CONVOCATORIA DE CONSULTA PRELIMINAR DEL MERCADO PARA EL PROYECTO "Sistema de Control de Accesos Plan Director de Seguridad Industrial"

NAVANTIA es una sociedad mercantil estatal perteneciente a la Sociedad Estatal de Participaciones Industriales (SEPI), referente en el diseño y la construcción de buques militares y buques civiles de alta tecnología.

Las líneas de actividad de Navantia son la Construcción Naval, Sistemas, Reparaciones, Propulsión, Apoyo al Ciclo de Vida, Eólica y Transferencia de Tecnología, negocios que le permiten contar con una gran diversidad de productos que incluye, entre otros, submarinos, destructores, fragatas, portaeronaves, buques anfibios, corbetas, patrulleros, lanchas, buques civiles complejos, buques civiles simples, eólica marina, sistemas SW y HW, motores, sostenimiento y reparaciones.

La presente Consulta Preliminar del Mercado (CPM) tiene por objeto obtener información del mercado, a fin de poder disponer de conocimientos suficientes y necesarios para la más adecuada definición de los pliegos, ante una eventual contratación del Sistema de Control de Accesos Plan Director de Seguridad Industrial, según se detalla en la documentación anexa.

Al respecto, la Instrucción VIII de las Instrucciones Internas de Contratación de Navantia establece que "*NAVANTIA podrá hacer uso, en la preparación de sus contratos, de las consultas preliminares de mercado de acuerdo con lo previsto al efecto en el artículo 115 de la Ley de Contratos del Sector Público.*", el cual a su vez indica que "*Los órganos de contratación podrán realizar estudios de mercado y dirigir consultas a los operadores económicos con la finalidad de preparar correctamente la licitación e informar a los citados operadores económicos acerca de sus planes y de los requisitos que exigirán para concurrir al procedimiento (...)*".

Con base en lo expuesto, se convoca la presente Consulta Preliminar del Mercado cuyo procedimiento, reto/s tecnológico y formulario, se detallan en los Anexos I, II y III adjuntos.

ANEXO I

1. Convocatoria

Se convoca una Consulta Preliminar al Mercado en el marco del proyecto Sistema de Control de Accesos Plan Director de Seguridad Industrial para el impulso en el desarrollo de un Sistema de Control de Accesos necesario por el Plan Director de Seguridad Industrial.

2. Objeto.

El objeto de la presente Consulta Preliminar del Mercado es el de obtener la información necesaria para preparar un eventual procedimiento de contratación de conformidad con las Instrucciones Internas de Contratación de Navantia y normativa aplicable de contratación pública, en el marco del proyecto Sistema de Control de Accesos Plan Director de Seguridad Industrial.

Esta Consulta busca promover la participación de operadores económicos activos en el mercado que puedan dar respuesta/s a la necesidad Sistema de Control de Accesos Plan Director de Seguridad Industrial que se describe en el Anexo II de esta convocatoria.

Concretamente se pretende que, a partir de los resultados de esta Consulta, Navantia disponga del conocimiento sobre las soluciones y capacidades existentes en el mercado y de información suficiente que le permita la mejor definición de las especificaciones técnicas y funcionales del/de los eventuales proyectos/alcances a licitar.

3. Participantes.

La convocatoria es abierta y se dirige a personas físicas o jurídicas, públicas o privadas.

Se admitirá la presentación de varias respuestas por una misma persona física o jurídica, ya sea individualmente o de forma conjunta con otras.

4. Presentación de respuestas.

Para la presentación de las respuestas, los participantes se ceñirán a las siguientes reglas:

1. los participantes deberán formular sus respuestas cumplimentando el entregable descrito que se encuentra en el apartado 11 del Anexo II de la presente convocatoria. Se podrá acompañar el entregable con la documentación complementaria que se estime oportuna, donde se podrá desarrollar la respuesta con mayor detalle, si bien se ruega atenerse al entregable para facilitar su análisis.

2. Las respuestas se enviarán a la siguiente dirección de correo electrónico: ***jgarciap@navantia.es***

3. Las respuestas se identifican con el acrónimo que quedará claramente expuesto en el asunto del correo electrónico.

4. Se podrán enviar sucesivas versiones de una respuesta a la consulta, con el mismo acrónimo, pero cada respuesta enviada sustituirá completamente a la anterior. Por ello, la nueva respuesta deberá incluir todo lo que se considere que sigue siendo válido de las anteriores.

5. En caso de que una respuesta se presente de forma conjunta por un grupo de personas o entidades, deberá emplearse una única dirección de correo electrónico para los efectos de identificación de la respuesta e interlocución con los participantes.

6. Navantia no se obliga a financiar ni a aceptar las respuestas presentadas en esta convocatoria.

7. Los costes derivados de la participación en la consulta correrán a cargo de los participantes.

5. Aplicación de los principios de transparencia, igualdad de trato y no discriminación ni falseamiento de la competencia.

La participación en la Consulta Preliminar del Mercado, los contactos mantenidos con los participantes o los intercambios de información se regirán bajo los principios comunitarios de transparencia, igualdad de trato y no discriminación, sin que puedan tener como efecto restringir o limitar la competencia, ni otorgar ventajas o derechos exclusivos en una eventual licitación posterior.

La participación en la Consulta Preliminar del Mercado no otorgará derecho ni preferencia alguna respecto de la adjudicación de los contratos que puedan celebrarse con posterioridad en el ámbito del objeto de esta convocatoria y, como consecuencia de ello, no conlleva ninguna obligación de financiación o aceptación de las respuestas presentadas.

Si se considerara necesario, Navantia podrá contactar con participantes concretos para recabar más información sobre su respuesta a la consulta, aclarar dudas o solicitar demostraciones.

Asimismo, se podrán realizar jornadas informativas, reuniones con los participantes, y cualesquiera otras actuaciones de comunicación y difusión que se estimen oportunas.

Durante el desarrollo de la consulta se podrá publicar la información intercambiada con los participantes que garantice el cumplimiento de los principios de transparencia, igualdad de trato y no discriminación. Esta información podrá hacerse pública mediante jornadas públicas, documentos de información, mapas de demanda temprana u otros medios destinados a tal efecto por Navantia.

Finalizada la consulta, además del informe de las actuaciones realizadas, se podrá publicar con suficiente antelación, el denominado "Mapa de Demanda Temprana" de la futura o futuras contrataciones que se pretendan convocar fruto de la consulta, a los efectos de informar al mercado para que pueda preparar las oportunas ofertas con tiempo suficiente, facilitando la planificación y la reducción del riesgo.

La ausencia de publicación del "Mapa de Demanda Temprana" no impedirá que en el futuro Navantia pueda promover licitaciones que satisfagan total o parcialmente las necesidades que han sido objeto de consulta previa.

6. Plazo y actualizaciones de la Consulta Preliminar del Mercado.

El plazo para la presentación de respuestas comenzará el día siguiente al de publicación de esta Convocatoria en la Plataforma de Contratación del Estado y finalizará a las **15:00 horas del día 15 de Julio de 2020.**

Navantia podrá publicar actualizaciones de las necesidades de la presente convocatoria mediante la publicación de una modificación sobre el Anexo II de la misma. Podrá por tanto añadir nuevas necesidades, o reformular las necesidades publicadas fruto de la evolución del propio proceso de consulta al mercado.

Se avisará de estas actualizaciones a todos los que hayan participado hasta ese momento en la consulta a través de la dirección de correo electrónico desde la que se envió la respuesta.

El cierre de la consulta se determinará para cada necesidad publicado cuando Navantia estime que:

- Dispone de información suficiente sobre las respuestas para esa necesidad como para iniciar un eventual proceso de contratación pública, o
- Considere que tal necesidad no ha generado suficiente interés en el mercado como para mantener la consulta, o
- Considere que la oportunidad de plantear esa necesidad ha pasado.

Se podrá revocar el aviso de cierre de una necesidad en cualquier momento informando de ello por los mismos medios con los que se comunicó su cierre.

7. Resultado de la Consulta Preliminar del Mercado.

Navantia estudiará las respuestas que se presenten y podrá utilizarlas para definir las especificaciones funcionales o técnicas detalladas que se puedan emplear en los procedimientos de contratación que con posterioridad se puedan convocar.

8. Protección de datos personales y confidencialidad.

Navantia almacenará los datos de contacto de los participantes en el procedimiento a los meros efectos de establecer un canal de comunicación con los participantes durante el proceso de Consulta Preliminar del Mercado.

Para asegurar la transparencia del proceso, la disponibilidad de la mayor información posible y el intercambio eficaz de experiencias y opiniones, los participantes harán constar expresamente su conformidad para que Navantia mantenga accesible y actualizada la información necesaria, total o parcial, sobre sus respuestas, sin perjuicio de aquella que haya sido marcada como confidencial.

Para ello, los participantes indicarán la documentación o la información técnica o comercial de su respuesta que tiene carácter confidencial, no siendo admisible que efectúen una declaración genérica o declaren que toda la información tiene carácter confidencial. Este carácter confidencial protege, en particular, a los secretos técnicos o comerciales y a los aspectos confidenciales de las soluciones.

El contenido de la información incluida en el entregable del apartado 11 del anexo II en ningún caso podrá ser calificado como confidencial y únicamente los adjuntos a ese formulario podrán designarse como tales.

9. Derechos de Explotación de la Propiedad Intelectual e Industrial.

El uso del contenido de las respuestas se limita exclusivamente a su posible inclusión en las especificaciones funcionales o técnicas de un eventual procedimiento de contratación posterior.

10. Contratación pública.

A partir de las ideas de soluciones recogidas como resultado de esta convocatoria, Navantia podrá definir las especificaciones técnicas y/o funcionales, que servirán de base para la definición, con el grado de concreción necesario, del objeto de contratación del correspondiente procedimiento de contratación pública ulterior.

Este eventual procedimiento posterior estará abierto a todas las ofertas que cumplan, en su caso, las condiciones de tal procedimiento hayan participado o no en esta consulta preliminar del mercado.

ANEXO II

Necesidad

El proyecto Sistema de Control de Accesos Plan Director de Seguridad Industrial tiene como objetivo principal lanzar una iniciativa descrita en el apartado 1.2 del presente anexo.

Las siguientes especificaciones de la necesidad no cubierta son orientativas y podrán evolucionar a medida que se vaya actualizando el estado del arte en cada uno de los ámbitos.

1. Introducción

1.1. Antecedentes

Como consecuencia de la evolución tecnológica y los nuevos retos industriales orientados hacia la consecución de la transformación digital, Navantia va a poner en marcha un Plan de Seguridad Industrial que responda a todas estas expectativas y conectadas con los conceptos básicos del proyecto Astillero 4.0 actualmente en curso.

1.2. Objetivo

Dentro del Sistema Integrado de Seguridad Industrial se ha definido que los sistemas de seguridad actuales necesitan una mejora y actualización para adaptarlos a las nuevas exigencias y que permita su interoperabilidad con los futuros sistemas, especialmente con la Plataforma Digital de Navantia.

El Sistema de Control de Accesos que desea implantar Navantia es un conjunto de equipos y soluciones TIC con los siguientes objetivos principales:

- Mejorar el Control de Accesos existente. Actualizando la tecnología y las aplicaciones existentes por otras con mejores prestaciones.
- Mejorar, sustituir o eliminar las Unidades de Control de Acceso distribuidas en 7 centros de trabajo existentes para adecuarlas a la nueva tecnología.
- Describir la estrategia de cambio de tecnología (migración del sistema de control actual al nuevo), minimizando riesgos para mantener operativo el Control de Accesos durante el período de cambio.
- Dar soporte aportando los datos necesarios, a los procesos de seguridad definidos que requieren operar con el control de accesos, tanto verticales (Procesos Operativos) como transversales (Procesos de Gestión).
- Generar y procesar eventos que permitan activar los recursos de los sistemas de seguridad contemplados en el alcance del proyecto PDS.
- Registrar los datos de los eventos significativos para Seguridad Industrial dentro de las instalaciones de Navantia.
- Gestionar los accesos para su uso en la seguridad de las operaciones dentro de los procesos de negocio.
- Facilitar las labores de mantenimiento incorporando un sistema BITE

Los requisitos funcionales principales que se van a solicitar al sistema a fin de cumplir con los objetivos descritos son:

- Gestionar la apertura de puertas y de mecanismos de cierre dotados de sensores.
- Importar perfiles de acceso gestionados por la Plataforma que determinan quien, cuando, cómo y por donde puede entrar o salir de una zona.
- Controlar la presencia de las personas y el aforo de los locales
- Registrar la entrada y salida de vehículos
- Implantar un Sistema Antipassback para las zonas que lo requieran
- Generación de eventos para activar los procesos en la Plataforma Digital y favorecer la interoperabilidad de los sistemas de seguridad
- Seguridad de los datos y la información según la normativa de Navantia.
- Autodiagnóstico de los equipos y sistemas.
- Envío de datos bajo demanda.

2. Objeto

El objeto del presente CPM es recabar, de los principales fabricantes del mercado, la información necesaria para poder establecer los condicionantes y criterios que se tendrán en cuenta en una próxima licitación para la "Implantación del Sistema de Control de Accesos dentro de un Sistema Integrado de Seguridad Industrial" que consistirá en el Suministro, Instalación, Integración y Puesta en Marcha de todos los equipos y aplicaciones necesarias para ello.

El CPM describe de forma aproximada, el futuro alcance de los trabajos a desarrollar por las empresas participantes de manera enumerativa y global y en ningún caso limitativa.

A lo largo del presente CPM se realizará una descripción del alcance de los trabajos que se requerirán en la futura licitación.

En el apartado 11 se detallan los entregables necesarios para cumplimentar este CPM.

3. Alcance

En el apartado 6 del presente documento se realiza una descripción detallada del alcance de la información requerida. No obstante, en términos generales se necesita conocer lo siguiente:

- Especificación detallada del sistema propuesto.
- Descripción y planificación de la implantación y pruebas del Sistema de Control de Accesos.
- Revisión y Especificación detallada de los requerimientos funcionales del sistema descritos en el apartado 1, así como de otras funcionalidades no descritas en este apartado.
- Especificación técnica de los equipos.
- Arquitectura física y funcional del Sistema de Control de Accesos.
- Descripción de una plataforma específica de integración y pruebas con capacidad para la simulación de todos los requisitos establecidos en el presente documento.
- Descripción de la formación del personal de Navantia y usuarios externos
- Descripción de la gestión global del proyecto, tanto su dirección y seguimiento como en el aseguramiento de la calidad, la configuración del sistema y la documentación requerida
- Especificación de los mecanismos aportados para la interoperabilidad del sistema de CCAA con los diferentes sistemas y subsistemas de seguridad
- Propuesta de mantenimiento evolutivo del sistema
- Valoración ROM del sistema de Control de Accesos no vinculante

4. Acrónimos

A lo largo del presente documento se usan siglas, abreviaturas o acrónimos cuyo significado queda definido en el siguiente cuadro resumen:

ACRÓNIMO	DESCRIPCIÓN
ANPR	Reconocimiento Automático de Matrículas (Automatic Number Plate Recognition)
BITE	Autodiagnóstico (Built-In Test Equipment)
BNF	Notación de Backus-Naur (Backus-Naur formalism)
CCTV	Circuito Cerrado de Televisión
CRA	Central Receptora de Alarmas
DFD	Diagrama de Flujo de Datos
DMBOK	Cuerpo del Conocimiento en lo que respecta a la Gestión de Datos (Data Management Body of Knowledge)
DVR	Grabador de Vídeo Digital (Digital Vídeo Recorder)
EDA	Arquitectura Dirigida por Eventos (Event Driven Architecture)
GIS	Sistema de Información Geográfica (Geographic Information Systems)
IA	Inteligencia Artificial
IIAA	Industria Auxiliar
IP	Protocolo de Internet. (Internet Protocol)
IVA	Analítica de Vídeo Inteligente (Intelligent Video Analytical)
LAN	Red de Área Local (Local Area Network)
MRD	Modelo de Referencia de Datos
MTBF	Tiempo medio entre Fallos (Medium Time Between Failures)
NVR	Grabador en Red de Vídeo (Network Vídeo Recorder)
PDS	Plan Director de Seguridad de Navantia
PoC	Prueba de Concepto (Proof of Concept)
PTZ	Zoom, Giro y Vista Panorámica (Pan, Tilt and Zoom)
CPM	Consulta Preliminar de Mercado (Request For Information)
RFP	Petición de Propuesta (Request For Proposal)
ROM	Estimación por Orden de Magnitud (Rough Order of Magnitud)
SIVAP	Sistema Integral de Vigilancia Activa de Buques
SLA	Acuerdo de Nivel de Servicio (Service Level Agreement)
SMD	Detección Inteligente de Movimiento (Smart Movement Detection)
SQL	Lenguaje de Consulta Estructurado (Structured Query Language)
SVAP	Sistema de Vigilancia en Aguas Próximas
SVD	Sistema de Vídeo Digital
TIC	Tecnologías de la Información y Comunicación
UML	Lenguaje Unificado de Modelado (Unificated Modeling Language)
URAM	Unidad Receptora de Alarmas
USV	Embarcación No Tripulada (Unmanned Surface Vehicle)
VMS	Sistema de Administración de Vídeo (Video Management System)
VTS	Sistema de Control de Tráfico Marítimo (Vessels Traffic System)

5. Descripción de la situación actual

5.1. Introducción

En este apartado se describen los principales condicionantes técnicos que deberá tener en cuenta la empresa participante para estimar la implantación del sistema de Control de Accesos, con el fin de que pueda estudiar y valorar el esfuerzo derivado del trabajo de instalación asociado.

Para ello, se describe el equipamiento del sistema de Control de Accesos actual y se recogen las características funcionales de los principales sistemas existentes que puedan interferir en los trabajos asociados al presente expediente ya sea de manera directa o a través de Procesos Transversales.

5.2. Centros objeto de actuación

Se considerarán actuaciones en todos los centros operativos de Navantia situados en la Ría de Ferrol, Bahía de Cádiz, Dársena de Cartagena y Madrid.

5.3. Equipamiento existente

En este apartado se presentan a la empresa participante los equipos y sistemas del Control de Accesos actuales y otros relacionados con la seguridad con los que cuenta en la actualidad Navantia con el objeto de que pueda valorar con exactitud los niveles de integración e interactuación tanto a nivel software como a nivel hardware.

No obstante, no puede considerarse una lista limitativa sino simplemente enumerativa. Existe la posibilidad de que algunos de los componentes aquí descritos hayan sido modificados en el momento de la implantación del sistema o que se hayan incorporado nuevos elementos.

5.3.1. Sistema de Control de Accesos

Navantia cuenta con un sistema completo de control de Accesos y Presencia. El software de gestión de todo el sistema es SpecManager. Es un sistema centralizado, con un servidor central y terminales distribuidos por todas las instalaciones conectados a través de la VLAN exclusiva e independiente de Seguridad Industrial.

Las tarjetas y los lectores son de tecnología ICode SLI. Los terminales son de las series RYT, RWT y XGA de SPEC. Los lectores son de la serie TGX. Incluye impedimentos físicos de paso como molinetes, tornos, portillones y ventosas magnéticas y cerraduras electrónicas en puertas para personas; y barreras para vehículos.

No dispone de lectores ni sensores biométricos para personas; ni lectores de matrícula, arcos de control de mercancías en camiones ni control y vigilancia de los parkings.

La siguiente tabla resume las cantidades instaladas de Terminales y Aparatos de Control de Acceso en cada centro

Las cantidades pueden sufrir una variación de un +- 15 % en el momento de elaborar el proyecto de detalle.

CENTRO	Madrid	Ferrol	Fene	Cartagena	San Fernando	Puerto Real	Cádiz	Total
EQUIPOS								
Terminales								
Acceso	22	83	30	100	60	32	26	**353**
Presencia		26	9	18	21	32	2	**108**
Aparatos								
Tornos		18	8	21	7			**54**
Portillones	3	4		1				**8**
Molinetes		12	2	10	5	23	18	**70**
Puertas	17	37	7	28	34	6	3	**132**
Barreras		10	8	6	2	4	2	**32**
Báculos		20	14	4		4	2	**44**
Casetas		4	3	2	5		1	**15**
Interfonos	3	48		34	9	6	4	**104**

5.3.2. Otras Infraestructuras y sistemas hardware

5.3.2.1. Red de Fibra Óptica

Navantia cuenta con una extensa red de fibra óptica propia, desplegada por prácticamente la totalidad del entorno y que da servicio a todos sus usuarios, ya sean cámaras de CCTV, edificios administrativos, terminales de control de accesos, etc.

Los sistemas de seguridad están conectados mediante la VLAN de Seguridad Industrial, que es una red lógica aislada dentro de la red corporativa que abarca todos los centros de Navantia.

Es una arquitectura basada en nodos distribuidos en las instalaciones, en los que está ubicada la electrónica de red, y a los que llega la Fibra Óptica. El equipamiento de seguridad típico de cada nodo consiste en grabadores de vídeo, codificadores de vídeo y centrales receptoras de alarma (URAM de Indra).

Los Terminales están conectados a los switches que existen en cada nodo.

Existe actualmente un plan de modernización de la infraestructura de red. No se considera necesario en esta fase entregar los planos en los que se pueden observar el recorrido de la infraestructura actual y futura.

En caso de que el sistema propuesto requiera una estructura de red específica, ésta deberá estar completamente documentada y justificada en la CPM.

5.3.2.2. Red de Alimentación segura

Navantia cuenta con una red de alimentación segura propia, desplegada por el entorno y que da servicio a parte del equipamiento de seguridad, ya sean cámaras de CCTV, centros de control, terminales, etc.

Existe actualmente un plan de modernización de la infraestructura de red, no se considera necesario en esta fase entregar los planos en los que se pueden observar el recorrido de la infraestructura actual y futura.

En caso de que el sistema propuesto requiera una estructura de red de alimentación segura específica, ésta deberá estar completamente documentada y justificada en la CPM.

5.3.2.3. Redes inalámbricas

Navantia dispone de cobertura Wi-fi local para su red corporativa, y en determinadas ubicaciones para dar cobertura a equipos de seguridad portátiles.

En caso de que el sistema propuesto requiera una estructura de red específica de este tipo, ésta deberá estar completamente documentada y justificada en la CPM.

5.3.2.4. Sistema de CCTV

Navantia cuenta con un sistema completo de CCTV, con equipos de captación distribuidos a lo largo de todas las instalaciones.

Existe actualmente un proyecto de actualización y mejora del sistema de CCTV para adecuarlo a los requerimientos de interoperabilidad con el resto de los sistemas de seguridad a través de la Plataforma Digital. Incluye dar cobertura de vídeo a todos los controles de acceso con un IVA avanzado de lectura de matrículas y reconocimiento facial entre otras funcionalidades.

5.3.3. Otras Infraestructuras y sistema software

5.3.3.1. Plataforma Digital de Seguridad Industrial

Actualmente Navantia está en proceso de adquisición de una Plataforma Digital de Seguridad que se orienta al control de la seguridad en Navantia mediante la gestión de procesos.

Es el núcleo principal de todos los sistemas y realiza la coordinación de la información en base a una arquitectura EDA (Event Driven Architecturre)

6. Alcance del suministro

6.1. Introducción

La presente CPM tiene como objeto el suministro de información de un sistema de control de accesos que incluirá el equipamiento y desarrollo de los trabajos para:

- La definición, diseño, adaptación y puesta en marcha de un sistema de control de accesos que permita la correcta gestión de la seguridad y el intercambio de información entre los sistemas implicados en la misma, con los objetivos descritos en el apartado 1.
- El suministro, instalación, configuración y puesta en marcha de los equipos necesarios para la implantación del sistema.
- La capacidad de reutilización de los equipos existentes
- Formación a los usuarios finales y administradores.
- Verificación de las capacidades de integración y pruebas de los diferentes sistemas y subsistemas de seguridad.
- Los mantenimientos y la garantía del sistema y de los equipos.

6.2. Arquitectura

Las empresas participantes deberán exponer de forma detallada la arquitectura del sistema de Control de Accesos de forma que Navantia analice la posibilidad de que esta arquitectura permita la interoperabilidad con todo tipo de sistemas legados y concretamente con la Plataforma Digital, necesitamos conocer con especial detalle los mecanismos de interoperabilidad propuestos y la combinación de datos, aplicaciones y componentes que permitan inferir una robustez en el funcionamiento, total modularidad y escalabilidad así como la continuidad del servicio en caso de fallo de alguno de sus componentes.

La empresa participante expondrá, los elementos que conforman el sistema y la interrelación entre ellos, tanto de forma gráfica como descriptiva, y las tecnologías de detección y gestión de datos (almacenamiento y tratamiento) en cada una de las áreas funcionales que conformen la arquitectura propuesta.

El sistema de control de accesos formará parte del conjunto de sistemas y aplicaciones que conforman el ecosistema de seguridad de Navantia que responde a una arquitectura tipo EDA (Event Driven Architecture) en tiempo real orientado a la gestión de procesos con un Modelo de Referencia de Datos (MRD) basado en el DMA – DMBOK en un entorno distribuido y basado en tecnologías *open- source* con el que deberá ser completamente compatible e interoperable.

A lo largo de este documento se describirán el alcance detallado y los requisitos de información de cada uno de los componentes.

6.2.1. Sistema de gestión del control de accesos

Se proporcionará un esquema de distribución del equipamiento que soporte la arquitectura del sistema, justificando su elección e indicando las funciones y capacidades de cada uno.

La empresa participante deberá exponer los mecanismos de configuración y administración, tanto de manera remota como local, identificando en el primer caso las herramientas (API´s, WS, etc..) que permiten dicha funcionalidad en base a los mecanismos de interoperabilidad intrínsecos al sistema.

6.2.1.1. Datos

Las empresas participantes deberán aportar la siguiente información:

- Modelo de Referencia de Datos (MRD).
- Modelo de Datos del sistema propuesto incluyendo, al menos, los siguientes diagramas:
  - Diagrama de Clases en notación UML.
  - Diccionario de Datos en notación BNF.
- Modelo de Transferencia de Datos incluyendo, al menos, los siguientes diagramas:
  - Diagramas de Casos de Usos en notación UML.
  - Diagramas de Secuencias en notación UML.
  - Diagramas de Flujo de Datos (DFD) en notación Yourdon DeMarco.
- Tipo (SQL / NoSQL), Estructura (Clave-Valor, Documentos, etc.) y Tecnologías (Propietarias / Open-Source) de las Bases de Datos propias del sistema y el tipo de datos que se gestionará en cada una de ellas de acuerdo al Modelo de Referencia de Datos (MRD).

6.2.2. Unidades de control de accesos

Se deberá definir y explicar la existencia o no de unidades de control de accesos de forma distribuida, en cualquier caso, la información sobre la solución aportada deberá permitir que se compruebe que las funciones definidas para cumplir con los objetivos descritos en el apartado 1 se implementen en cada uno de los accesos en los centros e instalaciones de Navantia a los que da cobertura el sistema de control de accesos.

Las empresas participantes incluirán la distribución de los equipos para cada tipo de acceso, especificando el tipo de tecnología y sensores y justificará esta distribución.

6.2.2.1. Eventos

De acuerdo a lo especificado en el apartado 6.2, el sistema propuesto formará parte de un ecosistema de seguridad de Navantia basado en una arquitectura EDA (Event Driven Architecture) con el que deberá interoperar. Se aportará la información necesaria para verificar la consecución o no de los siguientes objetivos:

- Mantener una completa independencia entre el sistema propuesto y la totalidad de elementos del ecosistema de Seguridad de Navantia.
- Generación / Recepción y Tratamiento de eventos en Tiempo Real.
- Intercambio de información basada en el paradigma de Publicación – Suscripción con garantía de integridad, enrutamiento y orquestación de eventos.
- Arquitectura de gestión de eventos basada en microservicios.
- Gestión de errores y mantenimiento de los enlaces.
- Gestión y mantenimiento de Metadatos.
- Reloj en Tiempo Real con mecanismo de sincronización.

Para comprobar si los eventos tienen una estructura según lo establecido en el ENI (Esquema Nacional de Interoperabilidad) necesitamos considerar, al menos, la siguiente información:

- Codificación.
- Identificación.
- Origen.
- Marca de tiempo.
- Datos
- Grado de confiabilidad de los datos.

Las empresas participantes deberán exponer el mecanismo de cifrado y/o algoritmo utilizado para preservar la integridad y seguridad de la información.

6.3. Redundancia

Dada la criticidad de los servicios incluidos en el sistema de control de accesos, especialmente su repercusión en el control y seguridad es necesario contemplar las situaciones en las que los equipos de captación de datos, la conectividad con las bases de datos y otros sistemas no estén operativos.

Las empresas participantes expondrán su propuesta para la redundancia de sistemas / equipos, exponiendo con detalle las razones de dicha elección, así como los mecanismos a implantar para obtener una operatividad mínima definida como modo degradado que resultará de la gestión de las redundancias.

6.4. Garantía

La empresa participante deberá aportar una propuesta de garantía.

6.5. Mantenimiento

La empresa participante deberá aportar una propuesta de mantenimiento.

6.6. Licencias

Se deberá incluir en la CPM la política de licencias de la empresa participante. Debería incluir un listado claro y conciso y valorado que contenga todos los tipos y número de licencias necesarias para la puesta en marcha y desarrollo de los trabajos del sistema adjuntando la siguiente documentación:

- Producto
- Modelo / Versión.
- Número de licencias necesarias.
- Función.
- Periodo de validez de cada una de las licencias.
- Coste de adquisición de nueva licencia.
- Coste de renovación.

6.7. Formación

Se deberá aportar una propuesta de formación.

7. Requisitos mínimos de la información a aportar de los sistemas

7.1. Migración

La empresa participante describirá una propuesta de la estrategia de cambio de tecnología, minimizando riesgos para mantener operativo el Control de Accesos durante el período de cambio.

7.2. Requisitos de Infraestructuras y sistemas hardware

Se especificarán las capacidades máximas habilitadas para los equipos que se proponen, indicando la capacidad de reserva prevista, así como la infraestructura de red y alimentación necesaria para su instalación y operación.

Además, se deberá indicar la tecnología, la marca y modelo del equipamiento utilizado, así como una justificación de la elección y su coste aproximado.

7.3. Infraestructura de red y alimentación.

La infraestructura de red que soportará el sistema de control de accesos será la ya existente en Navantia que como se ha explicado anteriormente está en proceso de mejora y ampliación.

Las empresas participantes deberán especificar los requisitos de red que necesitará para conectar sus equipos y sistemas, así como valorar su instalación, definiendo el cableado y recursos necesarios.

7.4. Equipos

Se detallarán las características funcionales y técnicas de cada equipo o sistema hardware que se proponga atendiendo a la siguiente clasificación que no es limitativa:

EQUIPO	FUNCIÓN/USO	CARACTERÍSTICAS
Terminal de Acceso		
Terminal de Presencia		
Lector en Torno		
Lector en pared		
Interfonos IP		
Paneles Digitales		
Semáforos		
Servidores		
Otros		

7.5. Requisitos funcionales

7.5.1. Sistema de gestión de control de accesos

Deberá administrar el sistema de control de accesos, y la empresa participante detallará sus principales funciones, incluyendo:

- Registro de marcajes.
- Estructura de datos. Diccionario.

- Generación de eventos para activar los procesos en la Plataforma Digital y favorecer la interoperabilidad de los sistemas de seguridad
- Procedimientos avanzados de búsqueda de información de accesos.
- Redundancia y Procedimientos de Backup
- Seguridad de los datos y la información.
- Explotación de la información

7.5.1.1. Configuración de los accesos

La empresa participante aportará la información necesaria para analizar las capacidades de adaptación del sistema a la realidad de las instalaciones y centros, y cubrir los siguientes requisitos funcionales generales:

- Configuración del sistema. Parámetros globales de personas, empresas y marcajes
- Centros de trabajo. Áreas de control
- Terminales
- Zonas. Incluyendo Antipassback
- Permisos
- Accesos. Perfiles, Calendarios y Horarios
- Parking.
- Listados

7.5.1.2. Monitores y Consultas

La empresa participante deberá informar sobre las herramientas de su propuesta para facilitar a la plataforma digital de seguridad el control en tiempo real o en diferido de la situación en los centros de trabajo y en los accesos, incluyendo:

- Comunicaciones. Con el estado de actividad de los terminales
- Presencia. En Zonas y Centros. En tiempo real y a petición. Control de aforo.
- Puertas y Barreras. Visualización de cada acceso
- Marcajes. Por persona o colectivo.
- Parking. Control de aforo

7.5.1.3. Autodiagnóstico

La empresa participante deberá definir el sistema de autodiagnóstico (BITE) que incorpora su propuesta. A modo de ejemplo se exponen algunas funcionalidades sin ánimo de ser exhaustivos:

- Autodiagnóstico de los equipos y sistemas.
- Detección de sabotaje.

- Detección de pérdida y recuperación de señal
- Programación de controles a los dispositivos

7.6. Prestaciones

7.6.1. Sistema de gestión del control de accesos

La empresa participante deberá detallar al menos:

- Capacidad de gestión y almacenamiento de personas y perfiles.
- Capacidad para operar de forma simultánea con las unidades del control de acceso distribuidas en 7 centros de trabajo.
- La capacidad de almacenamiento de fichajes y datos para cubrir las necesidades operativas y de seguridad.
- Capacidad de tratamiento simultaneo de marcajes.
- Capacidad en Offline.
- Capacidad de control de sensores y periféricos.
- Tipología de los lectores a conectar

8. Presupuesto

La empresa participante deberá incluir un presupuesto ROM inicial no vinculante.

Las partidas a valorar incluyen el equipamiento, las licencias y su instalación, así como todas las tareas necesarias para su entrega a Navantia llave en mano.

9. Plazo

La empresa participante incluirá una estimación del plazo tanto de la entrega de un plan del proyecto como de su implantación.

10. Equipo de trabajo

La empresa participante, presentará una estimación del equipo de trabajo necesario para llevar a cabo el proyecto.

11. Entregables

La empresa participante, deberá elaborar los entregables que se describen en la siguiente tabla para cumplimentar el presente CPM.

ID	Descripción
E.1	Especificación detallada del sistema propuesto.
E.1.1	Sistema de gestión del control de accesos
E.1.2	Unidades de control de accesos si se requieren
E.1.3	Especificación de los mecanismos aportados para la integración de los diferentes sistemas y subsistemas de seguridad
E.2	Revisión y Especificación detallada de los requerimientos funcionales del sistema descritos en el apartado 1 y en otros apartados.
E.3	Arquitectura física y funcional del Sistema de control de accesos
E.3.1	Sistema de gestión del control de accesos
E.3.1.1	Esquema
E.3.1.2	Datos. Según apartado 6.2.1.1
E.3.2	Unidades de control de accesos si se requieren
E.3.2.1	Esquema
E.3.2.2	Eventos. Según apartado 6.2.2.1
E.3.3	Redundancia
E.4	Especificación técnica de los equipos y software del sistema.
E.4.1	Modelos de unidades de control de accesos si se requieren
E.4.2	Instalación para cada tipo de acceso
E.4.3	Sensores y Periféricos
E.4.4	Software de gestión de control de accesos
E.5	Descripción y planificación de la implantación y pruebas del Sistema de control de accesos.
E.6	Descripción de una plataforma específica de integración y pruebas con capacidad para la simulación de todos los requisitos establecidos en el presente documento.
E.7	Especificación de licencias y futuras ampliaciones.
E.7.1	Sistema de control de accesos
E.7.1.1	Visitas
E.7.1.2	Autodiagnóstico
E.7.2	Unidades de control de accesos si se requieren
E.7.2.1	Controladores
E.7.2.2	Sensores y Periféricos
E.8	Describir la estrategia de cambio de tecnología, minimizando riesgos para mantener operativo el Control de Accesos durante el período de cambio.
E.9	Estimación del equipo de trabajo para llevar a cabo el proyecto
E.10	Descripción de la formación del personal de Navantia y usuarios externos
E.11	Propuesta de Garantía
E.12	Propuesta de mantenimiento evolutivo del sistema
E.13	Valoración ROM del sistema de control de accesos no vinculante

ANEXO III

Documento de Formulario

Todos los apartados del formulario de solicitud deben ser cumplimentados en su totalidad para su análisis.

1. Datos Básicos	
Nombre de la entidad participante:	
Nombre de la necesidad:	
Acrónimo:	

2.Datos participante			
Persona Física:	☐		
Persona Jurídica:	☐		
Sector o ámbito de actividad (CNAE):			
Principales actividades de la empresa (Diseño, Fabricación, Venta, Distribución, etc.):			
Tipo de Entidad (Autónomo, Empresa privada, Empresa pública, Centro de Investigación, Universidad, Centro Tecnológico, Otro):			
Año de constitución:			
Respuesta conjunta de varias personas físicas o jurídicas: Marque SÍ o NO.	SÍ ☐	NO ☐	
Tamaño de su entidad en la actualidad (Nº de personas en plantilla):			
Facturación total de su entidad en los últimos 3 ejercicios (€):	2018	2017	2016

3. Datos del interlocutor/representante	
Nombre del Interlocutor (o representante de la respuesta	

en caso de respuesta conjunta):	
Teléfono:	
Correo Electrónico:	
Dirección:	

4. Información adicional		
¿Su entidad tiene facturación de tecnologías similares a las de la presente respuesta en últimos 3 ejercicios?: Responda SÍ o NO.	SÍ ☐	NO ☐
En caso de haber respondido SÍ a la pregunta anterior, diga cuál fue la facturación aproximada de tecnologías similares a las de esta respuesta en los últimos 3 ejercicios (dato agrupado de los 3 ejercicios):		
¿Considera que su entidad dispone de certificaciones relevantes para acometer las necesidades que se propone?: Responda SÍ o NO.	SÍ ☐	NO ☐
En caso de haber respondido SÍ a la pregunta anterior, indique cuáles son esas certificaciones (máx. 300 caracteres):		
¿Considera que el personal de su entidad tiene calificaciones que son específicamente relevantes para acometer las necesidades que se propone?: Responda SÍ o NO.	SÍ ☐	NO ☐
En caso de haber respondido SÍ a la pregunta anterior, indique cuáles son esas calificaciones (máx. 300 caracteres):		
¿Su entidad cuenta con experiencia en la ejecución de proyectos en el ámbito de alguna de las necesidades que se proponen o similares?: Responda SÍ o NO.	SÍ ☐	NO ☐
En caso de haber respondido SÍ a la pregunta anterior indicar un breve resumen de la experiencia (ámbito, cliente, periodo de ejecución y breve descripción).		
Para la necesidad planteada, aportar información detallada con relación a investigaciones, desarrollo de soluciones, publicaciones, etc., realizados o realizándose cuyo objeto sea similar al indicado.	Investigaciones. Descripción detallada. Desarrollo de soluciones. Descripción detallada. Publicaciones. Descripción detallada. Otros. Descripción detallada.	

5. Descripción de la respuesta de solución	
Nombre del documento que recoge el entregable solicitado en el apartado 11 del anexo II.	
Duración estimada para la ejecución de la respuesta planteada (meses):	
Coste estimado del desarrollo de su solución (€):	
Su entidad, ¿tiene experiencia en desarrollos relacionados con el proyecto planteado? ¿Cuáles? (indicar por cada proyecto: año de ejecución, importe, breve descripción de los resultados):	

6.Despliegue	
Indique las regulaciones y normativa asociada a la necesidad planteada:	
Considera que existe alguna limitación o barrera específica para el despliegue del producto en el mercado ¿Cuál?:	
¿Cuáles son las principales ventajas que se encuentran de la solución?:	
¿Qué criterios considera importantes para evaluar las respuestas de solución?:	

7. Propiedad intelectual	
Sobre los Derechos de Propiedad Intelectual e Industrial (DPII), a priori y por las características de su entidad, ¿ésta tiene limitaciones para compartir los DPII con el organismo contratante o para establecer un royalty sobre las ventas futuras de la solución?	

8.Declaraciones Obligatorias

Autorizo a Navantia al uso de los contenidos de las respuestas. Este uso se limitará exclusivamente a la posible inclusión de los contenidos en el proceso de definición de las líneas de trabajo, que se concretará en los posibles pliegos de los posibles procedimientos de contratación que se tramiten con posterioridad bajo la fórmula de Compra Pública.

La respuesta presentada está libre de *copyright* o cualquier otro derecho de autor o empresarial que impida su libre uso por parte de Navantia o de cualquier otra empresa colaboradora en el desarrollo de futuros proyectos.

9.Autorización de uso de los datos aportados

Importante: Autorizo a Navantia al almacenaje y difusión de los datos de contacto, a mantener accesible y actualizada la información necesaria, total o parcial, sobre la respuesta presentada y a divulgar la información o documentación técnica o comercial que, en su caso, no sea identificada como confidencial.

Los derechos de acceso, rectificación, cancelación y oposición pueden ejercerse dirigiéndose a la Autoridad de Control en materia de Protección de Datos competente, la Agencia Española de Protección de Datos – Dirección: C/ Jorge Juan, 6 – 28001 MADRID (Madrid) – Sede electrónica: sedeagpd.gob.es.

No obstante, en primera instancia, podrá presentar reclamación ante el Delegado de Protección de Datos de Navantia a través de la dirección postal C/Velázquez, 132, – 28006 Madrid, indicando en el asunto: Ref. Protección de Datos, o a través de la dirección de correo: dpd@navantia.es

10.Relación de documentación adjunta aportada		
En el caso de que los hubiese, indique la documentación que acompaña a su respuesta y que proporcione más información acerca de la idea.		
Nombre del archivo:	Breve descripción:	Confidencial*
		☐
		☐
		☐
		☐
		☐
		☐

*Marcar en el caso de que la documentación correspondiente sea confidencial.

Esta información, o parte de ella, se podrá publicar en las conclusiones de la Consulta Preliminar del Mercado en aras de favorecer la colaboración entre los participantes, así como de estos agentes interesados que no hayan participado en la misma.