Eusko Jaurlaritzaren
Informatika Elkartea

Sociedad Informática
del Gobierno Vasco

EXPEDIENTE Nº: EJIE-147-2022

Suministro de equipos HSM y migración de claves criptográficas para DSGV.

Pliego de Condiciones Técnicas

Diciembre de 2022

Este documento es propiedad de Eusko Jaurlaritzaren Informatika Elkartea – Sociedad Informática del Gobierno Vasco, S.A. (EJIE) y su contenido es CONFIDENCIAL. Este documento no puede ser reproducido, en su totalidad o parcialmente, ni mostrado a otras partes, ni utilizado para otros propósitos que los que han originado su entrega, sin el previo permiso escrito de EJIE. En el caso de ser entregado en virtud de un contrato, su utilización estará limitada a lo expresamente autorizado en dicho contrato. EJIE no podrá ser considerada responsable de eventuales errores u omisiones en la edición del documento.

Versión	Fecha	Resumen de cambios	Elaborado por	Aprobado por
1.0	19/12/2022	Versión inicial	Josu Bagazgoitia	Aritza Iratzagorria

Índice

1 Introducción 4

1.1 Perfil de la compañía 4

2 Objeto y alcance del contrato 5

2.1 Justificación de la necesidad 5

2.2 Objeto y alcance del presente pliego 5

3 Detalle de suministros y puesta en marcha 7

3.1 Descripción de la situación actual 7

3.2 Suministros necesarios 7

3.3 Puesta en marcha 7

3.3.1 Migración de claves criptográficas 7

3.3.2 Instalación y puesta en marcha del equipamiento 8

3.3.3 Actualización de firmware y software 8

3.3.4 Proceso de migración de claves 8

3.3.5 Soporte del equipamiento 9

3.3.6 Documentación 9

4 Normas de seguridad relativas a los Sistemas de Información. 10

4.1 Seguridad laboral 10

4.2 Secreto y confidencialidad 10

4.3 Acceso y protección de datos 11

1 Introducción

1.1 Perfil de la compañía

EJIE, Eusko Jaurlaritzaren Informatika Elkartea – Sociedad Informática del Gobierno Vasco, es la Empresa pública de servicios de las tecnologías de la información y las comunicaciones (TIC), cuya razón de existir es contribuir a la consecución de un Sector Público Vasco, moderno y eficiente, en el Marco Legal establecido por el Gobierno, con la seguridad y calidad necesarias y con el debido respeto al medio ambiente.

EJIE tiene como meta final la consecución de la satisfacción de sus clientes, siendo el instrumento común de prestación de servicios TIC en el Sector Público Vasco, y comprometiéndose en:

- Construir y mantener con eficiencia y calidad la infraestructura de los Sistemas de Información, posibilitando su continuidad y seguridad.
- Garantizar la interoperabilidad entre las distintas administraciones.
- Servir de apoyo a las necesidades de planificación y realización de la función informática de los Departamentos y Organismos Autónomos del Gobierno, asegurando la cobertura de sus demandas con el compromiso y profesionalidad adecuados a las relaciones contractuales que se establezcan.

Por tanto, EJIE debe ser, un instrumento común de referencia para la prestación de servicios TIC en el Sector Público Vasco:

- Aportando valor añadido.
- Proporcionando soluciones competitivas.
- Transmitiendo confianza a sus clientes.
- Contando con personas cualificadas y comprometidas.

Se puede obtener información más detallada y extensa en nuestra dirección de Internet https://www.ejie.eus.

2 Objeto y alcance del contrato

2.1 Justificación de la necesidad

El DSGV cuenta con una Infraestructura de Clave Pública (PKI) que permite emitir certificados criptográficos utilizados en diversas operaciones de autenticación, cifrado y firma de documentos internos.

Dicha PKI utiliza un módulo de seguridad hardware, elemento conocido por sus siglas en inglés como HSM, "Hardware Security Module". Este dispositivo genera, almacena y protege las claves criptográficas privadas de la PKI asegurando mediante una estrategia de redundancia la disponibilidad continua de los activos protegidos.

Ante la próxima finalización del soporte de los dispositivos HSM de los que dispone el Departamento de Seguridad y tratarse de componentes básicos de la infraestructura de seguridad se hace imprescindible la adquisición de elementos necesarios para su adecuada sustitución, así como para la migración de las claves actuales a los nuevos dispositivos.

2.2 Objeto y alcance del presente pliego

El objeto del presente Pliego de Condiciones Técnicas (en adelante, PCT) es definir las condiciones técnicas que deben cumplir las ofertas de los licitadores para:

- Suministro de dos módulos de hardware criptográfico para la sustitución de los ***dos*** módulos de hardware criptográfico actualmente en funcionamiento de acuerdo con el Anexo Reservado *Descripción detallada del Suministro de equipos HSM y migración de claves criptográficas para DSGV*.
- Suscripción de soporte de los equipos suministrados.
- Puesta en marcha del equipamiento suministrado:
    - Instalación de los suministros, hardware, firmware y software necesarios para mantener actualizados los sistemas y evitar incompatibilidades con el software instalado.
    - Configuración y migración tecnológica incluyendo las claves criptográficas.
    - Pruebas, comprobaciones y test de aceptación.
    - Documentación de la solución desplegada.

Los equipos se ubicarán en armarios rack y deberán instalarse con los soportes y guías necesarios que garanticen la correcta instalación de los mismos, debiendo garantizarse la seguridad de los equipos (correcta fijación de los mismos a los perfiles).

Asimismo, se incluirá el desmontaje y retirada a los almacenes centrales del DSGV de los equipos y módulos que sean sustituidos en la nueva arquitectura y/o queden en desuso.

Los conceptos objeto del pliego quedan reflejado por lo tanto en la siguiente tabla:

OBJETO DEL EXPEDIENTE		
CONCEPTO	**DESCRIPCIÓN**	**Uds.**
Suministro de hardware y licencias	• Equipo especificado en el Anexo Reservado al PCT Descripción detallada del Suministro de equipos HSM y migración de claves criptográficas para DSGV.o equipo equivalente del mismo u otro fabricante con su part-number que soporte las mismas funcionalidades • Instalación y puesta en marcha del equipamiento	2
Servicios de puesta en marcha	• Migración de claves criptográficas • Actualización de firmware y software • Proceso de migración de claves • Soporte del equipamiento • Documentación	1
Suscripción de soporte de los equipos suministrados	Garantía de hardware del fabricante de ***al menos*** 5 años posteriores a la fecha de entrega que incluirá durante dicho periodo: • Soporte oficial del fabricante con acceso a las actualizaciones de firmware de los equipos • Apertura de casos de consulta técnica • En caso de avería, el suministro de un equipo de sustitución equivalente del mismo fabricante	1

3 Detalle de suministros y puesta en marcha

3.1 Descripción de la situación actual

El DSGV dispone en la actualidad de una solución HSM con una relativamente próxima finalización de su soporte (por motivos de seguridad, un mayor detalle se facilitará -sujeto a confidencialidad- a los licitadores que lo solicite-

3.2 Suministros necesarios

Con el objeto de asegurar la continuidad de las operaciones y poder conservar las claves criptográficas actuales, que son base de la infraestructura de clave pública gestionada por la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos, es necesaria la adquisición de dos dispositivos HSM que permitan la sustitución de los actuales.

Dichos nuevos dispositivos deberán permitir la migración directa de las claves criptográficas almacenadas en los equipos actuales.

Como referencia de los equipos necesarios se debe ofertar equipamiento de acuerdo con el Anexo Reservado al PCT *Descripción detallada del Suministro de equipos HSM y migración de claves criptográficas para DSGV.*

Los suministros incluirán los elementos hardware, latiguillos y accesorios necesarios para la conexión entre los módulos y la red del DSGV, así como el correspondiente cableado de alimentación, sistemas de montaje en rack, necesarios para la correcta realización de los trabajos objeto del pliego, junto con todo el material menor.

Los equipos objeto de suministro deberán contar con la ***Suscripción de soporte de los equipos suministrados***, una garantía de hardware del fabricante de al menos 5 años posteriores a la fecha de entrega. Durante el período de garantía, todo el equipamiento suministrado deberá disponer del soporte oficial del fabricante que deberá incluir el acceso a las actualizaciones de firmware de los equipos, así como la apertura de casos de consulta técnica y, en caso de avería, el suministro de un equipo de sustitución equivalente del mismo fabricante.

3.3 Puesta en marcha

3.3.1 Migración de claves criptográficas

La empresa adjudicataria deberá considerar la ejecución de todas aquellas tareas necesarias para asegurar la correcta puesta en marcha de la nueva infraestructura, siguiendo las indicaciones establecidas a continuación. Se identifican al menos los siguientes trabajos a realizar por la empresa adjudicataria en esta fase:

- Revisión de los datos de partida disponibles y objetivos del proyecto
- Metodología y procedimientos necesarios para la ejecución de los trabajos, así como su planificación global.
- Establecer el Plan de Migración para la renovación de la infraestructura que permita garantizar la migración paulatina del servicio y la convivencia de las diferentes tecnologías, incluyendo un plan de marcha atrás
- Planificación de los trabajos con los responsables designados (DGTSI, Oficina Técnica de gestión del proyecto, etc.), en cualquiera de las fases de proyecto, de acuerdo con los procedimientos y planes de migración que se determinen

Estos trabajos deberán realizarse de forma previa al inicio de la instalación definitiva y deberán ser aprobados por el personal designado por el DSGV. Todos los documentos y trabajos que forman parte de la Planificación Inicial deberán ser expresamente aprobados por el responsable del proyecto en el DSGV.

3.3.2 Instalación y puesta en marcha del equipamiento

Se incluirán los trabajos para:

- Almacenaje, traslado, instalación, configuración, etiquetado, migración y puesta en marcha del equipamiento incluyendo:
  - Configuración e instalación de los nuevos equipos
  - Configuración de la electrónica existente, aprovechando con ello la infraestructura actual
  - Reorganización de elementos en la totalidad de los armarios sobre los que se actúe, conectividad y peinado del total de cables
  - Alimentación de los nuevos equipos disponiendo regletas enrackables, según necesidad
  - Elaboración y ejecución de los planes de pruebas que aseguren la adecuada puesta en marcha de los servicios, en colaboración con los responsables de DGTSI, Oficina Técnica de gestión del proyecto y otros agentes implicados
  - Etiquetado de elementos en rack, siguiendo las indicaciones que a tal efecto establezcan DGTSI y Oficina Técnica de gestión del proyecto
- Retirada de material y equipamiento obsoleto y/o en desuso, siguiendo las indicaciones establecidas por la DGTSI y la Oficina Técnica de gestión del proyecto
- Validación de las instalaciones/resultado de migración por parte de la DGTSI.
- Desembalaje y reciclaje de los embalajes.

Todos los materiales necesarios para el correcto funcionamiento del sistema en su totalidad quedan incluidos y deberán ser suministrados por el adjudicatario previa aprobación del DSGV.

El adjudicatario deberá disponer a su cargo de los equipos y medios necesarios para la correcta ejecución de todos los trabajos incluidos en el contrato, siguiendo en todo momento lo especificado en el presente pliego, así como la normativa vigente aplicable en cada caso.

Los trabajos serán realizados en las instalaciones de la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos en Erandio.

Larrauri-Mendotxe Bidea, 18

48950 Erandio

Bizkaia

3.3.3 Actualización de firmware y software

Como paso previo a la migración de las claves se realizará una actualización de los equipos suministrados a las últimas versiones de software y firmware recomendadas por el fabricante.

Se realizará una prueba de aceptación con comprobación de las versiones y realización de los diagnósticos cuyo resultado se reflejará en un documento.

3.3.4 Proceso de migración de claves

Se realizará el proceso de migración de claves con el acompañamiento y supervisión del personal designado por la DGTSI con el objetivo de asegurar la integridad y privacidad de las claves criptográficas objeto de los trabajos.

Cualquier dispositivo intermedio utilizado en el proceso de migración se pondrá a disposición de la DGTSI para su custodia y posterior destrucción.

3.3.5 Soporte del equipamiento

Los licitadores ofertarán la garantía y soporte del fabricante durante un periodo de cinco años a partir de la fecha de entrega. Este soporte permitirá al Gobierno Vasco acceso a apertura de incidentes con el fabricante, descarga de nuevas versiones y actualizaciones del software y asistencia técnica para la resolución de incidentes.

3.3.6 Documentación

El adjudicatario deberá entregar, como mínimo, la siguiente documentación:

- Plan de Implantación y migración de las claves criptográficas.
- Diseño general de la solución técnica que se adopte para la infraestructura de CPD.
- Configuraciones y detalles técnicos de los dispositivos.
- Procedimiento de contingencia y escalado de incidentes.
- Documentación final con información técnica detallada, que facilite el traspaso de conocimiento al equipo técnico del DSGV.

4 Normas de seguridad relativas a los Sistemas de Información.

El adjudicatario se compromete a cumplir la política de Seguridad de la Información del DSGV y todas las normativas y procedimientos aplicables en el contexto del servicio. El adjudicatario y el personal a su cargo están obligados a guardar secreto y absoluta confidencialidad respecto de la información que les sea confiada en virtud del servicio prestado, así como seguir las siguientes normas de comportamiento respecto a los sistemas de información del DSGV:

- No introducir software informático ajeno al DSGV.
- No difundir ni publicar los sistemas de seguridad existentes o previstos.
- No revelar la información obtenida de los sistemas de información del Departamento de Seguridad, ni la documentación que se le suministre o la que pudiera tener acceso en el desempeño de sus funciones, con independencia del soporte en que se encuentre contenida.
- Acceder únicamente a la información necesaria para el desempeño de las funciones encomendadas.
- Utilizar exclusivamente la password-clave a él asignada y adquirir el compromiso de actuar de forma cuidadosa para que nadie conozca su palabra de paso.
- Utilizar adecuadamente y de forma cuidadosa los sistemas de seguridad implantados, de forma que se respeten y mantengan los niveles de seguridad.

El adjudicatario deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de la información y eviten su alteración, pérdida, sustracción, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural. Además, el adjudicatario adquirirá los siguientes compromisos, que a continuación se describen en cuanto a materia de seguridad se refiere:

- Los equipos conectados a la red del DSGV no podrán conectarse a ningún sistema informático o de telecomunicaciones ajeno al DSGV.
- Los equipos o sistemas que por su actividad requieran conexión a servicios externos al DSGV deberán estar aislados, es decir, separados física y lógicamente de la red informática del DSGV.
- Está expresamente prohibida la instalación de módems (o similar) en equipos (PCs, Servidores, etc.) conectados a la red del DSGV.

4.1 Seguridad laboral

El adjudicatario cumplirá todas las normas vigentes sobre Seguridad y Salud en el Trabajo. La utilización de todos los equipos necesarios para la correcta ejecución de los trabajos objeto del presente pliego se realizará de acuerdo con la normativa actual en Seguridad y Salud Laboral. Asimismo, se extremarán las precauciones y se formará al personal responsable de ejecutar los trabajos objeto de este expediente, con el fin de evitar que se expongan a trabajos y/o situaciones que puedan ser perjudiciales para su salud.

4.2 Secreto y confidencialidad

El personal del adjudicatario estará obligado a conocer y respetar las normas de confidencialidad que dicte el DSGV. El técnico responsable del DSGV facilitará al personal de la empresa las autorizaciones de entrada a los centros. El adjudicatario se verá obligado a guardar las normas vigentes sobre Copyright, propiedad intelectual, documentación clasificada o de difusión restringida, etc., aplicables a toda aquella información y documentación que, por necesidades del contrato, esté obligado a manejar.

4.3 Acceso y protección de datos

El adjudicatario quedará expresamente obligado a mantener absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento del contrato, especialmente los de carácter personal, que no podrá copiar o utilizar con fin distinto al que figura en este PCT, ni tampoco ceder a otros ni siquiera a efectos de conservación. A estos efectos, deberán establecerse las máximas cautelas en el acceso a los datos. Cualquier infracción en este sentido será calificada como grave y será causa de resolución del contrato, sin perjuicio de las responsabilidades penales, o de otro tipo, en que se puedan incurrir.

La realización por parte del adjudicatario del presente contrato, pueden conllevar la necesidad de tratar datos de carácter personal, considerando como tales todos aquellos afectados por lo dispuesto en Reglamento (UE) 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

El adjudicatario se compromete a garantizar y mantener el nivel de seguridad que corresponda en cada caso, a los tratamientos que contengan datos de carácter personal y que puedan serle facilitados o a los que hubiere de tener acceso para la realización del contrato.

A efectos del cumplimiento de la normativa de protección de datos de carácter personal, el adjudicatario deberá manifestar y garantizar que dispone y tiene implantados en su organización los procedimientos de seguridad de acuerdo con lo dispuesto en la normativa de protección de datos de carácter personal. Dicha normativa de seguridad deberá tener establecidos los oportunos mecanismos de identificación y comprobación de las personas que pueden tener acceso a sus recursos y sistemas de información, así como a los ficheros que contengan o puedan contener datos de carácter personal. Igualmente, la mencionada normativa de seguridad tendrá también establecidos los procedimientos de control de soportes en que puedan hallarse datos de carácter personal, así como los procedimientos de control de incidencias que pudieran afectar a la seguridad de los datos de carácter personal.