Defensor del Pueblo

CONTRATO DE SERVICIOS

PLIEGO DE DE PRESCRIPCIONES TÉCNICAS

SISTEMA DE ADJUDICACIÓN:
PROCEDIMIENTO ABIERTO

TRAMITACIÓN:
ORDINARIA

DESCRIPCIÓN DEL TRABAJO:
ADJUDICACIÓN DEL CONTRATO DE SUMINISTRO DE UNA PLATAFORMA DE FIRMA ELECTRÓNICA PARA EL DEFENSOR DEL PUEBLO

INDICE

I. OBJETO

El objeto del presente contrato queda definido en la cláusula tercera del pliego de cláusulas administrativas.

II. ELEMENTOS OBJETO DEL CONTRATO

Se pretende la adquisición y puesta en marcha, en perfecto estado de operatividad, de una plataforma de firma electrónica institucional, compuesta por un sistema de servicios de firma electrónica y de un sistema seguro para la custodia de certificados electrónicos, que funcionen de forma sincronizada. El suministro comprenderá la instalación, configuración y puesta en servicio en las dependencias del Defensor del Pueblo.

En concreto, los componentes objeto de suministro básicamente son:

- Plataforma de firma electrónica corporativa, compuesta por:
  - Un sistema de servicios de firma, que proporcione seguridad y confianza a las aplicaciones que necesiten implementar funciones relacionadas con la firma electrónica.
  - Un sistema de custodia de certificados, que resuelva la operativa de gestión de certificados electrónicos y el almacenaje de los mismos en condiciones de seguridad.
- Asistencia técnica para la total integración de esta nueva plataforma con los sistemas de información que hagan uso de la firma electrónica.
- Formación y documentación.

III. PLATAFORMA INSTITUCIONAL DE FIRMA ELECTRÓNICA

Los licitadores incluirán una justificación de las características técnicas del equipamiento ofertado, en función de su arquitectura interna, así como una exposición detallada de la manera en que dichas características dan cobertura a los requisitos mínimos exigidos, que se exponen a lo largo de este pliego.

La plataforma habrá de ser totalmente compatible con el entorno tecnológico del Defensor del Pueblo y abarcará como mínimo los elementos que a continuación se indican, que operarán de forma sincronizada entre ellos.

- Un sistema de servicios de firma, que proporcione seguridad y confianza a las aplicaciones que necesiten implementar funciones relacionadas con la firma electrónica.
- Un almacén de claves y certificados que garantice y resuelva la necesaria custodia de los certificados y sellos electrónicos utilizados en los procesos de firma electrónica.

Las características técnicas de los mismos se describen a continuación:

Sistema de servicios de firma. Este sistema tendrá una arquitectura orientada a servicios (SOA), ofrecerá una interfaz de acceso a todos los servicios de firma, sus funcionalidades serán accesibles mediante Web Services y tendrá las siguientes funcionalidades:

- Firma electrónica. Permitirá la verificación y generación de firmas electrónicas, reconociendo diferentes prestadores de certificación, así como la verificación de las mismas a lo largo del tiempo, para lo cual habrá de generar y custodiar las evidencias electrónicas necesarias, garantizando el no repudio.
- Gestión de claves. Permitirá registrar, revocar, consultar y verificar las claves de las entidades.
- Capacidades de cifrado digital. Servicios de cifrado, descifrado, ensobrado y des-ensobrado de datos que puedan estar disponibles en la plataforma para cuando el Defensor del Pueblo adecue sus procedimientos al Esquema Nacional de Interoperabilidad (ENI).
- No-repudio digital. Servicios de generación y validación de evidencias digitales, generalmente acompañadas de firma electrónica.
- Autenticación, autorización y control de acceso. Permitirá la autenticación, autorización y control del acceso de las entidades registradas haciendo posible el control de acceso único, así como la agrupación de dichas entidades (usuarios, servicios web y aplicaciones) en todo el sistema para la definición de perfiles y privilegios.
- Gestión de objetos y entidades. Dispondrá de funciones de registro, consulta y modificación de la información sobre entidades, en particular, información de identidad del titular de un certificado, nombre de los firmantes de un documento, la fecha y hora contenida en un sello de tiempo, configuración y auditoría.
- Protección y custodia de datos. Dispondrá de componentes que permitan la protección de datos, claves, firmas y documentos firmados, y su custodia, a lo largo del tiempo, garantizando su mantenimiento y el acceso a éstos por las personas autorizadas.
- Auditoría y registro. Disponible de forma centralizada y segura de toda la información de traza generada por cualquiera de los componentes de servicio del sistema, así como la información de uso y consumo de los servicios.
- Permitirá generar diversos tipos de informes.
- Servicios adicionales. Se incluyen los servicios de sellado de tiempo y de verificación de los certificados digitales a través de su integración con la plataforma @firma.

Además, estará integrado en los sistemas corporativos de gestión de usuarios, valorándose adecuadamente que disponga de un sistema de administración encargado de suministrar las políticas de decisión, con arreglo a la siguiente funcionalidad:

- Políticas de validación de documentos. Se utilizarán para definir cómo se va a llevar a cabo la verificación de documentos: sólo la firma, la firma y la caducidad del certificado, la firma y el estado de revocación del certificado, la firma, la caducidad y estado de revocación del certificado, etc. Se podrán definir niveles de validación global o por Autoridades de Certificación.
- Políticas de sellado y resellado de tiempo. Se aplicarán en el proceso de resellado de tiempo de los documentos en custodia, indicando los periodos y las cadencias de este proceso.
- Políticas de retención. Indicarán el periodo de tiempo que un documento permanece en custodia en la plataforma, durante el cual se le aplicarán operaciones de resellado para darle la validez en el tiempo.
- Políticas de control de acceso a documentos. Indicarán quién y con qué privilegios puede acceder a un documento.
- Políticas de control de acceso a servicios. Mostrarán los usuarios que van a poder acceder a los servicios de la plataforma y con qué permisos.
- Políticas de control de acceso generales. Determinarán a qué recurso puede acceder una entidad

A) Características técnicas: El sistema de servicios de firma se entenderá como una plataforma común de gestión de servicios, e incluirá la configuración, monitorización y control de acceso de cada uno de los componentes de servicio. Dicho sistema presentará las siguientes características:

- Los datos de configuración, personalización, monitorización, auditoría y control se expondrán en XML.
- El acceso a los servicios se realizará mediante SOAP, según la especificación WSDL de cada servicio en concreto, que será controlado mediante autenticación.
- La interacción cliente-servidor se realizará sobre transporte HTTP o HTTPS de forma que se puede securizar el canal con SSL/TLS con o sin autenticación mutua.

El sistema interactuará con otros elementos de la infraestructura, ya sean del Defensor del Pueblo o externos. En concreto:

- Terceras partes de confianza, a las que el sistema se conectará para validar los certificados digitales (Autoridades de Certificación o Autoridades de Validación) y para obtener sellos de tiempo (Autoridades de Sellado de Tiempo) de ámbito externo (@-firma, CERES-FNMT y las restantes reconocidas por la Administración Pública).
- Operará con los dispositivos criptográficos HSM que habrán de ser integrados como elementos en la respuesta a este pliego.

- Bases de datos, donde se almacenará la información de log sobre la actividad de los componentes de servicio para su auditoría posterior.
- Repositorio de documentos, Documentum, destinado a permitir que el componente de servicio de custodia de firmas pueda depositar y gestionar los documentos que contengan firmas, además de tener la posibilidad de agregar algún componente de cifrado de documentos. Se basará en la tecnología de almacenamiento del sistema de explotación actual.
- Directorio, donde el componente de servicio podrá leer y escribir información sobre las entidades (personas, aplicaciones o servicios web) reconocidas por el sistema.

B) Características de integración: Permitirá su integración con otros sistemas por las siguientes formas:

- Se incluirá una librería Java que pueda utilizarse por los clientes para invocar los diferentes servicios
- Mediante servicio web XML a partir de la especificación estándar WSDL de OASIS Digital Signature Service (DSS).
- Mediante una variante del método anterior a partir del WSDL pero utilizando únicamente XML y los estándares XPath y XSLT.
- Al nivel de Broker, Hub y/o ESB XML que permita la conexión de entornos Middleware de integración como WebLogic de Oracle, WebSphere de IBM, TIBCO BusinessWorks, etc.
- Al nivel de Gateway/Pipeline integrado al sistema, dispondrá de un front-end que permita recibir datos fuente de la aplicación, generalmente en XML pero no necesariamente (a través de HTTP/HTTPS, Mensajería –JMS-, SMTP, etc.), y mediante un lenguaje de pipeline sencillo se podrán establecer las reglas de procesado: transformar, firmar, verificar, cifrar, descifrar, autenticar, autorizar..., que serán ejecutadas para obtener la salida de datos deseada.

C) Estándares: El sistema cumplirá los siguientes estándares:

- Estándares de infraestructura: WSDL (Web Service Description Language), SOAP (Simple Object Access Protocol), XML/XSD (Extensible Markup Language / XML Schema Definition) y UDDI (Universal Description, Discovery, and Integration).
- Estándares de seguridad: SSL (Secure Socket Layer), TLS (Transport Layer Security), WS-Security (OASIS Web Services Security), SAML (Assertions and Protocol for the OASIS Security Assertion Markup Language) y OASIS
- Estándares de firma electrónica y cifrado: PKCS#7/CMS, S/MIME, PDF-Sig, XML-Dsig, XML-Enc, CAdES, XAdES y PAdES.
- Servicios de seguridad: DSS (Digital Signature Service Core Protocols, Elements, and Bindings, OASIS. Draft), valorándose adecuadamente el cumplimiento de alguno de los siguientes estándares de servicios de seguridad: Liberty ID-WSF (Liberty ID-WSF Authentication Service Specification), WSTrust (Web Services Trust

Language), WS-Federation (Web Services Federation Language), XACML (OASIS eXtensible Access Control Markup Language) y XKMS (Xml Key Management Service).

- Soporte de certificados digitales: X509 (ITU-T Recommendation X509v3).
- Soporte de los estándares de sobre digital: PKCS#7 (Public Key Cryptography Standard, IETF RFC 2315), CMS (Cryptographic Message Syntax, IETF RFC 3369), SMIME2 (Secure Multipurpose Internet Mail Extens ions Version 2, IETF RFC 2311), SMIME3 (Secure Multipurpose Internet Mail Extensions Version 3, IETF RFC 2633), CAdES (Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats, ETSI TS 101 733), XML-Dsig (XMLSignatureSyntax and Processing, W3C Recommendation), XML- Enc (Encryption Syntax and Processing. W3C Recommendation), XAdES (XML Advanced Electronic Signatures. ETSI TS 101 903), PDF (Firma electrónica PKCS#7/CMS en los documentos PDF según las especificaciones de firma digital y cifrado de clave pública para PDF de Adobe y de RFC 3778 de IETF) y PAdES.
- Soporte de sellado de tiempo digital: TSP (Time-Stamp Protocol, IETF RFC 3161).
- Verificación de estado de certificados digitales: CRL (ITU-T Recommendation X509v3) y OCSP (Online Certificate Status Protocol, IETF RFC 2560).
- Directorio: LDAP (Lightweight Directory Access Protocol).
- Gestor Documental: WEBDMS (HTTP/WebDAV, IETF RFC 2518).
- Soporte HSM: PKCS#11 (Cryptographic Token Interface Standard).
- Custodia de documentos: ISO 154891:2001 y MoReq (Modelo de requisitos para la gestión de registros electrónicos) de la UE.

Se valorará adecuadamente que la tecnología elegida disponga de algún reconocimiento y certificación de seguridad (Common Criteria, FIPS, etc.).

D) Equipamiento: El sistema de servicios de firma estará compuesto por varios equipos hardware de iguales características entre sí (tipo appliance o enracables), así como de otros equipos adicionales de iguales características entre cada tipo y de los elementos de software necesarios para la implementación de los servicios objeto del presente contrato.

El sistema deberá tener capacidad suficiente para soportar la carga de trabajo prevista. Y en cuanto al licenciamiento del software, no deberá existir ninguna limitación en cuanto al número de entidades (usuarios, aplicaciones, web services, etc.) que utilicen el sistema de servicios de firma, ni cualquier otro servicio otorgado por la plataforma.

El sistema interactuará con diversos elementos de la infraestructura, sean del Defensor del Pueblo o externos, para lo cual dispondrá de conexiones con los mismos en configuración redundante.

Se implantarán las políticas y mecanismos de salvaguarda (backup) necesarios para garantizar la recuperación del servicio en caso de desastre, además de un sistema similar al de producción para su utilización en el entorno de desarrollo.

Características de obligado cumplimiento de los equipos appliance:

- Sistema operativo diseñado para máxima seguridad, tanto en lo referido al kernel como a la pila de protocolos de red.
- Mínimo de 2 CPU con tecnología multicore.
- 2 discos duro SAS de al menos 150 GB cada uno, configurados en raid 1.
- Lector DVD.
- 1 tarjeta de red Gigabit de doble puerto o 2 tarjetas de 1 puerto.
- Rendimiento mínimo en firmas electrónicas por segundo:
  - 45 Firmas/Verificaciones - 1k - PKCS#7
  - 40 Firmas/Verificaciones - 1k – XMLDsig
  - 30 Firmas/Verificaciones - 100k - PKCS#7
  - 30 Firmas/Verificaciones - 100k – XMLDsig
  - 10 Firmas/Verificaciones - 1M - PKCS#7
  - 8 Firmas/Verificaciones - 1M – XMLDsig

Características de la solución destinada a servir de almacén y custodia de certificados de obligado cumplimiento:

- Seguridad física en la custodia de las claves
- Aceleración criptográfica (al menos 1.000 operaciones criptográficas por segundo - 1024 - bit RSA decrypt
- Certificado para funcionar con las CA del centro directivo
- Validación FIPS 140-2 Level 3
- Integración a través de la compatibilidad con diferentes estándares: PKCS#11, Microsoft CryptoAPI 2.0, JCA (Java Cryptographic Architecture), JCE (Java Cryptographic Extensions), OpenSSL y APIs.
- Administración remota segura.

IV. CARACTERÍSTICAS FUNCIONALES

Para una mayor claridad se han agrupado en los siguientes subsistemas:

IV.1 Subsistema de Autenticación

Se encargará de autenticar y autorizar a las diferentes entidades que acceden al sistema, con mecanismos de autenticación mediante usuario/contraseña y certificado (TLS/SSL) de forma directa estándar, y a través de mecanismos adicionales basados en firmas con certificados X.509.

Deberá soportar su integración tanto con plataformas de single sign-on como con la gestión federada de identidades con otros dominios (entre usuarios, servicios web y aplicaciones).

IV.2 Subsistema de Gestión de Identidades.

- Permitirá gestionar y organizar las diferentes comunidades de consumidores de servicios (usuarios, aplicaciones, servicios web, políticas, certificados, logs de auditorías, etc.).
- Permitirá llevar a cabo la gestión de usuarios: alta, baja, modificación de usuarios y la asignación de políticas de acceso a documentos y servicios.
- Permitirá gestionar los grupos de usuarios privilegiados, los usuarios, aplicaciones o servicios y los grupos de entidades finales.
- Permitirá organizarlos como mínimo por los siguientes conceptos:
  - Entidades: usuario, aplicaciones, servicios web, políticas, certificados, logs/auditoría, etc
  - Lista de entidades, definidos por el conjunto de las entidades que pertenecen a la misma.
  - Grupos organizativos, que contendrán todas las entidades que cumplan una determinada condición sobre el valor de los atributos del Distinguished Name.
  - Grupos dinámicos, que contendrán todas las entidades que cumplan una determinada condición de pertenencia al grupo, basada en:
    - Una plantilla X.509 que define la condición que cumple el certificado de cualquier entidad que pertenezca al grupo.
    - Una expresión XPath (Query) que define la condición que cumple la vista XML de la información registrada en el sistema para cualquier entidad que pertenece al grupo.
  - Grupos de grupos, que permite implementar un sistema de control de acceso basado en roles, en el que cada rol está definido como un determinado grupo de grupos.
  - También permitirá la realización de un sistema RBAC (Role Based Access Control) abierta, donde cada rol se mapea a un Grupo.
- Dispondrá de los siguientes servicios:
  - Servicio de información de entidades que permita de forma confiable para una identidad concreta (verificada en el proceso de autenticación), obtener información sobre un determinado usuario (persona o aplicación) registrado en el sistema o sobre los datos de configuración que utiliza una aplicación, o sobre cualquier otra información disponible.
  - Servicio de respuesta de información sobre las entidades servicios web basado en Universal Description, Discovery, and Integration, en concreto, el servicio de información de localización o binding de los servicios web dentro del sistema.

IV.3 Subsistema de Firma Electrónica

Permitirá disponer de un servicio de firma electrónica de datos que posibilitará a cualquier entidad, previa autenticación y autorización, solicitar el servicio de firma indicando la clave que quiere utilizar para ello.

Permitirá generar firmas digitales de datos en los diferentes formatos reconocidos: PKCS#7/CMS, PDFDsig, CAdES, XML-Dsig/XAdES y S/MIME):

El interfaz de este servicio seguirá la especificación de OASIS Digital Signature Service (DSS) de servicios de firma digital y dispondrá de una serie de perfiles configurables.

El sistema almacenará el material de firma de las entidades en los repositorios haciendo éste accesible de forma uniforme y controlada.

Para la generación de firmas electrónicas, deberá soportar la utilización de dispositivos seguros HSM a través de estándares para el almacenamiento y utilización de las claves.

Dispondrá de los siguientes perfiles de firma:

- Firmas PKCS #7 y CMS. Este perfil permitirá realizar firmas electrónicas que siguen el estándar PKCS#7 de RSA, CMS de IETF, CAdES de ETSI. Se permitirán firmas simples y múltiples (tanto secuenciales como paralelas), en formato de firma envolvente o separada.
- Firmas XML-Dsig/XAdES. Este perfil permitirá realizar las firmas en formato XML XML-Dsig y XAdES definidas por W3C y ETSI. Los elementos XAdES utilizados son los básicos de políticas y propiedades del firmante. Se pueden realizar firmas envolventes, incrustadas o separadas incluyendo firmas por referencia de cualquier nodo de un documento XML.
- Firmas S/MIMEv2 y S/MIMEv3. Este perfil permitirá generar mensajes seguros de correo electrónico de acuerdo con los formatos S/MIME definidos por IETF. Este perfil permite generar documentos PDF firmados de acuerdo con el formato definido por Adobe plasmado en las recomendaciones de IETF PDF-Sig.

IV.4 Subsistema de No Repudio

Permitirá disponer de un servicio de incorporación y recogida de evidencias electrónicas de la firma del titular cuando esté firme un documento, de tal forma que permitan otorgar valor probatorio a dicha firma. Además, permitirá su utilización para la renovación y actualización de los elementos de confianza para dotar a las firmas digitales de validez a lo largo del tiempo (firmas longevas).

Este subsistema permitirá realizar verificaciones de las firmas pasado el tiempo, para lo cual permitirá archivar dichas evidencias, que podrán extraerse y usarse por terceros, como elementos probatorios.

En este sentido, aunque deberá ser posible configurar el acceso a diferentes TSAs internas o externas, lo mismo que a diferentes VAs, y que estás puedan además configurarse por etapas para obtener niveles de redundancia ante caídas de estos servicios de terceros, para la ejecución del proyecto sólo será necesario configurar la integración de los servicios ofrecidos a través de la Red SARA.

En todo caso, este subsistema permitirá asegurar el no repudio de una firma electrónica durante el período de tiempo que establezca la normativa corporativa y el marco legislativo aplicable, reafirmando la validez de las evidencias electrónicas de la misma a lo largo del tiempo de forma periódica y automatizada.

Este subsistema custodiará y mantendrá los datos de validación de las firmas electrónicas longevas, encargando de forma periódica al subsistema correspondiente que actualice dicho material criptográfico, antes de que el sello de tiempo expire, o los algoritmos, claves y otros datos criptográficos usados sean vulnerables.

El subsistema podrá ser utilizado por otros servicios y aplicaciones para acceder a los datos de verificación de firma para verificar una firma electrónica concreta. Los documentos y las firmas de éstos se almacenarán en el repositorio de documentos.

Es por ello que este subsistema de No Repudio deberá estar muy directamente relacionado con el sistema de gestión documental, para que a partir de esa integración cumpla los siguientes requisitos:

- Gestionar los documentos que se entregan para su salvaguarda y, además, se guardará información relativa a su validación (CRLs, respuestas OCSP, cadenas de certificación, etc.), datos de resellados y la información de retención y expiración del documento.
- Realizar consultas sobre documentos que estén en custodia sin acceder directamente al repositorio o repositorios donde están guardados, separándose con ello las operaciones de consultas de las operaciones de acceso a documentos.

IV.5 Subsistema de Verificación

Permitirá verificar la validez de las firmas que se hayan generado mediante el subsistema de firma electrónica y las que se hayan actualizado mediante el subsistema de no repudio.

Para ello utilizará los servicios de una Tercera Parte Confiable (TTP) a través del protocolo OCSP (Online Certificate Status Protocol) y/o mediante conexión a una Autoridad o Plataforma de Validación que se encargue de validar en línea el estado de los certificados involucrados en la firma ofreciendo, además, el acceso directo a diferentes tipos de fuentes de información de revocación.

Para cada certificado deberá poder configurarse uno o varios mecanismos y etapas de obtención de la información de revocación. Por ejemplo, que para un determinado certificado, primero utilice OCSP y, en caso de fallo, se descargue la CRL correspondiente, etcétera.

La interfaz seguirá la especificación Digital Signature Service de OASIS (DSS).

IV.6 Subsistema de Encriptación

Se podrá contar con la posibilidad de permitir cifrar y descifrar datos según el formato de CMS de IETF CMS, PKCS #7 de RSA y el estándar de cifrado XML de W3C XML-Enc, obteniendo los certificados de cifrado de los destinatarios. En este sentido, el sistema deberá presentar la opción de soportar los perfiles siguientes:

- Cifrado PKCS #7 y CMS
- Cifrado XML-Enc

IV.7 Subsistema de Gestión de Claves

Se destina a permitir el acceso, utilizando XML a la generación, registro, consulta, verificación, revocación, o cualquier otra operación de claves públicas, estandarizando de esta forma el acceso a funciones de Autoridad de Certificación (CA), Autoridad de Registro (RA) y Autoridad de Validación (VA). Dicho subsistema deberá permitir el acceso a sus servicios mediante clientes ligeros basados íntegramente en XML.

IV.8 Subsistema de Custodia de Datos Criptográficos

Se destina a asegurar a lo largo del tiempo los certificados digitales usados por los distintos intervinientes en el proceso de firma electrónica, así como las credenciales, el mecanismo de autenticación y los privilegios de acceso a la información de los mismos.

Los objetos que contienen claves y certificados estarán autoprotegidos por hardware.

El sistema debe contemplar a lo largo del tiempo y de forma transparente los siguientes aspectos:

- Los funcionarios del centro directivo podrán renovar sus certificados, o podrán cambiar sus atributos.

- El centro directivo podrá cambiar de infraestructura de certificación.
- Los mecanismos de control de acceso pueden cambiar a lo largo del tiempo.
- Los accesos a los datos protegidos, se deben auditar cuando se acceda o se intente acceder a éstos.
- Este subsistema se encargará de:
    - Proteger las claves de cifrado de datos a lo largo del tiempo y entregarlas únicamente a los usuarios explícitamente autorizados, para lo cual utilizará un HSM.
    - Custodiar los documentos cifrados con las claves adecuadas y entregarlos únicamente a los usuarios explícitamente autorizados.
    - Procurar el adecuado nivel de protección del material criptográfico a lo largo del tiempo, así como la fortaleza del mecanismo de comunicación con los usuarios autorizados, asegurando de esta forma la longevidad del archivo.

También podrá gestionar los documentos, cifrándolos, almacenándolos en el repositorio de documentos y descifrándolos. Para lo cual, cuando una entidad solicite el cifrado de datos, debe hacerlo para un dominio de confidencialidad representado por una política concreta.

Permitirá implementar un sistema de clasificación de la información en el que los datos cifrados se puedan asociar a un grupo de usuarios, que pertenezcan a un dominio de confidencialidad, y sólo estos usuarios puedan tener acceso a ellos.

Este subsistema también podrá ser utilizado por otros servicios y aplicaciones para acceder a las claves de cifrado o a los datos de verificación de firma para verificar una firma electrónica concreta.

IV.9 Subsistema de Administración

Encargado de la realización de las tareas de administración del sistema de servicios de firma, dispondrá una consola de administración que permitirá, a través de un navegador, administrar y acceder a toda la información del sistema de una forma uniforme y centralizada.

Dispondrá de al menos las siguientes funcionalidades, que permitirán:

- La gestión de las Autoridades de Certificación, las Autoridades de Validación y las Autoridades de Sellado de Tiempo.
- Definir un conjunto de reglas y acciones a aplicar en función la forma de autenticación, de la entidad autenticada y del recurso solicitado.
- Configurar el uso de las claves privadas: firma, fechado (sellado) y, para el caso de haberse incluido en la propuesta, capacidades de cifrado y descifrado, así como configurar grupos de credenciales (pares de clave privada y pública junto al

certificado) que conjugan credenciales y el uso que se le desea dar: firma, cifrado, sellado, etc.

- Definir y modificar las políticas a aplicar en la generación de firmas electrónicas.
- Definir y gestionar las políticas de verificación de firma electrónica, incluyendo las de validación de certificados digitales.
- Definir la configuración de componentes de servicio propios del sistema y la configuración de las bases de datos, directorio, etcétera.
- La consulta de los eventos generados por todos los componentes de servicio del sistema.

IV.10 Subsistema de Auditoria

Encargado de realizar funciones de auditoría, proporcionará la trazabilidad de toda la operativa del sistema. Todas las operaciones que se pueden llevar a cabo en cualquiera de los componentes del sistema (control de acceso, custodia, criptografía, administración e incluso auditoría) serán registradas como trazas en ficheros de auditoría que posteriormente podrán ser analizados por auditores desde la interfaz gráfica del módulo.

En estos ficheros de auditoría se recogerá:

- Cuándo se hizo la operación
- Quién la realizó
- Qué operación realizó
- Cuál fue el resultado de la operación

Además de los ficheros de trazas de auditoría también existirán y deberán poder ser consultados los ficheros de trazas de actividad del sistema que registran el comportamiento de los servicios para todas las solicitudes de operación que reciben.

Dispondrá de funciones para consulta y realización de informes sobre los controles de auditoría de cualquiera de los módulos de la plataforma.

V. SERVICIOS DE ASISTENCIA TÉCNICA Y FORMACIÓN

En la oferta se incluirá el soporte técnico necesario para la instalación, puesta en marcha del sistema, integración y ajuste del mismo a la plena operatividad para su utilización en los sistemas de información que hagan uso de la firma electrónica dentro del Defensor del Pueblo. Para que los licitadores puedan ajustar mejor sus ofertas, en el siguiente punto de este pliego se detalla la situación del entorno tecnológico del Defensor del Pueblo.

También será necesario realizar como parte del proyecto la capacitación del personal técnico del Área de Informática para optativa la utilización del material ofertado.

Así pues, los licitadores deberán incluir un plan de formación que deberá ser aprobado por al dirección del Área de Informática y que comprenderá los siguientes aspectos:

Como mínimo se procederá a la formación de:

- Un grupo de 2 a 6 personas en la administración de las herramientas suministradas (60 horas).
- Un grupos de 2 a 6 personas en la operación del sistema y de las herramientas suministradas (20 horas).
- Un grupo de 2 a 5 personas en utilización de las herramientas suministradas (40 horas).

Todos estos cursos incluirán los manuales de formación en español y se impartirán en las instalaciones del Defensor del Pueblo, en fechas a determinar.

Los recursos y dedicaciones especificados se consideran meramente estimativos, por lo que durante la ejecución de los trabajos se podrán redistribuir las horas de cursos a realizar en función de las necesidades reales sobrevenidas, siempre que no se sobrepase el importe total del contrato.

VI. ENTORNO TECNOLÓGICO ACTUAL

Con el fin de que los licitadores puedan concretar su planteamiento respecto a sus ofertas, independientemente de que para cualquier otra aclaración se podrán dirigir a la dirección recogida en el apartado XVI, se reseñan a continuación los componentes básicos de la actual infraestructura tecnológica.

Elementos físicos:

- Sistema central:
  - Servidores IBM Blade HS21, HS22 y JS22 con diversos dominios.
  - Sistema de almacenamiento SAN basado en tecnología de IBM con equipos IBM Total Storage 16B
- Clientes: Ordenadores personales con arquitectura X86 Intel X.

Elementos lógicos:

- Sistema central:
  - Sistema operativo AIX 6.5 y Windows2003, pendiente de su migración a Windows2008.
  - Gestores de bases de datos: Oracle 11g y SQL Server 2010.
  - Plataforma servidor de aplicaciones: WebLogic Enterprise Suite.
  - Directorio LDAP: Microsoft Active Directory
- Clientes: Sistema operativo Windows, con navegador Internet Explorer.
- Sistemas de información que hacen uso de la firma electrónica:

- Sistema de información institucional para la gestión de los expedientes de quejas de los ciudadanos (GEX): Sistema desarrollado a la medida de las necesidades de la Institución sobre la gestión de procesos de TIBCO iProcess y las capacidades de gestión documental proporcionadas por Documentum, en el que se recogen todos los flujos de trabajado derivados de los procesos de investigación iniciados por el Defensor del Pueblo a partir de las quejas de ciudadanos o de oficio, así como los flujos de validación y firma de escritos derivados de la tramitación de estos expedientes.
- Registro electrónico. Sistema desarrollado a la medida de las necesidades de la Institución, que da soporte a la recepción de las quejas de ciudadanos y a los adjuntes a los expedientes ya iniciados a través del portal institucional.

VII. CONDICIONES ADICIONALES A CUMPLIR

VII.1 Disponibilidad de medios

El adjudicatario deberá contar con los medios propios de toda índole necesarios de cara al soporte técnico que pueda necesitar para llevar a cabo con éxito los servicios objeto del contrato.

Todos los gastos ocasionados como consecuencia del soporte y explotación del servicio que se requiere, así como de los desplazamientos del personal prestador del servicio durante el cumplimiento de las obligaciones derivadas del contrato serán por cuenta del contratista.

En el caso de que los servicios contratados puedan implicar para el contratista, por razones de cumplimiento de plazos, puestas en producción de servicios o cualesquiera otros motivos, la ejecución de los mismos en régimen de turnos, en sábados, festivos o en horario nocturno deberán ser asumidos siempre por el contratista y el Defensor del Pueblo no aceptará costes adicionales por estas circunstancias.

VII.2 Responsable del servicio

El adjudicatario designará al jefe de servicio como responsable del mismo ante el Defensor del Pueblo. Este responsable será el interlocutor único y se encontrará en permanente contacto con el personal que la dirección del Área de Informática del Defensor del Pueblo designe a los efectos de dirección del proyecto.

A través del responsable del servicio y con la periodicidad que en cada fase del mismo el Defensor del Pueblo determine, se informará sobre la planificación de trabajos, el estado de ejecución del contrato y, en su caso, sobre las incidencias producidas. En particular, el responsable realizará, entre otras, las siguientes tareas:

- Coordinar el apoyo técnico y la formación necesaria que el adjudicatario suministre al equipo humano que desarrolle los trabajos objeto del contrato, en todas aquellas materias precisas para el perfecto desempeño de los mismos.
- Cuando sea necesario, impartir instrucciones al personal asignado para la ejecución del contrato sobre el trabajo a realizar, siempre teniendo en cuenta la base de las instrucciones genéricas que se desprendan de lo establecido en el presente pliego y encaminadas al buen término del proyecto.
- Supervisar y controlar el trabajo y las actividades realizadas e informar al Defensor del Pueblo de las posibles incidencias y seguimiento o desviaciones de plazos.
- Ejercer el mando y las facultades organizativas sobre el equipo encargado de la prestación de los servicios objeto del contrato, que estará siempre bajo la disciplina laboral y el poder de dirección del contratista, con independencia de que, para el mejor cumplimiento del servicio, en determinados momentos el adjudicatario pueda destacar personal del equipo prestador del servicio en cualquier centro de trabajo del Defensor del Pueblo.
- Hacer entrega al Defensor del Pueblo de los productos desarrollados por su equipo.

El incumplimiento de las obligaciones precitadas, parcial o totalmente, facultará a esta Institución para acordar la resolución del contrato.

VIII. SEGUIMIENTO Y CONTROL DEL PROYECTO

La jefatura del proyecto (responsable del contrato) será asumida por la dirección del Área de Informática o por quien ésta designe para este cometido.

El responsable del contrato llevará el seguimiento y coordinación operativos de las actividades a realizar al amparo del objeto del contrato. A tal efecto, se reunirá, al menos, con una periodicidad mensual, con el responsable del servicio de la empresa adjudicataria.

Asimismo, el inicio del proyecto estará marcado por una reunión conjunta entre el responsable del contrato y el responsable del servicio de la empresa adjudicataria, en la que se revisarán los planes ofertados por el adjudicatario, para el ajuste a las circunstancias reales en que deberá ejecutarse el proyecto.

Además, con una antelación mínima de cuarenta y ocho horas a la fecha de cada reunión de seguimiento, el responsable del servicio de la empresa adjudicataria deberá entregar al Defensor del Pueblo un informe de seguimiento, en el que reflejará el grado de desarrollo de los servicios de acuerdo con la planificación establecida. Dicho informe, deberá además reflejar el progreso y desviación de los planes establecidos, señalando las siguientes magnitudes:

- Seguimiento y evaluación del progreso de las tareas y plazos planificados para la implantación y prestación de los servicios.
- Grado de satisfacción de los usuarios y nuevas necesidades detectadas por el Defensor del Pueblo.

IX. PLAZO DE GARANTÍA

Se establece un plazo de garantía de 12 meses, cuyo cómputo se iniciará desde la fecha de recepción o conformidad de los trabajos.

El adjudicatario facilitará, durante el periodo de garantía y sin coste adicional para el Defensor del Pueblo, todas las correcciones que, a solicitud del Defensor del Pueblo, sean necesarias para el adecuado funcionamiento de las modificaciones realizadas en los servicios ya existentes o sobre los nuevos servicios construidos al amparo de esta licitación.

Hasta que no tenga lugar la finalización del periodo de garantía, y debido a las particularidades propias de la elaboración de aplicativos y de la técnica de sistemas informáticos, el adjudicatario responderá de la correcta realización de los trabajos contratados y de los defectos que en ellos hubiera, sin que sea eximente ni le otorgue derecho alguno la circunstancia de que los representantes del Defensor del Pueblo los hayan examinado o reconocido durante su elaboración o aceptado en comprobaciones, valoraciones, certificaciones o recepciones parciales e incluso en la recepción total del trabajo, en previsión de la posible existencia de vicios o fallos ocultos en los trabajos ejecutados.

X. PROPIEDAD DE LOS TRABAJOS

Todos los estudios y documentos, así como los productos y subproductos elaborados por el contratista como consecuencia de la ejecución del contrato serán propiedad del Defensor del Pueblo, quien podrá usarlos, reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello el adjudicatario autor material de los trabajos.

El adjudicatario renuncia expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del contrato pudiera corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados a resultas de este procedimiento, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa del Defensor del Pueblo.

Específicamente todos los derechos de explotación y titularidad de las aplicaciones informáticas y programas de ordenador desarrollados al amparo del contrato, corresponden y exclusivamente al Defensor del Pueblo.

XI. DERECHOS SOBRE HARDWARE, SOFTWARE E INFRAESTRUCTURAS DEL DEFENSOR DEL PUEBLO

El contratista no adquiere ningún derecho sobre el hardware, software e infraestructuras propiedad del Defensor del Pueblo, salvo el de acceso indispensable al mismo para el cumplimiento de las tareas que se desprenden de las obligaciones dimanantes del contrato.

El contratista no podrá utilizar la información obtenida en la actividad desarrollada como consecuencia del contrato, no pudiendo transmitir dicho conocimiento, sin el consentimiento expreso y por escrito del Defensor del Pueblo.

XII. DOCUMENTACIÓN

Durante todo el periodo de ejecución del contrato y plazo de garantía ofertado, el adjudicatario se compromete a mantener actualizada toda la documentación relacionada con los productos ofertados.

El adjudicatario entregará al Defensor del Pueblo un juego completo de manuales de documentación de usuario y de documentación técnica en idioma castellano de los nuevos servicios desarrollados.

XIII. CALIDAD

Durante el desarrollo de los trabajos y la ejecución de las diferentes fases del proyecto, la Institución podrá establecer acciones de aseguramiento de la calidad sobre la actividad desarrollada y los productos obtenidos. A tal fin, el Defensor del Pueblo podrá incorporar al proyecto los recursos que considere oportunos para garantizar su correcta ejecución.

XIV. PLAZO DE EJECUCIÓN DE LOS TRABAJOS

El plazo total de ejecución del contrato será de 6 meses a contar desde el día siguiente a la formalización del contrato o el período en el que queden consumidas las jornadas ofertadas por los licitadores en sus ofertas. Asimismo, el adjudicatario, deberá tener la capacidad y la flexibilidad necesaria de abordar los trabajos, que les permita adaptarse a las necesidades del Defensor del Pueblo.

Si en la fecha de inicio de la ejecución de los trabajos, los suministros objeto del contrato no estuvieran disponibles, no se pudiera contar con una fecha concreta para garantizar tal disponibilidad o si dicha fecha, una vez establecida, pusiese en riesgo el cumplimiento de plazos de ejecución global del proyecto, el Defensor de Pueblo quedará facultado para acordar la resolución del contrato.