PLIEGO DE CONDICIONES TÉCNICAS

CONTRATACIÓN DEL SUMINISTRO, IMPLANTACIÓN Y PUESTA EN MARCHA DE UN SISTEMA INTEGRADO DE CONTROL DE PRESENCIA Y CONTROL DE ACCESOS

MARZO DE 2026

nasertic

Navarra de Servicios y Tecnologías, S.A.
| C/ Orcoyen, s/n. 31011 Pamplona - Navarra |
| info@nasertic.es | www.nasertic.es
| Tel: 848 420 500 | Fax: 848 426 751

Índice

1 Introducción

La sociedad pública **NASERTIC (Navarra de Servicios y Tecnologías, S.A.)**, en adelante NASERTIC, en el marco de su actividad y de sus necesidades de gestión interna y de seguridad, requiere la contratación de una **solución integral de software para el control de presencia**, así como para la **gestión de accesos, custodia y autorizaciones**.

Actualmente, NASERTIC dispone de distintos sistemas y terminales que requieren una **modernización y adaptación tecnológica**, tanto a nivel de software como de hardware asociado, con el objetivo de mejorar la seguridad, la eficiencia operativa y la trazabilidad de los accesos y presencias en sus instalaciones.

Mediante el presente pliego se definen las condiciones técnicas que han de regir la contratación de dichas soluciones, que deberán ser **robustas, escalables y adecuadas a un entorno con múltiples ubicaciones**, garantizando su correcto funcionamiento para el volumen actual de usuarios y autorizados, así como su posible crecimiento futuro.

2 Objeto

El objeto del presente contrato es la contratación, suministro, implantación y puesta en marcha de dos soluciones de software, **licitadas de forma conjunta e inseparable**, que cubran los siguientes ámbitos (Se pueden considerar dos sistemas siempre que estén interconectados):

- Sistema de control de presencia (fichaje) del personal.
- Sistema de control de accesos, custodia y gestión de autorizaciones para personal interno y autorizados externos.

Ambas soluciones deberán ser plenamente compatibles e integradas entre sí, de manera que la empresa licitadora deberá ofrecer una solución global para ambos sistemas, no admitiéndose ofertas parciales.

El alcance del contrato incluye, de forma no limitativa:

- La provisión del software necesario para ambos sistemas.
- La modernización de los terminales de fichaje y puntos de control de acceso, incluyendo su configuración y puesta en servicio.
- La implantación de la solución en un entorno compuesto por:
    - Hasta 250 empleados.
    - Hasta 600 autorizados permanentes.
    - 8 ubicaciones físicas diferenciadas.
    - 36 puntos de control de acceso.
    - 8 terminales de fichaje.
    - Provisión de 2 sistemas lectores/escritores de tarjetas y 500 tarjetas contactless.
    - Estudio de Integración de los 6 terminales existentes de acceso biométrico de la empresa Veridas.
    - Control de acceso a tres puntos en el CPD de Beloso. Se detalla este caso especial en el punto 3.5.
    - Sistema de custodia de material.

- La correcta integración e instalación de los sistemas en las infraestructuras existentes de NASERTIC.
- La puesta en producción y verificación del correcto funcionamiento de la solución.
- La formación del personal técnico y administrativo de Nasertic.
- Documentación tanto técnica como de usuario.

La solución ofertada deberá garantizar la seguridad, disponibilidad y trazabilidad de la información, así como cumplir con la normativa vigente en materia de protección de datos y seguridad de la información.

3 Detalle material a proveer

3.1 Material a proveer

La empresa adjudicataria deberá suministrar, instalar y dejar plenamente operativos los siguientes elementos:

- 8 terminales para control de presencia
- 36 terminales para control de accesos
- Las controladoras, unidades de control de accesos (UCA) o dispositivos asociados que resulten necesarios para garantizar la correcta operativa de los terminales de control de presencia y accesos con la solución software ofertada.
- 4 terminales para control de acceso alternativo en Beloso (detalle en punto 3.5)
- 2 sistemas lectores/grabador de tarjetas
- 500 tarjetas contactless compatibles con la solución propuesta.

Los dispositivos proporcionados deberán cumplir con las especificaciones mínimas detalladas en el punto 3.7

3.2 Sedes

Los terminales y puntos de control objeto del presente contrato se instalarán distribuidos en las sedes que se indican a continuación:

- Oficinas ubicadas en Pamplona, en el barrio de San Jorge, en la zona de la calle Orcoyen y en el entorno del Paseo de Pablo Sarasate.
- Laboratorio situado en Villava.
- Centro Vidaas situado en Sarriguren.
- Oficina de Atención a la Ciudadanía (OAC) en Tudela.
- Polo IRIS, ubicado en el entorno de la calle del Sadar (Pamplona).
- Instalaciones situadas en la zona de Beloso (Pamplona).

Las ubicaciones exactas y demás información detallada necesaria para la correcta ejecución del contrato serán facilitadas exclusivamente a la empresa que resulte adjudicataria, una vez formalizado el contrato y bajo las correspondientes obligaciones de confidencialidad.

3.3 Terminales de control de presencia

Será necesaria la instalación de terminales físicos de control de presencia, que permitan a los empleados realizar el fichaje y asociarlo a una incidencia concreta, en las siguientes sedes:

- San Jorge
- OAC Tudela
- Calle Orcoyen
- Laboratorio (2 terminales)
- Polo Iris

- Centro Vidaas
- Sarasate

3.4 Terminales de control de acceso

Será necesaria la instalación de puntos de control de acceso en las siguientes sedes, con el detalle que se indica a continuación:

- **Laboratorio**:
  - 6 puntos de control de acceso con control de entrada, de los cuales 2 estarán ubicados en el exterior.
- **San Jorge:**
  - 2 punto de control de acceso con control de entrada.
- **Beloso**:
  - 4 puntos de control de acceso con tarjeta combinados con sistema alternativo explicado en el punto 3.5
- **Calle Orcoyen**:
  - 3 puntos de control de acceso con control de entrada y salida.
  - 22 puntos de control de acceso con control de entrada.

3.5 Control de accesos en Beloso

Además del acceso con tarjeta, el acceso a las instalaciones de Beloso requiere un sistema de autenticación que no dependa de la entrega de elementos físicos y que pueda ser utilizado por usuarios autorizados que no dispongan de un teléfono móvil corporativo. Actualmente, estos usuarios acceden mediante un lector de DNI electrónico, tras la validación previa de su identidad por parte de un agente de la Policía Foral y la comprobación de que figuran en la lista de personas autorizadas. Los dispositivos de lectura de DNI existentes no pueden reutilizarse.

Es necesario implementar una solución para el control de acceso, ya sea manteniendo el uso del lector de DNI electrónico o mediante un sistema equivalente. Se considerarán válidos aquellos sistemas que puedan enviarse digitalmente al cliente y que permitan el acceso mediante un soporte físico, como un código QR imprimible. En caso de optar por esta alternativa, la credencial proporcionada deberá poder deshabilitarse desde el panel de administración.

Asimismo, la empresa deberá detallar la solución propuesta para esta sede, incluyendo los dispositivos que se instalarán y el procedimiento que se seguirá para garantizar el control de acceso.

3.6 Especificaciones técnicas mínimas

Los dispositivos proporcionados deberán cumplir al menos con las especificaciones mínimas aquí detalladas:

3.6.1 Terminales control de accesos:

- Compatible con DESFire EV3
- Rango de lectura: 0-4cm o superior
- Protección IP65 o superior
- Tiempo de lectura < 500ms
- Rango funcionamiento dentro del rango -5ºC hasta 50ºC
- Soporte del 90% humedad o superior

- Cumplir estándar ISO14443A
- Sistema auxiliar en caso de corte eléctrico o perdida de conectividad.

3.6.2 Terminales control de presencia:

- Posibilidad de marcar la incidencia/tipología del fichaje en el dispositivo.
- Teclado numérico incorporado
- Compatible con DESFire EV3
- Rango de lectura: 4cm o más
- Protección IP65 o superior
- Tiempo de lectura < 500ms
- Rango funcionamiento dentro del rango -5ºC hasta 50ºC
- Soporte del 90% humedad o superior
- Cumplir estándar ISO14443A

3.6.3 Lector/grabador de tarjetas

- Compatible con DESFire EV3
- Compatible con Windows 11 conexión a través de puerto USB
- Deberá permitir la grabación de tarjetas
- Cumplir estándar ISO14443A

3.6.4 Tarjetas inteligentes

- Formato: tarjeta de crédito
- Compatible con DESFire EV3
- Soporte AES-128 o superior
- Espacio de almacenamiento suficiente para operar con el sistema de control de accesos y presencia

4 Control de presencia

Se requiere la contratación de una solución de control de presencia que permita gestionar de manera eficiente los fichajes, saldos de jornada y horarios del personal, tanto desde terminales físicos como desde ordenadores y dispositivos móviles. La solución deberá garantizar la correcta contabilización de tiempo efectivo, ausencias, horas expandidas y vacaciones, cumpliendo la normativa laboral vigente y futuras actualizaciones o cambios en el funcionamiento laboral de la empresa.

4.1 Requisitos funcionales

1) **Fichaje y consulta** de fichajes y saldos desde terminales físicos, ordenadores y dispositivos móviles tipo smartphone. Los terminales físicos serán instalados por la empresa licitadora (8 unidades), cuyas ubicaciones se detallan en el punto 3.
2) **Modalidades de fichaje** diferenciadas: presencial y teletrabajo.
3) **Corrección de fichajes** por parte del usuario en caso de olvido o incidencia, sujeta a autorización del responsable.
4) **Detección automática de incidencias**, tales como fichajes incorrectos, ausencias de fichaje o faltas injustificadas.
5) **Gestión de calendarios y jornadas**, incluyendo:
   - Definición de múltiples calendarios para cada área.
6) **Control Calendario Guardias**: algunas Áreas de la empresa requieren la realización de guardias localizadas.
   - Configuración de diferentes duraciones de jornada, incluidas jornadas reducidas.
   - Gestión de turnos y tipos de jornada (partida, mañana, tarde, noche).
   - Soporte para horarios flexibles y horarios fijos.
7) **Gestión de jornada flexible**, conforme al modelo de funcionamiento de NASERTIC, que incluya:
   - **Bolsa de flexibilidad** de ±10 horas, sin caducidad y acumulable de un año a otro.
   - Limitar el tiempo de trabajo diario "normal" de flexibilidad al horario comprendido entre las 7:00 y las 21:00.
   - Limitar el tiempo máximo de trabajo en una jornada "normal" a 10 horas de trabajo efectivo.
   - Cómputo de tiempo de trabajo efectivo según flexibilidad con un acumulado máximo de ±10 horas. Las horas trabajadas por encima de +10 no computan con la salvedad del siguiente punto.

   Tratamiento especial horas excedidas de la flexibilidad (+10 horas). Estas horas darán derecho a horas de vacaciones de acuerdo a lo estipulado en el apartado de gestión de horas expandidas. (Prolongación de horario u horas expandidas 1x1)
   Tratamiento especial para las horas excedidas del horario máximo diario (10 horas) durante el horario comprendido entre las 07:00 y las 21:00: Estas horas darán derecho a horas de vacaciones de acuerdo a lo estipulado en el apartado de gestión de horas expandidas. (Prolongación de horario u horas expandidas 1x1)
   Tratamiento especial para el tiempo de trabajo fuera del horario "normal" de flexibilidad, es decir de 21:00 a 07:00 en días laborables o días festivos: Estas horas darán derecho a horas de vacaciones de acuerdo con lo estipulado en el apartado de gestión de horas expandidas. (Horas expandidas 1x2)
   - El empleado debe tener la posibilidad de consultar su saldo de horas

Gestión de horas expandidas y horas/días de vacaciones:
Bajo determinadas circunstancias detalladas en este punto el personal de Nasertic puede generar horas expandidas. Estas horas son independientes de la bolsa de horas de flexibilidad.
Estas horas expandidas deben disfrutarse en los 12 meses siguientes a su generación, la aplicación tendrá que contemplar la posibilidad de incluir la caducidad de las horas o que se calcule automáticamente. Superados los 12 meses de posibilidad de disfrute, estas horas caducarán y no se mantendrán en la bolsa de horas expandidas

- El empleado puede visualizar su saldo de horas expandidas, así como su caducidad.
- Este es el funcionamiento:
  - Prolongación de horario u horas expandidas 1x1:

Por necesidades del servicio se pueden dar dos situaciones que generan horas que dan derecho a vacaciones donde la relación de cambio es 1x1. Son los siguientes casos:

1er caso: Que una persona trabaje más del horario máximo diario (10 horas) durante el horario comprendido entre las 07:00 y las 21:00. El tiempo excedido de las diez horas habrá que solicitarlo por el frontal web como horas expandidas y deberán ser aprobadas por la persona Responsable de Área.

2º caso: Que supere su desfase máximo permitido (+10) por una carga de trabajo excepcional y prolongada.

En este caso, la persona NO solicita horas expandidas por el frontal web, sino que lo comunica a su responsable de Área vía mail. El procedimiento sería:
1º) Previamente, la persona Responsable de Área comunica a RRHH que existe una carga de trabajo excepcional y prolongada que puede provocar esta situación.
2º) Al final de mes, concretamente en los 3 primeros días laborales del mes siguiente, el/la trabajador/a sacará sus tiempos no computados del módulo web del control de presencia y por mail le traslada a su responsable de Área la petición de qué tiempos solicita que le sean considerados como horas expandidas.
3º) La persona Responsable de Área comunica a RRHH en los 5 primeros días laborales del mes siguiente que tiempos considera que hay que incluir como horas expandidas.
4º) RRHH introducirá las horas aceptadas como horas expandidas.

- Horas expandidas 1x2:

Por necesidades del servicio y con la aprobación de la persona Responsable de Área puede ser necesario que una persona trabaje fuera del horario flexible (es decir de 21:00 a 07:00 en días laborables) o días festivos. En el caso de que no pueda preverse (ej. Cortes de servicio), la persona afectada deberá comunicarlo a su responsable de Área en la siguiente jornada laboral.
En este caso, la persona Responsable de Área aprobará la realización de dichas horas aceptando la solicitud que deberá realizar la persona trabajadora a través del frontal web.
Estas horas darán derecho a horas de vacaciones y la relación de cambio es 1x2.

8) **Día de vacaciones por horas**: El personal de Nasertic dispone de un día de vacaciones que puede disfrutarse por horas. Actualmente, estas horas se registran como "horas expandidas" desde RRHH y funcionan de la misma manera que las horas expandidas. RRHH ingresará estas horas al inicio del año, estableciendo como fecha de caducidad el 31 de enero del año siguiente. La aplicación deberá permitir

añadir estas horas como "horas expandidas" o, alternativamente, contar con un sistema equivalente que facilite la gestión de los días de vacaciones por horas.

9) **Gestión de solicitudes y autorizaciones** (salidas, permisos, vacaciones, horas expandidas, ver calendario, hacer diversas consultas) y flujo y jerarquía de responsables para la aprobación

- La solicitud deberá de ser cursada previamente a la ausencia y en un plazo de tiempo razonable y para casos de urgencia podrán ser solicitadas a posteriori.
- Una vez solicitada, al responsable le llegará un aviso mail con toda la información y desde el smartphone o desde el ordenador aprobará o rechazará esa solicitud.
- Posteriormente al solicitante le llegará un aviso por mail con la decisión tomada por el responsable.
- Posibilidad de adjuntar documentación (justificantes), confidencialidad. Aviso en caso de que falte el adjunto: Es importante recordar que aquellas solicitudes que requieran un justificante externo, éste se deberá adjuntar.
- En caso de IT o vacaciones la solicitud deberá poder ser gestionada por su superior o sustituto designado temporalmente.

Ejemplos solicitudes:

- Nueva salida de trabajo (por horas)
- Nueva salida particular (por horas)
- Nueva salida particular especial (por horas)
- Nueva compensación de horas expandidas (por horas)
- Nueva solicitud de horas expandidas (por horas)
- Nuevo permiso no recuperable (por días)
- Nueva solicitud de vacaciones (por días)
- Consulta de mis solicitudes

10) **Registro y gestión de salidas distintas** (almuerzo, fumar, permisos, etc.) con posibilidad de tener distintos tratamientos de forma que computan como tiempo de trabajo efectivo o no. Estos podrán ser modificados desde el panel de administración, este es el listado inicial:

- Almuerzo (Se computa como tiempo efectivo hasta un límite configurable, pasado el cual no se considera tiempo trabajado.)
- Particular
- Particular Especial
- Trabajo
- Fumar
- Teletrabajo
- Huelga
- Horas sindicales

11) Posibilidad de que permita ciertos automatismos en el inicio o la finalización de la jornada, como sería:

    - Inicio: si comenzamos con una incidencia automáticamente registra la entrada.
    - Fin: si finalizamos la jornada cierra automáticamente si existe una incidencia abierta.
    - Por ejemplo, cuando un empleado comienza la jornada con una salida de trabajo que pueda fichar directamente la incidencia "Trabajo" y se abra la jornada en ese momento.

12) Posibilidad de **imputar ausencias de larga duración** que no necesitan solicitud:

    - Incapacidad Temporal (bajas por enfermedad o accidente)
    - Descanso por maternidad/paternidad
    - Ausencia del trabajo o reducción de jornada por lactancia
    - Excedencias / Licencia no retribuida / Permiso parental

13) Diversidad de **Informes** y que se puedan trabajar en Excel y PDF. Ejemplos de informes que se deberán poder extraer de la herramienta:

    - Informes de horas efectivas por rangos de tiempo
    - Informes de horas por tipos de salida y/o incidencia y por rangos de tiempo
    - Informe de horas expandidas por rangos de tiempo y su caducidad
    - Informes de ausencias
    - Informes de personas por áreas/responsable

14) Integración con ERP Sigrid, ya sea integración directa o que la aplicación ponga a **disposición una API** con la que hacer las integraciones, estas son las funcionalidades mínimas con las que debe contar la API.
    - Posibilidad de dar de alta y baja empleados. Así como modificar sus atributos.
    - Posibilidad de gestionar la jerarquía de responsables.
    - Poder consultar las horas efectivas realizadas agrupadas por empleado y día.
    - Poder consultar las horas realizadas por tipo de incidencia por empleado y día.
    - Poder consultar para un empleado y día sus ausencias, jornada asignada, fichajes…
    - Tener acceso a la información de las solicitudes realizadas a través de la aplicación.
    - Autenticación segura: OAuth 2.0, API Key, JWT…
    - Proveer entorno de pruebas para realizar integraciones de una manera segura sin afectar al sistema principal.

15) **Distintos perfiles de usuario**:
    - Perfil RRHH
    - Perfil para "vigilantes" (caso evacuación)
    - Perfil para responsables
    - Perfil usuario

16) **Control de auditoría**: Se registrarán todos los cambios realizados en los datos gestionados por la aplicación, incluyendo el autor, la fecha, los datos modificados y el motivo, para garantizar trazabilidad y un seguimiento completo de las modificaciones.
17) **Cumplimiento normativo y adaptaciones**: El sistema deberá cumplir en todo momento la normativa laboral vigente y futuras actualizaciones en materia de control de presencia y registro de jornada. Cualquier adaptación, actualización o ajuste necesario para garantizar dicho cumplimiento deberá estar incluida dentro del precio del plan de mantenimiento, sin coste adicional para NASERTIC.
18) **Fichajes georreferenciados:** La solución propuesta deberá incluir la funcionalidad de geolocalización asociada al registro horario, configurable para su activación o desactivación por grupos o usuarios concretos. Dicha funcionalidad deberá limitarse exclusivamente al momento del registro de entrada o salida, sin realizar en ningún caso un seguimiento continuo.

5 Control de acceso y autorizaciones

La aplicación tiene como objetivo gestionar los accesos físicos a cuatro Sedes mediante flujos de autorización diferenciados según el tipo de usuario. Se busca garantizar la trazabilidad, la seguridad y el cumplimiento normativo, adaptándose a las necesidades de trabajadores, contratas, clientes Housing y externos.

El detalle de sedes y ubicación de terminales a instalar se encuentra recogido en el punto 3 del presente documento. Adicionalmente, se amplía la información en el "ANEXO I. CONTROL DE ACCESOS", donde se definen, entre otros, los roles y flujos de autorización relacionados con el control de accesos.

5.1 Requisitos funcionales

1) **Gestión de usuarios y perfiles:** Capacidad para gestionar usuarios y roles, un usuario puede tener varios roles de manera concurrente y estos permisos pueden estar ligados a unos accesos/zonas determinadas. Los detalles de los roles necesarios se encuentran recogidos en el ANEXO I.
2) **Gestión de sedes:** Posibilidad para gestionar múltiples sedes y asociar puntos de acceso correspondientes a cada una de ellas.
3) **Gestión de zonas:** Los accesos se podrán agrupar en unidades lógicas (zonas) para simplificar la gestión de acceso que requieran múltiples puntos de control.
4) **Gestión de vehículos autorizados:** La aplicación deberá permitir gestionar datos de coches autorizados para el acceso a la sede de Beloso (matrícula, color, modelo y entidad asociada). La verificación de que un vehículo este autorizado se hace manualmente.
5) **Flujos de validación configurables:** La aplicación permitirá configurar los flujos de aprobación para diferentes casuísticas, como mínimo deberá ser capaz de dar soporte a los flujos definidos en el ANEXO I.
6) **Historial de accesos y autorizaciones:** El sistema deberá disponer de un registro histórico que permita consultar los accesos realizados y las autorizaciones, incluyendo fecha, hora y datos relevantes de la acción. Dicho historial deberá ser accesible para personal autorizado para tareas de auditoría y control interno. También debe poder consultarse el historial de modificaciones.
7) **Confirmación lectura de documentación:** La herramienta permitirá registrar que una entidad ha leído la documentación obligatoria requerida para el acceso. El acceso podrá configurarse para denegarse si esta no ha sido leída.
8) **Verificación del CAE:** El sistema deberá comprobar automáticamente el cumplimiento de los requisitos de Coordinación de Actividades Empresariales (CAE) antes de autorizar el acceso. En caso de incumplimiento, el acceso será denegado automáticamente a las entidades asociadas.
9) **Limitación temporal del acceso:** El acceso de una persona a una zona concreta deberá poder limitarse a un horario y/o fechas determinadas. Podrán fijarse fechas a futuro tanto de altas como de bajas.
10) **Integración con terminales**: La solución deberá incluir la instalación y configuración de los terminales de acceso suministrados, así como su integración con la plataforma central.
11) **Avisos y notificaciones vía email:** Se podrá configurar la herramienta para avisar a las personas responsables de las nuevas solicitudes pendientes que requieren su aprobación vía mail. También podrán configurarse avisos ligados a determinados sucesos (alarmas, accesos no autorizados…).

12) **Integración vía API**: La plataforma deberá proporcionar interfaces de programación de aplicaciones (API) abiertas y documentadas que permitan la integración con otros sistemas corporativos, como control de presencia, RRHH, ERP u otros sistemas de gestión, garantizando la interoperabilidad, el intercambio seguro de datos y la actualización en tiempo real de usuarios, accesos y autorizaciones.
13) **Informes**: La herramienta contará con un apartado de informes que permita sacar de alguna forma esta información:
    - Informe de personal presente en cada Sede en el momento de ejecución. Aplicable para situaciones de evacuación del edificio o emergencia. Este documento deberá poder obtenerse de manera sencilla y ágil.
    - Informes de acceso por persona, por contrata o cliente housing con posibilidad de envío directo al responsable de estos por email.
    - Informes de personal con acceso permanente por contrata, por clientes housing, por sede, por zona o por zona y sede.
    - Los responsables de Contrata o housing podrán obtener informe de su personal de alta.

5.2 Módulo: Gestión de custodia de material/llaves

Actualmente disponemos de un sistema de control de accesos con un software propio desarrollado ad hoc para este tema. Es un software muy obsoleto que es necesario renovar totalmente.

El SW actual gestiona los siguientes puntos:

- Materiales: alta, modificación, baja y borrado de materiales de custodia. Pueden ser llaveros, portátiles, móviles, sobres, …
- Personas: alta, modificación y baja de permisos de acceso a materiales.
- Llaves: gestión de llaves, alta de llaveros y llaves, ubicación y apertura.
- Consultas: búsqueda por DNI, descripción o material y fechas.

Este software debe estar integrado dentro del programa de gestión de accesos.

5.2.1 Requisitos funcionales

1) **Integración con control de accesos:** El sistema deberá integrarse con el software de gestión de accesos y utilizar la misma base de usuarios.
2) **Gestión de material:** El sistema deberá permitir registrar y mantener los elementos de custodia con sus datos básicos (identificador, nombre, ubicación, tipología y observaciones). Pueden ser llaveros, portátiles, móviles…
3) **Responsables de material:** el sistema permite marcar uno o varios responsables a un material que será quienes gestionen el uso de este.
4) **Búsqueda y filtrado:** El sistema permitirá buscar llaves por usuario asignado, identificador, nombre u tipología.
5) **Asignación y cesión de material:** El sistema permitirá asignar material a un usuario de forma temporal o indefinida, registrando el momento de entrega y de devolución.
6) **Autorizados permanentes a material:** El sistema deberá contar con un listado de autorizados para cada material, de tal forma que estas personas puedan recoger

ese material sin que sea necesaria autorización por responsable. El alta en este listado deberá ser aprobada o tramitada por un responsable de ese material.

7) **Baja de material**: El sistema permitirá dar de baja lógicamente del sistema el material, permitiendo consultar el histórico de llaves de baja junto con el histórico de acciones asociadas.
8) **Consulta de disponibilidad:** El sistema deberá permitir consultar en tiempo real el estado y la disponibilidad del material.
9) **Seguridad y trazabilidad:** La plataforma deberá registrar de forma completa todos los eventos de uso, incluyendo llave, usuario, fecha, hora y usuario que hace la asignación. Debe permitir ver el historial de usos y modificaciones, así como cumplir con RGPD y normativa de prevención.
10) **Integración vía API**: La plataforma deberá proporcionar interfaces de programación de aplicaciones (API) abiertas y documentadas que permitan la integración con otros sistemas corporativos, como control de accesos, presencia, RRHH, ERP u otros sistemas de gestión, garantizando la interoperabilidad, el intercambio seguro de datos y la actualización en tiempo real de los datos.

6 Requisitos técnicos

El objeto del contrato es **el suministro, instalación y puesta en marcha**, en modalidad llave en mano, de una solución software para el control de accesos y control de presencia.

Dada la criticidad de la infraestructura de control de accesos, el software asociado a dicha parte de la solución deberá implantarse obligatoriamente en modalidad On-Premise. Únicamente se valorarán aquellas soluciones ofertadas en modalidad On-Premise que cumplan los requisitos técnicos especificados en el apartado 6.1.

En el caso de las soluciones de control de presencia, la empresa licitadora deberá indicar expresamente la modalidad ofertada (On-Premise o SaaS), debiendo cumplir los requisitos establecidos en el apartado 6.1 para soluciones On-Premise o en el apartado 6.2 para soluciones en modalidad SaaS. Los dos tipos de modalidades de despliegue serán aceptadas para el software de control de presencia.

La empresa deberá presentar la documentación técnica de las soluciones propuestas incluyendo un diagrama lógico y físico de la misma.

6.1 Requisitos técnicos soluciones On-Premise

1) **Modalidad de despliegue:** Todos los servicios, así como los datos gestionados por la solución, deberán estar alojados en la infraestructura securizada proporcionada por Nasertic.
2) **Infraestructura virtualizada** en VMware vSphere, con Servidores Windows Server 2022 datacenter, servidores RedHat 9 enterprise, o infraestructura basada en Kubernetes.
3) **Base de datos:** La base de datos principal de la solución deberá estar implementada sobre instancias de SQL Server 2019 standard, proporcionadas y gestionadas por Nasertic.
4) **Servicios auxiliares y componentes adicionales:** Se permitirá la utilización de servicios auxiliares o componentes adicionales necesarios para el correcto funcionamiento de la solución, tales como:
   - Sistemas de caché o gestión de sesiones (por ejemplo, Redis).
   - Bases de datos NoSQL u otros sistemas para la captación y gestión de logs.

   En caso de que la solución requiera la instalación de este tipo de servicios complementarios, la empresa licitadora deberá:
   - Identificar claramente los servicios adicionales necesarios.
   - Describir su función dentro de la arquitectura de la solución.

   En caso de requerirse conexión con servicios externos, deberá justificarse su necesidad, garantizando que la solución pueda **seguir operando con normalidad ante una caída de dichos servicios.**
5) **Seguridad y aislamiento:** La solución deberá respetar las políticas de seguridad, segmentación y control de accesos definidas por Nasertic para sus entornos On-Premise.
6) **Esquema detallado de la infraestructura y comunicaciones:** La empresa licitadora deberá aportar un **esquema detallado de la infraestructura**, incluyendo las comunicaciones y las interconexiones entre los distintos servicios que componen la solución.

6.2 Requisitos técnicos soluciones SaaS

1) **Modalidad de despliegue:** La empresa licitadora será responsable del suministro, operación y mantenimiento de todos los componentes necesarios para la correcta prestación del servicio durante la vigencia del contrato.
2) **Infraestructura y alojamiento:** La infraestructura que sustente la solución deberá estar alojada en un **proveedor de servicios de computación en la nube de reconocido** prestigio, que haya figurado en los tres últimos años como líder o actor principal en informes de referencia del sector (Gartner, Forrester Wave o IDC MarketScape).

Los **centros de datos deberán estar ubicados en territorio europeo.**

3) **Plataforma y costes asociados**: La solución deberá incluir **todos los costes asociados a infraestructuras, software, licencias, mantenimiento y operación**, así como cualquier coste derivado del uso de la plataforma que exceda una conexión estándar a Internet desde los puestos de trabajo de la entidad contratante.
4) **Gestión de la seguridad de la información:** La solución deberá cumplir con la normativa vigente en materia de protección de datos de carácter personal y seguridad de la información.
5) **Disponibilidad:** La solución ofertada deberá contar con una disponibilidad equivalente a la de un centro de datos Tier II, es decir, la solución tolerará un **tiempo máximo de inactividad anual de 22 horas.**
6) **Auditoría y trazabilidad:** La solución deberá disponer de **mecanismos de auditoría** que permitan el registro, consulta y análisis de los eventos relevantes de la plataforma, incluyendo accesos, operaciones y detección de comportamientos anómalos.
7) **Cifrado de la información**: La solución deberá garantizar el **cifrado de las comunicaciones** mediante protocolos seguros (TLS) y el **cifrado de la información almacenada** mediante algoritmos robustos (AES o equivalentes).
8) **Evidencias técnicas**: La empresa licitadora deberá aportar en la memoria técnica **evidencias suficientes** o referencias a documentación pública que permitan verificar el cumplimiento de todos los requisitos técnicos establecidos en este apartado.

7 Tecnologías

El licitador deberá garantizar que la solución ofertada cumple con los siguientes requisitos:

- Todos los componentes de la solución estarán desarrollados y soportados con tecnologías actuales, y en ningún caso tendrán previsto su fin de vida (EOL) o fin de soporte del fabricante (EOS) antes de la finalización del contrato.
- El desarrollo de la solución deberá seguir buenas prácticas de seguridad y las directrices de SANS y OWASP.
- La solución deberá cumplir las directrices de accesibilidad para el contenido web (WCAG).
- Acceso desde móvil, nativo o web app para gestión de accesos desde smartphone. Esta debe ser responsive y permitir hacer las acciones desde el móvil que desde la web.
- La plataforma deberá contar con un compromiso de actualización continua, garantizando mejoras y mantenimiento a lo largo de la vigencia del contrato.
- Deberá existir un procedimiento documentado para la aplicación de actualizaciones de seguridad y de software, minimizando el tiempo de exposición a vulnerabilidades.
- Escalabilidad y rendimiento: Garantizar que la solución puede crecer en número de usuarios, terminales y puntos de control sin degradar el rendimiento.

8 Soporte y mantenimiento

La empresa adjudicataria deberá presentar un plan de soporte y mantenimiento, que integre tanto la gestión de incidencias del software como las consultas y la asistencia técnica funcional de la herramienta. El plan deberá incluir los horarios de atención, los métodos de comunicación y el tipo de actuaciones (remotas o in situ) necesarias para resolver incidencias y consultas relacionadas con la plataforma contratada.

La empresa adjudicataria deberá incorporar a este plan la atención específica de las incidencias y consultas por parte de NASERTIC. Asimismo, el adjudicatario deberá llevar a cabo las actuaciones de mantenimiento preventivo, correctivo y adaptativo requeridas durante toda la vigencia del contrato.

El sistema de información que forme parte de la solución técnica deberá permitir que el equipo interno de NASERTIC realice cambios basándose en la información proporcionada por el proveedor. El adjudicatario se compromete a proporcionar la asistencia técnica necesaria para que el equipo interno pueda realizar dichos cambios en la configuración de manera segura y eficiente.

8.1 Acuerdos de Nivel de servicios (SLA)

El adjudicatario se compromete a solucionar los errores de funcionamiento una vez hayan sido reportados. Asimismo, deberá registrar todas las incidencias y solicitudes y proporcionar respuesta, ya sea por teléfono o correo electrónico, incluyendo la solución propuesta o implementada.

Las incidencias se clasificarán de acuerdo con las siguientes categorías:

- **Baja:** Incidencia que no afecta al funcionamiento operativo de la solución.
- **Moderada:** Incidencia que afecta a una parte no crítica de la solución.
- **Urgente:** Incidencia que afecta a un gran número de usuarios y/o a funcionalidades críticas del proceso.
- **Crítica:** Incidencia que impide completamente el uso del sistema.

Los **tiempos de respuesta y resolución remota** desde la hora/fecha de aviso se establecerán en función de la categoría de la incidencia, garantizando una atención proporcional a la gravedad del problema, los tiempos son detallados en la siguiente tabla, todos ellos expresados en horas/días naturales:

Parámetro	Categoría	Tiempo máximo
Tiempo de respuesta	Baja	24 horas
	Moderada	8 horas
	Urgente	4 horas
	Crítica	2 horas
Tiempo máximo de resolución para las actuaciones según prioridad establecida.	Baja	5 días
	Moderada	3 días
	Urgente	8 horas
	Crítica	4 horas

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.

8.2 Plan de formación

El adjudicatario estará obligado a impartir todas las acciones formativas necesarias que requiera el órgano de contratación para garantizar el correcto manejo del equipamiento y de los sistemas de información, asegurando su óptima utilización tanto desde el punto de vista operativo como funcional. La amplitud y calidad de la formación deberán ser suficientes para asegurar el perfecto manejo y máximo rendimiento de los sistemas y del equipamiento objeto del contrato.

La formación deberá ser especializada según el tipo de usuario, de manera que cada perfil pueda utilizar el equipamiento y los sistemas conforme a las indicaciones del fabricante y ejecutar correctamente las rutinas de servicio.

Cualquier modificación o actualización del equipamiento o de los sistemas de información implicará la realización de un nuevo periodo de formación bajo los mismos criterios de especialización y cobertura.

Será obligatorio que el adjudicatario esté a disposición de NASERTIC para impartir la formación y el entrenamiento necesario, en las condiciones y plazos que se indiquen.

8.3 Documentación técnica y de usuario

La plataforma deberá incluir documentación técnica completa, que abarque guías de instalación, configuración, operación y mantenimiento, permitiendo a los equipos responsables gestionar y administrar correctamente la solución.

Asimismo, deberá proporcionarse documentación de usuario final, clara y accesible, que facilite la adopción y el uso eficiente de la plataforma por parte de todos los perfiles de usuarios previstos.

9 Planificación

Los licitadores deberán presentar cronogramas que especifiquen las **fases, tareas y su distribución temporal**. La primera tarea del adjudicatario será acordar un **diseño de solución integrado** y entregar una planificación detallada para su implantación.

La planificación deberá estructurarse en las siguientes fases:

Fase I: Implantación Gestión de Presencia: El objetivo de esta fase es implantar conforme los requerimientos de RRHH de la parte de la solución que gestiona las personas.

- Establecer y documentar los componentes necesarios para implementar el sistema de información y definir cómo se realizarán las integraciones con los demás sistemas corporativos indicados.
- Instalación de terminales de control de presencia.
- Implantación de la solución.
- Formación.

Fase II: Implantación Control de Accesos y Custodia: El objetivo de esta fase es implantar conforme los requerimientos del Área de Sistemas Distribuidos la parte de la solución que gestiona los accesos.

- Establecer y documentar los componentes necesarios para implementar el sistema de información y definir cómo se realizarán las integraciones con los demás sistemas corporativos indicados.
- Instalación de terminales de control de presencia.
- Instalación de componentes software de la instalación.
- Implantación de la solución.
- Formación.

En todo caso la puesta en marcha total de la solución se realizará según lo previsto en la cláusula 6 del PCA**.**

10 Seguimiento del contrato

Durante la ejecución del servicio objeto del contrato, la empresa adjudicataria se compromete a facilitar, en todo momento, a las personas designadas por la persona responsable de NASERTIC, la información y documentación necesarias para mantener un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los posibles problemas que puedan surgir y de las tecnologías, métodos y herramientas empleadas para su resolución.

La empresa contratista deberá informar periódicamente a la persona responsable de NASERTIC sobre distintos aspectos del funcionamiento y la calidad del servicio, siendo obligatorio presentar un informe de actividad y seguimiento de carácter trimestral.

Asimismo, la empresa adjudicataria deberá asistir y colaborar, mediante el personal que designe, a las reuniones de seguimiento del proyecto convocadas por NASERTIC, con la debida antelación para facilitar la asistencia de su personal.

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

En caso de que la empresa adjudicataria proponga la sustitución de la persona designada, deberá hacerlo por escrito y acreditar que la persona propuesta cuenta con la misma o mayor experiencia y titulación exigida.

ANEXO I. Control de Accesos

1. Introducción

La aplicación tiene como objetivo gestionar los accesos físicos a dos Sedes mediante flujos de autorización diferenciados según el tipo de usuario. Se busca garantizar la trazabilidad, la seguridad y el cumplimiento normativo, adaptándose a las necesidades de trabajadores, contratas, clientes Housing y externos.

2. Tipos de usuarios

- **Propietarios**
  - Personal que puede autorizar accesos a una u otra sede (rol *Responsable Sede*, perfil interno)
- **Trabajadores**
  - Responsables: Personal que puede autorizar accesos a alguna sede (rol *Responsable Sede*, perfil interno)
  - Trabajadores: Personal interno con acceso permanente o temporal. Algunos de ellos tendrán el rol de *Responsable Servicio* Contrata (perfil interno) o de *Responsable Servicio Cliente Housing* (perfil interno).
- **Subcontratas o proveedores de servicio**: Personal de empresas colaboradoras que cuentan con:
  - En cada subcontrata habrá uno o varios responsables que gestionarán los accesos permanentes y solicitarán los accesos temporales (rol *Responsable Contrata,* perfil externo))
  - Personal con acceso permanente o temporal
- **Clientes Housing**: Usuarios de espacios dedicados dentro de 1 de los edificios. Cuentan con:
  - Personas responsables: Mantiene los listados de personal con acceso permanente a su espacio y solicita accesos temporales (rol *Responsable* Housing, perfil externo)
  - Personal con acceso permanente o temporal.
- **Externos**: Visitantes, técnicos puntuales, auditores, etc. Tienen acceso temporal y su acceso deberá ser autorizado por un *Responsable Sede* (perfil interno)
- **Vigilante de Seguridad**: Personal que valida el acceso en una de las Sedes.

3. Estructura de autorización

Cada edificio cuenta con un grupo de personas autorizadas para validar accesos, las cuales tendrán el Rol de *responsable de Sede* (perfil interno). Estas personas pueden:

- Autorizar registros de personal con acceso permanente.
- Autorizar accesos temporales.

Hay listados de personal con autorización de distintas empresas externas, cada una de esas listas tiene un responsable interno (Responsable Servicio Contrata o Responsable Servicio Cliente Housing) y uno de la empresa externa (Responsable Contrata o Responsable Housing). La persona externa solicitará las modificaciones de los listados del personal con autorización al responsable Servicio interno asignado quien validará que todo es correcto y podrá continuar la tramitación, denegarla o solicitar información adicional.

Una misma persona interna puede tener más de un Rol y un responsable de Servicio podrá tener asignados más de una Contrata o cliente Housing. Asimismo, una contrata puede

tener más de un responsable de servicio asignado de modo que se garantice en todo momento la respuesta a las distintas solicitudes.

4. Sedes, zonas y horarios de acceso

Cada personal interno tendrá acceso a unas sedes, zonas determinadas y en un determinado horario. La tarjeta asignada o sistemas de acceso equivalente sólo debe permitir dichos accesos.

Cada Contrata tendrá acceso en principio a una o varias sedes y zonas y horarios. No se prevé una limitación de distintos accesos para personal de la misma contrata.

Los clientes de Housing sólo acceden a 1 sede y a una zona determinada.

5. Flujos de autorización

Acceso Permanente trabajadores internos

1. Inicio del proceso de registro por parte del propietario (rol Responsable Sede, puede autorizar), por parte de recursos humanos Nasertic (sin rol responsable, no puede autorizar, si puede solicitar) o por parte de un responsable de área (pueden tener rol Responsable Sede o no, puede o no autorizar, si puede solicitar). Se solicita: nombre, apellidos, DNI, Sede y coche (sede Beloso de ser necesario).
2. Autorización por parte de un responsable de Sede
3. Registro en sistema de control de accesos. Lo realiza unidad seguridad Mainframe
4. Acceso autorizado.
   Orcoyen: Tendrá asociada una tarjeta permanente
   Beloso: Accederá con tarjeta o sistema de acceso equivalente:

Acceso Permanente trabajadores subcontratas

1. Solicitud por responsable de la contrata (rol Responsable contrata, perfil externo) con los datos: nombre, apellidos, DNI, Sede, coche (sede Beloso de ser necesario), validación de lectura documento prevención y verificación CAE.

2. Validación por trabajador interno responsable del servicio Contrata, perfil interno
3. Autorización por responsable de Sede, perfil interno
   Registro en sistema de control de accesos. Lo realiza unidad Seguridad Mainframe
4. Verificación por tarjeta o sistemas de acceso equivalente en el acceso a la sede física.
   CPD Orcoyen. Se asigna tarjeta para el acceso in situ.
   CPD Beloso. Uso de tarjeta o sistema de acceso equivalente.

Acceso Permanente trabajadores clientes Housing

1. Solicitud por responsable de cliente Housing (rol Responsable Housing, perfil externo) con los datos: nombre, apellidos, DNI, Sede, validación de lectura documento prevención
2. Validación por trabajador interno responsable del servicio Housing (rol responsable servicio Housing, perfil interno)
3. Autorización por responsable de la sede (rol responsable Sede, perfil interno)
    a. Registro en sistema de control de accesos. Lo realiza unidad Seguridad Mainframe
4. Verificación por tarjeta o sistemas de acceso equivalente en el acceso a la sede física.
    a. Exclusivo para CPD Orcoyen. Se asigna tarjeta para el acceso.

Acceso Temporal solicitado por trabajadores internos

1. Solicitud por parte del trabajador interno con acceso permanente (puede tener o no rol responsable sede, si puede solicitar) al personal externo para que complete la información
2. Ingreso en aplicación por parte del externo de datos: nombre, apellidos, DNI, Sede, coche (sede Beloso de ser necesario) y confirmación de lectura de prevención.
3. Validación por parte del trabajador interno con acceso permanente que los datos son correctos
4. Autorización por responsable de la sede (rol responsable sede, perfil interno)
    a. Registro en sistema de control de accesos. Lo realiza unidad Seguridad Mainframe.
5. Verificación por tarjeta o sistemas de acceso equivalente en el acceso a la sede física.
    a. CPD Orcoyen. Se asigna tarjeta para el acceso.
    b. CPD Beloso. Uso de tarjeta o sistema de acceso equivalente

Acceso Temporal solicitado por subcontratas y clientes Housing

1. Solicitud por responsable de la contrata (rol Responsable contrata, perfil externo) o cliente Housing (rol Responsable Housing, perfil externo) al personal externo (trabajadores de la subcontrata o housing) para que complete la información
2. Ingreso en aplicación por parte del externo de datos: nombre, apellidos, DNI, Sede, coche (sede Beloso de ser necesario) y validación de lectura documento prevención
3. Validar por parte del responsable de la contrata (rol responsable contrata, perfil externo) o cliente Housing (rol responsable housing, rol externo) de los datos y completar datos de acompañante con acceso permanente de la contrata o housing. Adicionalmente indicar si es necesario acceder a zonas específicas indicando también trabajo a realizar.
4. Validación por trabajador interno responsable del servicio (rol responsable servicio contrata o rol responsable servicio housing, perfil interno)
5. Autorización por responsable de la sede (rol responsable sede, perfil interno)
    a. Registro en sistema de control de accesos. Lo realiza unidad Seguridad Mainframe
6. Verificación por tarjeta o sistemas de acceso equivalente en el acceso a la sede física.

    a. CPD Orcoyen. Se asigna tarjeta para el acceso.

b. CPD Beloso. Uso de tarjeta o sistema de acceso equivalente

6. Notificaciones

Las actualizaciones de listados permanentes de determinadas sedes pueden requerir la notificación de estos a distintas listas de distribución para su comprobación y actualización en caso de ser necesario (bajas o modificaciones) Los listados permanentes hacen referencia a listado de personas con acceso permanente tanto internos como externos. Se debería poder agrupar por personal interno, contratas externas y clientes housing.

Lo mismo puede ser necesario con accesos temporales.