Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

perfil de contratante

LICITACIÓN

Contratación de

Mantenimiento del software desarrollado y estudios técnicos de componentes, de diversos sistemas de expedición de documentos electrónicos

Referencia: CN-24-11-14-A

Entidad contratante	Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM)
Dirección	c/ Jorge Juan, 106 - 28009 Madrid
Tipo de contrato	Servicios
Tipo de procedimiento	Negociado con publicidad
Características y requerimientos	Según pliego adjunto
Plazo previsto de ejecución	2015
Presupuesto máximo de licitación	160.000.-€ (IVA NO INCLUIDO)
Aclaraciones y consultas	Cualquier consulta de tipo administrativo se dirigirá a la atención de: Área de Gestión – Dirección de Sistemas de Información Carlos Nieto Gómez e-mail: gestion.informatica@fnmt.es Tlf. 91 566 67 04 Cualquier consulta técnica relacionada con el presente pliego de condiciones, puede ser dirigida a las siguientes personas: José Tomas Baeza Oliva Teléfono: 91 566 69 24 e-mail: tbaeza@fnmt.es
Plazo de presentación de ofertas	Hasta 12 horas del 12 de diciembre de 2014

Departamento de Compras
Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda
Jorge Juan, 106 28071 – Madrid
Tel.: 91 566 66 66
Fax: 91 566 67 50
Web: www.fnmt.es/proveedores

perfil de contratante

Notas sobre presentación de ofertas	Las empresas interesadas en presentar sus ofertas de servicios, podrán incluir cuanta documentación consideren oportuna para presentación de la empresa, describir sus soluciones y explicar la forma en que cumplimentarán los requisitos de este pliego de prescripciones. Debiendo entregar en documentos separados la parte técnica de la económica y en sobres independientes, incluyendo una copia digital de los mismos en CD o memoria USB. Debiendo entregar documento original firmado por un responsable de la empresa con firma autorizada (Apoderado por la empresa ofertante para la presentación de ofertas) Dichas ofertas se deberán presentar en el Registro de la FNMT-RCM con la referencia CN-24-11-14-A
Lugar para presentación de ofertas	Fábrica Nacional de Moneda y Timbre–Real Casa de Moneda. Registro General, calle Jorge Juan, nº 106, 28009 Madrid. Horario de Registro General de 9:00 a 14:00 horas. *Salvo el día indicado para la finalización de ofertas que solo se admitirán las recibidas antes de las 12 h.* Las ofertas se dirigirán a la atención de: Área de Gestión - Dirección de Sistemas de Información

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

REAL CASA DE LA MONEDA

FÁBRICA NACIONAL DE MONEDA Y TIMBRE

DIRECCIÓN DE SISTEMAS DE INFORMACIÓN

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA CONTRATACIÓN DE SERVICIOS DE MANTENIMIENTO DEL SOFTWARE DESARROLLADO Y ESTUDIOS TÉCNICOS DE COMPONENTES, DE DIVERSOS SISTEMAS DE EXPEDICIÓN DE DOCUMENTOS ELECTRÓNICOS PARA LA DIRECCIÓN GENERAL DE LA POLICÍA.

ÍNDICE

1 INTRODUCCI ÓN.

La Dirección General de la Policía, dispone de varios sistemas de infraestructura de clave pública PKI sobre las que se implementan diversos sistemas de información, que le permiten el cumplimiento de las misiones legalmente encomendadas.

Entre dichos sistemas cabe destacar:

- Los asociados a la gestión de documentación de españoles y extranjeros (DNI electrónico y pasaporte electrónico).

- Los asociados a las labores de gestión de recursos humanos. (Carnet profesional electrónico)

Estos sistemas, especialmente los relativos a documentación, prestan servicios de misión crítica, ya que se utilizan masivamente por diversos usuarios policiales durante las 24 horas al día, los 365 días al año.

Con objeto de lograr una mejor prestación de servicios, resulta necesario efectuar sobre estos sistemas tanto el mantenimiento del software desarrollado para PKI, como realizar los estudios técnicos que permitan maximizar la disponibilidad de los mismos y hacer más eficiente su utilización por los usuarios finales, así como mejorar las técnicas de administración.

El presente proyecto se encuadra dentro del proyecto de modernización de los sistemas de información de la Dirección General de la Policía .

La Fábrica Nacional de Moneda y Timbre tiene adjudicada la Encomienda de Gestión para la realización de una serie de trabajos y servicios relacionados con la expedición y uso del documento Nacional de Identidad electrónico, Pasaporte Electrónico y otros documentos relacionados, entre los que se encuentran los correspondientes a la presente licitación, que a continuación se exponen

2 OBJETO DEL CONTRATO.

El presente pliego tiene como objeto la contratación de servicios, en forma de recursos externos, para realizar el mantenimiento adaptativo y perfectivo de los productos software asociados la expedición del DNI electrónico, pasaporte electrónico, y del carnet profesional, así como de los productos software de sistemas desarrollados dentro de las PKI existentes en la DGP, así como al desarrollo de los trabajos necesarios para mejorar la prestación de estos servicios.

Los trabajos a realizar se detallan en los siguientes conceptos:

- Mantenimiento correctivo y evolutivo del software desarrollado.
- Consultoría

3 ASPECTOS GENERALES DEL CONTRATO.

3.1. CENTRO DESTINATARIO.

Dirección General de la Policía, (Área de Informática)

3.2. PLAZO DE EJECUCIÓN.

Año 2015.

4 ENTORNO TECNOLÓGICO ACTUAL.

El entorno de explotación de los sistemas actuales dispone de los siguientes entornos físico y lógico:

4.1. ENTORNO CENTRAL.

4.1.1 Elementos físicos.

- Servidores de datos: Oracle T4-4 y T5-x: SunFire 5120, 5220 y T2000.
- Otros servidores de la firma Sun modelos V240 a V890 destinados a servicios complementarios de PKI.
- HSM de diferentes marcas.
- Durante el desarrollo de los trabajos objeto de contratación se tendrá en cuenta la posible migración del actual entorno tecnológico a nuevas plataformas basadas en procesadores Oracle T4 y T5.

4.1.2 Elementos lógicos.

- Sistema Operativo Solaris versión 2.8 en proceso de migración a 2.10
- Servidor de Aplicaciones Sun Java System Application Server 9.1. Servidor WEB Sun Java Web Server.
- Plataforma JAVA: JAVA SE 6 (Java Standard Edition 6) Base de Datos IBM Informix Dynamic Server V9.40. Directorio LDAP Sun One Directory Server
- SSO GetAccess.
- Tecnología PKI KeyOne de Safelayer.
- Autoridad de Certificación Raíz de Safelayer (KeyOne CA)
- Autoridad de Certificación Subordinada de Safelayer (KeyOne CA)
- Autoridad de Revocación de Safelayer (KeyOne CRA)
- Autoridad de Validación de Safelayer (KeyOne VA)
- Tecnología PKI de Entrust
- Autoridades de Certificación Subordinadas de Entrust (Entrust AuthoritynSecurity Manager)
- Toolkits de Entrust
- Comunicaciones TCP/IP sobre IPSEC

- Durante el desarrollo de los trabajos objeto de contratación se tendrá en cuenta la posible migración del actual entorno tecnológico JAVA a nuevas plataformas basadas en versiones superiores a JAVA SE 6.
- Durante el desarrollo de los trabajos objeto de contratación se tendrá en cuenta la posible migración del actual entorno tecnológico IBM Informix V9.40 a V11.

4.2. ENTORNO LOCAL.

Clientes con:

- Sistema Operativo Windows.
- Navegador Internet Explorer v6 v7 v8
- Durante el desarrollo de los trabajos objeto de la contratación se tendrá en cuenta ña posible actualización del S.O y versión de navegador.

5 TRABAJOS A REALIZAR.

Los trabajos objeto de la contratación tienen como objetivo proporcionar un entorno informático de producción en alta disponibilidad, evitando que se puedan sufrir daños a consecuencia de interrupciones de escasa duración.

Se pretende maximizar la disponibilidad del entorno y la seguridad de los usuarios finales, identificando paradas potenciales de los sistemas que soportan el sistema de información de la DGP, desde su origen, y prestar los servicios que las prevengan o minimicen su duración o su impacto, en la prestación de los servicios que la misma proporciona.

Existirán dos tipos básicos de trabajos en el marco de este contrato, y que se definen a continuación:

- Mantenimiento correctivo y evolutivo del software desarrollado.
- Consultoría.

5.1. MANTENIMIENTO.

El mantenimiento del software a realizar contemplará los siguientes extremos:

- Análisis y Diseño
- Revisión del Análisis Funcional
- Revisión del Diseño Técnico
- Cambios en la documentación Funcional y Técnica
- Resolución
- Modificación del aplicativo
- Realización de las pruebas de aceptación (garantía de calidad) Entrega para su puesta en explotación
- Documentación del desarrollo

5.1.1 MANTENIMIENTO DE SOFTWARE DE APLICACIÓN DE CONTROL y RA-PKIX.

La aplicación de control es el elemento de la infraestructura a través del cual se consumen los servicios de la infraestructura de certificación. Se integra con el sistema de expedición y sirve además de interfaz para la administración y la monitorización y estadísticas.

El servicio RA-PKIX proporciona un interfaz de autoridad de registro en las PKIs, implementando un subconjunto del protocolo PKIX-CMP. Dependiendo de la tecnología de PKI, se trata de software comercial o desarrollo específico.

Se prestarán los servicios de mantenimiento del software desarrollado en las diversas aplicaciones de control y desarrollos específicos de RA-PKIX, así como realizar las adaptaciones y mejoras a incluir en las actuales plataformas centrales de expedición del DNI-e, Pasaporte-e y Carné Profesional.

- Durante el desarrollo de los trabajos objeto de contratación se tendrá en cuenta la posible implementación de la firma en servidor para el DNIe (proyecto DNI 3.0 “DNIe en la nube”), por lo que el adjudicatario deberá incorporar a su oferta un escenario de colaboración para el citado proyecto.
- Durante el desarrollo de los trabajos objeto de contratación se tendrá en cuenta la posible implementación de la firma en servidor para el Carné Profesional, por lo que el adjudicatario deberá incorporar a su oferta un escenario de colaboración para el citado proyecto.

5.1.2 MANTENIMIENTO SERVICIO SAI (Servicio de autenticación de ICC)

Se prestará el mantenimiento sobre el aplicativo central SAI, encargado de implementar la autenticación interna/externa indicada en la norma CWA14890 para los ICC o la autenticación propietaria del pasaporte-e para su personalización.

5.1.3 MANTENIMIENTO SERVICIO EDIS

Se prestarán el mantenimiento sobre el servicio EDIS, que gestiona de forma centralizada la inspección de documentos de viaje.

5.1.4 MANTENIMIENTO SERVICIOS WEB ADMINISTRACIÓN, MONITORIZACIÓN Y ESTADÍSTICAS PKI

Se prestará el mantenimiento sobre el software desarrollado para los servicios de administración web de PKI, monitorización y estadísticas para los entornos DNIe, Pasaporte-e y Carnet Profesional del CNP.

5.1.5 MANTENIMIENTO MODULOS DE ARCHIVADO DE CLAVES ENTORNO CARNET PROFESIONAL

Este módulo está implementado como software comercial o como desarrollo específico dependiendo de la tecnología PKI. Se prestará mantenimiento a los desarrollos específicos realizados.

5.1.6 MANTENIMIENTO DE SOFTWARE CLIENTE.

Se prestarán los servicios de mantenimiento del software desarrollado para los puestos clientes de expedición, así como realizar las adaptaciones y mejoras a incluir en los componentes cliente ActiveX (captura, personalización física, personalización lógica) que forman parte del proceso de expedición del DNIe, Pasaporte-e y CP del CNP.

- Durante el desarrollo de los trabajos objeto de contratación se tendrá en cuenta la posible implementación de la firma en servidor para el DNIe (proyecto DNI 3.0 “DNIe en la nube”), por lo que el adjudicatario deberá incorporar a su oferta un escenario de colaboración para el citado proyecto.
- Durante el desarrollo de los trabajos objeto de contratación se tendrá en cuenta la posible implementación de la firma en servidor para el Carné Profesional, por lo que el adjudicatario deberá incorporar a su oferta un escenario de colaboración para el citado proyecto.

5.1.7 TIPOS DE MANTENIMIENTO

Sobre los sistemas anteriores se realizará el mantenimiento de software tanto correctivo como evolutivo, de acuerdo con las condiciones que a continuación se indican:

5.1.7.1 Mantenimiento correctivo

Este tipo de tareas de mantenimiento tiene como objeto el subsanar errores cuyo origen sea uno de los que a continuación se enumeran:

- Defectos en la construcción de los sistemas o aplicativos (errores de codificación, casos de prueba no contemplados, validaciones de datos no contempladas en el sistema o aplicativo, etc.).
- Integraciones defectuosas tanto entre las diversas partes o componentes del sistema o aplicativo, como con el entorno de actuación del sistema o aplicativo (interfaces con otros sistemas, traspasos de información entre ellos, etc.) Disfunción o desajuste entre las funcionalidades o características del sistema o aplicativo ofrecidas por el mismo en su puesta en explotación y la definición vigente de dichas funcionalidades, realizada en las etapas de especificación y análisis del sistema.
- Realización de acciones de contingencia, ante incidencias críticas, encaminadas a proporcionar soluciones rápidas pudiendo ser estas de carácter temporal.

5.1.7.2 Mantenimiento evolutivo

Dentro de las labores de este tipo mantenimiento se contemplan aquellas incidencias o peticiones que tengan como origen alguno de los que se detallan a continuación y teniendo en cuenta que el mantenimiento de carácter evolutivo puede tener un origen tanto técnico como funcional:

- Tareas que impliquen inclusión de nuevas funcionalidades o mejoras funcionales dentro de sistemas o aplicativos en estado de mantenimiento. Modificaciones a los sistemas o aplicativos para mejorar aspectos como rendimiento o como la calidad del software que los compone (adecuación a estándares, normas de codificación, etc.).

5.1.8 PLAN DE MANTENIMIENTO

Los oferentes facilitarán una memoria técnica sobre las tareas de mantenimiento exigidas en este pliego, que comprenderá como mínimo los siguientes ítems:

- Tareas particulares de mantenimiento de la aplicación desde el punto de vista correctivo y evolutivo tanto de usuarios como de bases de datos.
- Metodología para la gestión del servicio de mantenimiento. Componentes principales y descripción de la metodología:
    - flujo de los procesos de mantenimiento
    - relaciones de los procesos de mantenimiento entradas y salidas.
- Métricas, herramientas, etc.
- Métodos que garanticen la Calidad del Software
    - Revisiones
    - Verificaciones
    - Validaciones
- Criterios de aceptación o rechazo
    - Acciones preventivas
    - Acciones correctoras
- Plan de pruebas
    - Pruebas unitarias, de integración, del sistema, de implantación, de aceptación y de regresión.
- Procedimientos de usuario
- Niveles de servicio.
    - Indicadores.
    - Métricas, herramientas.

5.2. CONSULTORÍA

Tiene como objeto satisfacer peticiones o consultas de carácter técnico.

Incluirá cualquier tipo solicitud de soporte técnico relativa a instalaciones, puestas en marcha, operaciones de exportación, importación de datos, etc.

También están contempladas todas aquellas actividades contingentes o resolutivas que se deban llevar a cabo debido a un cambio en el entorno tecnológico, de forma que el sistema afectado siga prestando el mismo nivel de servicio.

Comprenderá lo siguiente:

- Realizar una consultoría técnica sobre los productos instalados que soportan los sistemas de PKI, consistente en:
    - Análisis del rendimiento.

  - Análisis del aprovechamiento en la utilización de los recursos.
- Prestación de asistencia técnica especializada en los productos de PKI
- aplicado a:
  - La gestión proactiva de revisiones (parches, bugs).
  - Intervenciones en el entorno lógico.
  - Instalación de nuevas versiones.
- Prestación de asistencia técnica especializada en las técnicas de administración y explotación de sistemas de PKI, aplicadas a:
  - El establecimiento, revisión y corrección, según proceda, de los procedimientos de administración de sistemas.
  - El establecimiento, revisión y corrección, según proceda, de los procedimientos de explotación de sistemas.
  - La planificación en los cambios de entorno.
  - La puesta en marcha de nuevos sistemas.
  - Explotación del sistema.

5.2.1 CONSULTORÍA TÉCNICA SOBRE LOS PRODUCTOS LÓGICOS.

Tiene como objetivo prestar ayuda para mantener la disponibilidad que se le exija a los diferentes sistemas de información de PKI, asesorando técnicamente sobre los diferentes productos lógicos de PKI que los soportan y que proporcionan una alta disponibilidad.

- Durante el desarrollo de los trabajos objeto de contratación se tendrá en cuenta la posible implementación de la firma en servidor para el DNIe (proyecto DNI 3.0 “DNIe en la nube”), por lo que el adjudicatario deberá incorporar a su oferta un escenario de colaboración para el citado proyecto.
- Durante el desarrollo de los trabajos objeto de contratación se tendrá en cuenta la posible implementación de la firma en servidor para el Carné Profesional, por lo que el adjudicatario deberá incorporar a su oferta un escenario de colaboración para el citado proyecto.

5.2.1.1 Análisis del rendimiento.

Tiene como objetivo analizar el rendimiento de los diferentes sistemas en producción, abordando los problemas, identificando donde se producen los bloqueos y proporcionando soluciones que puedan ser llevadas a cabo e implementadas por el personal de la DGPGC.

Proporcionará un informe relativo a los potenciales puntos débiles, sus consecuencias y posibles soluciones.

5.2.1.2 Análisis del aprovechamiento en la utilización de los recursos.

Se trata de proporcionar una visión detallada de la utilización de recursos en los sistemas

en explotación, informando de la actividad de los mismos (CPU, memoria, recursos de los discos, entradas / salidas, etc.).

Proporcionará un informe relativo a los potenciales puntos débiles, sus consecuencias y posibles soluciones.

5.2.1.3 Análisis de la gestión de discos, backup y procedimientos de recuperación.

Se trata de revisar los procedimientos específicos para identificar potenciales puntos débiles que puedan conducir a perdida de datos o a impedir una rápida recuperación de los datos tras un fallo del sistema.

Proporcionará un informe relativo a los potenciales puntos débiles, sus consecuencias y posibles soluciones.

5.2.2 ASISTENCIA TÉCNICA ESPECIALIZADA EN LOS PRODUCTOS LÓGICOS DE PKI.

Tiene como objetivo prestar asistencia técnica especializada para la realización de técnicas de sistemas y explotación sobre los diferentes productos lógicos que configuran el entorno que soporta los diferentes sistemas de información de PKI antes indicados, realizando las labores que se precisen y asesorando técnicamente sobre las mismas.

5.2.2.1 Gestión proactiva de revisiones.

Se trata de revisar periódicamente todo el estado de información de revisiones (parches, bugs, etc) tal y como se aplica en el entorno de la instalación, valorando el riesgo para cada acción posible y proponiendo las acciones a tomar. El director técnico, junto con el equipo de soporte del adjudicatario decidirá la instalación de las revisiones.

Esta acción permitirá prevenir paradas de sistema potenciales, debidas a los defectos de los productos, así como las debidas a la incorrecta instalación de las revisiones.

En cualquier caso se minimizará el tiempo de inactividad estimado para la instalación de aquellos.

5.2.2.2 Intervenciones en el entorno lógico.

Se trata de realizar técnicas de sistemas en los siguientes supuestos:

- Diagnostico in situ de los problemas detectados en el entorno de los productos software respectivos, valorando el riesgo para cada acción posible y proponiendo las acciones a tomar, dando cuenta de los mismos al director técnico, el cual procederá, si es el caso, a adoptar la solución propuesta o a solicitar ayuda del Solution Center de la firma propietaria de los mismos.

- Planificación, de acuerdo con el director técnico, de las intervenciones a realizar.
- Documentar la planificación utilizando los estándares de gestión de cambios utilizados por el Área de Informática.

5.2.2.3 Instalación de nuevas versiones.

Se prestará la asistencia técnica necesaria para la puesta en servicio de un entorno de alta producción en el Centro Directivo, instalando, configurando y parametrizando las nuevas versiones de los productos software de cada lote que el Área de Informática estime oportuno instalar.

Se trata de asegurar y minimizar los riesgos a la hora de llevar a cabo un cambio en el entorno de producción, minimizando el tiempo de inactividad, así como las paradas imprevistas a consecuencia de una instalación errónea de nuevas versiones.

5.2.2.4 Explotación del sistema.

Se prestará la asistencia técnica necesaria para el soporte a la explotación diaria del sistema de PKI consistente en:

- Soporte a la explotación del subsistema de PKI (equipamiento lógico y físico) y de la Aplicación de Control, que permite la integración de los procesos de negocio y de expedición de DNIe, Pass-e y Carné Profesional con los subsistemas correspondientes de PKI.
- Asistencia a los procesos periódicos de renovación de ARLs
- Soporte a la renovación periódica del material criptográfico de los Document
- Signers.
- Renovación de entidades de DNIe por volumen de emisión
- Revisión preventiva de logs, trazas, estadísticas de dichos subsistemas Asistencia a los procedimientos de archivo periódico de la información que pasa a offline
- Soporte a las tareas de explotación de mantenimiento, parada e inicio de los servidores que constituyen los sistemas objeto del presente.
- Mantener la disponibilidad que se le exija a los diferentes componentes del sistema de información, asesorando técnicamente sobre los diferentes productos lógicos que lo constituyen.
- Soporte para el análisis y diseño de nuevas funcionalidades o requerimientos del sistema.

5.2.3 ASISTENCIA TÉCNICA ESPECIALIZADA EN LAS TÉCNICAS DE SISTEMAS.

Tiene como objetivo prestar asistencia técnica especializada para la realización de técnicas

de sistemas y explotación sobre el entorno lógico, que soporta los diferentes sistemas de información descritos anteriormente, realizando las labores que se precisen y asesorando técnicamente sobre las mismas.

5.2.3.1 Establecimiento, revisión y corrección, según proceda, de los procedimientos de administración de sistemas.

Tiene como objetivo revisar los procedimientos y la documentación establecida por el Área de Informática, con objeto de identificar debilidades en el proceso que puedan originar problemas en la gestión diaria de los sistemas, estableciendo nuevos procedimientos, en el caso de que estos faltaran o corrigiéndolos si estos fueron defectuosos, de acuerdo con el director técnico.

5.2.3.2 Planificación en los cambios de entorno.

Tiene como objetivo proporcionar orientación de planes de contingencia, plan de pruebas y análisis de riesgos, en los supuestos que el Área de Informática considerase oportuno realizar algún cambio o ampliar el entorno de prestación de servicios.

Para ello, y con anterioridad a la realización del cambio, establecerá, de acuerdo con el director técnico, un plan de ejecución del cambio, teniendo en cuenta los aspectos señalados anteriormente.

5.2.3.3 Puesta en marcha de nuevos sistemas.

Tiene como objetivo proporcionar orientación de planes de contingencia, plan de pruebas y análisis de riesgos, en los supuestos que el Área de Informática considerase oportuno la puesta en marcha de nuevos sistemas de información.

Para ello, y con anterioridad a la realización de la puesta en marcha, establecerá, de acuerdo con el director técnico, un plan de ejecución de la misma, teniendo en cuenta los aspectos señalados anteriormente.

6 PLANIFICACIÓN DE LOS SISTEMAS OBJETO DE CONTRATACIÓN.

6.1. FASE UNO (ANUALIDAD 1).

6.1.1 *Descripción.*

- Plan de Desarrollo y en su caso, migración de datos y aplicaciones para los subsistemas objeto de contrato
- Análisis, diseño e implementación de las actuaciones de desarrollo objeto de contrato producidas hasta el 20 de diciembre de 2.015.
- Implementación.
- Realización de los planes de prueba,.

6.1.2 Fecha máxima de realización.

DOCE meses desde la fecha de adjudicación y siempre antes del 20 de diciembre de 2015.

6.1.3 Entregables

Toda la documentación se realizará según lo dispuesto en el documento de metodología de calidad aplicable en el Área de Informática. Además de los fuentes se entregarán necesariamente:

- Documentación del Plan de Migración de datos y aplicaciones de los subsistemas
- Documentación de planificación temporal de tareas y actividades para la incorporación completa de todos los subsistemas.
- Documento de Análisis de Riesgos en metodología MAGERIT.
- Documento de Plan de Calidad y Plan de Aseguramiento de Calidad.
- Documentación de los subsistemas.
    - Documento de análisis funcional. Modelo entidad-relación, Modelo de casos de uso. Diagramas de flujo de datos.
    - Documento de diseño técnico. Arquitectura y diagramas de estructuras. Modelo físico de datos.
    - Manual de usuario.
    - Manual de administración.
    - Documento de pruebas del sistema.
    - Documentación asociada al soporte a la implantación, problemas detectados y soluciones adoptadas.
- Documento de aceptación final de las nuevas funcionalidades.
- Implementación.
- Realización de los planes de prueba.

7 EQUIPO DE TRABAJO.

El oferente indicará el equipo de trabajo que piensa dedicar al proyecto, indicando los conocimientos generales y propios de la actividad de cada categoría profesional, incluyendo también los conocimientos técnicos previos, las tareas asociadas al trabajo, así como las responsabilidades a asumir (Anexo I).

También indicará la experiencia previa para la capacitación en el puesto.

7.1. DIRECTOR TÉCNICO.

El centro directivo designará un Director Técnico cuyas funciones en relación con estas prescripciones técnicas serán las siguientes:

- Velar por el cumplimiento de los trabajos exigidos y ofertados.
- Emitir las certificaciones parciales de recepción de los mismos.

El Director Técnico podrá delegar sus funciones en una persona de su equipo. Asimismo, podrá incorporar al proyecto durante su realización, las personas que estime necesarias para verificar y evaluar todas las actuaciones a su cargo.

No se autorizan los contactos directos de las personas del equipo de trabajo del contratista con el usuario final, sin el conocimiento previo y autorización del Director Técnico.

7.2. REGLAS ESPECIALES RESPECTO DEL PERSONAL LABORAL DE LA EMPRESA CONTRATANTE.

Corresponde exclusivamente a la empresa contratista la selección del personal que, reuniendo los requisitos de titulación y experiencia exigidos en este Pliego Técnico, formará parte del equipo de trabajo adscrito a la ejecución del contrato, sin perjuicio de la verificación por parte del Centro Directivo del cumplimiento es aquellos requisitos.

La empresa contratista asume la obligación de ejercer de modo real, efectivo y continuo, sobre su personal integrante del equipo de trabajo encargado de la ejecución del contrato, el poder de dirección inherente a todo empresario. En particular, asumirá la negociación y pago de los salarios, la concesión de permisos, licencias y vacaciones, la sustitución de los trabajadores en casos de baja o ausencia (siempre bajo la acreditación del cumplimiento de los requisitos de titulación y experiencia exigidos en este Pliego Técnico), las obligaciones legales en materia de Seguridad Social, incluido el abono de cotizaciones y el pago de prestaciones, cuando proceda, las obligaciones legales en materia de prevención de riesgos laborales, el ejercicio de la potestad disciplinaria, así como cuantos derechos y obligaciones se deriven de la relación contractual entre empleado y empleador.

La empresa contratista velará especialmente porque los trabajadores adscritos a la ejecución del contrato desarrollen su actividad sin extralimitarse en las funciones desempeñadas respecto de la actividad delimitada en los pliegos como objeto del contrato.

7.3. COORDINADOR TÉCNICO DE LA EMPRESA CONTRATISTA.

La empresa contratista deberá designar un coordinador técnico integrado en su propia plantilla que tendrá entre sus obligaciones las siguientes:

- Actuar como interlocutor de la empresa contratista frente al Centro Directivo, canalizando la comunicación entre la empresa contratista y el personal integrante del equipo de trabajo adscrito al contrato, de un lado, y el Centro Directivo, de otro lado, en todo lo relativo a las cuestiones derivadas de la ejecución del contrato.
- Distribuir el trabajo entre el personal encargado de la ejecución del contrato, e impartir a dichos trabajadores las órdenes e instrucciones de trabajo que sean necesarias en relación con la prestación con la prestación del servicio contratado.
- Supervisar el correcto desempeño por parte del personal integrante del equipo de

trabajo de las funciones que tienen encomendadas, así como controlar la asistencia de dicho personal al puesto de trabajo sin perjuicio del control efectivo de seguridad de acceso al Centro Directivo que corresponde en exclusiva a éste último

- Organizar el régimen de vacaciones del personal adscrito a la ejecución del contrato, debiendo a tal efecto coordinarse adecuadamente la empresa contratista con el Centro Directivo a efectos de no alterar el buen funcionamiento del servicio.

  Informar al Director Técnico acerca de las variaciones, ocasionales o permanentes, en la composición del equipo de trabajo adscrito a la ejecución del contrato.

8 CONDICIONES ADICIONALES A CUMPLIR POR LA EMPRESA OFERTANTE

La empresa adjudicataria deberá cumplir las siguientes condiciones adicionales:

- Tener conocimiento y experiencia en las infraestructuras de DNI y Pasaporte Electrónico.
- Deberá incluirse en la oferta compromiso de cumplimiento completo del presente Pliego de condiciones técnicas.
- Las ofertas presentadas deberán asumir la posibilidad de que la FNMT, una vez adjudicado el concurso, podrá, si el proveedor no cumple con lo ofertado y acorde con lo estipulado en el PCT o no proporciona la calidad de servicio necesaria, rescindir cualquier contrato de mantenimiento y soporte de inmediato y sin que ello suponga penalización alguna para la FNMT.
- Deberá incluirse en la oferta compromiso de acuerdo de confidencialidad entre la empresa ofertante, la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda y la Dirección General de la Policía, en relación con cualquier información o documento, identificado o no como confidencial.
- No publicitar ninguna relación con la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda y la Dirección General de la Policía sin previo consentimiento.
- Cumplimentar las políticas de seguridad, Calidad, Prevención de Riesgos, Protección de Medioambiente y Confidencialidad, de la Dirección General de la Policía.
- La empresa adjudicataria remitirá a la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda informes mensuales durante todo el período de vigencia de los contratos, detallando los trabajos realizados y el grado de avance de las tareas.

9 FACTURACIÓN

El pago se realizará mediante trasferencia bancaria en un plazo de 30 días desde la fecha de finalización de la prestación del servicio, previa recepción de la factura correspondiente, siendo la fecha efectiva de pago los días 10 y 25 de cada mes o el día hábil inmediatamente posterior.

En caso de prestación de servicio continuado, el pago se realizará mensualmente (a mes vencido) sobre los servicios realizados en el mes inmediatamente anterior.

Cualquier pago previo a la realización de conformidad del servicio debe ser garantizado mediante un aval bancario por el mismo importe adelantado.

10 CRITERIOS DE VALORACIÓN DE LAS OFERTAS

La oferta técnica tendrá una valoración del 45% y la económica del 55%.

El criterio de puntuación de la oferta técnica (de 0 a 100 puntos) será el siguiente:

CONCEPTO A VALORAR	RANGO DE VALORACIÓN
Cumplimiento del presente pliego de prescripciones técnicas.	Excluyente
Experiencia previa con el software de certificación Entrust	[0-20]
Experiencia previa con el software de certificación Safelayer	[0-20]
Experiencia previa en desarrollo J2EE e integración de sistemas.	[0-15]
Experiencia previa con hardware criptográfico Safenet / Thales	[0-10]
Conocimiento de los servicios de certificación de la DGP.	[0-15]
Metodología y flexibilidad del servicio ofrecido y del plan de mantenimiento.	[0-10]
Prestigio, solvencia y posicionamiento de la empresa ofertante.	[0-5]
Mejoras ofrecidas al PPT	[0-5]
TOTAL	[0-100]

El criterio de puntuación de la oferta económica será: Se asignarán 55 puntos a la oferta más económica, al resto proporcionalmente.

11 PRESENTACIÓN DE OFERTAS Y ACLARACIONES

Las empresas interesadas en presentar sus ofertas de servicios, podrán incluir cuanta documentación consideren oportuna para presentación de la empresa, describir sus soluciones y explicar la forma en que cumplimentarán los requisitos de este pliego de prescripciones.

Dichas ofertas se deberán presentar en el **Registro de FNMT-RCM** con la referencia CN-24-11-14-A, en documentos **separados la parte técnica de la económica** y en sobres independientes, incluyendo una copia digital de los mismos en CD o memoria USB. Se entregarán hasta la **fecha y hora indicadas en el anuncio correspondiente del Perfil del contratante,** debiendo entregar documento original firmado por un responsable de la empresa con firma autorizada.

Las ofertas se dirigirán a la atención de:

Área de Gestión - Dirección de Sistemas de Información
Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda
C/ Jorge Juan, 106
28009 Madrid

Cualquier consulta de tipo administrativo se dirigirá a la atención de:

Área de Gestión – Dirección de Sistemas de Información
Carlos Nieto Gómez
e-mail: gestion.informatica@fnmt.es
Tlf. 91 566 67 04

Cualquier consulta técnica relacionada con el presente pliego de condiciones, puede ser dirigida a las siguientes personas:

José Tomas Baeza Oliva
Teléfono: 91 566 69 24
e-mail: tbaeza@fnmt.es

12 ANEXO I.

Las denominaciones y las correspondientes definiciones de las categorías profesionales requeridas para la presente contratación, y a las que se aludirá en lo sucesivo, se incluyen a continuación:

12.1. JEFE DE PROYECTO.

12.1.1 Tareas / responsabilidades.

Es responsable técnico del proyecto, es decir, de la consecución de los objetivos y resultados establecidos por la dirección del proyecto. Sus responsabilidades son:

- Dirigir el equipo de desarrollo del proyecto.
- Elaborar el plan de calidad del proyecto.
- Elaborar informes periódicos de seguimiento del proyecto.
- Gestionar las acciones correctivas debidas a problemas, no conformidades en las verificaciones de productos o no conformidades durante el desarrollo de las pruebas.
- Documentar y evaluar los cambios que aparezcan, así como supervisar su implantación posterior.
- Elaborar el plan de gestión de riesgos del proyecto y controlar los riesgos a lo largo de la vida del proyecto.
- Establecer una comunicación efectiva con los usuarios / clientes finales y supervisar la comunicación que se establezca a niveles inferiores.
- Supervisar la correcta coordinación entre los integrantes del equipo asignado al proyecto.

12.1.2 Conocimientos previos

- Debe tener el conocimiento suficiente y la experiencia en gestión de grupos humanos y administración de proyectos como para guiar de una manera eficaz a los miembros del equipo de trabajo, establecer la adecuada relación con el área usuaria y mantener correctamente los canales de comunicación con los elementos decisorios de la organización.
- Conocimientos precisos y extensos sobre el *estado del arte* de la seguridad de documentos de viaje electrónicos EAC/PACE e ICAO, de las PKIs implicadas en su expedición, y de los medios de distribución que permiten su verificación, así como de los distintos niveles de las infraestructuras implicadas en la expedición de documentos electrónicos de identificación (eIDs que implican un gran número de emisiones, particularmente documentos de identificación nacionales):
    - arquitecturas de sistemas de expedición incluyendo, entre otros, las posibles dependencias entre sus distintos componentes, su criticidad, o los recursos e

infraestructuras que implica cada uno de ellos. Asimismo, relación de los sistemas de expedición con sistemas externos (entre otros, conexión con sistemas que dan servicio a la expedición de pasaportes desde dependencias diplomáticas, o comunicaciones típicamente implicadas en la expedición de documentos electrónicos de identificación nacionales).

- infraestructuras de PKI que implementan el ciclo de vida de los certificados y material criptográfico, así como elementos de seguridad asociados a ambos. Posibilidades de modificación y ampliación de estas infraestructuras.
- servicios y componentes *backend* que securizan las infraestructuras de PKI y las integran con los sistemas de expedición – entre otros, servicios de autenticación según norma CWA14890-1 2004, aplicaciones multiplataforma que intercomuniquen los sistemas de expedición con infraestructuras de PKI heterogéneas -, así como las opciones que éstos ofrecen en cuanto a la mejora o transformación de sus capacidades.
- infraestructuras de personalización física y lógica: impresoras, para policarbonato, escáneres de huella dactilar, lectores/grabadores de tarjetas, componentes software de personalización. Integración de estas infraestructuras en los procesos de expedición de documentación electrónica de identificación y pasaportes electrónicos.
- Estándares ICAO y de la Unión Europea aplicables. Problemas asociados con el cumplimiento de los estándares. Arquitecturas que dan respuesta a esta problemática. Tipologías de documentos de viaje y procedimientos de inspección asociados a ellos. Particularidades y problemática de las certificaciones internacionales exigidas por la Unión Europea en el contexto de las infraestructuras de clave pública de Verificación de País, con particular énfasis en las formas de comunicación contempladas. Implicaciones de los estándares, normativas, y recomendaciones de ICAO, la Unión Europea, y organismos dependientes de ellos, en la generación y distribución de material criptográfico necesario para la verificación de documentos electrónicos.
- Eventos oficiales de test de pasaporte electrónico EAC/PACE europeo. Resultados (especialmente de la tecnología de PKI usada en España), conclusiones, recomendaciones.
- Infraestructuras de clave pública implicadas en la securización de los documentos, incluyendo la relación entre ellas y las implicaciones prácticas de sus particularidades. Conocimientos profundos sobre las PKIs de Pasaporte-e y Permiso de residencia-e (de Firma de País y de Verificación de País) actualmente desplegadas en España (DGP).
- Relación entre los distintos documentos de viaje electrónicos expedidos en España: elementos compartidos, elementos diferenciados, implicaciones y motivación.
- Tecnologías y productos, tanto hardware como software, que dan respuesta a las necesidades de este tipo de documentos electrónicos.

  - Evolución futura de la seguridad de los documentos de viaje electrónicos EAC/PACE: estándares en discusión, adhesión prevista de estados a los estándares actuales, proyectos en curso de armonización transnacional de documentación electrónica. Impacto en los sistemas actuales de la probable evolución futura.
  - Conocimientos de los trabajos realizados en los grupos de trabajo al amparo del Mandato M460 de la Comisión Europea a CEN y ETSI para la modificación de los estándares en firmas y autenticación electrónicas.
  - Conocimientos profundos de los distintos niveles de las infraestructuras de PKI de expedición de documentos electrónicos de viaje actualmente implantadas, y de sus posibles implicaciones en los sistemas que den servicio a la inspección de pasaportes electrónicos.
- Amplios conocimientos sobre la familia de productos KeyOne de Safelayer.
- Productos de PKI de Entrust.
- Algoritmos de curva elíptica. Tecnologías disponibles para su utilización segura y eficiente.
- Metodología de desarrollo Métrica v3.
- Sistema operativo Solaris.
- Bases de datos INFORMIX.
- Lenguajes de programación Java (particularmente las opciones que ofrece en aplicaciones que hacen un uso intensivo de servicios de PKI y criptografía), C ++, C y Visual Basic.
- Desarrollo de aplicaciones web; tecnologías de desarrollo web.
- Integración de aplicaciones en Sun System Web Server.
- Metalenguaje XML
- ActiveX.
- Productos de PKI de Safelayer (KeyOne) de Pasaporte/Permiso de residencia electrónicos, incluyendo protocolos de comunicación con los mismos.
- HSMs: estándares de comunicación con ellos, integración de aplicaciones Java; módulos criptográficos de nCipher y Safenet. Particularidades de los modelos existentes.
- Directorios LDAP.
- Amplios conocimientos de tecnologías PKI, incluyendo estándares internacionales, legislación española y europea aplicables, definición de perfiles de certificación, protocolos, formatos, tecnologías, productos, mecanismos de validación (OCSP, CRLs), intercambio de mensajes PKIX-CMP.

12.1.3 Experiencia previa para la capacitación en el puesto.

- Mínimo de 4 años desarrollando tareas de jefe de proyecto / consultor.
- Mínima de 48 meses como jefe de proyecto / consultor en proyectos de personalización lógica de documentos de identidad nacionales electrónicos y pasaportes electrónicos.
- Mínimo de 36 meses en proyectos que incluyeran la implantación de productos de la familia KeyOne de Safelayer.
- Mínima de 24 meses como jefe de proyecto / consultor en proyectos de securización de chips de pasaportes electrónicos españoles (a ser posible pasaportes EAC/PACE, al menos una parte de ese tiempo).
- Mínima de 48 meses como jefe de proyecto / consultor en entorno Sist. Operativo Solaris.
- Mínima de 48 meses como jefe de proyecto / consultor en entorno de base de datos INFORMIX.
- Mínima de 48 meses como jefe de proyecto / consultor en entorno de lenguaje de programación JAVA, C++, C, Visual Basic.
- Mínima de 48 meses como jefe de proyecto / consultor en PKI Safelayer y PKI Entrust.
- Mínima de 48 meses como jefe de proyecto / consultor en el desarrollo de aplicaciones Java de integración de infraestructuras de PKI de sistemas de expedición de documentos de identidad nacionales electrónicos y pasaportes electrónicos.
- Mínima de 24 meses como jefe de proyecto / consultor en productos de PKI de Safelayer para Pasaportes Electrónicos.
- Mínima de 48 meses como jefe de proyecto / consultor en HSMs de nCipher/Thales y Retemsa
- Mínima de 12 meses como jefe de proyecto / consultor en HSMs Luna de Safenet.
- Mínima de 48 meses como jefe de proyecto / consultor en sistemas basados en autenticación según norma CWA14890-1 2004.
- Mínima de 24 meses como jefe de proyecto / consultor en LDAP.
- Mínima de 24 meses como jefe de proyecto / consultor en Web Services.
- Mínima de 9 meses como jefe de proyecto / consultor en proyectos de implantación o uso de PKIs de Verificación de País de pasaporte EAC/PACE del tipo de las descritas en los estándares correspondientes.
- Mínima de 4 meses como jefe de proyecto / consultor en proyectos de implantación de PKIs, y de elementos de integración asociados a ellas, de sistemas de expedición de Permisos de residencia electrónicos europeos del tipo de los descritos en los estándares correspondientes.
- Participación, directa o indirecta, en pruebas oficiales europeas de interoperabilidad de PKI de pasaporte electrónico EAC/PACE.

12.2. CONSULTOR.

12.2.1 Tareas / responsabilidades.

- Es responsable de la organización, del desarrollo y control permanente del proyecto, supervisando el ajuste a los programas y objetivos iniciales establecidos. Desarrolla, en colaboración con el Jefe de Proyecto, el plan de trabajo y elabora informes periódicos de avance.
- Establece una comunicación efectiva con los usuarios / clientes finales y supervisa la comunicación que se establezca a niveles inferiores.
- Identifica problemas, desarrolla soluciones y recomienda acciones.
- Garantiza la calidad de los productos finales.
- Propone al cliente la aprobación de los hitos establecidos en el proyecto, solicitando su concurso en caso necesario para el tratamiento de asuntos extraordinarios.
- Propone la participación de expertos funcionales.
- Planifica y organiza la formación de usuarios.
- Dirige la elaboración de propuestas u ofertas y presentaciones divulgativas del Sistema.
- Proporciona, cuando es necesario, asesoramiento técnico a los componentes del equipo del proyecto.

12.2.2 Conocimientos previos.

- Debe tener el conocimiento suficiente y la experiencia, en gestión de grupos humanos, administración de proyectos, así como en las tecnologías y metodologías utilizadas en el proyecto, para apoyar de una manera eficaz a los miembros del equipo de trabajo, establecer la adecuada relación con el área usuaria y mantener correctamente los canales de comunicación con los elementos decisorios de la organización.
- Debe tener el conocimiento suficiente y la experiencia en gestión de grupos humanos y administración de proyectos como para guiar de una manera eficaz a los miembros del equipo de trabajo, establecer la adecuada relación con el área usuaria y mantener correctamente los canales de comunicación con los elementos decisorios de la organización.
- Conocimientos precisos y extensos sobre el *estado del arte* de la seguridad de documentos de viaje electrónicos EAC/PACE e ICAO, de las PKIs implicadas en su expedición, y de los medios de distribución que permiten su verificación, así como de los distintos niveles de las infraestructuras implicadas en la expedición de documentos electrónicos de identificación (eIDs que implican un gran número de emisiones, particularmente documentos de identificación nacionales):
    - arquitecturas de sistemas de expedición incluyendo, entre otros, las posibles dependencias entre sus distintos componentes, su criticidad, o los recursos e infraestructuras que implica cada uno de ellos. Asimismo, relación de los sistemas de expedición con sistemas externos (entre otros, conexión con sistemas que dan servicio a la expedición de pasaportes desde dependencias diplomáticas, o comunicaciones típicamente implicadas en la expedición de documentos electrónicos de identificación nacionales).
    - infraestructuras de PKI que implementan el ciclo de vida de los certificados y material criptográfico, así como elementos de seguridad asociados a ambos.

Posibilidades de modificación y ampliación de estas infraestructuras.

- servicios y componentes *backend* que securizan las infraestructuras de PKI y las integran con los sistemas de expedición – entre otros, servicios de autenticación según norma CWA14890-1 2004, aplicaciones multiplataforma que intercomuniquen los sistemas de expedición con infraestructuras de PKI heterogéneas -, así como las opciones que éstos ofrecen en cuanto a la mejora o transformación de sus capacidades.
- infraestructuras de personalización física y lógica: impresoras, para policarbonato, escáneres de huella dactilar, lectores/grabadores de tarjetas, componentes software de personalización. Integración de estas infraestructuras en los procesos de expedición de documentación electrónica de identificación y pasaportes electrónicos.
- Estándares ICAO y de la Unión Europea aplicables. Problemas asociados con el cumplimiento de los estándares. Arquitecturas que dan respuesta a esta problemática. Tipologías de documentos de viaje y procedimientos de inspección asociados a ellos. Particularidades y problemática de las certificaciones internacionales exigidas por la Unión Europea en el contexto de las infraestructuras de clave pública de Verificación de País, con particular énfasis en las formas de comunicación contempladas. Implicaciones de los estándares, normativas, y recomendaciones de ICAO, la Unión Europea, y organismos dependientes de ellos, en la generación y distribución de material criptográfico necesario para la verificación de documentos electrónicos.
- Eventos oficiales de test de pasaporte electrónico EAC/PACE europeo. Resultados (especialmente de la tecnología de PKI usada en España), conclusiones, recomendaciones.
- Infraestructuras de clave pública implicadas en la securización de los documentos, incluyendo la relación entre ellas y las implicaciones prácticas de sus particularidades. Conocimientos profundos sobre las PKIs de Pasaporte-e y Permiso de residencia-e (de Firma de País y de Verificación de País) actualmente desplegadas en España (DGP).
- Relación entre los distintos documentos de viaje electrónicos expedidos en España: elementos compartidos, elementos diferenciados, implicaciones y motivación.
- Tecnologías y productos, tanto hardware como software, que dan respuesta a las necesidades de este tipo de documentos electrónicos.
- Evolución futura de la seguridad de los documentos de viaje electrónicos EAC/PACE: estándares en discusión, adhesión prevista de estados a los estándares actuales, proyectos en curso de armonización transnacional de documentación electrónica. Impacto en los sistemas actuales de la probable evolución futura.
- Conocimientos profundos de los distintos niveles de las infraestructuras de PKI de expedición de documentos electrónicos de viaje actualmente implantadas, y de sus posibles implicaciones en los sistemas que den servicio a la inspección de pasaportes electrónicos.
- Conocimientos de los trabajos realizados en los grupos de trabajo al amparo del Mandato M460 de la Comisión Europea a CEN y ETSI para la modificación de los estándares en firmas y autenticación electrónicas.

- Amplios conocimientos sobre la familia de productos KeyOne de Safelayer.
- Productos de PKI de Entrust.
- Algoritmos de curva elíptica. Tecnologías disponibles para su utilización segura y eficiente.
- Metodología de desarrollo Métrica v3.
- Sistema operativo Solaris.
- Bases de datos INFORMIX.
- Lenguajes de programación Java (particularmente las opciones que ofrece en aplicaciones que hacen un uso intensivo de servicios de PKI y criptografía), C ++, C y Visual Basic.
- Desarrollo de aplicaciones web; tecnologías de desarrollo web.
- Integración de aplicaciones en Sun System Web Server.
- Metalenguaje XML
- ActiveX.
- Productos de PKI de Safelayer (KeyOne) de Pasaporte/Permiso de residencia electrónicos, incluyendo protocolos de comunicación con los mismos.
- HSMs: estándares de comunicación con ellos, integración de aplicaciones Java; módulos criptográficos de nCipher y Safenet. Particularidades de los modelos existentes.
- Directorios LDAP.
- Amplios conocimientos de tecnologías PKI, incluyendo estándares internacionales, legislación española y europea aplicables, definición de perfiles de certificación, protocolos, formatos, tecnologías, productos, mecanismos de validación (OCSP, CRLs), intercambio de mensajes PKIX-CMP.

12.2.3 Experiencia previa para la capacitación en el puesto.

- Mínimo de 4 años desarrollando tareas de consultor.
- Mínima de 36 meses como jefe de proyecto / consultor en proyectos de PKI.
- Mínima de 36 meses como jefe de proyecto / consultor en proyectos de personalización lógica de documentos de identidad nacionales electrónicos y pasaportes electrónicos.
- Mínimo de 36 meses en proyectos que incluyeran la implantación de productos de la familia KeyOne de Safelayer.
- Mínima de 24 meses como jefe de proyecto / consultor en proyectos de securización de chips de pasaportes electrónicos españoles (a ser posible pasaportes EAC/PACE, al menos una parte de ese tiempo).
- Mínima de 36 meses como jefe de proyecto / consultor en entorno Sist. Operativo Solaris.
- Mínima de 36 meses como jefe de proyecto / consultor en entorno de base de datos INFORMIX.

- Mínima de 36 meses como jefe de proyecto / consultor en entorno de lenguaje de programación JAVA, C++, C, Visual Basic.
- Mínima de 36 meses como jefe de proyecto / consultor en productos de PKI de Safelayer y Entrust.
- Mínima de 36 meses como jefe de proyecto / consultor en el desarrollo de aplicaciones Java de integración de infraestructuras de PKI de sistemas de expedición de documentos de identidad nacionales electrónicos y pasaportes electrónicos.
- Mínima de 24 meses como jefe de proyecto / consultor en productos de PKI de Safelayer para Pasaportes electrónicos y/o Permiso de residencia electrónico.
- Mínima de 36 meses como jefe de proyecto / consultor en HSMs nCipher/Thales y Retemsa.
- Mínima de 12 meses como jefe de proyecto / consultor en HSMs Luna SA de Safenet.
- Mínima de 36 meses como jefe de proyecto / consultor en sistemas basados en autenticación según norma CWA14890-1 2004.
- Mínima de 24 meses como jefe de proyecto / consultor en LDAP.
- Mínima de 24 meses como jefe de proyecto / consultor en Web Services.
- Mínima de 9 meses como jefe de proyecto / consultor en PKIs de Verificación de País de pasaporte EAC/PACE.
- Mínima de 4 meses como jefe de proyecto / consultor en proyectos de implantación de PKIs, y de elementos de integración asociados a ellas, de sistemas de expedición de Permisos de residencia electrónicos europeos del tipo de los descritos en los estándares correspondientes.
- Se valorará participación directa en pruebas oficiales europeas de interoperabilidad de PKI de pasaporte electrónico EAC/PACE.

12.3. TÉCNICO DE SISTEMAS

- Tareas / responsabilidades.
- Apoyo y supervisión en el establecimiento de las estrategias de comunicaciones, seguridad, soporte físico y lógico e instalación de proyectos complejos.
- Es responsable de la definición de soluciones técnicas (arquitectura, comunicaciones, bases de datos, etc.) para un proyecto de desarrollo de sistemas.
- Participa en el establecimiento de estrategias generales de soporte físico y lógico.
- Apoya y supervisa la instalación y *tuning* de productos complejos.
- Dirige la elaboración de propuestas y ofertas en sus aspectos técnicos. Es el responsable de realizar presentaciones de carácter técnico.
- Mantiene relación con el responsable de sistemas del cliente.
- Establece con el Jefe de Proyecto y el Consultor los objetivos a largo plazo y realiza el seguimiento, establece objetivos a corto plazo, planifica y asigna responsabilidades.

- Transmite y explica los valores propios de la organización. Orienta a su equipo a la consecución de objetivos.

12.3.1 Conocimientos previos.

- Conocimientos precisos y extensos sobre el *estado del arte* de la seguridad de documentos de viaje electrónicos EAC/PACE e ICAO, de las PKIs implicadas en su expedición, y de los medios de distribución que permiten su verificación, así como de los distintos niveles de las infraestructuras implicadas en la expedición de documentos electrónicos de identificación (eIDs que implican un gran número de emisiones, particularmente documentos de identificación nacionales):
    - arquitecturas de sistemas de expedición incluyendo, entre otros, las posibles dependencias entre sus distintos componentes, su criticidad, o los recursos e infraestructuras que implica cada uno de ellos. Asimismo, relación de los sistemas de expedición con sistemas externos (entre otros, conexión con sistemas que dan servicio a la expedición de pasaportes desde dependencias diplomáticas, o comunicaciones típicamente implicadas en la expedición de documentos electrónicos de identificación nacionales).
    - infraestructuras de PKI que implementan el ciclo de vida de los certificados y material criptográfico, así como elementos de seguridad asociados a ambos. Posibilidades de modificación y ampliación de estas infraestructuras.
    - servicios y componentes *backend* que securizan las infraestructuras de PKI y las integran con los sistemas de expedición – entre otros, servicios de autenticación según norma CWA14890-1 2004, aplicaciones multiplataforma que intercomuniquen los sistemas de expedición con infraestructuras de PKI heterogéneas -, así como las opciones que éstos ofrecen en cuanto a la mejora o transformación de sus capacidades.
    - infraestructuras de personalización física y lógica: impresoras, para policarbonato, escáneres de huella dactilar, lectores/grabadores de tarjetas, componentes software de personalización. Integración de estas infraestructuras en los procesos de expedición de documentación electrónica de identificación y pasaportes electrónicos.
    - Estándares ICAO y de la Unión Europea aplicables. Problemas asociados con el cumplimiento de los estándares. Arquitecturas que dan respuesta a esta problemática. Tipologías de documentos de viaje y procedimientos de inspección asociados a ellos. Particularidades y problemática de las certificaciones internacionales exigidas por la Unión Europea en el contexto de las infraestructuras de clave pública de Verificación de País, con particular énfasis en las formas de comunicación contempladas. Implicaciones de los estándares, normativas, y recomendaciones de ICAO, la Unión Europea, y organismos dependientes de ellos, en la generación y distribución de material criptográfico necesario para la verificación de documentos electrónicos.
    - Eventos oficiales de test de pasaporte electrónico EAC/PACE europeo. Resultados (especialmente de la tecnología de PKI usada en España), conclusiones, recomendaciones.
    - Infraestructuras de clave pública implicadas en la securización de los documentos, incluyendo la relación entre ellas y las implicaciones prácticas de sus particularidades. Conocimientos profundos sobre las PKIs de Pasaporte-e y

Permiso de residencia-e (de Firma de País y de Verificación de País) actualmente desplegadas en España (DGP).

- Relación entre los distintos documentos de viaje electrónicos expedidos en España: elementos compartidos, elementos diferenciados, implicaciones y motivación.
- Tecnologías y productos, tanto hardware como software, que dan respuesta a las necesidades de este tipo de documentos electrónicos.
- Evolución futura de la seguridad de los documentos de viaje electrónicos EAC/PACE: estándares en discusión, adhesión prevista de estados a los estándares actuales, proyectos en curso de armonización transnacional de documentación electrónica. Impacto en los sistemas actuales de la probable evolución futura.
- Conocimientos profundos de los distintos niveles de las infraestructuras de PKI de expedición de documentos electrónicos de viaje actualmente implantadas, y de sus posibles implicaciones en los sistemas que den servicio a la inspección de pasaportes electrónicos.

- Profundos conocimientos sobre arquitecturas, parametrización y configuración de los productos KeyOne de Safelayer.
- Algoritmos de curva elíptica. Tecnologías disponibles para su utilización segura y eficiente.
- Metodología de desarrollo Métrica v3.
- Sistema operativo Solaris.
- Bases de datos INFORMIX.
- Lenguajes de programación Java (particularmente las opciones que ofrece en aplicaciones que hacen un uso intensivo de servicios de PKI y criptografía), C ++, C y Visual Basic.
- Desarrollo de aplicaciones web; tecnologías de desarrollo web.
- Integración de aplicaciones en Sun System Web Server.
- Metalenguaje XML
- ActiveX.
- Productos de PKI de Entrust.
- Integración con el software de monitorización Patrol de BMC.
- Productos de PKI de Safelayer (KeyOne) de Pasaporte/Permiso de residencia electrónicos, incluyendo protocolos de comunicación con los mismos.
- HSMs: estándares de comunicación con ellos, integración de aplicaciones Java; módulos criptográficos de nCipher y Safenet. Particularidades de los modelos existentes.
- Directorios LDAP.
- Amplios conocimientos de tecnologías PKI, incluyendo estándares internacionales, legislación española y europea aplicables, definición de perfiles de certificación, protocolos, formatos, tecnologías, productos, mecanismos de validación (OCSP, CRLs),

intercambio de mensajes PKIX-CMP.

- Mecanismos de autenticación y gestión de claves según norma CWA14890-1 2004.

12.3.2 Experiencia previa para la capacitación en el puesto.

- Mínimo de 4 años desarrollando tareas de técnico de sistemas.
- Mínimo de 36 meses como técnico de sistemas en proyectos que incluyeran la implantación, configuración o migración de productos de la familia KeyOne de Safelayer.
- Mínima de 24 meses definiendo soluciones técnicas que den servicio a sistemas de expedición de documentos de identidad nacionales electrónicos y pasaportes electrónicos.
- Mínima de 24 meses definiendo soluciones técnicas en proyectos de securización de chips de pasaportes electrónicos españoles (a ser posible pasaportes EAC/PACE, al menos una parte de ese tiempo).
- Mínima de 36 meses como técnico de sistemas en entorno Sist. Operativo Solaris.
- Mínima de 18 meses como técnico de sistemas en entorno de base de datos INFORMIX.
- Mínima de 18 meses como técnico de sistemas en entorno de lenguaje de programación JAVA, C++, C y Visual Basic.
- Mínima de 36 meses como técnico de sistemas en PKI Entrust y PKI Safelayer.
- Mínima de 18 meses como técnico de sistemas en productos de PKI de Safelayer para Pasaportes Electrónicos.
- Mínima de 36 meses como técnico de sistemas en los HSM de nCipher y Retemsa.
- Mínima de 12 meses como técnico de sistemas en los HSM Luna SA de Safenet.
- Mínima de 24 meses como técnico de sistemas en LDAP.
- Mínima de 9 meses como técnico de sistemas en proyectos de implantación o uso de PKIs de Verificación de País de pasaporte EAC/PACE del tipo de las descritas en los estándares correspondientes.
- Mínima de 4 meses como técnico de sistemas en proyectos de implantación de PKIs, y de elementos de integración asociados a ellas, de sistemas de expedición de Permisos de residencia electrónicos europeos del tipo de los descritos en los estándares correspondientes
- Mínima de 36 meses como técnico de sistemas en PKIX-CMP.
- Mínima de 36 meses como técnico de sistemas basados en autenticación según norma CWA14890-1 2004.
- Se valorará participación, directa o indirecta, en pruebas oficiales europeas de interoperabilidad de PKI de pasaporte electrónico EAC/PACE.

12.4. ANALISTA FUNCIONAL.

12.4.1 Tareas / responsabilidades.

- Obtiene información para la realización o mejora de módulos. Mantiene relación con usuarios finales y con el responsable funcional del proyecto.
- Realiza el diseño funcional y técnico del sistema o de módulos en sistemas complejos.
- Revisa el diseño detallado de módulos y la programación del equipo, comprobando que los programas se adecuan a los requisitos.
- Analiza incidencias.
- Define, planifica y realiza la prueba del sistema y la conversión.
- Participa en la elaboración y realización de presentaciones divulgativas del Sistema.
- Supervisa un pequeño equipo, responsabilizándose de la consecución de objetivos a corto plazo.
- Transmite y explica los valores propios de la organización. Orienta a su equipo a la consecución de objetivos. Promueve la formación del equipo de trabajo.

12.4.2 Conocimientos previos.

- Conocimientos precisos y extensos sobre el *estado del arte* de la seguridad de documentos de viaje electrónicos EAC/PACE e ICAO, de las PKIs implicadas en su expedición, y de los medios de distribución que permiten su verificación, así como de los distintos niveles de las infraestructuras implicadas en la expedición de documentos electrónicos de identificación (eIDs que implican un gran número de emisiones, particularmente documentos de identificación nacionales):
    - arquitecturas de sistemas de expedición incluyendo, entre otros, las posibles dependencias entre sus distintos componentes, su criticidad, o los recursos e infraestructuras que implica cada uno de ellos. Asimismo, relación de los sistemas de expedición con sistemas externos (entre otros, conexión con sistemas que dan servicio a la expedición de pasaportes desde dependencias diplomáticas, o comunicaciones típicamente implicadas en la expedición de documentos electrónicos de identificación nacionales).
    - infraestructuras de PKI que implementan el ciclo de vida de los certificados y material criptográfico, así como elementos de seguridad asociados a ambos. Posibilidades de modificación y ampliación de estas infraestructuras.
    - servicios y componentes *backend* que securizan las infraestructuras de PKI y las integran con los sistemas de expedición – entre otros, servicios de autenticación según norma CWA14890-1 2004, aplicaciones multiplataforma que intercomuniquen los sistemas de expedición con infraestructuras de PKI heterogéneas -, así como las opciones que éstos ofrecen en cuanto a la mejora o transformación de sus capacidades.
    - infraestructuras de personalización física y lógica: impresoras, para policarbonato, escáneres de huella dactilar, lectores/grabadores de tarjetas, componentes software de personalización. Integración de estas infraestructuras en los procesos de expedición de documentación electrónica de identificación y pasaportes electrónicos.
    - Estándares ICAO y de la Unión Europea aplicables. Problemas asociados con el

cumplimiento de los estándares. Arquitecturas que dan respuesta a esta problemática. Tipologías de documentos de viaje y procedimientos de inspección asociados a ellos. Particularidades y problemática de las certificaciones internacionales exigidas por la Unión Europea en el contexto de las infraestructuras de clave pública de Verificación de País, con particular énfasis en las formas de comunicación contempladas. Implicaciones de los estándares, normativas, y recomendaciones de ICAO, la Unión Europea, y organismos dependientes de ellos, en la generación y distribución de material criptográfico necesario para la verificación de documentos electrónicos.

  - Eventos oficiales de test de pasaporte electrónico EAC/PACE europeo. Resultados (especialmente de la tecnología de PKI usada en España), conclusiones, recomendaciones.
  - Infraestructuras de clave pública implicadas en la securización de los documentos, incluyendo la relación entre ellas y las implicaciones prácticas de sus particularidades. Conocimientos profundos sobre las PKIs de Pasaporte-e y Permiso de residencia-e (de Firma de País y de Verificación de País) actualmente desplegadas en España (DGP).
  - Relación entre los distintos documentos de viaje electrónicos expedidos en España: elementos compartidos, elementos diferenciados, implicaciones y motivación.
  - Tecnologías y productos, tanto hardware como software, que dan respuesta a las necesidades de este tipo de documentos electrónicos.
  - Evolución futura de la seguridad de los documentos de viaje electrónicos EAC/PACE: estándares en discusión, adhesión prevista de estados a los estándares actuales, proyectos en curso de armonización transnacional de documentación electrónica. Impacto en los sistemas actuales de la probable evolución futura.
  - Conocimientos profundos de los distintos niveles de las infraestructuras de PKI de expedición de documentos electrónicos de viaje actualmente implantadas, y de sus posibles implicaciones en los sistemas que den servicio a la inspección de pasaportes electrónicos.
  - Conocimientos de los trabajos realizados en los grupos de trabajo al amparo del Mandato M460 de la Comisión Europea a CEN y ETSI para la modificación de los estándares en firmas y autenticación electrónicas.

- Sistema operativo Solaris: integración de aplicaciones, programación de scripts.
- Implementación y análisis de aplicaciones que hacen uso de bases de datos Informix.
- Diseño y programación utilizando lenguajes de programación Java (incluyendo programación de comunicación basada en RMI seguros, y las opciones que ofrece en aplicaciones que hacen un uso intensivo de servicios de PKI y criptografía), C++, C y Visual Basic.
- Programación de componentes ActiveX.
- Análisis y diseño de aplicaciones web: servlets/JSPs, Javascript, HTML, CSS.
- Integración de aplicaciones en Sun System Web Server.
- Metalenguaje XML (intercambio de datos XML, desarrollo de aplicaciones que explotan

y construyen estructuras XML).

- Estándares de OACI y de la Unión Europea aplicables a la expedición de documentos de viaje MRTD. Implicaciones de los mismos en las PKIs que dan servicio a la personalización de los documentos. Implementación de componentes software que manejen grupos de datos, así como objetos de seguridad asociados a ellos, de acuerdo con lo dictado por OACI/ICAO para la securización de información contenida en chips de documentos de viaje.
- Conocimientos precisos de los protocolos, mecanismos y algoritmos criptográficos implicados en las operaciones descritas en los estándares EAC/PACE, incluyendo las distintas tecnologías existentes – tanto software como hardware – disponibles para implementarlos.
- Conocimientos profundos en el desarrollo de sistemas centralizados de inspección de documentación electrónica ICAO y EAC/PACE: librerías y componentes disponibles en el mercado, tecnologías disponibles.
- Metodología de desarrollo Métrica v3.
- IDEs Eclipse, Visual Studio.
- Desarrollo de componentes software que utilizan interfaces Pkcs#11.
- Desarrollo de interfaces con directorios LDAP.
- Integración de aplicaciones – generación de información de estado – con Patrol de BMC.
- Tecnologías PKI: amplios conocimientos de estándares, distintos estándares de intercambio de mensajes de certificación, mecanismos de validación, intercambio de mensajes PKIX.
- HSMs Retemsa, nCipher y Safenet: estándares de comunicación con ellos, integración de aplicaciones Java; módulos criptográficos de Safenet. Particularidades de los modelos existentes. Desarrollo de aplicaciones que hacen uso de ellos. Se requiere certificación de Safenet.
- Certificados y peticiones de certificación CV-EAC/PACE: desarrollo de aplicaciones que hagan uso de ellos.
- Administración de productos KeyOne de Safelayer; comunicación de aplicaciones con ellos; análisis y diseño de componentes auxiliares – crEAC/PACEión, adaptación de existentes.
- Captura y tratamiento de información biográfica y biométrica de acuerdo a los estándares internacionales.
- Tecnología de PKI de Entrust.
- Comunicación de aplicaciones con brokers EntireX.
- Mecanismos de autenticación y gestión de claves según norma CWA14890-1 2004.
- Análisis y diseño de Web Services seguros.

12.4.3 Experiencia previa para la capacitación en el puesto.

- Mínimo de 4 años desarrollando tareas de analista-programador.

- Mínima de 36 meses en el análisis y diseño de aplicaciones utilizando metodología Métrica-3.
- Mínima de 36 meses desarrollando aplicaciones embebidas en sistemas de expedición de documentos de identidad nacionales electrónicos y pasaportes electrónicos.
- Mínima de 36 meses como analista en el desarrollo de aplicaciones Java de integración de infraestructuras de PKI de sistemas de expedición de documentos de identidad nacionales electrónicos y pasaportes electrónicos.
- Mínima de 24 meses como analista/programador en proyectos de personalización o verificación de datos lógicos de documentos electrónicos (de identidad o viaje) españoles (a ser posible pasaportes EAC/PACE, al menos una parte de ese tiempo).
- Mínima de 18 meses como analista/programador en entorno sistema operativo Solaris.
- Mínima de 36 meses desarrollando aplicaciones en Java (JSE) o C/C++.
- Mínima de 18 meses como analista en programación de interfaces con tarjetas criptográficas.
- Mínima de 36 meses como analista en PKI Entrust y PKI Safelayer.
- Mínima de 36 meses como analista en mensajería PKIX-CMP.
- Mínima de 12 meses como analista programador en entorno XML.
- Mínima de 12 meses como analista en LDAP.
- Mínima de 36 meses como analista en sistemas de autenticación según norma CWA14890-1 2004.
- Mínima de 24 meses como analista en los HSM de nCipher y Retemsa.
- Certificación en HSMs Luna SA de Safenet.
- Mínima de 12 meses como analista o analista-programador en proyectos en los que se haga uso de certificados CV-EAC/PACE
- Mínima de 12 meses en el desarrollo o mantenimiento de sistemas de inspección de inspección de documentación electrónica ICAO y EAC/PACE.
- Mínima de 8 meses como analista o analista-programador en Web Services

12.5. ANALISTA / PROGRAMADOR.

12.5.1 Tareas / responsabilidades.

- Elabora el diseño detallado de programas con un elevado grado de supervisión.
- Codifica, revisa y prueba los programas.
- No participa directamente, pero atiende a las incidencias que surgen durante la prueba del sistema o durante la conversión de datos.
- Realiza el seguimiento de las incidencias que se le asignan.
- Evalúa y analiza cambios con un elevado grado de supervisión.

12.5.2 Conocimientos previos.

- Sistema operativo Solaris: integración de aplicaciones, programación de *scripts*.
- Implementación de aplicaciones que hacen uso de bases de datos Informix.
- Diseño y programación utilizando lenguajes de programación Java (incluyendo programación de comunicación basada en RMI seguros, y las opciones que ofrece en aplicaciones que hacen un uso intensivo de servicios de PKI y criptografía), C++, C y Visual Basic.
- IDEs Eclipse, Visual Studio.
- Programación de componentes ActiveX.
- Programación de aplicaciones web: servlets/JSPs, Javascript, HTML, CSS.
- Integración de aplicaciones en Sun System Web Server.
- Implementación de nuevas funcionalidades, y modificación de las existentes, en aplicaciones Java de integración de infraestructuras de PKI de sistemas de expedición de documentos de identidad nacionales electrónicos y pasaportes electrónicos.
- Metalenguaje XML (intercambio de datos XML, desarrollo de aplicaciones que explotan y construyen estructuras XML).
- Implementación de componentes software que manejen grupos de datos, así como objetos de seguridad asociados a ellos, de acuerdo con lo dictado por OACI (ICAO) para la securización de información contenida en chips de documentos de viaje.
- Conocimientos precisos de los protocolos, mecanismos y algoritmos criptográficos implicados en las operaciones descritas en los estándares EAC/PACE, incluyendo las distintas tecnologías existentes – tanto software como hardware – disponibles para implementarlos.
- Conocimientos profundos en el desarrollo de sistemas centralizados de inspección de documentación electrónica ICAO y EAC/PACE: librerías y componentes disponibles en el mercado, tecnologías disponibles.
- Certificados y peticiones de certificación CV-EAC/PACE: desarrollo de aplicaciones que hagan uso de ellos.
- PKI Entrust (CA, autoridad de registro desarrollada específicamente para la expedición del DNI-e) y PKI Safelayer (productos KeyOne: integración con procesos del ciclo de vida de certificació; lenguaje *Scryptor;* comunicación de aplicaciones con ellos; análisis y diseño de add-ins – crEAC/PACEión, adaptación de existentes –; comunicación de aplicaciones con ellos).
- Programación y securización de Web Services.
- Desarrollo de drivers basados en Pkcs#11.
- Integración de aplicaciones – generación de información de estado – con Patrol de BMC.
- Tecnologías PKI: mecanismos de validación (OCSP, CRLs), intercambio de mensajes PKIX-CMP, desarrollo de aplicaciones que hacen uso de mecanismos básicos de clave pública.

- Integración de aplicaciones en el ciclo de vida de los certificados de los sistemas de expedición de documentos de identidad nacionales electrónicos y pasaportes electrónicos.
- HSMs Retemsa, nCipher y Safenet: estándares de comunicación con ellos, integración de aplicaciones Java; módulos criptográficos de Safenet. Particularidades de los modelos existentes. Desarrollo de aplicaciones que hacen uso de ellos. Se requiere certificación de Safenet.
- Captura y tratamiento de información biográfica y biométrica de acuerdo a los estándares internacionales.
- Desarrollo de interfaces con directorios LDAP.
- Integración de aplicaciones – generación de información de estado – con Patrol de BMC.
- Integración de aplicaciones Java con brokers de tecnología EntireX.
- Mecanismos de autenticación y gestión de claves según norma CWA14890-1 2004.
- Programación de Web Services seguros.

12.5.3 Experiencia previa para la capacitación en el puesto.

- Mínimo de 4 años desarrollando tareas de analista-programador.
- Mínimo de 2 años desarrollando aplicaciones de integración de componentes de expedición de documentos de identidad nacionales electrónicos y pasaportes electrónicos.
- Mínimo de 6 meses desarrollando aplicaciones de integración de componentes de expedición de permisos de residencia electrónicos EAC/PACE.
- Mínima de 20 meses como analista-programador en proyectos en los que se haga uso de certificados CV-EAC/PACE
- Mínima de 12 meses en el desarrollo o mantenimiento de sistemas de inspección de inspección de documentación electrónica ICAO y EAC/PACE.
- Mínima de 36 meses desarrollando aplicaciones en Java (JSE).
- Mínima de 36 meses desarrollando software que utilice el HSM netHSM de nCipher/Thales.
- Mínima de 12 meses desarrollando software que haga uso del HSM de Retemsa.
- Mínima de 12 meses desarrollando software que haga uso del HSM Luna SA de Safenet.
- Mínima de 12 meses desarrollando aplicaciones en C/C++.
- Mínima de 12 meses como analista programador en entorno XML.
- Mínima de 36 meses como analista programador en mensajería PKIX-CMP.
- Mínima de 6 meses como analista/programador de Web Services.