PLIEGO DE CONDICIONES PARA EL DISEÑO, DESARROLLO, PILOTO Y EVALUACIÓN DE UN SISTEMA QUE PERMITA EL RASTREO DE CONTACTOS EN RELACIÓN A LA PANDEMIA OCASIONADA POR LA COVID-19

1. ANTECEDENTES

La Organización Mundial de la Salud elevó el pasado 11 de marzo de 2020 la situación de emergencia de salud pública ocasionada por la COVID-19 a pandemia internacional. La rapidez en la evolución de los hechos, a escala nacional e internacional, ha requerido la adopción de medidas inmediatas y eficaces para hacer frente a esta coyuntura.

El Real Decreto 463/2020 por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria, establecía en el artículo 4.2.d) del Real Decreto 463/2020, de 14 de marzo, que para el ejercicio de las funciones a que se hace referencia en dicho real decreto, bajo la superior dirección del Presidente del Gobierno, el Ministro de Sanidad es la autoridad competente delegada en su área de responsabilidad y en las áreas de responsabilidad que no recaigan en la competencia de los Ministros de Defensa, del Interior y de Transportes, Movilidad y Agenda Urbana.

Tras el confinamiento de la población para contener la crisis sanitaria provocada por la COVID-19, se inician las primeras fases de la desescalada. En esta etapa de desconfinamiento, como en el posterior régimen que se ha dado en llamar la nueva normalidad, el rastreo de contactos se presenta como uno de los métodos más eficaces para el control de la pandemia: identificando los contactos estrechos que hayan tenido los usuarios, mientras se respeta la privacidad de los mismos; permitiendo reportar los confirmados positivos; y alertando a aquellas personas que hayan estado en contacto con la persona afectada de esta situación, a fin de que procedan al autoconfinamiento, así como a la puesta en contacto con los Servicios Públicos de Salud.

La Orden SND/297/2020, de 27 de marzo, del Ministro de Sanidad encargó a la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA), del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19. En particular, dicha Orden establece en su resolución primera, el Desarrollo de soluciones tecnológicas y aplicaciones móviles para la recopilación de datos con el fin de mejorar la eficiencia operativa de los servicios sanitarios, así como la mejor atención y accesibilidad por parte de los ciudadanos.

Adicionalmente, la Dirección General de Salud Pública, Calidad e Innovación, de la Secretaría General de Sanidad (Ministerio de Sanidad) ha dado el Visto Bueno a una prueba piloto de rastreo de contactos en relación a la COVID-19, encargando a la SEDIA el desarrollo de una aplicación móvil para tal fin.

[redacted]

Siendo de interés general para el Gobierno de la Nación dar respuesta al objetivo común de contribuir a la gestión de la situación de crisis sanitaria ocasionada por el COVID-19, la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría General de Administración Digital (SGAD en adelante), desarrollará un conjunto de actividades para la definición y construcción de un sistema que permita el rastreo de contactos estrechos (de forma segura y anónima para el usuario) y su posterior evaluación a través de un piloto.

En relación a las tecnologías habilitadoras para el rastreo de contactos, hay que reseñar que Apple y Google, empresas que manejan los sistemas operativos instalados en la práctica totalidad de dispositivos móviles a nivel mundial, anunciaron el pasado 10 de abril de 2020 una alianza para crear un sistema interoperable, integrado en los sistemas operativos iOS y Android, para el seguimiento de contactos, que no utiliza geolocalización sino Bluetooth de baja energía (Bluetooth LE o BLE), para identificar dispositivos presentes a una distancia próxima. El enfoque de Apple/Google está basado en el protocolo DP-3T, que preserva la privacidad mediante el empleo de identificadores efímeros sobre los que no es posible realizar ingeniería inversa para obtener datos personales del propietario del dispositivo. Apple y Google liberaron el kit para desarrolladores (SDK, https://apple.com/covid19/contracttracing) el pasado 20 de mayo, lo que permite a los distintos Estados desarrollar soluciones de rastreo de contactos sobre las nuevas funciones incorporadas en sus sistemas operativos, siempre bajo la tutela de las autoridades sanitarias nacionales.

El Sistema que se desarrollará mediante este contrato hará uso de este SDK, sobre el que se construirá una aplicación móvil que permita activar el sistema de rastreo de contactos; que en conexión con las autoridades sanitarias pueda recibir un código de confirmación de positivo en COVID-19; y que mediante una plataforma servidora (backend) con la que se comunica la aplicación móvil se pueda alertar a las personas con las que se ha tenido un contacto estrecho en fechas recientes.

2. OBJETO DEL CONTRATO

Las necesidades a cubrir con la prestación prevista en este contrato son las siguientes:

- **Fase pre-piloto**
  - Análisis técnico del Sistema de Rastreo de Contactos, conforme a los requerimientos de alto nivel del Anexo I.
  - Desarrollo de un primer producto viable.
  - Testeo del mismo.
  - Auditoría de seguridad.
  - Optimización de la adopción por parte del colectivo piloto.
- **Fase piloto**
  - Lanzamiento de la App piloto.

[redacted]

- Seguimiento del uso.
- Evolución funcional de la App.
- Aprendizaje.

- **Fase post-piloto**
  - Evolución funcional de la App con el aprendizaje obtenido en la fase anterior.

- **Infraestructura en la nube (cloud)**
  - Plataforma de servicios requeridos para alojar el Backend de la Aplicación, en modo de autogestión.

El detalle de las prestaciones será:

2.1. Fase pre-piloto (2-3 semanas)

Análisis técnico del Sistema, incluyendo una aplicación móvil de rastreo de contactos (en sistemas operativos iOS y Android), como una plataforma en la nube pública para el seguimiento de balizas (identificadores anónimos que se generan periódicamente en los dispositivos móviles). Se incluye el diseño técnico de la App como del Backend conforme a los requerimientos técnicos que figuran en el Anexo I.

Desarrollo de un primer prototipo de Sistema que sea viable para su lanzamiento como piloto. Se atenderán especialmente los aspectos de usabilidad y buena experiencia de usuario (UX) para minimizar barreras de entrada.

Testeo del mismo, incluyendo tanto pruebas funcionales como de ciberseguridad.

Optimización de la adopción por parte del colectivo piloto, incluyendo la selección de colectivos objetivo y creación de grupos de usuarios (focus group). También se incluye la definición de los casos de uso necesarios para el testeo del sistema por los usuarios.

Al final de la fase pre-piloto, se incluirán, al menos, los siguientes entregables:

Entregables:

1. Bloque funcional

   1.1. Documento de detalle funcional

2. Bloque Análisis Técnico y desarrollo

   2.1. Aplicación móvil

   2.2. Documento de diseño de la arquitectura

   2.3. Informe Auditoría de Seguridad

   2.4. Guía desarrollo seguro

   2.5. Análisis de riesgos

   2.6. Evaluación de impacto

[redacted]

2.7. Declaracion de aplicabilidad (medidas del ENS)

3. Testeo

   3.1. Plan de pruebas

   3.2. Resultado plan de pruebas

      3.2.1. Informe de incidentes (resultados), incluyendo:

      3.2.2. Casos de prueba completados

      3.2.3. Resultados por cada caso de prueba: número de pruebas realizadas por caso, incidencias detectadas en cada prueba, resolución, resultado final

4. User Experience (optimización de adopción)

   4.1. Estrategia de lanzamiento

   4.2. Gap analysis UX

   4.3. Documento UX (incluye maquetas/prototipos de UX de la APP del pre-piloto)

Adicionalmente, el software será sometido a una auditoría de seguridad por parte del Centro Criptológico Nacional (CCN), y la empresa queda obligada a corregir todas las vulnerabilidades que se reporten en la misma.

4.4. Fase piloto (2 semanas)

Se procederá al lanzamiento de la App piloto, poniéndola a disposición en los mercados de aplicaciones de Google y Apple.

Se realizará un seguimiento del piloto midiendo el éxito sobre la base de indicadores clave de desempeño (KPI) de adopción y objetivos establecidos. Se irán tomando decisiones respecto a mejoras funcionales y de experiencia de usuario según se vaya valorando la evolución de los KPI.

Evolución del sistema a lo largo del periodo piloto funcional, técnica y de seguridad del Sistema, con especial atención a:

1. Evolución funcional, técnica y de seguridad
2. Actualización de diseño UX
3. Desarrollo de nuevas funcionalidades
4. Testeo de nuevas funcionalidades
5. Análisis de interoperabilidad e integración con servicios sanitarios

Aprendizaje, incluyendo:

1. Suministro de datos de interés para análisis epidemiológico en función de resultados de la App
2. Generación de ideas (insights) y optimización de capacidad de aprendizaje con diferentes supuestos de información centralizada para reconocer los patrones de contagio

Al final de la fase piloto, se incluirán, al menos, los siguientes entregables:

[redacted]

Entregables:

1. Seguimiento del piloto
   1.1. Indicadores clave de seguimiento (KPIs)
   1.2. Cuadro de Mando
   1.3. Documento de diagnóstico y recomendaciones
2. Evolución funcional
   2.1. Documento funcional
   2.2. Documento de diseño de la arquitectura. Si es necesario
   2.3. Diseño UX
   2.4. Actualizaciones Informe auditoria de seguridad
3. Análisis integraciones
   3.1. Propuestas Integración Sistema Sanitario (sujeto información SGAD)
   3.2. Propuestas Integración Sistemas Europeo (sujeto información SGAD)
4. Aprendizaje
   4.1. Reporte de insights
5. Reportes Operación Cloud
   5.1. Reporte de cumplimiento KPI
   5.2. Informes de consumos

5.3. Fase post-piloto

Se contará con una bolsa de 905 horas que permita la evolución de la aplicación según lo aprendido en el piloto, que podrá ejecutarse hasta la finalización del contrato. Se facturará por lo efectivamente consumido.

5.4. Infraestructura en la nube (cloud)

Se precisará que los desarrollos del Backend se realicen en una infraestructura en la nube en modo de autogestión, para facilitar la agilidad en el desarrollo de la solución. No obstante lo anterior, tanto el almacenamiento como cualquier actividad de tratamiento de datos se ubicarán en el territorio de la Unión Europea, ya sean éstos provistos y gestionados por la empresa adjudicataria o por sus contratistas y colaboradores, y se alojarán en servidores y/o centros de proceso de datos de la propia empresa adjudicataria o de sus contratistas.

El presente contrato incluirá los costes derivados de cualquier plataforma, propia o subcontratada por el adjudicatario, para la prestación y mantenimiento del servicio, sin coste adicional para la SGAD.

En la medida de lo posible, se procurará la utilización de componentes en la infraestructura cloud que permitan la migración futura de la solución a la nube SARA de la AGE.

[redacted]

6. CONFIDENCIALIDAD

6.1. Confidencialidad en general

El contratista se compromete a garantizar la más estricta confidencialidad y reserva sobre cualquier dato o información a los que pueda tener acceso o pudiera conocer con ocasión de la ejecución del contrato, así como sobre los resultados obtenidos de su tratamiento, y a que únicamente se utilizarán para la consecución del objeto del contrato, no pudiendo comunicarlos, utilizarlos, ni cederlos a terceros bajo ningún concepto, ni siquiera para su conservación. Estas obligaciones se extiende a todas las personas que, bajo la dependencia del contratista o por su cuenta, hayan podido intervenir en cualquiera de las fases de ejecución del contrato.

La obligación de confidencialidad y reserva conlleva la de custodia e impedir el acceso a la información y documentación facilitadas y a las que resulten de su tratamiento de cualquier tercero ajeno al servicio contratado, entendiéndose como tal tanto cualquier persona ajena a la empresa contratista como cualquiera que, aun no siéndolo, no esté autorizada para acceder a tal información.

Asimismo, el contratista se compromete a velar por la integridad de los datos, es decir, a la protección de la información facilitada y a la que resulte de su tratamiento contra la modificación o destrucción no autorizada de los datos.

6.2. Protección de datos personales

Se deberá cumplir lo estipulado en la ley orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, adaptada al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y por el que se deroga la Directiva 95/46/CE(Reglamento General de Protección de Datos), incluyendo lo dispuesto en la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre y en el Real Decreto 3/2010, de 8 de enero.

Conforme a la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Medidas de seguridad en el ámbito del sector público, las medidas de seguridad a aplicar en el marco de los tratamientos de datos personales se corresponderán con las de la Administración púbica de origen y se ajustarán al Esquema Nacional de Seguridad.

Se requerirá a INDRA SOLUCIONES TECNOLOGÍAS DE LA INFORMACIÓN, SLU la manifestación expresa del sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos conforme a los artículos 35.1d y 122.2 de la LCSP modificado por artículo 5 del Real Decreto Ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

6.3. Seguridad

INDRA SOLUCIONES TECNOLOGÍAS DE LA INFORMACIÓN, SLU implementará las medidas técnicas y organizativas de seguridad apropiadas y elaborará la

[redacted]

documentación pertinente, de acuerdo con el correspondiente análisis de riesgos, según lo establecido en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica.

7. PROPIEDAD INTELECTUAL

Sin perjuicio de lo dispuesto en la legislación vigente en materia de propiedad intelectual, el adjudicatario acepta expresamente que la propiedad de todos los productos que sean elaborados por el adjudicatario, incluidos sus empleados y en su caso cualquier empresa subcontratada, en ejecución del Contrato y, en particular, todos los derechos de propiedad intelectual y/o industrial que deriven de los mismos, corresponde únicamente a la administración contratante, con exclusividad y sin más limitaciones que las que vengan impuestas por el ordenamiento jurídico.

A los efectos previstos en el párrafo anterior, la empresa adjudicataria se compromete a la entrega a la SGAD de toda la documentación técnica, trabajos y materiales generados, en cuyo poder quedarán a la finalización del Contrato sin que el contratista pueda conservarla, ni obtener copia de la misma, ni utilizarla o facilitarla a terceros sin la expresa autorización de la SGAD, que la daría, en su caso, previa petición formal del contratista con expresión del fin.

8. CUANTIFICACIÓN ECONÓMICA DEL PRESUPUESTO

El presupuesto máximo de la contratación será de 273.171,50€ IVA excluido, 330.537,52€ IVA incluido, con cargo a la aplicación presupuestaria 22.03.467G.640.06 del actual ejercicio presupuestario.

Este presupuesto se ha estimado sobre la base de los siguientes elementos:

Piloto para el rastreo de contactos	**Uds**	**Precio unitario (sin IVA)**	**Importe sin IVA**
Pre-piloto			
Sistema mínimo viable para piloto (App y Backend)	1		114.278,00
Experiencia de usuario (UX)	1		27.133,00
Piloto			
Evolución y soporte piloto	1		43.847,00
Post-piloto			
Evolución y soporte (variable)	905 horas	58,10	52.580,50
Infraestructura en la nube (cloud)			
Servicios de infraestructura (coste primer mes)	1		9.733,00

[redacted]

Servicios de infraestructura piloto (coste meses segundo a quinto)	4 meses	6.400,00	25.600,00

TOTAL 273.171,50

9. PLAZO DE EJECUCIÓN Y PAGO DEL SERVICIO

La duración total prevista del contrato es de un máximo de cinco meses a partir del 1 de junio, o fecha de adjudicación definitiva si ésta fuera posterior.

La facturación se realizará en un único pago a la finalización del servicio por todos los conceptos fijos y por el número de unidades efectivamente consumidas de los conceptos variables, según los cuadros que se adjuntan, aplicando el 21% de IVA al importe resultante:

Conceptos fijos por importe unitario	**Importe unitario sin IVA**
Sistema mínimo viable para piloto (App y Backend)	114.278,00
Experiencia de usuario (UX)	27.133,00
Evolución y soporte piloto	43.847,00
Servicios de infraestructura cloud – primer mes	9.733,00

Conceptos variables por importe unitario	**Número máximo de unidades (1)**	**Importe unitario sin IVA**
Evolución y soporte (variable)	905 horas	58,10
Servicios de infraestructura cloud (meses segundo a quinto)	4	6.400,00

(1) Solo podrá facturarse un número entero de unidades

EL SUBDIRECTOR GENERAL DE IMPULSO
DE LA DIGITALIZACIÓN DE LA ADMINISTRACIÓN

Santiago Graña Domínguez

[redacted]

ANEXO I. CARACTERÍSTICAS DEL SISTEMA

APLICACIÓN MÓVIL

1. Inicio y bienvenida aplicación: aviso legal, onboarding informativo, activación de seguimiento Bluetooth. Uso de SDK Google/Apple anónimo y redirección a repositorio genérico (Backend).
    a. Permite al usuario la transmisión y recepción de identificadores aleatorios a través del Bluetooth
    b. Verificación del código de autorización por parte de la autoridad sanitaria ante positivo por COVID-19. De cara al piloto, como es previsible que no se disponga del servicio de la autoridad sanitaria se simulará la validación del positivo que desencadene el proceso de tracing y se pueda pilotar.
    c. Envía al servidor su baliza generadora de claves efímeras en caso de positivo.
    d. Pantallas estáticas informativas.
    e. Interacción con el SDK google/apple, de acuerdo a la funcionalidad proporcionada:
        i. Gestionar las claves aleatorias diarias:
            1. Generar diariamente las claves de exposición temporales y rotar los identificadores efímeros basados en ellos.
            2. Proveer las claves al Backend para usuarios diagnosticados, incluyendo los valores temporales.
            3. Acepta las claves de la App para la detección de exposición, incluyendo las fechas y los niveles de riesgo de transmisión.
            4. Almacena claves en el dispositivo.
        ii. Gestionar el envío y escaneo Bluetooth:
            1. Gestión del envío de claves.
            2. Escanea claves emitidas por otros dispositivos.
            3. Almacenar las claves observadas en un almacenamiento en el dispositivo.
            4. Identificar cuando otro usuario en contacto ha sido un caso confirmado.
            5. Calcular y proveer el riesgo de exposición a la aplicación.
            6. Presentar las siguientes peticiones de permiso al usuario:
                a. Antes de empezar a escanear y enviar las claves.

b. Antes de proveer al servidor las claves al servidor central tras haber sido contagiado.

2. Comunicación de casos positivos:
    a. Introducción QR/código COVID-19 (manual, escáner o importación) personal y de uso único.
    b. Aviso confirmación QR validado positivo: pantalla informativa.
    c. Cuestionario opcional (en caso de positivo): recoge datos anónimos básicos para su tratamiento Backend App (código postal, sintomatología y su fecha, patologías previas,…).
3. Notificación de riesgo: aviso de contacto con positivo confirmado y pantalla de recomendaciones.
4. Salida de la aplicación: posibilidad de salida de la aplicación en cualquier momento, eliminando cualquier rastro de claves efímeras utilizadas.

ELEMENTO BACKEND EN INFRAESTRUCTURA PÚBLICA

1. Gestión de datos en Backend
    a. Servir información necesaria para funcionamiento de la App (si se estima necesario. Alternativamente la App puede ser autocontenida).
    b. Validación con el sistema de autorización sanitaria ante diagnósticos positivos (si este sistema no estuviera disponible se realizaría una Simulación de esta validación). La aplicación debe comunicarse con un servidor externo (sanitario) que provea el código de autorización que confirme el positivo y pueda autorizar a subir las balizas al servicio en función del siguiente ciclo propuesto:
        i. Sistema médico solicita token/QR autenticación al Backend para confirmar positivo COVID-19.
        ii. Paciente recibe token/QR autenticación para confirmar el positivo COVID-19.
        iii. Paciente envía el token/QR autorizado al Backend para subir su histórico de contactos.

        Como es previsible que no se disponga del servicio de la autoridad sanitaria en el alcance inicial se simulará la validación del positivo que desencadene el proceso de tracing para que se pueda probar su funcionamiento.
    c. Base de datos con servicio de información centralizada que permita el rastreo de contactos y la gestión de balizas.
        i. Recolectar las balizas de los usuarios que hayan sido diagnosticados de COVID-19.

[redacted]

i. Distribuir las balizas de los casos confirmados hacia los dispositivos.

ii. Integración servicio de autorización de positivos.

iii. Integración con sistemas Terceros. Estudio de la interoperabilidad con Backends de otros Estados para asegurar funcionalidad transfronteriza.

2. Seguridad

   a. Implantación de controles para prevenir ataques específicos a nivel de aplicación.

   b. Securización comunicaciones con otros dispositivos y con sistemas sanitarios.

   c. Anonimización de señales entre dispositivos.

3. Simulación: capacidad de emular respuesta COVID-19 positivo, a efectos de testing (testear comportamiento de tracing).