



**PLIEGO DE CONDICIONES TÉCNICAS
PARA LA CONTRATACIÓN DE UNA
PLATAFORMA LLAVE EN MANO PARA
LA GESTIÓN DEL TRANSPORTE
SANITARIO**

INDICE

1. INTRODUCCIÓN.....	3
2. OBJETO.....	3
3. REQUISITOS FUNCIONALES.....	3
4. REQUERIMIENTOS TÉCNICOS	13
5. DEFINICIÓN DE TECNOLOGÍAS.....	22
6. INTEGRACIÓN CON SISTEMAS DE INFORMACIÓN.....	22
7. ASPECTOS RELATIVOS A LA SEGURIDAD.....	24
8. ENTORNO DE MOVILIDAD.....	25
9. SOPORTE Y MANTENIMIENTO	25
10. PLAN DE FORMACIÓN.....	27
11. PLANIFICACIÓN	28
12. SEGUIMIENTO DEL CONTRATO	29
13. DOCUMENTACIÓN TÉCNICA	29
14. LICENCIAMIENTO.....	29
15. MEMORIA TÉCNICA DISPOSITIVOS MÓVILES A SUMINISTRAR (LOTE 2).....	30
16. SOPORTE DE DISPOSITIVOS MÓVILES.....	31

1. INTRODUCCIÓN

La Sociedad Pública BIDEAN va a asumir la responsabilidad y gestión del transporte sanitario de la Comunidad Foral de Navarra.

Para la correcta ejecución de dicho cometido se necesita un sistema de gestión llave en mano que incluya todo el proceso de solicitudes, traslados, rutas, stocks, etc.

Deberá incluirse en la oferta todo el software, dispositivos móviles (formato tablet) y servicios necesarios para la puesta en marcha de la solución.

2. OBJETO

El objeto del contrato es el suministro llave en mano del desarrollo, licenciamiento necesario, dispositivos móviles definidos, formación de usuarios, soporte y mantenimiento de la solución completa para el Transporte Sanitario.

La oferta deberá ofrecer los siguientes servicios:

- Desarrollo e implantación de la solución.
- Aprovisionamiento de los dispositivos móviles ubicados en las ambulancias.
- Servicio de mantenimiento y soporte hardware y software.
- Formación a usuarios y a técnicos IT.
- Integración con diferentes productos utilizados por BIDEAN o Gobierno de Navarra

3. REQUISITOS FUNCIONALES

La plataforma de gestión integral debe englobar todas las necesidades y requisitos que a continuación se definen:

1. *Gestión de pacientes y trazabilidad*

- a. Registro y Datos de los Pacientes. El software debe incluir un módulo de gestión de usuarios que permita la captura de los siguientes datos de los pacientes:
 - i. Nombre completo y DNI.
 - ii. Datos de filiación, incluyendo NASS, CIP y CIPNA
 - iii. Fecha de nacimiento, sexo y domicilio habitual.
 - iv. Teléfonos de contacto y un campo para anotaciones relevantes.
- b. Trazabilidad del Paciente. Debe existir un sistema de trazabilidad que permita:
 - i. El seguimiento del histórico de tratamientos de cada paciente.
 - ii. La visualización de todos los traslados realizados.
 - iii. La gestión y documentación de incidencias o reclamaciones en las que el paciente haya estado involucrado.

2. Procesamiento de Solicitudes de Traslado

El sistema debe posibilitar la introducción y gestión de solicitudes de traslado a través de múltiples vías:

- a.** De manera manual directamente desde la aplicación.
- b.** A través de una interfaz web telemática destinada a los centros, que incluirá:
 - i.** Un circuito de validación de la prescripción médica que requiere la aprobación por parte de un facultativo antes de proceder a la fase de planificación.
 - ii.** Dicho circuito deberá adaptarse a distintos perfiles de usuarios, incluyendo un perfil con autorización para validar los traslados sugeridos por los usuarios de su área.
 - iii.** En todos los casos, se priorizará la agilidad de gestión, habilitando un formulario único donde se recopilen los datos esenciales del paciente, los detalles específicos del traslado y la información sobre la recurrencia del mismo cuando sea pertinente.
 - iv.** El sistema digital de acceso a la plataforma deberá ser mayoritario.
- c.** Capacidad de integrarse con aplicaciones del sistema navarro de salud, con la única finalidad de confirmar la cita a través del TOKEN

3. Coordinación de Traslados y Acciones

- a.** El sistema deberá contar con un módulo de coordinación que gestione las diferentes acciones a tomar en el proceso de traslado, permitiendo:
 - i.** Asignación, reasignación y anulación de traslados, tanto agrupados como individuales, basándose en la optimización de rutas y recursos disponibles.
 - ii.** Interacción en tiempo real con el personal de coordinación para la toma de decisiones basadas en la prioridad, urgencia y eficiencia del servicio.
 - iii.** Capacidad para enviar directamente al vehículo o flota de vehículos la información del traslado o traslados, de manera individual o agrupada por rutas ya planificadas.
 - iv.** Comunicación bidireccional entre la central de coordinación y los vehículos para la transmisión de órdenes de servicio y la confirmación de su aceptación o rechazo.
 - v.** Debe integrar mensajería instantánea con los vehículos.
- b.** Herramientas para el seguimiento en tiempo real de cada traslado, que incluyan:
 - i.** Visualización de la ubicación de los vehículos en tiempo real a través de GPS.
 - ii.** Alertas y notificaciones sobre el estado de los traslados, incluyendo retrasos, llegadas anticipadas o cualquier desviación del plan de traslado.
 - iii.** Registro y reporte de los tiempos de respuesta, tiempos de viaje y tiempos de espera para análisis de rendimiento y mejora continua.

- c. Sistema de Alertas y respuestas automáticas. Implementación de un sistema de alertas que notifique automáticamente a los coordinadores y conductores sobre actualizaciones críticas o cambios en las condiciones del servicio.
- d. Análisis y Reportes.
 - i. Capacidad de generar reportes detallados sobre la coordinación de traslados, incluyendo análisis de tiempos de ciclo completos desde la solicitud hasta la finalización del servicio.
 - ii. Herramientas analíticas para evaluar la eficacia de las acciones tomadas y las interacciones con los vehículos, orientadas a la mejora de la calidad del servicio.
 - iii. Exportación de datos para realizar analítica de los traslados, con filtros por diferentes KPI (terapias, tipos de traslado, tipo de ambulancia, origen, destino, personal asignado...)

4. Planificación

- a. Sistema de Ayuda a la Planificación: El sistema contará con una herramienta que ayude a los usuarios a configurar diariamente las rutas fijas de pacientes (dejando, en la medida de lo posible, espacio en los vehículos para articular el grueso de la actividad no prevista en esas rutas). Este sistema permitirá:
 - i. Copiar por defecto la asignación del día o semana anterior.
 - ii. Si surge un servicio, o servicios nuevos, recomendar la mejor ruta fija para añadirlo teniendo en cuenta horarios, tráfico previsto, etc.
 - iii. Tener en cuenta, en la configuración de la ruta, la configuración de vehículos en función de la tipología de pacientes.
 - iv. Una vez configurada la ruta ordenarla de la forma más eficiente teniendo en cuenta horarios y tráfico.
- b. Sistema de optimización de rutas: Permite optimizar rutas de “X” servicios entre “Y” recursos sin utilizar variables de configuración de carga de los vehículos. Entre las variables utilizables en el optimizador se encuentran:
 - i. Ventanas de tiempo (franjas horarias entre las que deben ejecutarse los servicios).
 - ii. Coste de espera (permite minimizar o no el coste de espera de cada recurso permitiendo soluciones con más o menos recursos).
 - iii. Coste de recorrido (permite priorizar unos recursos frente a otros).
 - iv. Habilidades: Permite limitar que recursos realizar determinada tipología de servicio.

La optimización utiliza algoritmos de distinta naturaleza ofreciendo, en función de las variables de entrada, un escenario óptimo de distribución de los “X” servicios a realizar entre los “Y” recursos disponibles.

El resultado puede analizarse y modificarse manualmente antes de guardarse como escenario real.

- c. Sistemas que faciliten el trabajo de los coordinadores, proponiendo rutas y alternativas con el fin de mejorar los procesos.
- d. Se valorará innovación en uso de herramientas y capacidad para generar reportes detallados (en varios formatos Excel, pdf, acces) y análisis predictivos que faciliten la toma de decisiones y la planificación estratégica.
- e. Herramientas de visualización de datos que permitan un fácil seguimiento de los indicadores clave de rendimiento (KPIs) y de la eficacia del sistema.

5. Control y Seguimiento de la Flota

- a. El software debe integrar un sistema de localización GPS que proporcione la ubicación en tiempo real de cada vehículo de la flota.
- b. Visualización del estado actual de las unidades incluyendo:
 - i. Servicios adjudicados y en curso.
 - ii. Información del personal asignado a cada vehículo.
 - iii. Horarios y planificación de tareas pendientes.
- c. Integración de datos de tráfico en tiempo real para facilitar la planificación y adaptación de rutas.
- d. Visualización de incidencias de tráfico, como accidentes o congestiones, que puedan afectar la eficiencia del servicio.
- e. Funcionalidad para delimitar zonas geográficas específicas y clasificar vehículos por categorías o asignaciones.
- f. Capacidad para alternar rápidamente entre diferentes visualizaciones y enfoques de seguimiento según la necesidad operativa.
- g. El sistema debe mostrar claramente la ubicación de los centros de destino.
- h. Indicadores gráficos de los lugares de recogida programados para cada traslado, mejorando la visión general de la planificación de la actividad.
- i. Herramientas para extraer y consultar un registro completo del histórico de acciones y movimientos de cada vehículo.
- j. Capacidad para realizar un seguimiento exhaustivo y detallado de la actividad pasada, para fines de auditoría y mejora de procesos.
- k. Implementación de un sistema externo de alertas proactivo para monitorear y notificar eventos críticos en tiempo real, tales como:

- i. Aceleraciones bruscas y situaciones de conducción agresiva.
 - ii. Excesos de velocidad y otros incumplimientos de las normativas de tráfico.
 - iii. Niveles bajos de combustible que puedan requerir una atención inmediata.
 - iv. Activación de señales acústicas o luminosas de emergencia.
 - v. Configuración personalizable de los umbrales y parámetros que disparan las alertas.
- l. La interfaz de usuario debe ser intuitiva y fácil de utilizar, permitiendo a los operadores gestionar y supervisar eficientemente toda la flota.
 - m. Posibilidad de acceder a la información y las funciones de seguimiento desde dispositivos móviles para facilitar la gestión en movimiento.
 - n. El módulo de gestión de la flota debe incluir herramientas para la revisión de los recorridos de las rutas planificadas por la coordinación, permitiendo una visión detallada de cada itinerario antes de ser ejecutado.
 - o. El sistema estará equipado con capacidades analíticas para identificar ineficiencias en el orden de las rutas, como desviaciones innecesarias, redundancias o posibles conflictos de horario.
 - p. Funcionalidad de optimización que permita realizar ajustes y correcciones a las rutas antes de que sean finalizadas y enviadas a los conductores de los vehículos.

6. Interacción con Usuarios del Servicio (Pacientes)

- a. Implementación de un sistema de notificaciones que envíe automáticamente un SMS/Whatsapp al paciente con la hora estimada de recogida y la hora de activación real del servicio.
- b. Cada SMS/Whatsapp incluirá un enlace directo (puede ser a través de una app específica) a una aplicación web segura para que el paciente pueda realizar acciones adicionales:
 - i. Permitirá a los pacientes validar la información personal registrada y, si fuera necesario, solicitar correcciones de manera sencilla y rápida.
 - ii. Garantizar la conformidad con las regulaciones de protección de datos durante el proceso de validación y actualización de información personal.
 - iii. Los pacientes tendrán acceso a un histórico completo de todos los traslados realizados por la empresa, con detalles como fechas, horarios y destinos. Esta funcionalidad proporcionará transparencia y facilitará la gestión de futuros traslados o consultas relativas a servicios pasados.
 - iv. Opciones para que los pacientes soliciten servicios de retorno de forma sencilla.
 - v. Posibilidad de solicitar un contacto telefónico directo con la central de coordinación en caso de requerir asistencia personalizada.
 - vi. Una vez activado el servicio, la aplicación web dará la posibilidad de mostrar en un mapa la ubicación en tiempo real de la ambulancia asignada, proporcionando al paciente una estimación visual del tiempo de llegada del vehículo.

- vii. Inclusión de un buzón de sugerencias dentro de la aplicación web para que los usuarios puedan compartir sus opiniones y propuestas de mejora.
- viii. Sistema de encuestas integrado para recopilar feedback de los pacientes respecto a su experiencia con el servicio, contribuyendo así a los procesos de gestión de la calidad y mejora continua.
- ix. Ofrecer la posibilidad de valorar el servicio inmediatamente después de la realización del traslado para capturar impresiones frescas del servicio recibido.
- x. Facilitar la sincronización con calendarios electrónicos personales para que los pacientes puedan tener un seguimiento integrado de sus traslados y citas médicas.
- xi. Se valorará incluir opciones de asistencia en línea y chat en vivo para ayudar a los pacientes con dudas o problemas en tiempo real.
- xii. La interfaz de la aplicación web debe ser intuitiva, fácil de usar y accesible para personas con diferentes niveles de habilidad tecnológica.
- xiii. Diseño responsivo que asegure la correcta visualización y funcionalidad en diferentes dispositivos, como smartphones, tabletas y computadoras de escritorio.
- xiv. Asegurar la confidencialidad y seguridad de la información del paciente en todas las fases del proceso de notificación y uso de la aplicación web.
- xv. El sistema debe cumplir con las normativas vigentes en materia de seguridad de la información y protección de datos personales.

Este conjunto de requerimientos busca ofrecer una experiencia de usuario centrada en el paciente, aumentando la confianza en el servicio y mejorando la comunicación y satisfacción general del usuario. La transparencia, la facilidad de acceso a la información y la capacidad de interacción directa son pilares fundamentales de este módulo de interacción con los usuarios.

7. Gestión de Stock y Almacenes

- a.** El software debe poder considerar cada ambulancia como un almacén individual, permitiendo una gestión de inventario detallada y específica para cada una.
- b.** Capacidad para gestionar múltiples almacenes físicos y virtuales, facilitando el seguimiento centralizado del stock de material médico y operativo.
- c.** Funcionalidad para definir y mantener un stock mínimo requerido para cada artículo en las ambulancias, asegurando así la disponibilidad ininterrumpida de material esencial.
- d.** La aplicación debe permitir la personalización de los niveles mínimos de stock según las necesidades específicas de cada unidad de la flota.
- e.** Implementar herramientas para realizar revisiones de stock automatizadas vinculadas directamente a las inspecciones regulares de las ambulancias.
- f.** Generación de avisos automáticos cuando el inventario de un artículo específico caiga por debajo del umbral mínimo establecido.

- g.* Sistema de rastreo que permita seguir la vida útil de los artículos críticos, como medicamentos y equipamiento médico, para asegurar su uso dentro de los periodos de validez.
- h.* Función de trazabilidad para rastrear el movimiento de stock entre diferentes almacenes y ambulancias.
- i.* Controles de seguridad para restringir el acceso a la gestión de inventario basados en roles y responsabilidades.
- j.* Sistema de alertas en caso según el nivel de criticidad.
- k.* Accesibilidad a la gestión de inventarios a través de tabletas o similar permitiendo a los empleados realizar revisiones y gestionar stock desde cualquier ubicación.

8. Aplicación para Dispositivos Embarcados en Ambulancias

a. Gestión de Traslados y Estados:

- i.* Interfaz intuitiva para la gestión de los traslados, incluyendo la creación, seguimiento y actualización de diferentes estados del servicio: pendiente, en curso, en origen, evacuado, en destino, completado o cancelado.
- ii.* Visualización clara y actualización en tiempo real del estado de los traslados para la coordinación efectiva con la central.
- iii.* Funcionalidad integrada para que los trabajadores puedan fichar su entrada y salida directamente desde la aplicación.
- iv.* Registro de pausas y tiempos de descanso para cumplir con las normativas laborales sobre jornadas de trabajo.
- v.* Opción para crear y gestionar checklists personalizables según el tipo de unidad de la ambulancia, asegurando que todos los procedimientos preoperatorios sean completados.

b. Control de Repostajes y Gastos:

- i.* Sistema para registrar y controlar los repostajes de combustible, incluyendo fecha, hora, cantidad, coste y kilómetros.
- ii.* Gestión de otros gastos asociados con la operación de la ambulancia para una contabilidad detallada y seguimiento de costos.
- iii.* Registro de paradas de la dotación tales como los desayunos, almuerzos o cenas.
- iv.* Registro de todas las paradas no programadas, con motivos y duración, para analizar su impacto en la eficiencia del servicio.

c. Mensajería Instantánea propia:

- i.* Implementación de un sistema de mensajería instantánea integrado para una comunicación fluida y segura entre el personal de las ambulancias y la central de coordinación.
- ii.* Notificaciones y alertas en tiempo real para informar al personal sobre actualizaciones importantes o cambios en la planificación.

d. Navegador Integrado:

- i.* Inclusión de un sistema de navegación adaptado a las necesidades de los traslados, con información sobre rutas óptimas, tráfico y estimaciones de tiempo de llegada.
- ii.* Capacidad para recibir actualizaciones de ruta en tiempo real desde la central de coordinación.

9. Cuadro de Mando Integral

Implementación de un cuadro de mando con flujo de datos en tiempo real idealmente en un formato PowerBi o similar, que permita su acceso y visualización desde cualquier dispositivo. Debe abarcar todas las áreas de gestión de la empresa, y permitir una personalización completa y mejora continua, para cumplir con las necesidades cambiantes de la entidad.

- a.** El cuadro de mando debe proporcionar un flujo de información actualizado en tiempo real, permitiendo la visualización instantánea de datos operativos, financieros y de recursos humanos.
- b.** La interfaz del cuadro de mando debe ser accesible y completamente funcional en una variedad de dispositivos, incluyendo computadoras de escritorio, laptops, tablets y smartphones.
- c.** Debe seguir un diseño responsivo que se adapte automáticamente al tamaño y resolución de la pantalla del dispositivo utilizado.
- d.** Debe incluir indicadores clave de rendimiento (KPIs) y métricas de todas las áreas de gestión de la empresa, como operaciones, finanzas, recursos humanos, atención al cliente, logística y mantenimiento.
- e.** Posibilidad de personalizar los paneles para enfocar en áreas específicas según las necesidades de diferentes usuarios o departamentos.
- f.** La interfaz debe ser intuitiva y fácil de usar, permitiendo a los usuarios navegar, filtrar y profundizar en los datos específicos sin necesidad de formación técnica avanzada.
- g.** Inclusión de gráficos interactivos, tablas y widgets que faciliten la interpretación de los datos y la toma de decisiones.
- h.** Integración de Datos:

- i.* Capacidad para integrarse con diversas fuentes de datos, tanto internas como externas, asegurando una visión unificada de la información.
- ii.* Debe soportar la integración con sistemas de gestión de la empresa, bases de datos, aplicaciones en la nube y otras plataformas relevantes.
- iii.* Sistema de alertas configurable para notificar a los usuarios sobre eventos críticos o desviaciones significativas en los KPIs.
 - Las notificaciones pueden ser enviadas por email, SMS o directamente dentro de la plataforma.
- iv.* La solución debe ser escalable para adaptarse al crecimiento de la empresa y al aumento del volumen de datos.
- v.* Debe incluir soporte técnico para la resolución de problemas y asistencia en la configuración y personalización del cuadro de mando.

10. Requerimientos Técnicos del Software: Seguridad y Trazabilidad

- a.** Sistema de Registro de Actividades (Logs):
 - i.* Implementación de un sistema de logs completo que registre todas las acciones realizadas dentro del sistema, incluyendo accesos y modificaciones de datos.
 - ii.* Los registros deben contener información detallada como el identificador del usuario, la acción realizada, la fecha y hora, y la dirección IP del dispositivo utilizado.
- b.** Gestión de Perfiles de Operadores:
 - i.* El software debe permitir la creación de perfiles de operadores con diferentes niveles de acceso y permisos personalizados, según el rol que se le asigne (Bidean, Osasunbidea, empresas externas) y subroles en cada uno de los roles principales.
 - ii.* Capacidad para definir políticas de seguridad granulares que controlen la visibilidad y modificación de datos por perfil.
- c.** Restricciones de Acceso a Datos Sensibles:
 - i.* Restricciones estrictas para proteger el acceso a información sensible y personal, asegurando que solo el personal autorizado pueda ver o modificar dichos datos.
- d.** Auditoría y Trazabilidad:
 - i.* Herramientas de auditoría que permitan la revisión de los registros de actividad para detectar y analizar cualquier comportamiento anómalo o inseguro.
 - ii.* Trazabilidad completa de las modificaciones de datos para cumplir con regulaciones de responsabilidad y gestión de información.
- e.** Control de Funciones Según Perfiles:
 - i.* Asignación de permisos que restrinjan o permitan el uso de funciones específicas de la aplicación basándose en los roles de los operadores.

- ii.* Posibilidad de personalizar el entorno de trabajo de cada perfil para simplificar la operativa y mejorar la eficiencia.
- f.* Sistema de Autenticación y Autorización:
 - i.* Implementación de mecanismos de autenticación robustos, preferiblemente de múltiples factores (MFA), para verificar la identidad de los usuarios.
 - ii.* Un sistema de autorización para conceder o negar permisos basado en roles, asegurando que cada operador tenga acceso solo a las áreas permitidas.
- g.* Cifrado de Datos:
 - i.* Cifrado de datos tanto en tránsito como en reposo para proteger la información contra interceptaciones o accesos no autorizados.
 - ii.* Utilización de protocolos de seguridad estándar del sector, como TLS/SSL, para el cifrado de datos en tránsito.
- h.* Políticas de Seguridad y Cumplimiento:
 - i.* El sistema debe adherirse a las políticas de seguridad corporativas y cumplir con los estándares y regulaciones pertinentes como GDPR, HIPAA, o equivalentes nacionales.
 - ii.* Procedimientos para la gestión regular de las políticas de seguridad, incluyendo revisiones y actualizaciones según sea necesario.
- i.* Prevención de Pérdida de Datos:
 - i.* Herramientas para prevenir la pérdida de datos, incluyendo copias de seguridad automáticas y redundancia de sistemas.
 - ii.* Planes de recuperación ante desastres y continuidad del negocio en caso de incidentes de seguridad.
- j.* Actualizaciones y Parches de Seguridad:
 - i.* Proceso establecido para la aplicación regular de actualizaciones y parches de seguridad para el software y las plataformas subyacentes.
 - ii.* Evaluaciones de seguridad periódicas para identificar y mitigar vulnerabilidades potenciales.

11. Pruebas y Calidad

- a.* Se deben establecer protocolos de pruebas rigurosas para garantizar la calidad del software, incluyendo pruebas unitarias, de integración, funcionales y de seguridad.
- b.* Se debe facilitar la trazabilidad desde los requisitos hasta las pruebas para garantizar que todas las funcionalidades y requisitos de seguridad estén cubiertos.

12. Integración y Escalabilidad del Sistema

- a. Se requiere que el sistema esté diseñado para admitir integraciones futuras con los sistemas informáticos del sistema de salud Navarro, garantizando así la escalabilidad y actualización del sistema a largo plazo.

13. Control de calidad asistencial

- a. Se deben establecer un sistema digital para la realización de la revisión mecánica y la parte asistencial en ambulancias de urgencia y programado, integrada los puntos de solución (mecánico, stock, electromedicina,...)
- b. Parte asistencial para las ambulancias de urgencias/programadas con el fin de poder dejar constancia de la situación clínica del paciente y modificaciones durante el traslado.

4. REQUERIMIENTOS TÉCNICOS

La solución a entregar deberá implantarse en servidores on premise, por lo que todos los sistemas deben adaptarse al [Escenario Tecnológico del Gobierno de Navarra](https://gespublica.navarra.es/SistemasInformacionGN/) (publicado en <https://gespublica.navarra.es/SistemasInformacionGN/>), prestando especial atención a las características de la plataforma de comunicaciones (apartado II), a la infraestructura básica (III.1) y a los servicios de infraestructura común (III.2).

Se recomienda alojar los componentes del sistema de información en las plataformas descritas en la infraestructura genérica para sistemas de información (III.4) debido a su alto nivel de servicio.

Si se requiere mayor flexibilidad, también es posible alojar los componentes en servidores corporativos con sistema operativo gestionado (III.1) o, en última instancia, en máquinas virtuales del sistema de virtualización (III.2). Sin embargo, estas opciones implican un mayor costo y un nivel de servicio inferior para la organización.

Es importante destacar que todos los componentes web deberán ofrecerse a través de la Plataforma de publicación de aplicaciones en Internet e Intranet (III.4).

Además, el sistema de información puede utilizar otros servicios corporativos (III.3), servicios de infraestructura común (III.4) y plataformas (apartados IV a IX) bajo las condiciones especificadas en el escenario tecnológico.

Además, deberán cumplir los siguientes requisitos específicos para lo cual en cada oferta se entregará esta tabla completada junto a la propuesta técnica de conformidad con el modelo adjunto en el Anexo V del Pliego, donde constará la siguiente información:

Requisitos	Aceptación (Sí)
------------	-----------------

Todos los sistemas de información de servidor serán virtualizables y alojados en la plataforma de virtualización VMware de Gobierno de Navarra con las características y condiciones descritas en el Escenario Tecnológico del mismo.	
Los parámetros de red de los sistemas de información tanto para equipos servidor como cliente o equipo tipo <i>appliance</i> serán asignados por Gobierno de Navarra. Incluidos dirección IP (fija o DHCP), máscara de red, DNS y puerta de enlace. • Interfaz física: 1Gb mediante RJ45 o 10Gb mediante fibra óptica. • Estándar de red de área local: Ethernet. • Protocolo de red: TCP/IP.	
Los dispositivos que hagan uso de la red wifi utilizarán alguno de los siguientes estándares dependiendo de las características de los APs que doten de cobertura la ubicación: IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac o IEEE 802.11ax. A su vez, los dispositivos deberán soportar el método de autenticación WPA2/WPA3 Enterprise que utiliza el estándar IEEE 802.1X para autenticación de red basados en la estructura EAP (Protocolo de Autenticación Extensible) con un servidor RADIUS.	
Los cambios necesarios en los parámetros de red de los sistemas de información serán posibles durante toda la vida útil de los sistemas de información y estará debidamente documentada la ejecución de los mismos por parte del fabricante, instalador o proveedor. Los cambios en los parámetros de red de los sistemas de información necesarios durante el periodo de soporte, serán realizados por el proveedor del soporte sin ocasionar gastos a Gobierno de Navarra.	
Los sistemas de información estarán colocados en una VLAN asignada por Gobierno de Navarra, detrás de un cortafuegos aportado por Gobierno de Navarra y los cuales están descritos en el escenario tecnológico. La VLAN asignada podrá estar compartida con otros equipos del mismo u otros fabricantes.	
El acceso remoto a los sistemas de información únicamente será posible mediante las opciones tecnológicas que provee Gobierno de Navarra y que son: • Acceso VPN SSL mediante extranet con doble factor • VPN de sitio a sitio, pudiendo requerir portal de autenticación o doble factor	
Los sistemas e información basados en sistemas operativos Microsoft y RedHat Linux deberán disponer de un software Antimalware/antivirus instalado, licenciado y que se actualice automáticamente durante todo el tiempo que dure el soporte del mismo. Aun en los casos en que la operación y soporte del	

equipamiento la proporcione el proveedor, Gobierno de Navarra ofrece la inclusión de su sistema antivirus corporativo.	
Obligación de notificar al Responsable de Explotación de Gobierno de Navarra las vulnerabilidades, parches existentes o brechas de seguridad que puedan afectar a los sistemas de información según normativa vigente.	

Requisitos	Aceptación (Sí)
El sistema de información se monitorizará con las herramientas que forman parte del escenario de monitorización: • Centreon: Herramienta de monitorización de disponibilidad y rendimiento de infraestructuras y aplicaciones. • QRadar de IBM: Herramienta de tipo SIEM orientada a la recolección y monitorización de eventos de seguridad que permite garantizar el cumplimiento de normativas de seguridad.	
El sistema de información NO podrá usar <i>applets</i> de Java. El sistema de información no podrá usar la arquitectura de plugin de plataforma cruzada NPAPI en la que se basa entre otros el plugin de Java para exploradores web, ya que los navegadores modernos no soportan esta arquitectura. Esta restricción no afecta a las aplicaciones Java Web Start, solo afecta a los <i>applets</i>.	
Licenciamiento del software base. Las licencias de software base se adquirirán a nombre del BIDEAN con una duración ilimitada. Cuando el sistema de información se despliegue en los servidores corporativos, compartidos con varias aplicaciones más y con acceso restringido por parte del proveedor, no será necesario que se adquieran las licencias del sistema operativo, del servidor de aplicaciones o del gestor de base de datos. Si el sistema de información se despliega en servidores exclusivos, la empresa adjudicataria deberá aportar las licencias del sistema operativo, servidor de aplicaciones y gestor de base de datos (así como cualquier otro elemento software específico necesario) que se adapten a la infraestructura existente en Gobierno de Navarra, y siempre en las versiones, ediciones, y dimensionamiento (número de usuarios, procesadores, servidores, etc. licenciados) que se	

definan desde la Dirección General de Transformación Digital (en adelante DGTD) como necesarias y adecuadas, siempre de acuerdo al Escenario Tecnológico.	
Licenciamiento del producto. Las licencias del producto serán de tipo software.	
Usuarios y contraseñas: • Las cuentas de usuario de los sistemas de información deben ser nominales. No se permiten cuentas genéricas. • Si es posible los sistemas de información se integrarán en el Directorio Activo de Gobierno de Navarra y utilizarán usuarios dentro del mismo. • Política de contraseñas a aplicar en los sistemas de información y requerimientos de seguridad para todos los usuarios (está política no se aplica a usuarios de servicio, genéricos o de pruebas): ○ La contraseña debe tener una longitud mínima de ocho caracteres. o ○ Deben combinarse tres tipos distintos de caracteres elegidos entre mayúsculas, minúsculas, números y caracteres especiales: @ \$. ○ Se obliga a un cambio de contraseña inicial tanto cuando se realice la primera conexión a la red de Gobierno de Navarra como tras la restauración de la contraseña (cuando por olvido se solicite un cambio de contraseña y sea asignada una provisionalmente, esta deberá ser sustituida inmediatamente para que cumpla los requisitos anteriores). ○ Se obliga al cambio de contraseña cada 30 días. El equipo integrado en dominio avisa al usuario cinco días antes de que caduque la contraseña. ○ No se pueden reutilizar las últimas 24 contraseñas. ○ La cuenta de usuario será desactivada si no se utiliza durante 90 días. Para volver a entrar a la red debe solicitar la activación de la cuenta.	

○ No se permitirán palabras en cualquier idioma, secuencias lógicas deducibles, permutaciones sencillas, ni secuencias de teclado. ○ La política de contraseñas deberá adaptarse a futuro a cualquier evolución que pueda requerirse por normativa o por política de Gobierno de Navarra	
---	--

Además, la propuesta que se presente en la oferta contendrá la respuesta a los siguientes apartados:

Requerimientos	
Necesidad de adquisición de Infraestructura. El proveedor deberá detallar la infraestructura servidora y puesto cliente necesaria para soportar su propuesta.	
Dimensionamiento de los sistemas de información:	
CPU (nº de núcleos)	
Memoria (GB)	
Disco (GB)	
Sistema gráficos (resolución)	
Puertos de entrada y salida	
Periféricos	
Almacenamiento externo	
Latencia	
Rendimientos (<i>Throughputs</i>)	
Sistema operativo	
Software específico	
Se detallarán al máximo los requisitos y especificaciones en cuanto a previsión de crecimiento y se entregará un plan de capacidad durante la vigencia del contrato. (Especificar documento y página de la oferta donde se especifica)	

Bidean/Nasertic definirán la necesidad de realizar copias de seguridad de los sistemas de información indicando los parámetros necesarios de tipo de copia, periodicidad y retención. Tendrá en cuenta lo siguiente: • Se realizan sobre la infraestructura servidora de Gobierno de Navarra. Las estaciones de los usuarios no se respaldarán (aunque pueden existir excepciones tras un estudio previo entre gestión de copias y el responsable de la información de la estación). • Sistemas operativos vigentes en el escenario tecnológico de Gobierno de Navarra. • Software base vigente en el escenario tecnológico de Gobierno de Navarra (Especificar documento y página de la oferta donde se especifica)	
El acceso a Internet de los sistemas de información se verá limitado sólo a aquello estrictamente necesario y justificado (listas blancas). Se deberán definir los accesos necesarios a Internet, especificando las <i>URLs</i> de destino y los puertos necesarios. Gobierno de Navarra se reserva el derecho a no aceptar accesos a Internet de los sistemas de información si los considera un riesgo innecesario. (Especificar documento y página de la oferta donde se especifica)	
Los accesos de los sistemas de información a los recursos de la red corporativa de Gobierno de Navarra se verán limitados a sólo a aquello estrictamente necesarios y justificados (listas blancas). Se deberán definir los accesos necesarios a los recursos internos en la propuesta. (Especificar documento y página de la oferta donde se especifica)	
No se permitirá la conexión a Internet de los sistemas de información por métodos distintos a los autorizados por Gobierno de Navarra. Se definen estos métodos de conexión en equipos como encaminadores 3G/4G, encaminadores ADSL, tarjetas SIM, etc. En cada caso se deberá evaluar y autorizar la solución por lo que se deberá especificar en la propuesta si existe alguno de estos dispositivos junto con una evaluación de riesgos para poder ser evaluado y autorizado si corresponde. (Especificar documento y página de la oferta donde se especifica, en caso de que existan)	

Por regla general no se permite el <i>autologon</i> en los sistemas de información y los servicios de aplicación de los sistemas de información tienen que poder ejecutarse sin haber iniciado sesión. En caso de que el sistema de información requiera <i>autologon</i>, se deberá especificar en la oferta y Gobierno de Navarra evaluará si se autoriza según los riesgos que se encuentren. (Especificar documento y página de la oferta donde se especifica, en caso de que existan)	
--	--

Requerimientos	
Es obligatorio realizar actualizaciones de seguridad y seguir una política al respecto. Como mínimo se seguirá la siguiente política de actualizaciones. En caso de justificar no poder seguir esta política se deberá presentar una política alternativa de actualizaciones de seguridad. Que será valorada por Gobierno de Navarra. Actualizaciones de seguridad en servidores Windows: - Las actualizaciones de seguridad incluidas son aquellas designadas por Microsoft como 'críticas' e 'importantes'. - Periodicidad mínima: con una cadencia trimestral se realizará una actualización a los servidores Windows de las actualizaciones de seguridad (parches) publicadas por el proveedor desde la última iteración del ciclo de parcheado. - Adicionalmente se establece la posibilidad de ejecutar actualizaciones extraordinarias sin atender a la cadencia trimestral establecida en el apartado anterior en el caso de la publicación de actualizaciones críticas cuyo impacto real en caso de explotación maliciosa pueda ser alto. Actualizaciones de seguridad en servidores Linux: - Periodicidad mínima: con una cadencia trimestral. El parcheo completo de un servidor Linux nuevo es parte obligatoria del despliegue. - Adicionalmente, se establece la posibilidad de ejecutar actualizaciones extraordinarias sin atender a la cadencia trimestral establecida en los apartados anteriores en el caso de la publicación de actualizaciones críticas cuyo impacto real en caso de explotación maliciosa pueda ser alto. Actualizaciones de seguridad de puesto de trabajo: - Con una cadencia trimestral, se realizará una distribución de software en los puestos de trabajo de las últimas actualizaciones de seguridad (parches) publicadas por los proveedores, con la particularidad de los productos Microsoft, que se incluirán aquellas publicadas en el mes anterior, para garantizar la estabilidad de las estaciones cliente. - Adicionalmente, se establece la posibilidad de ejecutar actualizaciones extraordinarias, sin atender a la cadencia trimestral establecida en el apartado anterior, en el caso de la publicación de actualizaciones críticas cuyo impacto real en caso de explotación maliciosa pueda ser alto. Actualizaciones de seguridad en <i>appliances</i> o con sistemas embebidos:	

• Para <i>appliances</i> que se encuentren en redes que ofrecen servicio <i>frontend</i> hacia Internet, la cadencia es mensual de la distribución de las actualizaciones de seguridad (erratas) publicadas por el proveedor. • Para el resto de <i>appliances</i> la cadencia es trimestral. • Adicionalmente, se establece la posibilidad de ejecutar actualizaciones extraordinarias sin atender a la cadencia trimestral establecida en los apartados anteriores en el caso de la publicación de actualizaciones críticas cuyo impacto real en caso de explotación maliciosa pueda ser alto. (Indicar la aceptación de la política de Gobierno de Navarra, o especificar la política de actualización detallando el documento y página de la oferta).	
--	--

Diseño Web adaptable

El sistema de información deberá estar convenientemente adaptado para su uso sin dificultad tanto en dispositivos móviles, como en teléfonos inteligentes y tablets, contando con un diseño web adaptable que garantice la correcta visualización y uso del sistema en dispositivos móviles.

Integración con sistemas de información

El sistema de información deberá tener capacidad para integrarse con diversas fuentes de datos, tanto internas como externas, asegurando una visión unificada de la información. (Ver apartado 6. Integración con sistemas de información).

Funcionalidades Técnicas del Software: Seguridad y Trazabilidad

- Sistema de Registro de Actividades (Logs):
Implementación de un sistema de logs completo que registre todas las acciones realizadas dentro del sistema, incluyendo accesos y modificaciones de datos.
Los registros deben contener información detallada como el identificador del usuario, la acción realizada, la fecha y hora, y la dirección IP del dispositivo utilizado.
- Gestión de Perfiles de Operadores:
El software debe permitir la creación de perfiles de operadores con diferentes niveles de acceso y permisos personalizados.
Capacidad para definir políticas de seguridad granulares que controlen la visibilidad y modificación de datos por perfil.
- Restricciones de Acceso a Datos Sensibles:
Restricciones estrictas para proteger el acceso a información sensible y personal, asegurando que solo el personal autorizado pueda ver o modificar dichos datos.
- Auditoría y Trazabilidad:

Herramientas de auditoría que permitan la revisión de los registros de actividad para detectar y analizar cualquier comportamiento anómalo o inseguro.

Trazabilidad completa de las modificaciones de datos para cumplir con regulaciones de responsabilidad y gestión de información.

- Control de Funciones Según Perfiles:

El sistema de información deberá permitir la asignación de permisos que restrinjan o permitan el uso de funciones específicas de la aplicación basándose en los roles de los operadores.

Posibilidad de personalizar el entorno de trabajo de cada perfil para simplificar la operativa y mejorar la eficiencia.

- Sistema de Autenticación y Autorización:

El sistema de información deberá tener implementado mecanismos de autenticación robustos, de múltiples factores (MFA), para verificar la identidad de los usuarios.

Un sistema de autorización para conceder o negar permisos basado en roles, asegurando que cada operador tenga acceso solo a las áreas permitidas.

- Cifrado de Datos:

Cifrado de datos tanto en tránsito como en reposo para proteger la información contra interceptaciones o accesos no autorizados.

Utilización de protocolos de seguridad estándar del sector, como TLS/SSL, para el cifrado de datos en tránsito.

- Políticas de Seguridad y Cumplimiento:

El sistema debe adherirse a las políticas de seguridad corporativas y cumplir con los estándares y regulaciones pertinentes como GDPR, HIPAA, o equivalentes nacionales.

Procedimientos para la gestión regular de las políticas de seguridad, incluyendo revisiones y actualizaciones según sea necesario.

- Prevención de Pérdida de Datos:

Herramientas para prevenir la pérdida de datos, incluyendo copias de seguridad automáticas y redundancia de sistemas.

Planes de recuperación ante desastres y continuidad del negocio en caso de incidentes de seguridad.

- Actualizaciones y Parches de Seguridad:

Proceso establecido para la aplicación regular de actualizaciones y parches de seguridad para el software y las plataformas subyacentes.

Evaluaciones de seguridad periódicas para identificar y mitigar vulnerabilidades potenciales.

5. DEFINICIÓN DE TECNOLOGÍAS

Uso de Tecnologías Modernas y Actualizadas:

- La plataforma debe ser desarrollada utilizando lenguajes de programación y sistemas que estén en la vanguardia tecnológica, asegurando la eficiencia, escalabilidad y seguridad del sistema. Las tecnologías elegidas deben ser ampliamente reconocidas y adoptadas en la industria para garantizar la compatibilidad y el soporte continuo.

Soporte Oficial de Tecnologías:

- Todos los componentes de software, incluyendo frameworks, bibliotecas y herramientas, deben tener soporte oficial activo en el momento de la implementación.

Compatibilidad Futura:

- La arquitectura de la plataforma y la elección de tecnologías deben considerar la compatibilidad futura con sistemas y estándares emergentes. Debe existir un compromiso de actualización continua para mantener la plataforma alineada con las últimas tendencias tecnológicas y de seguridad.

Seguridad y Actualizaciones:

- La plataforma debe incorporar mecanismos para la implementación rápida y segura de actualizaciones críticas, especialmente aquellas relacionadas con la seguridad. Debe existir un procedimiento claro para la aplicación de parches de seguridad y actualizaciones de software, minimizando el tiempo de exposición a vulnerabilidades conocidas.

6. INTEGRACIÓN CON SISTEMAS DE INFORMACIÓN

Los sistemas de información que formen parte de la solución ofertada por el Adjudicatario deberán integrarse con los sistemas de información del SNS-O de Gobierno de Navarra y con el ERP corporativo (Sigrid) utilizado en las Sociedades Públicas a la que pertenece BIDEAN, siendo responsabilidad del adjudicatario:

- El esfuerzo de integración desde su sistema de información.
- Las adecuaciones necesarias del software corporativo y propio del SNS-O que sean requeridas para garantizar las prestaciones actuales de los sistemas de información del SNS-O.

Estas adaptaciones no supondrán ningún coste directo ni repercutido a través de otros proveedores del SNS-O. El desarrollo será realizado por las empresas que la DGTD determine en cada momento, principalmente los adjudicatarios de sus contratos de mantenimiento.

Los interfaces de comunicación del sistema de información ofertado serán, preferiblemente, servicios web, tanto REST como SOAP. De manera excepcional, justificando su utilización en base a criterios concretos relativos a necesidades de disponibilidad, asincronismo o interoperabilidad tecnológica y siempre con el acuerdo expreso de BIDEAN, se podrán utilizar los siguientes tipos de interfaces de comunicación con sistemas externo:

- Ficheros de intercambio.
- Acceso directo a base de datos a través de tablas, vistas o procedimientos almacenados.

En función del caso de uso, los sistemas de información a integrar pueden requerir incrustar un frontal web del sistema de información ofertado. Se dispone de la *“Guía Técnica STS de Integración entre frontales”* para incrustar un frontal web en los productos del SNS-O. Para incrustar un frontal web en los productos, se dispone de guía técnica que se suministrará al adjudicatario. En la guía se describen con detalle todas las cuestiones a tener en cuenta a la hora de incrustar un frontal web, entre ellas:

- **Token de acceso.** Los productos del SNS-O aportarán un token de acceso, cifrado y firmado, con datos de identificación del profesional y del paciente. La solución ofertada por el adjudicatario deberá ser capaz de leer el token, autorizar el acceso al profesional y cargar los datos del paciente y del profesional en el frontal. El contenido del payload del token de acceso será:
 - Datos de profesional:
 - DNI del profesional
 - Nombre y apellidos.
 - Zona Básica
 - Centro y Servicio
 - Número de colegiado
 - Datos del paciente:
 - CIPNA
 - NHC
 - Número de afiliación
 - Nombre y apellidos
 - Edad
 - Domicilio
 - Localidad
 - Provincia

- Nombre y apellidos del médico titular.
- Teléfonos

Así mismo, el sistema de información que forme parte de la solución ofertada por el adjudicatario puede requerir ser notificado de eventos sucedidos en los sistemas de información o puede requerir publicar eventos sucedidos en su sistema de información que son de interés para los productos a integrar. Para ello, se dispone de la “*Guía Técnica de Feeds en el STS*” donde se detalla la solución técnica para tanto el suscriptor como el publicador. La guía será suministrada al adjudicatario.

Si fuese necesario, se dispone de plataformas para la ejecución desatendida de componentes contruidos para facilitar las integraciones. Estos componentes (tareas programadas o paquetes de transformación de datos) deben implementarse específicamente para cubrir aspectos tales como transformación de información o la monitorización del sistema para la notificación de eventos.

El sistema de información que formen parte de la solución ofertada por el adjudicatario deberá integrarse con los del SNS-O para permitir al profesional solicitar transporte para un paciente, autorizar la solicitud de transporte, agendar el transporte tras acuerdo con el paciente, consultar los transportes realizados o agendados, remitir información de los desfibriladores y consultar el posicionamiento y estado de las ambulancias. También se integrará con el ERP corporativo (Sigrid) utilizado en las Sociedades Públicas a la que pertenece BIDEAN.

Las integraciones entre la solución ofertada por el adjudicatario y los productos del SNS-O y ERP corporativo (Sigrid) serán diseñadas *ad hoc* en función de las características funcionales y técnicas. Todas estas integraciones serán analizadas en trabajos específicos, realizando un estudio de viabilidad. El SNS-O acordará con el adjudicatario un plan de trabajo para estudiar la viabilidad de las integraciones necesarias.

7. ASPECTOS RELATIVOS A LA SEGURIDAD

El Sistema de Información deberá cumplir la normativa de seguridad aplicable, en particular con el ENS en categoría media.

Si el Adjudicatario suministra un Sistema de Información web, deberá cumplir con buenas prácticas de programación segura existentes (en un sentido amplio, pudiendo basarse en recomendaciones de entidades internacionales reconocidas como OWASP, WASC, etc.), reservándose BIDEAN la facultad de realizar una auditoría al respecto para evaluar el grado de cumplimiento y detectar posibles deficiencias que pudiesen existir. En caso de detectarse incumplimientos y/o vulnerabilidades que puedan comprometer gravemente la seguridad del servicio prestado por la aplicación o de sus usuarios, el Adjudicatario se compromete a subsanarlas en tiempo y forma, antes de poner dicho servicio a disposición de los usuarios.

8. ENTORNO DE MOVILIDAD

El adjudicatario deberá aportar todos los elementos para la gestión del servicio desde los dispositivos móviles (formato Tablet) instalados en los vehículos de BIDEAN.

Deberá incluir herramientas adicionales de backup de localización, actualización de la propia App o control de actividad y seguridad.

El dispositivo móvil debe ser compatible con el sistema MDM corporativo Ivanti EPMM (Ivanti Endpoint Manager for Mobile).

9. SOPORTE Y MANTENIMIENTO

9.1. Soporte de los Sistemas Operativos y Software Base

El sistema de información se implanta atendiendo a alguno de los escenarios normalizados para proveedores especificados en los requerimientos técnicos.

En relación con el soporte del sistema operativo, como mínimo existirá un soporte que atenderá las peticiones de los técnicos que mantienen la infraestructura.

A tal efecto, el adjudicatario se compromete a ofrecer un plan de soporte en el que se reflejarán los horarios de atención, los métodos de comunicación (teléfono, correo electrónico o herramienta de gestión de incidencias donde se registren y solucionen las incidencias y consultas), y el tipo de actuaciones (si son remotas o in situ).

La empresa adjudicataria se integrará en el modelo de soporte de referencia del cliente.

La empresa deberá garantizar un soporte que comprenderá todo el horario potencial de funcionamiento del sistema de información en el que se establecerán sus condiciones de tiempos de atención, tiempos de respuesta, etc.

9.2. Soporte Funcional y Mantenimiento

La empresa adjudicataria debe presentar un plan de soporte y mantenimiento en el que se reflejarán los horarios de atención, los métodos de comunicación, el tipo de actuaciones (si son remotas o in situ) con el fin de solventar las incidencias y consultas técnicas en relación a la plataforma desarrollada.

Para ello, la empresa adjudicataria deberá integrar en su plan de soporte y mantenimiento a fin de atender las incidencias y consultas por parte de BIDEAN.

El adjudicatario deberá realizar las actuaciones de mantenimiento preventivas, correctivas y adaptativas requeridas durante el periodo de vigencia del contrato.

El sistema de información que forme parte de la solución técnica ofertada debe permitir cambios, por parte del equipo interno de BIDEAN, basándose en la información facilitada por el proveedor. El Adjudicatario se compromete a proporcionar asistencia técnica al equipo interno para realizar cambios en la configuración anteriormente citados.

El Adjudicatario se compromete a solucionar los errores de funcionamiento una vez hayan sido reportados.

Tal y como se detalla en el Pliego de Cláusulas Administrativas, la empresa licitadora deberá detallar en su oferta el procedimiento de soporte y mantenimiento.

Asimismo, el adjudicatario estará obligado a realizar las acciones formativas que precise el órgano de contratación para asegurar el manejo del equipamiento y los sistemas de información, para su óptima utilización, tanto desde el punto de vista operativo como funcional entendiéndose, en cualquier caso, que la amplitud y la calidad de la formación propuesta será precisa para el perfecto manejo y máximo rendimiento del equipamiento y los sistemas de información objeto del contrato.

Esta formación deberá ser especializada para cada tipo de usuario para utilizar el equipamiento y los sistemas de información en la forma prevista por el fabricante y efectuar adecuadamente las rutinas de servicio.

Cualquier modificación/actualización del equipamiento y los sistemas de información conllevará un periodo de formación del personal en los mismos términos señalados anteriormente.

Será, por tanto, de naturaleza obligatoria, que el/los adjudicatarios/s estén a disposición de BIDEAN para realizar la formación y entrenamiento adecuado en el uso del equipamiento y los sistemas de información en las condiciones que se indiquen.

9.3. Disposiciones comunes a los Soportes al Sistema Operativo, Software Base, Soporte Funcional y Mantenimiento

- El horario de soporte funcional será como mínimo 12x5, de 08:00 a 20:00 horas, en laborables de lunes a viernes, siendo el calendario de referencia para el soporte el calendario oficial publicado por el Gobierno de Navarra en el Boletín Oficial de Navarra.
- El Adjudicatario registrará todas las peticiones y dará respuesta telefónicamente o por email con la consiguiente solución.
- El Adjudicatario deberá aportar la documentación de apoyo necesaria para poder prestar el soporte indicado.
- Las incidencias se clasificarán de acuerdo a las siguientes categorías:
 - **Baja:** Incidencia que no afecte al funcionamiento operativo.
 - **Moderada:** Incidencia que afecte a una parte no crítica del proceso.
 - **Urgente:** Incidencia que afecta a un gran número de usuarios y/o a funcionalidades críticas del proceso.
 - **Crítica:** Incidencia que no permite trabajar con el sistema.
- Los tiempos de respuesta y resolución remota en función de la categoría de la incidencia serán:

Parámetros	Categoría	Nivel mínimo
Tiempo de respuesta	Baja	24 horas
	Moderada	8 horas
	Urgente	4 horas
	Crítica	2 horas
Tiempo máximo de resolución para el 90% de las actuaciones según la prioridad establecida	Baja	5 días laborables
	Moderada	3 días laborables
	Urgente	2 días laborables
	Crítica	8 horas

- El ámbito de actuación de todos los elementos que componen la solución del sistema de información, incluyendo los dispositivos móviles.

9.4. Documentación técnica y de usuario

La plataforma debe venir acompañada de documentación técnica completa, incluyendo guías de instalación, configuración y operación.

Debe proporcionarse documentación de usuario final que facilite la adopción y el uso eficiente de la plataforma.

10. PLAN DE FORMACIÓN

El adjudicatario estará obligado a realizar las acciones formativas que precise el órgano de contratación para asegurar el manejo del equipamiento y los sistemas de información, en su más óptima utilización, tanto desde el punto de vista operativo como funcional entendiéndose, en cualquier caso, que la amplitud y la calidad de la formación propuesta será precisa para el perfecto manejo y máximo rendimiento del equipamiento y los sistemas de información objeto del contrato.

Esta formación deberá ser especializada para cada tipo de usuario para utilizar el equipamiento y los sistemas de información en la forma prevista por el fabricante y efectuar adecuadamente las rutinas de servicio.

Cualquier modificación/actualización del equipamiento y los sistemas de información conllevará un periodo de formación del personal en los mismos términos señalados anteriormente.

Será, por tanto, de naturaleza obligatoria, que el adjudicatario esté a disposición de BIDEAN para realizar la formación y entrenamiento adecuado en el uso del equipamiento y los sistemas de información en las condiciones que se indiquen.

11. PLANIFICACIÓN

Es necesario que los ofertantes presenten los cronogramas en los que se deben especificar las fases y tareas a realizar y su distribución en el tiempo.

La primera tarea del Adjudicatario será acordar un diseño de solución integrado y entregar una planificación en detalle para su implantación.

La planificación tendrá las siguientes fases:

- Fase de análisis y diseño: el objetivo de esta fase es realizar un análisis de la situación actual. En la que se llevarán a cabo las tareas:
 - Establecer y documentar los componentes necesarios para implementar el sistema de información y definir como se realizarán las integraciones con otros sistemas de información indicados anteriormente.
 - Elaborar la hoja de ruta y la planificación para alcanzar los objetivos del presente pliego en los plazos que se establezcan.

El licitador deberá incluir en su oferta un plan de análisis y diseño que describa los objetivos, fases, tarea, actividades y plazos temporales correspondientes.

- Fase de implantación: en esta fase se llevarán a cabo las tareas:
 - Instalación y configuración de componentes de infraestructura
 - Desarrollo de funcionalidades identificadas por BIDEAN
 - Desarrollo de adaptaciones y configuraciones necesarias para la integración con otros sistemas de información.
 - Elaboración, entrega y ejecución de los planes de pruebas que permitan validar el correcto funcionamiento del sistema a implantar. El plan deberá cubrir las pruebas de los componentes o pruebas unitarias, pruebas de integración, de conectividad, etc...
 - Suministro de documentación técnica, funcional y manuales de usuario
 - Formación en la nueva plataforma, tanto a nivel de usuario como de técnicos/administradores.
 - Pilotaje.

El licitador deberá incluir en su oferta un plan de implantación que describa los objetivos, tareas, actividades adaptaciones y plazos temporales correspondientes.

- Fase de funcionamiento del sistema: en esta fase se comprenden las tareas relacionadas con el funcionamiento del sistema una vez implantado.
 - Servicios de alta disponibilidad.
 - Acuerdos de nivel de servicios
 - Equipo de trabajo
 - Planificación, dirección y seguimiento de los trabajos

El licitador deberá incluir en su oferta un plan de funcionamiento del sistema en el que se detallará el contenido de este punto.

12. SEGUIMIENTO DEL CONTRATO

Durante la ejecución del servicio objeto del contrato la entidad adjudicataria se compromete, en todo momento, a facilitar a las personas designadas por la persona responsable de BIDEAN, la información y documentación que éstas soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizados para resolverlos.

En este sentido, la entidad contratista deberá informar a persona responsable de BIDEAN con la periodicidad necesaria sobre distintos aspectos del funcionamiento y calidad del Servicio. Se establece la obligatoriedad de presentar un informe de actividad y seguimiento de los servicios de carácter trimestral.

Asimismo, la entidad contratista estará obligada a asistir y colaborar a través del personal que designe, a las reuniones de seguimiento del proyecto convocadas por BIDEAN, que se compromete a citar con la debida antelación al personal del contratista, a los efectos de poder facilitar su asistencia.

Para una correcta ejecución contractual y seguimiento del mismo, la empresa licitadora designará al menos a un coordinador técnico o responsable integrado en su propia plantilla con una experiencia mínimo de 3 años en contratos de análoga naturaleza.

Si la empresa adjudicataria propusiera el cambio de la persona citada, se deberá solicitar por escrito y deberá acreditar que la persona que sustituye cuenta con la misma o mayor experiencia y titulación exigida.

13. DOCUMENTACIÓN TÉCNICA

Durante el contrato el Adjudicatario elaborará y entregará a BIDEAN los documentos necesarios que permitan una explotación y soporte adecuado de los sistemas de información. Como mínimo deberá aportar los siguientes: Diseño Lógico y Físico, Plan de Explotación, Manual de Operación y Soporte y Modelo Administrativo y cualquier otro documento que sea necesario para el correcto funcionamiento del equipamiento y software entregados.

14. LICENCIAMIENTO

El modelo de licenciamiento no requerirá ningún dispositivo físico (mochilas, etc.) en los equipos cliente con el fin de facilitar la explotación del sistema por los diferentes equipos de soporte de BIDEAN.

Las licencias del software implantado serán propiedad de BIDEAN de manera indefinida y BIDEAN tendrá derecho a su actualización durante la vigencia del contrato.

El software (sistema operativo, aplicativos, drivers, etc.) incluido en el equipamiento tendrá un ciclo de vida equivalente al del equipamiento. Con el fin de garantizar el funcionamiento y el soporte del equipamiento, la fecha de fin de soporte del software deberá ser posterior a la vida útil estimada del equipamiento o garantizar su evolución a versiones del software que estén soportadas.

15.MEMORIA TÉCNICA DISPOSITIVOS MÓVILES A SUMINISTRAR (LOTE 2)

CARACTERÍSTICAS:

Los dispositivos móviles, en formato tablet, deberán cumplir con las siguientes características técnicas mínimas:

- **Pantalla:** Mínimo 8 PULGADAS, multi-táctil 8 puntos, y máximo 10 pulgadas, alta luminosidad
- **Sistema Operativo:** Android 11 o superior, compatible con Android Enterprise
- **Procesador:** Octa Core con 2× Cortex-A76 a 2.2 GHz y 6× Cortex-A55 a 2 GHz.
- **Memoria RAM:** 3GB
- **Almacenamiento Interno:** 32 GB Flash + 512GB SD
- **Conectividad:**
 - Wi-Fi 802.11
 - Bluetooth 5.0.
 - NFC
 - Modem 4G LTE con soporte para múltiples bandas.
 - GPS.
- **Puertos:** USB 3.2 Tipo C, Micro-SD
- **Batería:** 7.000mAh.
- **Resistencia:** Protección IP68 total contra polvo y agua, resistencia a caídas y golpes según normativa MIL-STD 810H, equipo operativo en rangos de temperatura de -25°C a 60°C.
- Dispositivo con opción de conexión de lector de código de barras integrado.
- Debe disponer de un POGO-PIN para conectarse al soporte para vehículo y poder replicar los puertos sin perder la certificación IP-65 del dispositivo.

El dispositivo móvil debe ser compatible con el sistema MDM corporativo Ivanti EPMM (Ivanti Endpoint Manager for Mobile).

ACCESORIOS COMPATIBLES QUE DEBERÁ TENER EL DISPOSITIVO MÓVIL

Cada una de las tablets deberá disponer de una gama de accesorios compatibles, que se detallan a continuación:

- Soporte cuna para vehículo con replicador de puertos.
- Docking de escritorio con replicador de puertos.
- Cargador de batería.
- Batería de recambio.
- Fuente de alimentación para vehículo USB-C.

CARACTERÍSTICAS DEL SOPORTE CUNA PARA VEHÍCULO

El soporte cuna para vehículo/pared deberá cumplir con las siguientes características técnicas:

- **Compatibilidad:** Específicamente diseñado por el fabricante del modelo de tableta robusta
- **Replicador de Puertos:**
 - 1 x USB 2.0 para conexión de dispositivos periféricos.
 - 1 x RS-232 para conexión de equipos o dispositivos seriales.
 - 1 x RJ45 para conexión de red Ethernet.
 - 1 x USB-C para alimentación eléctrica.
- **Sistema de Sujeción:** Debe incluir un sistema robusto anti-vibración y anti-choques para garantizar la seguridad y estabilidad de la tableta bajo condiciones de movimiento y uso en vehículos o entornos con vibración.
- **Seguridad:** Deberá incluir una llave de seguridad para restringir el acceso y la retirada de la tableta del soporte, asegurando la protección contra robos o manipulaciones no autorizadas.
- **Base de Carga de escritorio:** La cuna debe proveer de base de carga para la tableta, permitiendo su uso continuado y carga simultánea durante su operación en el soporte con los siguientes puertos:
 - 1 x USB 2.0 para conexión de dispositivos periféricos.
 - 1 x RS-232 para conexión de equipos o dispositivos seriales.
 - 1 x RJ45 para conexión de red Ethernet.
 - 1 x DC-in Jack para alimentación eléctrica.
- **Sistemas de Sujeción Compatibles:** El soporte debe ser compatible con sistemas de sujeción RAM y estándares VESA 75 / 100, para facilitar su instalación en diferentes tipos de vehículos o paredes.

16.SOPORTE DE DISPOSITIVOS MÓVILES

El Adjudicatario se compromete a ofrecer un plan de soporte para dispositivos móviles. Se debe detallar los horarios de atención, los métodos de comunicación, el tipo de actuaciones (si son remotas o in situ).

Se deberá disponer de un remanente de cinco dispositivos mínimo ya configurados para que, en caso de avería, poder sustituir rápidamente los dispositivos que se tengan que reparar.