

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HAN DE REGIR LA CONTRATACIÓN DE UN DESARROLLO E IMPLANTACIÓN DEL WALLET DIGITAL EN EL MARCO DEL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA
FINANCIADO CON FONDOS DE LA UNIÓN EUROPEA –
NEXT GENERATION EU

Octubre – 2023

ÍNDICE

1	<u>NECESIDADES A SATISFACER</u>	3
2	<u>OBJETO</u>	5
3	<u>REQUISITOS DEL SERVICIO</u>	9

1 NECESIDADES A SATISFACER

En la actualidad, los ciudadanos de la Comunidad Foral de Navarra tienen la posibilidad de realizar trámites ONLINE a través de la Sede Electrónica del Gobierno de Navarra, además de la tradicional forma presencial.

Para ello, resulta necesario emplear uno de los siguientes métodos: certificado digital emitido por la Fábrica Nacional de Moneda y Timbre (FNMT), DNI electrónico que reúna los requisitos establecidos en la LPACAP (Ley del Procedimiento Administrativo Común de las Administraciones Públicas), o el sistema de verificación de identidades electrónicas Cl@ve.

A modo de ejemplo, se muestra uno de los trámites actuales:

Centro de día o estancia diurna para personas con discapacidad

Incluye servicio de comedor, cuidados asistenciales, apoyo y supervisión en las actividades de la vida diaria, atención social, médica, psicológica y fisioterapia, terapia ocupacional, logopedia y actividades de ocio y tiempo libre

EN PLAZO Mostrar todo [Suscribirse a este trámite](#)

INFORMACIÓN BÁSICA

Dirigido a ▼

Descripción ▼

Documentación a presentar ▼

Normativa ▼

TRAMITACIÓN

Solicitud ▲

Se puede tramitar con las siguientes credenciales:

- Con certificado digital o DNI electrónico
- Con Cl@ve

SOLICITAR

**Trámite de la Agencia Navarra de Autonomía y Desarrollo de las Personas (ANADP), dependiente del Departamento de Derechos Sociales del Gobierno de Navarra.*

Conforme a la experiencia recabada por el Departamento de Derechos Sociales de Gobierno de Navarra, se ha observado que estos sistemas generan dificultades para una parte importante de la población, como, por ejemplo:

- Personas de edad avanzada.

- Personas vulnerables.
- Personas con determinadas tipologías de discapacidad.
- Personas con menor formación en competencias digitales.

A modo de ejemplo, una persona con movilidad reducida tendrá mayores dificultades a la hora de tramitar la obtención del certificado digital o del sistema Cl@ve que requieren la presencialidad de la persona para verificar su identidad.

Del mismo modo, una persona con avanzada edad podría tener más problemas a la hora de gestionar las claves para la utilización de estos sistemas o bien la utilización de los certificados electrónicos, que requieren de un ordenador o dispositivos electrónicos para su utilización.

Unido a lo anterior, existe un riesgo de suplantación de identidad, como el que podría producirse en el caso de sustracción de las claves del DNI electrónico, la instalación de un certificado electrónico en un ordenador distinto al del titular o bien por una cesión indebida del mismo, no pudiendo verificar estos sistemas la identidad real de la persona.

En consecuencia, el Gobierno de Navarra quiere llevar a cabo la implantación de un sistema de identificación que:

- a. Facilite la accesibilidad a la totalidad de las personas.
- b. Sea de uso sencillo y efectivo.
- c. Garantice la identidad de la persona, mediante la utilización de tecnologías biométricas de forma segura.

Este sistema de identificación y firma complementará a los ya vigentes en la actualidad (Cl@ve, certificado digital o DNI electrónico), incluyéndose como un sistema completamente voluntario para la ciudadanía, que garantice tanto los derechos de las personas físicas, como la normativa vigente (incluida, pero no limitada, la normativa de protección de datos personales).

Será un requisito necesario la posibilidad de limitar el acceso a un determinado colectivo de personas. Si fuese necesario, el Departamento de Derechos Sociales de Gobierno de Navarra determinará las personas destinatarias de este servicio, en adelante 'público objetivo'.

2 OBJETO

El objeto del presente procedimiento es la contratación de los servicios necesarios para llevar a cabo el diseño e implantación de un Wallet de Identidad Digital con identificación biométrica, como sistema de identificación alternativo, así como la asesoría necesaria para definir los casos de uso (en adelante el “servicio”) para el Departamento de Derechos Sociales del Gobierno de Navarra.

El servicio cubrirá las siguientes funciones:

2.1. Consultoría y asistencia para la ‘Evaluación de Impacto’ para el departamento responsable de protección de datos de Gobierno de Navarra.

Deberá asistir al Responsable del tratamiento en la realización de un informe de Evaluación del Impacto de la tecnología y funcionalidad de la solución ofertada en el ámbito de la protección de datos personales.

2.2. Desarrollo de una app móvil que integre los componentes del Wallet de Identidad Digital.

Se desarrollará una aplicación móvil para los sistemas operativos Android e iOS, que permita llevar a cabo el registro o alta en la aplicación (onboarding) y el acceso a los servicios (autenticación) del Departamento de Derechos Sociales mediante el uso de biometría. Esta aplicación deberá ser compatible al menos con iOS 16,15,14,13 y Android 12,11,10,9.

El alta en la aplicación (onboarding) deberá contar al menos con las siguientes etapas:

- Captura del documento de identificación (Documento Nacional de Identidad o permisos de residencia vigentes en España).
- Posible validación de que este documento corresponde a un titular del ‘público objetivo’ en caso de decidirse limitar la solución al mismo.
- Validación del documento de identificación.
- Captura de autofoto (‘selfi’) del usuario.
- Comparación biométrica.
- Prueba de vida.
- Validación a posteriori del proceso por agente humano.

La solución incluirá una herramienta de monitorización preparada para la revisión manual y validación a posteriori de todos los procesos realizados por parte de un agente humano.

En relación con el funcionamiento de la app de onboarding:

- La aplicación solicitará al usuario la realización de una fotografía tanto del anverso como del reverso del documento de identificación.
- Posteriormente, la aplicación llevará a cabo un proceso de lectura de los datos impresos en el documento (OCR). Se recogerá el nombre, apellidos, número de identificación, número del soporte, sexo, fecha de nacimiento, fecha de expiración, nacionalidad, domicilio y lugar de nacimiento.
- Obtenidos los datos anteriores, se llevarán a cabo las siguientes verificaciones
 - Vigencia del documento de identidad
 - La mayoría de edad del usuario
 - Realización de una suma de verificación ('checksums') de la zona de lectura mecánica ('MRZ').
 - Que la fotografía del anverso y del reverso corresponden al mismo documento.
 - Autenticidad del documento
 - Que la fotografía del documento de identificación es auténtica y que no ha sido manipulada (por ejemplo, mediante la fotografía a una pantalla).
- Verificado el documento de identificación, se solicitará a la persona usuaria de la aplicación que se tome una autofoto ("selfi").
- Dicha fotografía deberá ser validada mediante el empleo de un motor de biometría facial, que lleve a cabo la comparación biométrica entre la autofoto y la foto del documento de identificación.
- La autofoto deberá ir acompañada de la realización de una prueba de vida pasiva, para la detección de ataques de representación y deepfakes.

Como resultado de la aplicación del proceso descrito, y basándose en los datos obtenidos del documento de identidad y la autofoto del usuario, se generará una credencial de identidad en el Wallet de Identidad Digital del usuario, que podrá ser usada para la autenticación de este en los distintos trámites o servicios. Estos procesos de autenticación se podrán ejecutar tanto en el entorno digital (como una página web, por ejemplo), como en el entorno físico (a través de sistemas de control de acceso o similares).

Esta credencial de identidad no estará activa hasta la aprobación y validación por el agente humano.

La solución permitirá el registro o acceso en páginas web mediante un plug-in integrado en ésta, que muestre un código QR que se deberá poder escanear y procesar por el Wallet de Identidad Digital. Una vez escaneado y procesado por el Wallet, se solicitará autorización al usuario para compartir con la página web sólo aquellos datos que sean necesarios y requeridos por la web.

El wallet contará con un proceso de verificación que permita asegurar que se trata de la misma persona que llevó a cabo el proceso de alta.

Nota: todos estos componentes y procedimientos que conforman el servicio deberán cumplir las normativas de seguridad y accesibilidad aplicables y vigentes. De la misma forma, deberán cumplir los compromisos en materia de comunicación, encabezamientos y logos que se contienen en el artículo 9 de la Orden HFP/1030/2021, de 29 de septiembre, (<https://planderecuperacion.gob.es/identidad-visual>).

2.3. Servicio de Supervisión de alta por parte de Agente Humano

Dicho servicio se dará de forma desasistida y a posteriori del acto de onboarding. Se deberá establecer el protocolo de comunicación en el dispositivo del usuario de que la credencial está lista en el momento que el agente humano valide el mismo.

El alcance mínimo de este servicio incluye:

- Establecimiento de un protocolo de validación conforme a la normativa vigente.
- Software de gestión de los onboardings efectuados para validarlos.

La solución ofertada deberá contar con un servicio de formación para el personal del Departamento de Derechos Sociales, como mínimo incluirá:

- Formación sobre el uso de la herramienta.
- Formación sobre las características del método de identificación, procedimientos, métodos de prueba, métodos comunes de falsificación... con el objetivo de que tenga capacitación suficiente para detectar potenciales fraudes.
- Formación en materia de protección de datos personales.
- Formación en el manejo de la herramienta e interpretación de la información y datos que suministra.

Dichas formaciones no podrán ser inferiores a 15 horas, cuyo plan formativo se pondrá a disposición del Departamento de Derechos Sociales a fin de poder realizar la formación al menos una vez al año durante la vigencia de las licencias.

2.4. Servicio de atención al usuario

El adjudicatario deberá proveer un servicio de atención a las personas usuarias. El servicio será vía telefónica o por video llamada, y mediante correo electrónico, para solventar los problemas y/o dudas que puedan tener las personas usuarias durante su utilización.

Se valorará positivamente la posibilidad de que, mediante un botón de ayuda, la persona usuaria pueda conectarse directamente por vídeo llamada con un operador del servicio de atención y que pueda finalizar el proceso de onboarding en la misma llamada, con la asistencia del operador.

2.5. Trabajos de integración

El adjudicatario deberá realizar los trabajos necesarios para llevar a cabo la integración de la solución en el marco tecnológico de Gobierno de Navarra, incluyendo, pero no limitado, la creación de un registro de usuarios dados de alta en el sistema, una aplicación web que gestione dicho registro y un plug-in en las páginas web del Gobierno de Navarra para poder llevar a cabo los procesos de autenticación.

Esta integración deberá cumplir las siguientes directrices:

- Comunicación mediante el protocolo de OAuth 2.0 OpenIDConnect.
- Los proveedores de identidad se deben integrar mediante comunicación por servicio web.
- El equipo técnico de la Dirección General de Telecomunicaciones y Digitalización de Gobierno de Navarra deberá tener conocimiento de la URL del servicio al que se debe invocar y planificar de manera coordinada el desarrollo.
- El proveedor de la credencial biométrica deberá desarrollar la lógica del servicio de autenticación de Gobierno de Navarra (sistema Ateka) con una interfaz que cumpla con los requisitos indicados en la 'Guía de Integración de Ateka', que podrán solicitar a través del correo licitacion@nasertic.es.
- Este proveedor deberá devolver, como mínimo la siguiente información sobre la persona autenticada:
 - Identificador
 - Nombre
 - Primer apellido
 - Segundo apellido
- Este proveedor deberá gestionar y devolver correctamente los posibles errores.
- Tanto el proveedor de identidad como su integración en Ateka deberán pasar la auditoría de seguridad pertinente que realiza la Sección de Seguridad de la Dirección General de Telecomunicaciones y Digitalización (o equivalente) de Gobierno de Navarra. Esta auditoría se compone de una auditoría de código fuente del componente al que debe invocar Ateka y una auditoría de seguridad dinámica.

2.6. Servicios de asesoría

El adjudicatario deberá llevar a cabo los servicios de asesoría y consultoría necesarios para la adecuada implantación del Wallet de Identidad Digital, así como la definición y ampliación de los casos de uso.

Para el cumplimiento de este servicio, se estiman un mínimo de 150 horas de Consultor Senior.

Todos los trabajos descritos en los puntos del 2.2 al 2.6 estarán supeditados al resultado del análisis del informe de Evaluación de Impacto (descrito en el punto 2.1), por parte de Unidad Delegada de Protección de Datos del Gobierno de Navarra, en cuanto al uso de la tecnología y los datos en este proyecto.

3 REQUISITOS DEL SERVICIO

El servicio debe cumplir con los siguientes requisitos:

3.1. Wallet digital

Se distinguen entre requerimientos funcionales, de verificación de identidad, de accesibilidad y de seguridad. A continuación, se detalla cada uno de esos requerimientos.

Requerimientos funcionales:

- La APP estará escrita en lenguajes nativos (Swift u Objective-C para iOS, Kotlin o Java para Android) o en cualquier otro lenguaje híbrido (ej: React Native, IONIC). Esta APP deberá ser compatible al menos con los sistemas iOS 16,15,14,13 y Android 12,11,10,9.
- El Wallet incorporará un proceso que verificará que el documento a validar pertenece a una persona del 'público objetivo' (en caso de que se establezca esta limitación en el uso del servicio para un segmento de la población). Este procedimiento aplicará las garantías de seguridad necesarias para garantizar la seguridad de la información.
- El Wallet debe contar con un proceso de verificación de identidad del usuario como mecanismo de alta en el Wallet. Como resultado, se generará la credencial de identidad en el Wallet a partir de los datos del documento de identidad y la foto tipo selfi del usuario.
- En el proceso de registro del ciudadano se valorará la opción de captura de un audio para que posteriormente se pueda ofrecer la opción de autenticarse mediante la voz para algunos trámites digitales.
- El Wallet debe permitir llevar a cabo procesos de autenticación en un servicio compatible. Los procesos de autenticación deben poder ejecutarse tanto en el entorno digital (a través de una web), como en el entorno físico (por ejemplo, a través de sistemas de control de acceso).
- La solución debe incluir un plug-in web que se pueda integrar en una web, de manera que se puedan llevar a cabo el registro y autenticación en el entorno digital.

- El registro en la web debe llevarse a cabo mediante el escaneo de un código QR mostrado por el plug-in web, que será escaneado por el Wallet.
- Tanto en el onboarding, como en el acceso al servicio web, la solución debe permitir compartir los datos almacenados en el Wallet. En concreto, se debe poder compartir los datos personales extraídos del documento de identidad, así como la foto del usuario. El proceso de compartición de información debe contar con el consentimiento expreso del usuario tanto para el onboarding, como para cada uso del servicio de identificación.
- El Wallet debe contar con un proceso de verificación unívoca de la identidad del usuario como mecanismo para autorizar registros y autenticaciones en sistemas compatibles (digital y físico) que permita asegurar que se trata de la misma persona que llevó a cabo el proceso de alta en el Wallet. A estos efectos, no se admitirá el uso del código PIN o de la biometría del propio dispositivo móvil (ej: FaceID) como verificadores, al ser elementos que pueden ser compartidos por más de una persona. Se deben emplear verificadores biométricos que permitan asegurar que la persona que llevó a cabo el alta en el Wallet es la misma que lleva a cabo los procesos de registro y acceso.
- El Wallet debe contar con un proceso de revocación de credenciales.
- El Wallet debe contar con un registro de la actividad del usuario, solo accesible por el propio usuario en el dispositivo en el que opera el Wallet. El registro de actividad deberá informar sobre los siguientes puntos:
 - Alta, edición o borrado de credenciales.
 - Webs en las que el usuario se ha registrado empleando el Wallet.
 - Información compartida por el usuario en cada una de las webs en las que el usuario se ha registrado.
 - Accesos a cada una de las webs en las que el usuario se ha registrado a través del Wallet.
- El Wallet debe ofrecer un sistema de verificación/autenticación biométrica 1:1 o uno a uno.
- Será obligación del contratista adaptar el Wallet a los requerimientos de todo tipo que establezca el Marco Europeo de Identidad Soberana (ESSIF) compatible con eIDAS. Así, el wallet será actualizado en la medida en la que los requerimientos y estándares europeos así lo requieran durante la duración de este contrato.

Requerimientos asociados a la verificación de la identidad:

- El proceso de verificación de identidad debe constar de las siguientes etapas:
 - Captura del documento de identificación (Documento Nacional de Identidad o permisos de residencia vigentes en España).

- Validación del documento.
 - Captura de autofoto ("selfi") del usuario.
 - Comparación biométrica.
 - Prueba de vida.
 - Validación de cada identidad registrada y validada por parte de un agente humano cualificado.
- Se debe capturar una fotografía del anverso del documento y una fotografía del reverso del documento. La fotografía obtenida deberá reunir las condiciones de calidad y nitidez que permitan su uso en investigaciones o análisis, no reputándose válida a estos efectos la mera captura de fotogramas o frames.
 - La adquisición de imágenes del documento se debe realizar mediante captura automática del documento una vez detectados todos los parámetros de calidad correctos para realizar la validación. No se admitirán archivos pregrabados, ni soluciones en las que el usuario tenga que decidir de forma manual el momento de la captura, por considerar que la experiencia de usuario no es buena, causaría rechazo de uso y una alta tasa de fallo por calidad insuficiente en las capturas.
 - Se debe soportar el alta con DNIs y permisos de residencia vigentes en España, en concreto:
 - Todos los modelos de DNI españoles en vigor (DNIe, DNIe 3.0, y DNIe 4.0 (formato europeo)).
 - Todos los modelos de tarjetas de residentes en España en vigor (TIE y certificado de registro de ciudadano de la Unión Europea).
 - Debe ser posible la inclusión de nuevos documentos de identificación en el servicio a petición del cliente, con un proceso poco intrusivo y en un plazo no superior a 60 días.
 - Se debe llevar a cabo un proceso de lectura de los datos impresos en el documento de identidad (OCR). Se deben leer los siguientes datos impresos en el documento: nombre, apellidos, número de identificación, número del soporte, sexo, fecha de nacimiento, fecha de expiración, nacionalidad, domicilio y lugar de nacimiento.
 - Es necesario verificar que el usuario tiene un documento de identidad vigente. Esta verificación se hará extensible a cualquier uso del Wallet. No se permitirá validarse en ningún servicio a un usuario con el documento de identificación caducado. Para ello se implementarán los controles necesarios para que la identidad biométrica no sea válida más allá de la fecha de caducidad del documento con la que ha sido generada.
 - Se debe verificar que el usuario es mayor de edad.
 - Se deberá garantizar que el vector biométrico generado tenga una caducidad a los 5 años de su generación.

- Se requiere la verificación automática de los checksums de seguridad del MRZ.
- El proceso de verificación documental deberá asegurar que la fotografía capturada del anverso del documento de identificación y la fotografía capturada del reverso de este, corresponden al mismo documento.
- El proceso de verificación documental debe asegurar que el documento sea auténtico, no admitiéndose el uso de fotocopias del documento. Se chequeará la información obtenida por el OCR con la información obtenida del NFC (Near Field Communication).
- Se debe verificar que el documento fotografiado debe ser el original y auténtico, desechando la utilización de fotografías de pantalla, fotocopias, fotos impresas, manipulaciones, etc...
- El servicio permitirá la captura de una imagen facial del portador del documento.
- El servicio realizará un análisis biométrico de la imagen facial capturada.
- Se debe emplear un motor de biometría facial para la comparación biométrica entre la foto selfi y la foto impresa en el documento.
- El motor de biometría facial debe demostrar un funcionamiento correcto con independencia de las características de las personas usuarias.
- El proceso de verificación de identidad debe incluir una prueba de vida pasiva para la detección de ataques de presentación (PAD).
- La prueba de vida debe contar con la conformidad ISO/IEC 30107 para los niveles 1 y 2 por parte de un organismo certificador cualificado a tal efecto.
- La prueba de vida debe contar con la capacidad para detectar deepfakes.
- El modelo de generación de vectores biométricos deberá estar basado en la inteligencia artificial para garantizar el cumplimiento del principio de exactitud del dato impuesto por el RGPD.
- En el proceso de registro del ciudadano se valorará la incorporación de la captura de un audio para que posteriormente se pueda ofrecer la opción de autenticarse mediante la biometría de voz. Este vector biométrico se podría incorporar como una forma más de identificación o como un factor de identificación por sí mismo para algunos trámites.

- La solución de motor biométrico ofertada deberá estar evaluada por el National Institute of Standards and Technology (NIST). Se valorará el rendimiento del motor biométrico en función de los últimos informes publicados.
- La solución global deberá cumplir con los requerimientos establecidos en el anexo F11 de la guía de seguridad de las TIC CCN-STIC-140, del Centro Criptológico Nacional. Se valorará el estar inscrito en catálogo de 'Productos Cualificados' de dicho CCN en la categoría de 'Herramientas de Videoidentificación'

Requerimientos asociados a la accesibilidad:

- Al iniciarse, se solicitará al usuario de la aplicación que confirme que acepta que la información que va a proporcionar quede almacenada en el sistema, además de mostrarle una información (configurable por el Departamento de Derechos Sociales mediante literales) en la que se le ponga en antecedentes de cómo será el proceso y la documentación que necesitará para completarlo. En cualquier caso, no se almacenarán vectores biométricos en ningún sistema ajeno al dispositivo del usuario.
- El Servicio de verificación incluirá un diseño gráfico de aspecto y comportamiento completamente integrado con el software del Gobierno de Navarra, de tal manera que el usuario no tenga la sensación de que realiza una operación externa a la misma. El aspecto gráfico del Servicio deberá ser aprobado por el Departamento de Derecho Sociales del Gobierno de Navarra previo a su implementación y podrá modificarse a petición de este para adecuarlo al diseño gráfico de su web y Apps.
- El Wallet debe contar con infografías explicativas de todos los procesos que se ejecutan por vez primera. Cada una de las infografías explicativas debe estar disponible para posteriores reproducciones si el usuario lo estima oportuno.
Al igual que en el punto anterior, el diseño gráfico de aspecto y comportamiento de las mismas estará completamente integrado con el software del Gobierno de Navarra.
- El Wallet debe estar disponible en castellano y euskera.
- El proceso contará con un sistema de trazas de negocio que permita analizar los puntos negros donde los usuarios abandonan el proceso o tienen dificultades y que permita acometer cambios rápidos en los puntos más críticos.

Requerimientos de seguridad:

- El sistema debe garantizar que la interacción del usuario en el proceso de verificación de identidad se realiza en un único dispositivo y en un acto secuencial en el tiempo.

- El Wallet debe almacenar en el dispositivo móvil del usuario los datos asociados al proceso de verificación de identidad:
 - Datos OCR extraídos del documento.
 - Datos NFC extraídos del documento.
 - Fotografía del documento de identidad.
 - Fotografía tipo autofoto (selfi) del usuario o vector biométrico.
- El almacenamiento de datos personales en el dispositivo debe hacerse empleando mecanismos criptológicos como el cifrado simétrico (AES).
- Todas las comunicaciones deben utilizar el protocolo TLS v1.2 o superior.
- De conformidad con lo dispuesto en el artículo 9.3 de la LPACAP, al encontrarse los datos biométricos entre las categorías especiales de datos a los que se refiere el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de los sistemas de identificación, deberán encontrarse en territorio español.
- La extracción OCR, validación documental y comprobación NFC que se ejecutan en el proceso de verificación de identidad deberán llevarse a cabo por seguridad en un servidor. No se permite el uso de tecnologías de extracción OCR, NFC y validación documental que tomen la decisión en el dispositivo móvil del usuario por motivos de seguridad. En cualquier caso, no se almacenarán vectores biométricos en ningún sistema ajeno al dispositivo del usuario.

El sistema implantado debe garantizar el cumplimiento de la normativa aplicable al caso y citada en el pliego administrativo.

3.2. Servicio de atención al usuario

El adjudicatario deberá proveer un número de teléfono, de tarificación reducida o gratuita (900xxx, 901xxx, 902xxx y su equivalente número fijo 9xxxxxxxxx), a través del que suministrará un servicio de atención telefónica a las personas usuarias del Wallet para solventar los problemas y/o dudas que puedan tener en el uso del Servicio.

El adjudicatario deberá proveer una dirección de correo electrónico a través de la que se suministrará un servicio de atención por correo a las personas usuarias del Wallet para solventar los problemas y/o dudas en relación con el uso de ese Servicio.

Características del servicio:

- El adjudicatario dispondrá de los medios humanos necesarios para garantizar los niveles de calidad en la atención al cliente.
- El Servicio cubrirá el alcance máximo definido en la presente licitación para la prestación del soporte de atención al cliente.
- El adjudicatario remitirá informes mensuales con:
 - Llamadas recibidas
 - Llamadas atendidas
 - Llamadas perdidas en cola
 - Llamadas perdidas en saturación
 - Llamadas abandonadas
 - Llamadas realizadas
 - Tiempo medio de espera
 - Tiempo medio de la llamada
 - Verificaciones de identidad manuales realizadas, diferenciando según su resultado (verificado o no verificado)

Horario de atención a las personas usuarias.

- De lunes a viernes de 08:00 h a 17:00 h.
- Durante toda la duración del contrato.

Nivel de calidad del Servicio.

Para la valoración de los recursos destinados a este servicio de atención a las personas usuarias, se cumplirán los siguientes parámetros:

- El tiempo medio para resolución de un problema debe ser inferior a 10 minutos.
- El servicio debe ser atendido, por un 'operador/a', en menos de 1 minuto, en el 85% de las llamadas.
- Las personas operadoras deberán ser capaces de recoger las evidencias documentales de aquellas personas usuarias que no hayan sido capaces de ejecutar el servicio automatizado y realizar el proceso de onboarding en ese mismo acto de forma asistida. Este procedimiento deberá ser confirmado como todos los demás onboardings por el servicio de validación por agente humano.
- Con dichas evidencias deberán completar el proceso de verificación de forma manual.
- Esta verificación de identidad y las correspondientes evidencias se incluirán en la base de datos de usuarios, anotando adicionalmente que el proceso ha sido manual.

Registro de las incidencias:

- Las incidencias se registrarán en una herramienta de registro del adjudicatario.
- Las incidencias se tipificarán.
- Se valorará positivamente la opción de ayuda online mediante videoconferencia, establecida desde la misma app y en la cual se pueda realizar el onboarding con la asistencia de la persona operadora en el mismo momento.

3.3. Trabajos de integración

Creación de un registro de usuarios denominado 'público objetivo'

Se deberá crear una aplicación donde los responsables de la aplicación puedan dar de alta, baja o modificar a los usuarios denominados 'público objetivo'. Denominamos 'público objetivo' al conjunto de usuarios que eventualmente puedan acceder a la app de onboarding.

El adjudicatario será responsable de la carga inicial de los registros dentro de este aplicativo.

Esta funcionalidad deberá poder habilitarse o deshabilitarse en función de la decisión de limitar o no el proyecto a un 'público objetivo'. En cualquier caso, deberá estar incluido en el proyecto.

Creación de un registro de usuarios dados de alta en el sistema:

De conformidad con lo que se dispone en el artículo 9.2 letra c) de la LPACAP, los sistemas de identificación de los interesados en los procedimientos distintos de los sistemas basados en certificados electrónicos que se prevén en las letras a y b del mismo artículo, requerirán contar con un registro previo como usuario que permita garantizar su identidad.

Por consiguiente, dentro de los trabajos de integración del sistema se debe llevar a cabo la creación de un registro de usuarios que permita dejar constancia de las personas usuarias que se encuentren dados de alta en el mismo.

Este registro deberá cumplir los siguientes requisitos:

- a) Posibilitar conocer que una persona se encuentra dada de alta en el sistema en cada momento.
- b) Posibilitar conocer si la persona ciudadana puede hacer uso del wallet de identidad digital para el acceso electrónico a los servicios públicos.
- c) Permanecer bajo el control del Departamento de Derechos Sociales del Gobierno de Navarra.

- d) Debe contener la mínima información imprescindible para la identificación del interesado (nombre, apellidos y DNI).
- e) En el supuesto de que una persona que se hubiera dado de alta en el Wallet de Identidad Digital, revocara el consentimiento prestado para el uso del mismo, deberá constar en el registro su baja y la fecha en la que la revocación tuvo lugar. Para lo cual es necesario que la app contenga dicha funcionalidad.
- f) Deberá contar con un sistema de fácil consulta y acceso a través de una aplicación web.
- g) Posibilitar dar de baja por parte del Departamento de Derechos Sociales a cualquier usuario, deberá constar en el registro su baja y la fecha en la que la misma tuvo lugar, y el motivo de la misma.

Implantación del plug-in en los servicios del Gobierno de Navarra:

El Gobierno de Navarra dispone de una sede electrónica (<https://www.navarra.es/es/tramites>), en la que se pueden consultar y llevar a cabo todos los trámites concernientes a la administración de este Gobierno.

El adjudicatario debe tener la capacidad de poder desarrollar plug-ins para que la solución del Wallet de Identidad Digital se pueda incorporar fácilmente en los distintos servicios digitales del Gobierno de Navarra. Se podrá solicitar el envío del documento de características de la integración con Ateka (servicio de autenticación de Gobierno de Navarra), que podrán solicitar a través del correo licitacion@nasertic.es.

El adjudicatario será el responsable de integrar estos plug-ins que permitan la autenticación con el wallet en dicha página web, para lo cual debe desarrollar o adaptar los interfaces de usuario y los componentes software apropiados, que deberán quedar personalizados para que su aspecto sea homogéneo con el software del Gobierno de Navarra.

Quedará incluido dentro del precio ofertado, la realización por parte del adjudicatario de todos los trabajos que sean necesarios para garantizar, durante toda la vigencia del contrato, la integración del servicio con los aplicativos del Gobierno de Navarra en los términos señalados en el presente Pliego, incluyendo, pero no limitado, la realización de todas las tareas de adaptación en los interfaces de usuarios y componentes que fuesen necesarios como consecuencia de las modificaciones correctivas o evolutivas que, en su caso, lleve a cabo el Gobierno de Navarra en sus aplicativos, así como, la realización de las tareas de integración que sean necesarias con cualquier nuevo canal que el Gobierno de Navarra pueda desarrollar durante la duración del presente contrato.

Infraestructuras necesarias:

La oferta deberá detallar la arquitectura definida detallando las infraestructuras hardware y software intervinientes en el proyecto. Se documentará el modelo necesario para el desarrollo, implantación y evolución del proyecto.

El proveedor, dotará de las infraestructuras servidoras hardware y software necesarias en modalidad de servicio y estas necesariamente deberán estar ubicadas en **territorio español**.

3.4. Servicio de asesoramiento

El servicio de asesoramiento a llevar a cabo incluirá todas aquellas actuaciones que resulten necesarias para:

- Asesoramiento y consultoría sobre casos de uso a los que se pueda aplicar la solución desarrollada, así como los supuestos a los que pueda extenderse. En particular, deberá exponerse las nuevas situaciones en las que puede utilizarse la nueva solución, informará al personal sobre cómo llevarlo a cabo, los requisitos necesarios para su puesta en producción, etc.
- Desarrollos y puesta en marcha de solución Wallet de Identidad Digital en el Gobierno de Navarra. Se prestará el asesoramiento necesario al Gobierno de Navarra para que la solución se adecúe lo máximo posible a las necesidades de la administración, en particular en lo referido a la personalización de la aplicación para su integración en el ecosistema del Gobierno.
- Asistencia en la integración. La empresa deberá prestar todo el asesoramiento necesario al Gobierno de Navarra para llevar a cabo una adecuada integración del Wallet de Identidad Digital. Esta asistencia deberá estar directamente relacionada con las anteriores.
- Para dicho servicio se ha estimado una dedicación mínima de 200 horas.

3.5. Servicio de Asistencia Técnica

Con el objeto de atender a las incidencias, deberá contar con un Servicio de atención técnica inmediata 24/7 donde poder ser atendidos por técnicos de, al menos, segundo nivel que den una respuesta rápida y puedan solucionar o escalar la incidencia con la prioridad establecida.

Todas estas incidencias deberán ser registradas y reportadas a NASERTIC con una periodicidad mensual, indicando, como mínimo, la relación de incidencias, duración de las mismas y tiempo de solución para cada una de ellas.

En este informe se detallará además las medidas adoptadas a posteriori para evitar dichas incidencias.

CRÍTICA	Servicio caído. App, servicio de autenticación o portal de entrada.	Resolución 2 horas
ALTA	Servicio degradado. El servicio responde lento	Resolución 8 horas
MEDIA	No afectan al servicio. Nuevos despliegues.	Sin SLA
BAJA	Resto de peticiones	Sin SLA

3.6. Seguimiento del Servicio

La programación de los trabajos será establecida en la reunión de arranque de proyecto, que se celebre tras la formalización del contrato.

NASERTIC aprobará, al inicio de los trabajos, la Planificación de los mismos y sus fases, en base a la propuesta presentada por la licitadora en su oferta y al objeto de verificar los calendarios y objetivos referidos.

En la planificación se definirán los hitos de reuniones semanales, mensuales, semestrales, y las diferentes entregas del Proyecto, plazos de las correcciones y modificaciones a introducir en la propuesta.

La planificación deberá actualizarse rigurosamente de manera periódica, debiendo disponer de un documento actualizado y accesible en todo momento en el que se puede apreciar el desarrollo y evolución de la programación.

Cualquier incidencia o evento que pueda derivar en un no cumplimiento de la programación deberá ser informado de manera inmediata a NASERTIC. Cualquier modificación deberá ser acordada y aceptada por parte de NASERTIC.

Inicialmente se prevé la realización de una reunión semanal en la fase de consultoría y asistencia para la 'Evaluación de Impacto'. Posteriormente una reunión quincenal hasta la implantación de la solución y de una reunión mensual de seguimiento hasta el final del periodo de licencia ofertado.

3.7. Documentación entregable asociada al software

En relación a los trabajos de desarrollo e implantación hechos a medida para NASERTIC y para Gobierno de Navarra, la empresa adjudicataria deberá documentar y proporcionar como mínimo la siguiente información:

- . Análisis funcional y orgánico de las soluciones desarrolladas
- . Documentación exhaustiva de las infraestructuras necesarias.
- . Código fuente de los softwares desarrollados.
- . Documentación para la generación de ejecutables e instalación.
- . Manuales de usuario, de operación y de soporte.