas
1.13. Modelo de negocio	Se deberá detallar el posible modelo de negocio en torno al caso, indicando su viabilidad económica, implicaciones, cadena de valor, actores implicados, etc y en general todas aquellas variables que afectan al modelo de negocio que se podría crear en torno al caso.	4 páginas
2.- Glosario	Glosario de terminología usada en cada caso de uso	
3.- Anexos	Anexos con toda la información necesaria de cada caso de uso	

El licitador presentará en la oferta para su posterior aprobación por parte de la Dirección General de Estrategia Digital la siguiente documentación:

- **Estudio de la situación de la Ciberseguridad en la Comunidad de Madrid** con un apartado específico relativo al sector salud.
- **Ficha técnica de cada uno de los 15 casos de uso** incluyendo la información de la ficha solicitada por cada caso de uso, como mínimo.

3.2 LOTE 1 ACTUACIÓN 2 DESPLIEGUE DE UN ENTORNO TECNOLÓGICO

El centro demostrador debe situarse en el espacio disponible en el Centro de Innovación Digitaliza Madrid ubicado en la calle Embajadores 181, Madrid. El plano de la sede se encuentra como Anexo I al presente Pliego y se enmarca en rojo el espacio disponible para situar el centro demostrador.

3.2.1 ACTUACIÓN 2 ETAPA 1. DISEÑO INICIAL

El adjudicatario procederá a llevar a cabo un diseño inicial del centro demostrador que deberá contemplar, al menos el equipamiento mínimo de software para el correcto funcionamiento del centro como, por ejemplo:

- Portal web del centro demostrador
- Herramienta de CRM multicanal
- Gestor Documental
- Intranet del centro demostrador
- Plataforma de simulación de ciberseguridad multifunción que modele sistemas informáticos de IT/OT y represente escenarios realistas, incluidos ciberataques reales.

El diseño deberá incluir todos los componentes a suministrar, así como todos los servicios necesarios para la gestión del mismo.

El despliegue de este entorno tecnológico deberá permitir reproducir de la forma más realista posible los casos de uso diseñados en la actuación anterior.

Esta infraestructura garantizará que el acceso a las tecnologías y a los casos de uso se pueda realizar tanto de forma presencial como remota. El objetivo es reproducir el entorno tecnológico, los activos de datos y el catálogo de amenazas, de forma que sirvan para construir un conjunto de servicios orientados a ser utilizados por todas las partes interesadas.

Algunos ejemplos para considerar son:

- Los equipos de red que proporcionan la columna vertebral de conectividad para apoyar a los hospitales inteligentes y a los pequeños centros de consulta y atención. El equipo requerido no es diferente del equipo estándar utilizado en un centro sanitario tradicional, pero se caracteriza por su mejora en las características.
- Dispositivos médicos en red cuyo uso extensivo suele caracterizar a los hospitales inteligentes y también permiten la monitorización de pacientes, que es un servicio clave que los hospitales inteligentes pueden proporcionar a la gestión sanitaria a nivel nacional, en comparación con los hospitales tradicionales.
- Sistemas de información clínica interconectada, que se despliegan juntamente con dispositivos médicos y componentes de identificación para permitir procesos inteligentes de atención al paciente de extremo a extremo.
- Datos recopilados anonimizados como, por ejemplo:
 - Datos clínicos y administrativos de los pacientes: historiales médicos, resultados de pruebas, datos de contacto, etc.
 - Datos financieros, organizativos y otros datos hospitalarios.
 - Datos de investigación (por ejemplo, informes de ensayos clínicos) y datos destinados a un uso secundario.
 - Datos de personal.
- Registros de seguimiento.

3.2.1.1 Espacios mínimos disponibles en el Centro Demostrador

Consideraciones mínimas sobre equipamientos del centro demostrador que deberán de tenerse en cuenta en la propuesta:

Espacios de demostración singulares

Estos espacios serán concebidos como un laboratorio de ideas y diseño de estrategias de negocio, el Centro Demostrador dará así respuesta al desafío e importancia estratégica que la ciberseguridad supone ya en la gestión de clientes.

Estos espacios funcionarán como un laboratorio para diseñar nuevos servicios y sus modelos de negocio basados en casos de uso en ciberseguridad y actuarán a modo de factoría de soluciones en la que testar pruebas de concepto y prototipos antes de su implantación.

El Centro pondrá a disposición estos espacios, el acceso y contacto entre las empresas con los equipos y especialistas en ciberseguridad del Centro, con el propósito de facilitar a los clientes soluciones innovadoras en este campo destinadas a revolucionar la manera de hacer negocios en el campo de la ciberseguridad en los próximos años.

Deberán existir espacios en el Centro Demostrador, de diseños singulares, que sirvan de laboratorios, para incubar estas ideas y facilitar la innovación.

3.2.1.2 Herramientas de gestión mínimas del Centro Demostrador

Dadas las características del centro demostrador y la cantidad de actores con los que interactuará se hace imprescindible contar con una serie de herramientas de gestión que faciliten las relaciones con terceros y permitan hacer un seguimiento de los servicios ofrecidos por el centro demostrador.

Estas herramientas permitirán también actuar de puntos de información y ofrecer servicios de información de asesoramiento, registro de actividades, notificación de eventos, gestionar la agenda de actividades, actuar como repositorio común, etc.

Estas herramientas, que serán facilitadas por la empresa adjudicataria con las licencias necesarias para todo el Centro Demostrador, estará destinada a la gestión de los datos relacionados con los servicios prestados y debe contemplar la posibilidad de elaborar diferentes informes a partir de dichos datos.

También tendrá como finalidad la coordinación de las actividades del Centro, facilitando un medio de comunicación y de intercambio de información entre todos los actores disponibles, también se proporcionará un entorno colaborativo que permita una adecuada gestión documental.

Portal web del centro Demostrador

El portal web del centro Demostrador servirá de punto de referencia multicanal a todas las actividades del centro. Por un lado, tendrá una parte pública que actuará como punto de información a cualquiera que quiera obtener información general del centro demostrador, las actividades que ofrece, la agenda de los eventos, talleres, servicios y en general la solicitud de cualquier tipo de servicio que preste el centro.

Por otro lado, actuará como una intranet de servicios internos del centro, atendiendo a todos aquellos clientes que soliciten sus servicios. Existirá un área privada de los usuarios que se den

de alta en el centro, pudiendo acceder a través de ella, a información personalizada de informes y en general documentación de interés en función de sus intereses y características de empresa.

El portal web constará de una parte pública donde se muestre la información del proyecto, organizada con una estructura que, como mínimo, contendrá los siguientes apartados:

- Descripción del proyecto
- Objetivos del proyecto
- Actuaciones del proyecto
- Formulario web para el envío de consultas de asesoramiento
- Contenidos de difusión de información:
 - Noticias o novedades de interés
 - Agenda de actividades de los centros
 - Galería multimedia
 - Documentos de interés: publicaciones, informes, buenas prácticas, casos de éxito, guías, etc.
 - Recursos formativos
 - Enlaces de interés
- Módulo de alertas
- Los usuarios podrán suscribirse a los diferentes contenidos de difusión existentes
- Los usuarios recibirán un correo electrónico en el que se informará de la incorporación de algún contenido al que estén suscritos

El portal web podrá permitir la inclusión de contenidos con los siguientes formatos: contenidos textuales y gráficos, acceso a documentos en diferentes formatos (pdf, word...), contenidos multimedia (audiovisuales, sonoros...), etc. Además, se valorará la incorporación al portal de catálogos de búsqueda de ayudas y subvenciones relacionadas con el ámbito de la Ciberseguridad y cuyos beneficiarios serán las empresas de la Comunidad de Madrid.

El portal también contará con una parte privada de acceso restringido para los participantes que lo soliciten a través del propio portal web. Esta parte deberá contener, como mínimo:

- Módulo de cita previa de asesoramiento en alguno de los centros disponibles
- Acceso a la documentación, recursos formativos y enlaces de interés específicos a su solicitud de asistencia
- Foros

En esta parte privada existirán los perfiles de acceso:

Administrador:

- Tendrá los mismos permisos que el gestor de contenidos para todos los tipos de contenidos existentes
- Podrá asignar usuarios a la parte privada y asignarles un perfil de acceso a ella

Gestor de contenidos:

- Podrá crear contenidos entre los descritos en el apartado anterior en función de los permisos que tenga asignados

- Este perfil podrá tener acceso como gestor de contenidos sólo de determinados tipos de contenidos en función de los permisos asignados por el administrador

Contribuidor:

- Tendrá acceso al portal en modo lectura y podrá crear contenidos en los foros

El licitador deberá realizar una propuesta detallada de las funcionalidades que se van a incluir dentro del portal web del Centro Demostrador, así como un cronograma sobre la periodicidad de las actualizaciones de la información y contenidos de cada uno de los apartados.

Herramienta de Gestión de las relaciones con los terceros y gestión documental

Las herramientas deberán cubrir, por lo menos, los siguientes requisitos funcionales:

- Gestión de las actividades de los consultores de asesoramiento en ciberseguridad prestadores de servicios. Deberá incluir funcionalidades como:
 - Gestión de la agenda personalizada de los asesores
 - Gestión y planificación de reuniones. Asignación de técnicos a los servicios y contactos
 - Gestión de los terceros interesados en el centro demostrador, que incluirá una ficha de información básica (nombre, razón social, descripción de la empresa, localización, servicios que presta, responsables, persona de contacto etc).
 - Gestión de usuarios potenciales a los que se debería realizar una acción proactiva de contacto y asesoramiento para que se adscriban al centro y empiecen a recibir información del centro
- Gestión de los servicios prestados por el centro:
 - Gestión individualizada a cada empresa de cada uno de los servicios ofrecidos por el centro demostrador.
 - Gestión del historial de contactos establecidos con el usuario, que incluirá entre otros:
 - Relación de todos los contactos/servicios realizados por fecha
 - Gestión del estado y trazabilidad de cada contacto
 - Analítica de contactos
 - Herramientas de gestión de la comunicación con el usuario:
 - Envío masivo de email. Programación y envío de mensajes, publicaciones y novedades a usuarios, contactos potenciales y usuarios del portal web.
 - Posibilidad de aplicar filtros a la BBDD de usuarios para realizar comunicaciones segmentadas, Informes e historial de envíos.
 - Seguimiento de notificaciones
- Cuadro de mando:
 - La herramienta deberá permitir el seguimiento de los indicadores por parte del equipo del proyecto
- Herramientas de gestión de la documentación:

- Deberá existir un repositorio colaborativo común que permita la recopilación y categorización de toda la información generada en el centro demostrador.
- La herramienta deberá tener capacidades de búsqueda de la información generada en el centro demostrador
- Categorización de los documentos e informes generados a través de una nomenclatura común.
- Almacenamiento de los documentos e informes generados
- Establecimiento de flujos de trabajo sobre la elaboración y aprobación de los documentos e informes generados

La herramienta deberá cubrir, por lo menos, los siguientes requisitos técnicos:

- El sistema deberá ser un sistema web accesible a través de los navegadores más comúnmente usados en sus versiones más recientes.
- La imagen de la aplicación debe ajustarse a las especificaciones de los manuales de identidad corporativa que se identifiquen para el proyecto.
- Todas las licencias de las herramientas propuestas correrán a cargo del adjudicatario.
- Las herramientas podrán estar on premise o en la nube según estime más adecuado el licitador.
- El licitador deberá entregar un informe detallado de las características técnicas de todo el equipamiento, tanto software como hardware, que quiera instalar en el centro y este deberá ser aprobado por la Consejería de Digitalización previo paso a su instalación en el centro.

Plataforma de simulación de ciberseguridad multifunción

La solución propuesta deberá modelar sistemas informáticos de IT/OT compuestos por decenas a cientos de componentes virtuales y representar escenarios realistas, incluidos ciberataques reales. Deberá abordar los siguientes objetivos:

- Ser una plataforma abierta y personalizable, que permita a los usuarios finales integrar sus propios activos virtuales, vectores de ataque y sistemas IT/OT representativos de los modelos.
- Ser una plataforma escalable, capaz de gestionar varios entornos de simulación al mismo tiempo.
- Ser una plataforma fácil de usar con una instalación simple basada en el protocolo HTTPS/HTTPS estándar que no requiera instalación de software adicional. La interfaz web deberá estar diseñada para ocultar la complejidad de administrar miles de componentes virtuales, permitiendo a los usuarios finales concentrarse en modelar sus sistemas.
- Ser una plataforma sencilla de operar diseñada para minimizar los esfuerzos de administración durante su operación.
- Permitir organizar actividades de tipo “captura la bandera”.

La plataforma deberá permitir a los usuarios sumergirse en un entorno personalizado que se asemeje a su sistema en uso. Deberá admitir múltiples casos de uso, incluida capacitación, ejercicios operativos y pruebas.

El tiempo máximo de ejecución será de un mes a contar desde la fecha de inicio del contrato.

Entregables:

- **E1 - Memoria técnica de diseño** que incluirá al menos el siguiente detalle:
 - Descripción detallada del centro demostrador, su distribución física y su propósito.
 - Infraestructura física y cloud: Listado y características del material Hardware (HW) y Software (SW) necesario, incluyendo: referencia, cantidad, marca/fabricante, modelo/versión, y descripción detallada de cada uno de los elementos. En la medida de lo posible el material deberá ser multifabricante.
 - Necesidades y requisitos de la ubicación final de los armarios racks (red, fuerza, suelo técnico, aislamiento, etc.).
 - Evaluación de riesgos del proyecto y tratamiento.
- **E2 – Memoria necesidades de personal y gestión física del centro demostrador** incluyendo definición de todo el personal necesario, gestión de acceso al centro tanto de forma física como en remoto, condiciones y horario de apertura, sistema de gestión de incidencias, etc.
- **E3 – Plan Operativo** del centro Demostrador. Se presentará un documento con el plan operativo del centro en el que se detallarán los mecanismos a implementar por el centro para su funcionamiento interno que incluirá un mapa de procesos detallado, personal asignado y operativa de todo el centro para su correcto funcionamiento.

3.2.2 ACTUACIÓN 2 ETAPA 2. DESPLIEGUE, CONFIGURACIÓN Y PUESTA EN MARCHA

En esta etapa el adjudicatario procederá a llevar a cabo el despliegue, configuración y puesta en marcha del centro demostrador en función del diseño acordado en la etapa anterior.

Como parte final de la misma, el licitador entregará el centro demostrador completo y procederá a su puesta en marcha en la ubicación especificada en el apartado 3.2 del presente pliego.

En esta etapa del proyecto deberán desarrollarse, como mínimo, las siguientes actividades:

- Despliegue, configuración y puesta en marcha del centro demostrador
- Habilitar los espacios físicos
- Poner en marcha el plan de implantación fijado en la etapa 1 de todo el software y hardware necesario:
 - Instalación y configuración de la herramienta informática de gestión
 - Instalación y configuración del portal web del Centro Demostrador
 - Puesta en marcha del plan operativo del Centro Demostrador
- En colaboración y bajo las directrices del adjudicatario del Lote 2, inauguración con un acto institucional del centro demostrador invitando a todo el ecosistema de ciberseguridad de la Comunidad de Madrid para presentar el Centro y los servicios que va a prestar.
- Puesta en marcha efectiva del Centro Demostrador y prestación de servicios de asesoramiento tecnológico mediante la realización de las siguientes acciones:
 - Poner en marcha y dar soporte técnico la herramienta informática de gestión del centro demostrador

- Poner en marcha y dar soporte técnico al portal web de difusión del Centro Demostrador
- Prestar los servicios del catálogo del Centro Demostrador
- Elaborar, mantener y explotar una base de datos de terceros que colaborarán con el Centro Demostrador.

El tiempo máximo de ejecución serán 14 semanas a contar desde la finalización de la Etapa 1. Trascurrido ese periodo de tiempo el centro demostrador debe estar operativo, aunque puede ser admisible que alguno de los casos de uso no esté accesible previa justificación de la no disponibilidad en el mercado de alguno de los componentes o equipos necesarios para el mismo.

Entregables:

- **E4 – Planos y esquemas del centro demostrador**, que deben incluir al menos: tanto disposición física como de arquitectura de los sistemas planteados, así como una explicación detallada de la conexión en remoto.
- **E5 - Hojas de características técnicas (DataSheets)** de todos los elementos HW y SW suministrados. Todos ellos deben tener licencia de uso válida, como mínimo, hasta la finalización del contrato.
- **E6 – Manuales de mantenimiento, operación y montaje** de los componentes del centro demostrador. Debe incluir aspectos como:
 - Configuración inicial de los equipos.
 - Realización y recuperación de copias de seguridad (en caso necesario, junto a este documento también se deben entregar el conjunto de ficheros de back up para cada uno de los componentes después de su configuración inicial).
 - Procedimiento para actualización de los componentes.
- **E7 – Listado de personal del centro demostrador**

3.2.3 ACTUACIÓN 2 ETAPA 3. GESTIÓN Y EXPLOTACIÓN

El adjudicatario se encargará de la gestión y explotación del centro demostrador, llevando a cabo todas las actividades necesarias para su correcta operatividad, incluyendo al menos:

- Control de apertura y cierre del centro demostrador.
- Gestión y mantenimiento de la infraestructura física y cloud.
- Gestión de las solicitudes de acceso a los servicios.
- Gestión de la ejecución del catálogo de servicios.

Además, el adjudicatario prestará un servicio de soporte y mantenimiento para el centro demostrador que incluya todos los componentes y equipos del mismo, así como la infraestructura cloud necesaria y la resolución de todas las incidencias relacionadas con la gestión del acceso virtual por parte de los usuarios a las aplicaciones del centro demostrador.

El adjudicatario se hará cargo de toda la operativa del centro durante todo el periodo del contrato, debiendo guardar los siguientes principios rectores de la prestación de los servicios del centro:

- Los servicios de asesoramiento deberán prestarse desde una perspectiva neutral, tanto comercial como tecnológica, proporcionando a las empresas y demás actores del

ecosistema ciber en la Comunidad de Madrid toda la información necesaria para que puedan tomar sus propias decisiones al respeto de los productos o servicios comerciales que van a incorporar a sus negocios en base a los casos de uso estudiados.

- Todo el proceso de puesta en marcha del centro, así como la prestación de los servicios del mismo a las empresas y demás actores involucrados, deberá tener capacidad para generar confianza y credibilidad entre las empresas, agentes empresariales y demás actores interesados.
- Toda la gestión de la prestación de los servicios que realice el centro debe ser totalmente transparente. Esto implica que en todo momento se documentaran las sesiones, eventos, talleres, demostraciones que se realicen para elaborar una memoria de actividad del centro.
- La prestación de los servicios del centro demostrador deberá ser flexible, dinámica y adaptarse lo máximo posible a los horarios y circunstancias de las empresas.

Durante la ejecución de todas las actividades del Centro Demostrador será preciso establecer un sistema transversal de seguimiento y control del cumplimiento de los indicadores establecidos.

Para eso la empresa adjudicataria deberá elaborar un cuadro de mando para evaluar la efectividad de los servicios prestados, desarrollando, por lo menos, las siguientes actividades:

- Definición de los objetivos por actuación
- Seguimiento de los indicadores establecidos en este proyecto
- Preparación de documentos de buenas prácticas
- Evaluación de resultados respecto a los objetivos
- Preparación de documentos de comunicación de resultados
- Elaboración de informes de control y seguimiento trimestrales que reflejen el grado de ejecución y de cumplimiento de los acuerdos de nivel de servicio.

Este cuadro de mando deberá proporcionar información sobre los siguientes aspectos:

- Grado de avance global de las actuaciones del Centro demostrador
- Grado de avance por separado de las actuaciones del Centro demostrador
- Grado de cumplimiento de los indicadores de objetivos
- Grado de cumplimiento de cualquier otro indicador que se proponga durante la ejecución de las actividades previstas en este proyecto

Como mínimo, la empresa adjudicataria deberá contemplar los siguientes indicadores:

- Número de empresas dadas de alta en el Centro Demostrador
- Número de empresas asesoradas por los diferentes servicios
- Número de actividades realizadas en el centro
- Número total de asistentes a las distintas actividades
- Número de visitas realizadas al Centro Demostrador

El tiempo de ejecución se iniciará con la finalización de la Etapa 2 y terminará a la finalización del contrato.

Entregables:

- **E8 – Informe mensual de mantenimiento** que incluirá, al menos, los siguientes apartados:
 - Periodo y alcance del informe
 - Listado de las acciones de mantenimiento preventivo llevadas a cabo durante el periodo abarcado por el informe.
 - Listado de acciones de mantenimiento correctivo llevadas a cabo (incidencias) para el periodo abarcado por el informe, ofreciendo el detalle de su resolución siempre que sea conveniente para evitar futuras incidencias.
 - Listado de incidencias relacionadas con la conexión remota, así como el detalle de su resolución.
 - Riesgos y lecciones aprendidas actualizadas.
- **E9 – Informe mensual detallando los servicios prestados y el uso del centro**, conforme a lo establecido en los cuadros de mandos descritos en este pliego.

3.3 LOTE 1 ACTUACIÓN 3. DEFINICIÓN Y DISEÑO DE UN CATÁLOGO DE SERVICIOS

El adjudicatario llevará a cabo la definición y diseño de un catálogo de servicios que aporte valor a todas las partes interesadas: organizaciones sanitarias públicas y privadas, empresas especializadas, emprendedores, profesionales y personas interesadas en adquirir conocimientos para entrar en el mercado profesional de la ciberseguridad.

El objetivo de este catálogo de servicios es aportar valor a la sociedad española permitiendo que esta iniciativa alcance la autosostenibilidad económica. Este catálogo se pondrá a disposición de todos los interesados a través de la web propia del centro demostrador.

Dentro de los servicios a recoger, obligatoriamente deberá incluirse:

- Asesorar, capacitar y formar tecnológicamente a las empresas mediante:
 - Cursos de formación especializada incluyendo un catálogo de certificaciones, básicas y avanzadas, de empresas del sector. Las certificaciones deberán estar emitidas por proveedores del sector de ciberseguridad o acreditadas por el sistema nacional de acreditación de formación o cumplir los estándares internacionales de certificación. Deberá incluirse como mínimo una certificación básica y una certificación avanzada que cumplan con las siguientes especificaciones:

Certificaciones Básicas:

- Certificación en Fundamentos de Ciberseguridad: Esta certificación cubre los principios básicos de la ciberseguridad, incluyendo conceptos como amenazas, vulnerabilidades y medidas de protección.
- Certificación en Seguridad de Redes: Se centra en los fundamentos de la seguridad en redes, abordando temas como firewalls, VPNs y detección de intrusiones.
- Certificación en Concienciación sobre Ciberseguridad: Orientada a empleados y usuarios finales, esta certificación enseña las mejores prácticas para evitar ataques comunes como phishing y malware.

Certificaciones Avanzadas:

- Certificación en Gestión de Riesgos de Ciberseguridad: Esta certificación se enfoca en la identificación, evaluación y mitigación de riesgos relacionados con la ciberseguridad dentro de una organización.
- Certificación en Respuesta a Incidentes: Proporciona conocimientos avanzados sobre cómo manejar y responder a incidentes de seguridad, incluyendo análisis forense y recuperación.
- Certificación en Seguridad en Aplicaciones Web: Aborda técnicas avanzadas para asegurar aplicaciones web contra diversas amenazas y vulnerabilidades.
- Se exigirá que, tras la superación de los cursos de formación especializada, se emitan los certificados correspondientes a las certificaciones básicas y avanzadas mencionadas. Estos certificados deberán ser otorgados por entidades acreditadas en el ámbito de la ciberseguridad y deberán incluir información detallada sobre el contenido del curso, la duración, así como la fecha de emisión y el nombre del participante. La entrega de estos certificados es un requisito indispensable para validar la formación recibida y garantizar que los participantes han adquirido las competencias necesarias en ciberseguridad. El número mínimo de certificados emisibles tras haber superado las certificaciones establecidas en el apartado anterior será de 500.
- Ejercicios de entrenamiento ataque-defensa.
- Ciberejercicios para mejorar la capacidad de coordinación entre los actores involucrados.
- Benchmarking comparativo entre soluciones de mercado.
- Pruebas de configuración y arquitecturas de seguridad. Generación de procedimientos, guías y estándares.
- Banco de pruebas para proyectos de investigación e iniciativas de emprendimiento.
- Observatorio de la ciberseguridad del sector salud que permita identificar la evolución del escenario de riesgos y amenazas, y de las infraestructuras digitales y tecnológicas en las que se soportan los “hospitales inteligentes”. En este observatorio participará el Clúster de ciberseguridad de la Comunidad de Madrid, el Instituto Nacional de Ciberseguridad de España, INCIBE y, al menos, un representante de la Comunidad de Madrid.

Otros posibles servicios a recoger son:

- Apoyar a las empresas en el desarrollo de nuevos productos y servicios.
- Estimular la demanda de los gestores de las organizaciones que forman parte del sector de la Salud.
- Impulsar la creación de espacios de encuentro entre la oferta y la demanda de las pequeñas y medianas empresas.
- Convertirse en el escaparate de productos y servicios de ciberseguridad en el ámbito sanitario.

- Contribuir a fortalecer el sector de la Ciberseguridad de España y contribuir a mejorar el nivel de madurez del sector Salud.

El catálogo de servicios actuará como una plataforma de inteligencia competitiva en ciberseguridad en la Comunidad de Madrid, donde confluya la oferta y la demanda, Deberá estar compuesto por un completo set de herramientas que permita crear un repositorio de información con el que se definirán entre otras las siguientes funcionalidades: Vigilancia tecnológica; vigilancia de competidores; vigilancia de novedades legislativas e institucionales de interés, vigilancia de eventos relevantes, oferta de productos y servicios, demandas en ciber que cubran necesidades específicas, etc.

Las principales necesidades que satisfará esta plataforma son:

- Definir un estándar de intercambio de información entre la plataforma del catálogo de servicios y los sistemas de relación externos.
- Establecer los mecanismos de cooperación entre los diferentes actores que interactúan con el catalogo
- Identificar los requisitos técnicos y funcionales necesarios para el desarrollo del catálogo.
- Definir las funcionalidades de cada uno de los sistemas que compondrán el catálogo.
- Análisis de necesidades y requisitos para unificar los datos existentes en diversas bases de datos desagregadas.
- Definir los requisitos funcionales y técnicos del modelo objetivo final teniendo en cuenta la unificación de bases de datos, la definición de las interfaces necesarias para el intercambio de información y los mecanismos de cooperación de los principales actores.

El catálogo de servicios será un entorno abierto conectado con numerosos sistemas externos: Cámaras de Comercio, ICEX, CDTI, INCIBE, ministerios relacionados, empresas públicas y privadas, etc. Por ello resulta de esencial relevancia definir el protocolo y tipología de relación entre organismos que proveen la información necesaria y el gestor del catálogo, debiendo de esta manera definir las reglas, metodologías y protocolos de comunicación que se implemente para la interlocución entre los sistemas.

Así mismo, uno de los ejes vertebradores del catálogo será la relación entre los principales actores: Centro Demostrador - proveedores de información (cámaras de comercio, otras administraciones, empresas, etc.) - y usuarios o consumidores de la información (grandes empresas, pymes, autónomos, etc.). Para modelar esta relación se definirán los mecanismos de cooperación que se deberían implementar de tal forma que se permita establecer procedimientos el intercambio de información entre actores.

En este sentido para definir todos estos aspectos se realizará una toma de requisitos tras la cual se procederá a la definir qué funcionalidades deberán poseer los sistemas del catálogo.

Se deberá de hacer una definición de requisitos que debe cumplir el catálogo en base a los análisis realizados y las prioridades establecidas en el Centro Demostrador. Para ello se realizará un análisis pormenorizado de cada uno de los componentes del catálogo definiendo los requisitos funcionales de cada uno de ellos, y que entre ellos cabe destacar los siguientes:

- Intranet para el acceso a la información orientada a los técnicos gestores de la plataforma y portal web externa, que será un módulo del portal web del Centro Demostrador
- Solución CRM para la explotación de todo el contenido que se introduzca en el sistema de información a través de los portales web mediante la interacción con los proveedores de datos y los profesionales usuarios de los datos de la plataforma. Este CRM será el mismo que use para el resto de los servicios del Centro demostrador.
- Necesidades de comunicación/interoperabilidad con terceros.
- Plataforma web orientada a proveedores y usuarios de datos.
- Unificación de las Bases de datos: Será necesario identificar, analizar y establecer procedimientos para realizar la unificación de los datos estructurados almacenados en las diferentes bases de datos existentes.
- Definición de las Interfaces de intercambio de Información: Debido a que la plataforma estará formada por varios sistemas internos y puede conectarse con diversos sistemas externos, se procederá a definir una serie de interfaces que modelen y estandaricen el intercambio de información.
- Mecanismos de Cooperación: De manera análoga a las interfaces de intercambio de información para sistemas tecnológicos, se deberá definir y estructurar los mecanismos de cooperación entre los diferentes agentes de interés de la plataforma. De esta manera se podrán establecer procedimientos de actuación para cada una de las acciones que pueda realizar cada uno de los actores, modelando el escenario completo.
- Las principales directrices operativas de promoción y de personalización se definirán en el módulo CRM. Buena parte de la plasmación de la estrategia de comunicación y prestación del servicio deberá residir en el módulo CRM, a partir del cual, se concretará en cómo y cuáles servicios y contenidos se van a poner a disposición de los usuarios a través del portal del Centro Demostrador. Igualmente será el lugar en donde se almacenará la información que va a caracterizar a la tipología de usuarios y, por ello, tendrá una importancia decisiva en los servicios de personalización y contextualización de la información.
- La bidireccionalidad de la información entre los usuarios y El Catálogo deberá estar garantizada. Los usuarios no son considerados como simples consumidores de contenidos y servicios, sino que se deberán considerar como contribuidores activos de contenidos a los distintos componentes del Catálogo de servicios.

Se deberá definir el modelo de relación con los proveedores de datos y el modelo de colaboración público-privada que garantice la sostenibilidad del modelo de servicios y de la plataforma. En este sentido, se definirá/n:

- el modelo de relación con los proveedores de datos.
- el modelo de relación con los usuarios de los datos
- el modelo de relación con otros agentes clave de interés
- el modelo de colaboración que garantice la sostenibilidad.
- los mecanismos de intercambio de información.
- los sistemas de calidad a aplicar en el marco del proyecto.

- la viabilidad jurídico-legal a tener en cuenta en el marco del proyecto, anticipando potenciales riesgos o requisitos legales para las distintas alternativas
- los modelos de comercialización de la plataforma
- los mecanismos de transferencia de capacidades y conocimiento.
- los elementos identificadores que permitan una mejor comercialización, una imagen integrada y con ello un mejor posicionamiento de la plataforma en el mercado.

Los trabajos a realizar se centrarán en el modelo de prestación de servicios del catálogo, para ello se pondrá el foco en el posicionamiento de la oferta en base a las necesidades, canales y actores analizados en fases anteriores.

Asimismo, la definición de los diferentes elementos que integrarán el modelo objetivo del proyecto, desde herramientas tecnológicas, modelos de comercialización, mecanismos de transferencia de capacidades y conocimiento, etc., requerirá que se lleven a cabo las siguientes tareas:

- Identificación de los activos intangibles que deriven de la definición del modelo propuesto para la puesta en valor y optimización de los activos de la plataforma (tecnología, software, bases de datos, etc.).
- Validación de los mecanismos de transferencia de capacidades y conocimientos a la plataforma e identificación de los posibles riesgos derivados de aquéllos.
- Verificación de que la plataforma cumple con las indicaciones en materia gestión de intercambio (venta, etc.) de información, de defensa de la competencia, etc., consignadas en el apartado relativo a la determinación del modelo.

Se analizarán los siguientes aspectos de la plataforma de Inteligencia competitiva:

- Diseño de las entidades, módulos y componentes de la solución.
- Relación a alto nivel entre los mismos.
- Diagramas de componentes e infraestructura.
- Arquitectura técnica

Durante esta fase se definirá los requisitos de arquitectura lógica de la solución a desarrollar que inicialmente se basará en una arquitectura separada en tres capas, por un lado, la capa de Interfaz Gráfica de Usuario, la cual estará en contacto continuo a través de internet con la capa del bus de integración. La arquitectura física de la solución consistirá en diferentes entornos dependiendo del escenario de la aplicación. La Arquitectura de Integración que deberá permitir el desarrollo y gestión de servicios tanto de negocio como técnicos, y que interactuando entre sí proporcionarán la lógica necesaria para construir aplicaciones o servicios compuestos de una manera rápida y cumpliendo siempre con los principios de la orientación a servicios. Así mismo, durante el desarrollo de esta fase se definirán las características y capacidades necesarias de cada uno de los módulos de los que se compondrá la plataforma.

Es imprescindible que el catálogo cuente con un cuadro de mandos que recoja una serie de indicadores que permitan medir su funcionamiento y su evolución para tomar las medidas necesarias. A continuación, detallamos algunos de los posibles indicadores de la plataforma:

- Indicadores de comportamiento del catálogo
 - Nivel de amigabilidad de la navegación
 - Numero de fuentes públicas usadas
 - Tiempo de actualización de la información
 - Media/mín/máx tiempo para integrar una nueva temática
 - Promedio diario de usuarios activos
 - Promedio diario del tiempo que los usuarios pasan en la plataforma
 - Tiempo de procesamiento promedio consulta o informe
 - Número de informes activos/total de informes generados
 - Número de informes solicitados nuevos semanal, mensualmente.
- Indicadores de actividad del catalogo
 - Nivel de precisión de la información ofrecida.
 - Nivel de detalle de la información.
 - Relevancia de la información.
 - Velocidad de respuesta - cuando se hacen peticiones especiales.
 - La información buscada se ofrece en tiempo suficiente para que los usuarios (empresas principalmente) puedan desarrollar planes estratégicos y/o tomar decisiones a tiempo y de manera eficaz.
 - Anticipación
 - Efectividad de los datos ofrecidos por la plataforma de inteligencia competitiva.
 - Estadísticas de usuarios de la Plataforma de inteligencia: seguimiento de fuentes de inteligencia más populares.
 - Tipología de servicios solicitados.
 - Tipología de clientes.
 - Geografía de los clientes
- Indicadores de resultado de la plataforma de inteligencia competitiva
 - Número de solicitudes: seguimiento del número de solicitudes de datos
 - Comentarios de los principales agentes de interés: las percepciones de los beneficios obtenidos de los servicios ofrecidos
 - Valor de negocio generado:
 - Número de nuevas oportunidades de negocio y tendencias objetivos analizados por la plataforma.
 - Estimación de ROI obtenido por los usuarios tras usar la plataforma de Inteligencia.
 - Ahorro de costes: estimación del porcentaje de ahorro de costes provenientes del uso de los datos ofrecidos.
 - Benmarck: comparación de los resultados obtenidos por la Plataforma en comparación con los resultados obtenidos por otras plataformas similares.

Tiempo de ejecución: comenzará al finalizar la Etapa 1 y terminará a la finalización del contrato.

Entregables:

- **E10 Catálogo de servicios:** entrega de la primera edición del catálogo en 1 mes desde la finalización de la Etapa 1 y entrega de ediciones actualizadas con carácter semestral.

- **E11 Informe anual del estado de la ciberseguridad** donde se refleje la situación actual con especial foco en el sector salud y una comparativa respecto a los resultados del informe inicial. Además de los requisitos solicitados para el informe presentado como parte de la oferta, el adjudicatario deberá realizar en la actualización, como mínimo, las siguientes actividades:
 - Involucrar a todo el sector desde el principio del proceso. Trabajo de campo con el tejido empresarial y el sector de la ciberseguridad para conocer sus necesidades actuales y expectativas del proyecto.
 - Entrevista personalizada con los diferentes “stakeholders” , A través de un modelo colaborativo que comprenda organizaciones que formen parte de la demanda (hospitales, clínicas, laboratorios, tanto públicos como privados), oferentes de tecnología (gran, mediana y pequeña empresa de ciberseguridad), universidades y centros de investigación aplicada.
 - Organización de al menos dos mesas de trabajo de identificación de debilidades, amenazas, oportunidades y fortalezas enfocadas en la ciberseguridad.
 - Estudiar las diferentes iniciativas puestas en marcha por el sector, la situación actual y las tendencias del mercado con el fin de identificar los factores críticos de éxito para el desarrollo del proyecto y las oportunidades a futuro para mejorar la competitividad del sector en el ámbito de la ciberseguridad.
 - Análisis de la oferta de servicios e infraestructuras: El análisis de la oferta se realizará desde dos ámbitos diferenciados:
 - El análisis del proceso de prestación de servicios, incluyendo el posicionamiento, la comercialización, la interacción con el cliente y la gestión de las expectativas del cliente.
 - Análisis de los recursos y activos tecnológicos disponibles, desde el ámbito de la calidad, la utilización y la variedad y volumen de la oferta.
 - Definir un conjunto de acciones coordinadas en las dimensiones clave, como son las empresas ofertantes, las tecnologías implícitas, la comercialización de las soluciones y activos tecnológicos y un modelo de gestión consensuado que forme parte del modelo objetivo
 - Analizar las características específicas de la demanda, tanto a nivel de recursos como de productos y servicios, realizando una segmentación en base a tipologías.

3.4 LOTE 1 ACTUACIÓN 4. TRANSFERENCIA DEL SERVICIO

Con el objetivo de la sostenibilidad y continuidad futura del Centro Demostrador, se deberán realizar las siguientes actividades:

De manera previa a la transferencia del servicio, al menos tres meses antes de la finalización del contrato, se deberá presentar un plan de continuidad del servicio que contemple las distintas alternativas propuestas para garantizar la continuidad del centro demostrador una vez que termine el proyecto.

Se deberá realizar una memoria de todas las actividades que se han realizado en el centro demostrador

Se debe de realizar un mapa pormenorizado de agentes que han intervenido durante toda la vida del centro demostrador con una ficha con la información básica y personas de contacto

Se deberá realizar un inventario de todos los activos del centro demostrador que incluya tanto el catálogo de servicios como los activos físicos tanto software como hardware de los que disponga el centro en el momento de determinar el proyecto, así como sus condiciones de mantenimiento y garantía.

3.5 LOTE 1 EQUIPO DE TRABAJO

Las ofertas deberán especificar el equipo que aportará la empresa adjudicataria para la realización de los trabajos, con sus correspondientes perfiles, formación académica, cualificación y experiencia.

El equipo de trabajo que la empresa adjudicataria pondrá a disposición del proyecto deberá estar constituido como mínimo por los siguientes equipos coordinados por un Director del proyecto apoyada por una oficina técnica de gestión.

- Director de proyecto y oficina de proyectos
 - 1 Director del proyecto
 - 1 Responsable de equipo Oficina técnica
 - 1 Gerente del equipo de oficina técnica
 - 2 Consultores Senior
 - 2 Consultores de apoyo
- Equipo de consultoría formado por:
 - 1 Responsable de equipo Consultoría
 - 1 Gerente del equipo de Consultoría
 - 3 Consultores Senior
 - 3 Consultores de apoyo
 - 2 Consultores Senior en fondos europeos
 - 1 Consultor jurídico en sector publico
- Equipo 2 de ciberseguridad formado por:
 - 1 Responsable de equipo Ciberseguridad
 - 1 Gerente del equipo de Ciberseguridad
 - 3 Consultores Senior en ciberseguridad
 - 3 Consultores de apoyo
 - 3 Analistas TI
 - 6 Arquitecto de soluciones de TI
 - 1 Arquitecto de software
- Equipo 3 de operaciones del centro:
 - 1 Responsable de Operaciones
 - 1 Gerente coordinador del centro
 - 6 Consultores/asesores de casos de uso en ciberseguridad

- 6 Consultores de apoyo
- 4 Operadores del call center
- 2 Personal de mantenimiento centro

La dedicación del equipo de trabajo deberá corresponderse con la siguiente:

	Meses 15		Meses 1		14 semanas		Meses 10 y medio		Meses 14	
	Oficina de proyectos		Diseño Inicial		Despliegue		Gestión y explotación		Catálogo de servicios	
	Personas	Dedicación (horas)	Personas	Dedicación (horas)	Personas	Dedicación (horas)	Personas	Dedicación (horas)	Personas	Dedicación (horas)
Director del proyecto	1	2640								
Responsable de equipo	1	2640	1	146,67	1	440	1	1760	1	2346,67
	1	2640					1	1760		
Gerente de equipo										
Consultor Senior	2	2640	2	146,67	2	440	1	1760	2	2346,67
Consultor	2	2640	4	146,67	4	440	3	1760	4	2346,67
Analista			6	146,67	6	440	2	1760	6	2346,67
Consultor Senior en fondos	1	2640							1	2346,67
Consultor senior jurídico	1	2640							1	2346,67
Analista TI			2	146,67	2	440	1	1760		
Arquitecto de soluciones TI			2	146,67	2	440	2	1760	2	2346,67
Arquitecto software			2	146,67	2	440	2	1760	2	2346,67
Operadores de call center							6	1760		
Personal de mantenimiento			2	146,67	2	440	6	1760		

4 LOTE 2 COMUNICACIÓN Y DIFUSIÓN

4.1 LOTE 2 ACTIVIDADES

En paralelo a las actuaciones del Lote 1, el adjudicatario llevará a cabo acciones de divulgación que permitan poner al centro demostrador en conocimiento de la ciudadanía, de las empresas y de las instituciones. Para ello, desarrollará las siguientes actividades:

- Diseño y puesta en marcha de acciones de dinamización del centro demostrador con el objetivo de mejorar la visibilidad de los servicios proporcionados por el mismo.
- Organización de eventos y jornadas específicas de ciberseguridad en el sector salud.
- Diseñar y gestionar la convocatoria e inscripciones en las actividades del centro demostrador a fin de asegurar un nivel óptimo de asistencia.
- Gestionar, ampliar, reorganizar y segmentar la base de datos de contactos del centro demostrador para lograr un mayor impacto en las acciones de difusión.
- Producir, publicar y mantener actualizados los contenidos del portal web del Centro demostrador. Esta tarea se extiende a la publicación de entradas en los canales de las redes sociales habilitados.
- Diseño, producción y distribución de material promocional del centro demostrador (folletos, presentaciones...).
- Producción y divulgación de materiales audiovisuales relacionados con las actividades del centro demostrador especialmente la grabación de las sesiones y su posterior publicación en el portal web del centro demostrador.
- Establecer canales de información y atención a empresas y profesionales, tanto de modo presencial como telefónico y telemático en relación con los distintos servicios prestados por el centro demostrador. Estos canales serán atendidos por personal del LOTE1 de este pliego.
- Diseño y ejecución de acciones promocionales dirigidas a maximizar la visibilidad del centro demostrador entre las empresas del sector salud y el resto de los sectores empresariales, así como la identificación de asociaciones o entidades representativas de las empresas con las que establecer mecanismos de colaboración en materia de difusión y divulgación de los servicios del centro demostrador.
- Definir el plan de comunicación al público objetivo y empresas del sector, haciendo especial énfasis en las medidas a implementar en sectores de interés en lo relativo a comunicación institucional, campañas a realizar o incentivos a proponer.
- Definir, cuantificar y ejecutar el plan de medios que será propuesto para su aprobación al organismo competente de la Comunidad de Madrid. Este plan de medios deberá incluir, entre otras actuaciones:
 - publicaciones en medios online, publicaciones en TV y publicaciones en medios off-line;
 - actuaciones en redes sociales como campañas con influencers, campañas de publicidad programática y software de escucha activa; y
 - eventos en el centro demostrador.

La aprobación final del plan de medios corresponderá al organismo competente de la Comunidad de Madrid, que tendrá en cuenta para ello las estimaciones económicas de los servicios de difusión empleadas en la preparación del presente contrato y que forman parte de la documentación preparatoria del mismo.

Algunos de los elementos que, como mínimo, debe contemplar el plan de comunicación serán:

- Posicionamiento orgánico: Auditoría SEO del portal web del centro demostrador, situación y propuesta de mejoras técnicas y de contenidos. Realización de campañas de publicidad digital y de marketing on line referidas a las actuaciones del plan digital:
 - Estudio de palabras clave. Definición de palabras clave objetivo para captar tráfico no solo genérico sobre ciberseguridad sino sobre cada una de las actividades y servicios del centro demostrador.
 - Estrategia onsite. Optimización de velocidad web, definición de textos optimizados, creación de tittles y metas descripción apropiados para la consecución de los objetivos SEO.
 - Estrategia offsite. Análisis de enlaces entrantes y propuesta de estrategia de enlaces. Coordinación con los acuerdos de medios de comunicación para mejorar el posicionamiento del portal web del centro demostrador.
- Campañas en Redes Sociales: se busca ampliar el número de seguidores en las redes sociales del centro demostrador para garantizar un elevado alcance cuando se publiquen noticias y acciones relacionadas con el centro demostrador de ciberseguridad de la Comunidad de Madrid. De la misma manera se realizarán campañas específicas para promocionar actividades específicas y general más impacto en acciones concretas de interés.
- Segmentación. Las redes sociales nos permitirán el máximo nivel de segmentación tanto geográfica como por intereses. Así pues, toda la comunicación estará enfocada al público objetivo que se haya definido.
- Audiovisual. Utilización de material audiovisual durante las campañas de comunicación. Este material será susceptible de utilización en acciones offline o incluso podrán ser mostrados en distintas pantallas instaladas en las instalaciones del centro demostrador.
- Publicidad en Internet. Se plantea realizar distintas campañas de publicidad en internet, publicidad programática o afiliación que nos permita maximizar el alcance de las campañas y de los mensajes que queremos hacer llegar segmentando al máximo y afinando los mensajes dependiendo de cada público. Igualmente se plantea la inserción de artículos patrocinados en medios y blogs digitales de medios especializados en aquellos aspectos en los que se quiera hacer foco.
- Sistema de Alertas. Se establecerá también un sistema de alertas que permita identificar cualquier crisis reputacional que se produzca cuando el número de menciones o el alcance de estas supere los rangos habituales de tal forma que se pueda actuar con rapidez para neutralizar esa crisis en aquellos temas que afecten especialmente a la Comunidad de Madrid en Ciberseguridad.
- Escucha activa: El Centro Demostrador necesita conocer de forma proactiva, las preocupaciones, intereses, opiniones y las valoraciones y sugerencias de los distintos actores del ecosistema ciber en la Comunidad de Madrid. Consiste en la utilización de

las redes sociales como un método de obtención de información. Normalmente se utilizan como un medio más de difusión y publicación de mensajes de manera unidireccional. Al usar las redes sociales como método relacional, el objetivo va más allá de la mera información, y se busca identificar en las redes sociales la información que se obtendría en una encuesta de satisfacción a los usuarios.

- Conocer las valoraciones y opiniones de toda la comunidad ciber en la comunidad de Madrid a través de diferentes mecanismos como encuestas online/offline, entrevistas, sesiones de ideación, tormentas de ideas, talleres de análisis de amenazas, etc.
- Monitorizar constante de la opinión y estado del arte en redes sociales e internet.
- Identificar áreas de mejora en las políticas públicas, fortalezas y debilidades.
- Definir la mejor estrategia de comunicación para cada una de las iniciativas que se vayan a llevar a cabo.
- Conocer la opinión sobre la percepción de seguridad y poder tomar las medidas necesarias para su mejor

La oferta deberá incluir todos los componentes a suministrar, así como todos los servicios necesarios para la gestión del mismo.

El tiempo de ejecución: comenzará con la firma del contrato y terminará a la finalización del mismo.

Entregables:

- **E12 – Plan de comunicación**, entrega de la primera edición en 1 mes desde la reunión de lanzamiento 1 y entrega de ediciones actualizadas con carácter semestral.
- **E13 – Plan de medios**, entrega de la primera edición en 1 mes desde la reunión de lanzamiento 1 y entrega de ediciones actualizadas con carácter semestral.
- **E14 – Informes trimestrales**: Trimestralmente se presentará un informe recopilatorio en el que el contratista incluirá la relación de actividades y tareas realizadas, detallando los recursos asignados y el número de horas por recurso consumidas en el período en cuestión.
- **E15 - Dossier anual** de todas las medidas de comunicación y difusión llevadas a cabo, así como los diseños en formato editable de todos los diseños, grafismos o materiales audiovisuales que se hayan elaborado en el marco del presente contrato.
- **E16 - Informe final del proyecto**: Al final del período de vigencia del proyecto el adjudicatario deberá presentar el informe global del proyecto que incluya la relación de tareas y entregables asociados al proyecto.

4.2 LOTE 2 EQUIPO DE TRABAJO

Las ofertas deberán especificar el equipo que aportará la empresa adjudicataria para la realización de los trabajos, con sus correspondientes perfiles, formación académica, cualificación y experiencia.

El equipo de trabajo que la empresa adjudicataria pondrá a disposición del proyecto deberá estar constituido como mínimo por:

- 1 Responsable de Comunicación y difusión

- 1 Gerente de comunicación y difusión
- 1 Relación con medios, prescriptores y eventos
- 2 Diseñador web
- 3 Gestor de contenidos
- 3 Técnicos de audiovisuales (Fotos, videos, etc)
- 2 Community Manager

La dedicación del equipo de trabajo deberá corresponderse con la siguiente:

	Meses 15	
	Personas	Dedicación (horas)
Responsable de equipo	1	2640
Gerente de equipo	1	2640
Relación con medios, prescriptores y eventos	1	2640
Diseñador web	2	2640
Gestor de contenidos	3	2640
Técnicos audiovisuales	3	2640
Community mánager	2	2640

5 CUMPLIMIENTO NORMATIVO DE AMBOS LOTES

5.1 PRINCIPIO DNSH (ARTÍCULO 5 ORDEN HFP/1030/2021)

La empresa adjudicataria deberá respetar los principios de economía circular y evitar impactos negativos en el medio ambiente (DNSH, por sus siglas en inglés, “do no significant harm”) en la ejecución de las actuaciones llevadas a cabo en el marco del PRTR.

5.2 ETIQUETADO VERDE Y ETIQUETADO DIGITAL (ARTÍCULO 4 ORDEN HFP/1030/2021)

El contratista estará obligado al preceptivo cumplimiento de las obligaciones asumidas en materia de etiquetado verde y etiquetado digital y los mecanismos establecidos para su control, así como al preceptivo cumplimiento de las obligaciones asumidas por la aplicación del principio de no causar un daño significativo y las consecuencias en caso de incumplimiento.

El Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo de 12 de febrero de 2021 por el que se establece el Mecanismo de Recuperación y Resiliencia, establece en sus Anexos VI y VII la Metodología de seguimiento para la acción por el clima y la metodología para el etiquetado digital en el marco del Mecanismo, respectivamente. Según estos anexos, el Campo de Intervención 021quinquies – Desarrollo y despliegue de tecnologías, medidas e instalaciones de apoyo en materia de ciberseguridad para los usuarios de los sectores público y privado, contribuye con un 0% al cálculo de la ayuda de los objetivos climáticos y medioambientales, y con un 100% al cálculo de la ayuda a la transición digital.

El Plan de Recuperación, Transformación y Resiliencia, en su componente 15, Programa de Impulso a la Industria de la Ciberseguridad Nacional y en aplicación del Reglamento (UE) 2021/241, recoge que la contribución a la transición ecológica de este componente es de un 0% y a la transición digital de un 100%.

El contrato en tramitación corresponde a la ejecución de la inversión C15.I7, por lo que la contribución a los objetivos de transición ecológica y digital será de un 0% y 100% respectivamente. Con el objetivo de facilitar el seguimiento y evaluación del cumplimiento del compromiso de etiquetado verde y digital, se incorporará al sistema de información y seguimiento la aportación del subproyecto indicado al objetivo fijado.

5.3 PROTECCIÓN DE DATOS PERSONALES

En virtud de lo establecido en el Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante, RGPD), 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, así como la Ley Orgánica 3/2018, de 5 de diciembre de 2018, de Protección de Datos Personales y Garantías de los Derechos Digitales (en adelante, LOPDGDD), el adjudicatario deberá evaluar y documentar de forma conjunta con la Dirección General de Estrategia Digital la necesidad de ejecutar una Evaluación de Impacto de Privacidad con el objeto de identificar el conjunto de medidas técnicas y organizativas que, con carácter preventivo, y antes de la puesta en marcha del centro demostrador deben encontrarse implantadas con el objeto de atender el Principio de Privacidad por Diseño, y garantizar el cumplimiento en materia de protección de datos.

En cualquier caso, si la Evaluación de Impacto de Privacidad no fuese precisa, quedando debidamente justificado, la empresa adjudicataria colaborará con la Dirección General de Estrategia Digital, en la ejecución del análisis de riesgos de privacidad demandado por los artículos 24 y 32 de la norma RGPD, garantizando la implantación de las medidas técnicas y organizativas que resulten de dicho análisis, y que conformará el Programa de Privacidad de la competición gestionada por la empresa adjudicataria. Al efecto se referencia expresamente la Disposición adicional primera de la norma LOPDGDD, relativa a las medidas de seguridad en el ámbito del sector público.

5.4 SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN

El contratista queda expresamente obligado a mantener absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento del contrato, especialmente los personales, con especial atención a los denominados “de categorías especiales” (entre los que se incluyen los que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física). En cualquier caso, no podrá copiar ni utilizar con fin distinto al que figura en los Pliegos, ni tampoco ceder a otros ni siquiera a efectos de conservación, sin el previo consentimiento por escrito de las Comunidad de Madrid.

Se considerará información confidencial cualquier información a la que el contratista acceda en virtud de los contratos, en especial la información y datos propios del contratista o de los

usuarios y beneficiarios del servicio, que con tal carácter se indique, a la que haya accedido durante la ejecución del mismo, así como la documentación.

El contratista informará a su personal, colaboradores, suministradores y subcontratistas de las obligaciones de confidencialidad establecidas en los pliegos, así como de las obligaciones relativas al tratamiento de datos personales. El contratista pondrá todos los medios a su alcance para que su personal y colaboradores cumplan tales obligaciones. Al efecto deberán suscribir el correspondiente compromiso de confidencialidad. Cuando el contratista desee utilizar los resultados parciales o finales, en parte o en su totalidad, para su publicación como artículos, conferencias, etc., deberá solicitar con carácter previo la conformidad de la Comunidad de Madrid mediante petición dirigida al responsable de la misma.

Se excluye de la categoría de información confidencial toda aquella que haya de ser revelada de acuerdo con las leyes o con una resolución judicial o acto de autoridad competente.

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.

El contratista responderá por cualquier daño directo que pudiera resultar del incumplimiento de las obligaciones de confidencialidad previstas en el presente contrato.

A la finalización del contrato el contratista devolverá a la Comunidad de Madrid toda la información recibida, incluidas todas aquellas copias o reproducciones que de la misma se hubieran realizado. Asimismo, finalizado el objeto del contrato deberá eliminar o borrar toda aquella Información que hubiera sido almacenada en soporte no susceptible de devolución.

5.5 COMUNICACIÓN Y PUBLICIDAD


El artículo 34 del Reglamento Europeo 2021/241 del Parlamento Europeo y del Consejo, por el que se establece el Mecanismo de Recuperación y Resiliencia, recoge que “los perceptores de fondos de la Unión harán mención del origen de esta financiación y velarán por darle visibilidad, incluido, cuando proceda, mediante el uso del emblema de la Unión y una declaración de financiación adecuada que indique “financiado por la Unión Europea – NextGenerationEU”, en particular cuando promuevan las acciones y sus resultados, facilitando información coherente, efectiva y proporcionada dirigida a múltiples destinatarios, incluidos los medios de comunicación y el público”.

En este sentido, el artículo 9 de la Orden HFP/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia, recoge la necesidad de incorporar el logo oficial del Plan de Recuperación del Reino de España en las iniciativas de comunicación y divulgación de las actuaciones financiadas con cargo al MRR: “Las actuaciones de comunicación relacionadas con la ejecución del Plan incorporarán el logo oficial del Plan de Recuperación, Transformación y Resiliencia del Reino de España, en los términos que se comuniquen por la Autoridad Responsable”. Deberá exhibirse de forma correcta y destacada el emblema de la UE con una declaración de financiación adecuada que diga (traducida a las lenguas locales cuando proceda) “financiado por la Unión Europea - NextGenerationEU”, junto al logo del PRTR.

Para la incorporación del logotipo del Plan de Recuperación, Transformación y Resiliencia (PRTR) elaborado por el Gobierno, se deberá mantener la misma proporción y peso en el tamaño de todos los logotipos. El logo del PRTR irá siempre acompañado de su texto identificativo y del emblema del Gobierno de España. Los logotipos e información de las distintas fuentes de financiación deberán realizarse de manera conjunta y en el orden establecido en el Manual de Identidad Visual del PRTR. En el caso específico del uso del logotipo de la Unión junto con el de INCIBE, ambos deberán mostrarse al menos de forma tan prominente y visible como los otros logotipos. Siendo el logotipo de la UE como mínimo del mismo tamaño, medido en altura y anchura, que el mayor de los demás logotipos. Si se quiere añadir el emblema de la organización, municipio o CCAA beneficiaria de las ayudas, éste también debe ubicarse en la esquina contraria a la de la UE, tener una tipografía y colores distintos y ser más pequeño o, como mucho, del mismo tamaño que el emblema europeo.

Madrid, a fecha de la firma

EL DIRECTOR GENERAL DE ESTRATEGIA DIGITAL

Firmado digitalmente por: IGNACIO JULEN AZORIN GONZALEZ - 
Fecha: 2025.02.21 14:05