



Eusko Jurlaritzaren
Informatika Elkartea

Sociedad Informática
del Gobierno Vasco

Suministro Infraestructura HCI y Servicios Asociados para la Agencia Vasca de Ciberseguridad - Cyberzaintza

Pliego de Condiciones Técnicas

Abril 2026

Este documento es propiedad de Eusko Jauriaritzen Informatika Elkarte – 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 otros, 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	14/04/2026	Versión inicial	Alfonso Rubio	Javier Cela

Índice

1	Contexto	4
1.1	Agencia Vasca de Ciberseguridad (Cyberzaintza)	5
2	Necesidad e idoneidad de la contratación.....	¡Error! Marcador no definido.
3	Objeto de la contratación	7
4	Alcance del contrato	8
4.1	Tecnología	8
4.2	Duración del contrato	8
4.3	Ámbito.....	8
5	Configuración técnica del servicio	10
5.1	Especificaciones técnicas	10
5.2	Diseño de la solución	10
5.3	Suministro de la infraestructura	14
5.4	Mantenimiento de la solución	14
5.5	Servicios profesionales	15
5.6	Requisitos de los servicios profesionales	16
6	Control y seguimiento.....	19
7	Condiciones de Seguridad/Generales.....	¡Error! Marcador no definido.

1 Contexto

EJIE, Eusko Jauriaritzaren Informatika Elkartea – Sociedad Informática del Gobierno Vasco, S.A., es la empresa pública responsable de la prestación de servicios de Tecnologías de la Información y las Comunicaciones (TIC) al Sector Público Vasco. Su misión es contribuir a la modernización y eficiencia de dicho sector, dentro del marco legal establecido por el Gobierno Vasco, garantizando los niveles adecuados de seguridad, calidad y respeto al medio ambiente.

EJIE tiene como objetivo último la satisfacción de sus clientes, actuando como instrumento común de referencia para la prestación de servicios TIC en el Sector Público Vasco, y asumiendo los siguientes compromisos:

- Construir, mantener y evolucionar con eficiencia y calidad las infraestructuras de los Sistemas de Información, garantizando su continuidad y seguridad.
- Asegurar la interoperabilidad entre las distintas administraciones públicas.
- Dar soporte a las funciones de planificación y ejecución de la función informática de los Departamentos y Organismos Autónomos del Gobierno Vasco, garantizando la adecuada cobertura de sus necesidades mediante relaciones contractuales basadas en el compromiso y la profesionalidad.

En este contexto, EJIE actúa como proveedor estratégico de servicios TIC, aportando valor añadido, soluciones competitivas y confianza a sus clientes, apoyándose para ello en equipos humanos cualificados y comprometidos.

Puede obtenerse información adicional en el sitio web corporativo de EJIE: <https://www.ejie.eus>.

1.1 Agencia Vasca de Ciberseguridad (Cyberzaintza)

La Agencia Vasca de Ciberseguridad (Cyberzaintza), en adelante la Agencia, es un ente público de derecho privado del Sector Público de la Comunidad Autónoma Vasca. La Agencia se adscribe al departamento del Gobierno Vasco competente en materia de seguridad, a través de la persona titular de la Viceconsejería de Seguridad.

La Agencia tiene por objeto promover y coordinar la ciberseguridad en el sector público vasco delimitado en la Ley 3/2022, de 12 de mayo, del Sector Público Vasco, en el ámbito de la seguridad de los sistemas de información y de las redes electrónicas de su competencia, y apoyar e impulsar la capacitación en ciberseguridad y el desarrollo digital seguro de la Comunidad Autónoma Vasca, de su Administración Pública, de su ciudadanía y de su tejido empresarial.

La [LEY 7/2023, de 29 de junio, de creación de la Agencia Vasca de Ciberseguridad](#) en su Artículo 2 establece que las funciones que corresponden a la Agencia para el cumplimiento de su objeto son las siguientes:

- Promover una estrategia de ciberseguridad para el conjunto de las administraciones públicas de la Comunidad Autónoma Vasca, y potenciar y coordinar el alineamiento en la ciberseguridad en dicho conjunto.
- Impulsar un marco de estándares, directrices y normas técnicas de seguridad recomendables para el sector público vasco.
- Informar, con carácter preceptivo, en los procedimientos de elaboración de disposiciones normativas tramitadas por la Administración de la Comunidad Autónoma Vasca en materia de ciberseguridad.
- Realizar evaluaciones anuales de las políticas públicas en materia de ciberseguridad desplegadas en el ámbito del sector público vasco.
- Prevenir y detectar incidentes de ciberseguridad en la Comunidad Autónoma Vasca y responder a ellos, estableciendo criterios y promoviendo el despliegue de las medidas de protección pertinentes ante las ciberamenazas y los riesgos inherentes sobre las infraestructuras tecnológicas, los sistemas de información, los servicios de las tecnologías de la información y la comunicación, y la información que estos tratan, todo ello con respeto del marco competencial aplicable.
- Recoger los datos pertinentes de las entidades que gestionan servicios públicos o esenciales en la Comunidad Autónoma Vasca en relación con el estado de la seguridad de la información, prestando especial atención a los sistemas considerados como críticos para el funcionamiento de los servicios públicos o la seguridad de las personas, con vistas a informar al Gobierno Vasco, así como a las administraciones públicas del territorio que intervengan en la prestación de dichos servicios críticos y esenciales, y proponer las medidas adecuadas llevando a cabo la gestión de riesgos en materia de ciberseguridad.
- Ejercer las funciones del equipo de respuesta a emergencias (CERT) dentro de las competencias de la Comunidad Autónoma Vasca. Dado que se trata de un fenómeno transfronterizo, es necesario colaborar con las administraciones y Agencias de otros territorios con el objetivo de minimizar los daños y el tiempo de recuperación en caso de ciberataque.
- Coordinar los equipos de respuesta a incidentes de ciberseguridad (CSIRT) y los equipos de respuesta a emergencias o las entidades equivalentes que actúen en su ámbito de actuación y de acuerdo a la legislación vigente, estableciendo modelos de colaboración con otros CSIRT estatales e internacionales. Asimismo, la Agencia ejercerá funciones de alerta temprana y de ayuda en la respuesta ante amenazas, vulnerabilidades, ataques e incidentes de seguridad en el ámbito del sector público vasco.
- Trabajar en pro de una cooperación más estrecha con las universidades y los organismos de investigación con el fin de contribuir a un planteamiento estratégico para reducir la dependencia de productos y servicios de ciberseguridad de fuera de la Unión Europea y reforzar las cadenas de suministro de dentro de la Unión Europea.

- Investigar y analizar tecnológicamente los ciberincidentes y ciberataques sobre infraestructuras tecnológicas, sistemas de información y servicios de tecnologías de la información.
- Garantizar un nivel adecuado de ciberseguridad en el uso de medios electrónicos.
- Organizar actividades de difusión, promoción, formación y concienciación en materia de ciberseguridad.
- Organizar actividades para promocionar el talento en la ciberseguridad, y participar en actividades de ciberseguridad, dando a conocer referentes, haciendo especial hincapié en las mujeres profesionales de la ciberseguridad.
- Proponer medidas técnicas de ciberseguridad en la utilización de los recursos informáticos y de las comunicaciones existentes, y proponer la formación en estas medidas del personal de la Administración de la Comunidad Autónoma Vasca y del propio personal de la Agencia.
- Actuar como apoyo, en materia de ciberseguridad, de cualquier autoridad competente para el ejercicio de sus funciones públicas y, en particular, en las tareas de lucha contra las conductas ilícitas, incluidas la intervención directa y la obtención de pruebas electrónicas.
- Coordinar al sector público vasco en la elaboración de sus respectivos planes de ciberseguridad, así como en la consecución de los objetivos establecidos en los mismos.
- Poner sus servicios materiales y técnicos de ciberseguridad a disposición del sector público vasco.
- Impulsar la coordinación del sector público vasco en todo lo que se considere necesario para la consecución de los objetivos especificados en los planes de ciberseguridad, estableciendo para ello las líneas de colaboración que se entiendan necesarias.
- Ostentar la representación oficial del sector público vasco ante organismos internacionales, estatales y regionales en materia de ciberseguridad.
- Apoyar e impulsar la capacitación en materia de ciberseguridad y el desarrollo digital seguro en el ámbito empresarial y en los sectores esenciales de la Comunidad Autónoma Vasca, como son el sector sanitario, el sector de emergencias y seguridad, el sector de servicios sociales y de intervención social, el sector educativo, el sector del transporte y el sector de la energía y las telecomunicaciones, o cualquier otro sector que pudiera considerarse sensible.
- Cualesquiera otras competencias que le sean conferidas por la legislación vigente o le sean expresamente delegadas o atribuidas.

2 Objeto de la contratación

El objeto de esta contratación es el suministro, instalación, configuración y puesta en marcha de una nueva infraestructura de hiperconvergencia que sustituya a la actual que queda obsoleta. Dicha plataforma aloja las herramientas de investigación y análisis de evidencias, el laboratorio de *malware*, herramientas de inteligencia y detección de amenazas, sondas y resto de aplicaciones que dan soporte al equipo de Operaciones y que utiliza la Agencia Vasca de ciberseguridad para el desempeño de sus funciones.

A continuación, se detalla el alcance del contrato cuyo contenido se complementa con los requerimientos descritos en el apartado 5 y que además de asegurar la prestación de los servicios busca realizar la migración sobre una tecnología que asegure el menor impacto posible en dichas operaciones.

3 Alcance del contrato

3.1 Tecnología

La solución deberá proporcionar:

- Plataforma hiperconvergente completamente integrada.
- Capacidad de ejecución de máquinas virtuales críticas.
- Subsistema de almacenamiento distribuido, tolerante a fallos, sin RAIDs tradicionales.
- Consola única de administración, para gestión de computación, almacenamiento, red, *snapshots*, seguridad, analítica y operaciones, sin plugins externos ni bases de datos adicionales.
- Red de interconexión de alto rendimiento mínimo 25Gbps entre nodos.
- Migración del entorno actual con mínimo impacto en la continuidad del servicio.

La plataforma deberá proporcionar:

- Ejecución de máquinas virtuales en entorno hiperconvergente.
- Almacenamiento distribuido con autosanación y reconstrucción inteligente.
- Gestión centralizada sin necesidad de herramientas externas.
- Analítica avanzada de comportamiento del entorno.
- Integración nativa con AD/LDAP.
- Integración con SNMPv3 para monitorización.

3.2 Duración del contrato

En la siguiente tabla se resume la duración requerida tanto de los suministros como de los servicios a contratar:

Suministros	Duración
Hardware (tres nodos HCI + nodo de storage)	5 años
Switches de red	3 años
Licencias Nutanix + soporte oficial	1 año
Servicios	
Nutanix ITAM	6 meses
Formación oficial NCP x 2	No aplica
Servicios profesionales:	1 año
Instalación, migración y puesta en marcha	
Mantenimiento avanzado de la solución	

3.3 Ámbito

La Agencia Vasca de Ciberseguridad (Cyberzaintza), es un ente público de derecho privado del Sector Público de la Comunidad Autónoma Vasca. La Agencia se adscribe al departamento del Gobierno Vasco competente en materia de seguridad, a través de la persona titular de la Viceconsejería de Seguridad.

La Agencia adquiere las licencias, infraestructura y los servicios objeto de contratación para uso propio.

El adjudicatario desplegará su solución en la Sala Técnica del Agencia ubicada en el Parque Tecnológico de Álava.

4 Configuración técnica del servicio

4.1 Especificaciones técnicas

El licitador deberá acreditar cada uno de los requisitos que se presentan en el presente capítulo de especificaciones técnicas, mediante documentación oficial del fabricante, además también deberá aportar matrices de compatibilidad oficiales, emitidas por el fabricante, que acrediten la compatibilidad del hardware y del software ofertado. A efectos del presente pliego, se entenderá por “documentación oficial del fabricante” las matrices de compatibilidad, guías técnicas, certificaciones de soporte, arquitectura de referencia y cualquier documento técnico emitido directamente por el fabricante que acredite la compatibilidad y validez del hardware y software ofertado. No se aceptará documentación comercial, folletos, presentaciones o material de marketing.

4.1.1 Consideraciones

Actualmente la Agencia dispone de una infraestructura de hiperconvergencia basada en una plataforma Nutanix, la cual es necesario renovar por haber finalizado su ciclo de vida. Para ello, el adjudicatario deberá suministrar y poner en marcha una nueva solución que cubra las necesidades indicadas y realizar la migración de las máquinas virtuales existentes a la nueva infraestructura garantizando la continuidad del servicio.

La migración de las máquinas virtuales deberá realizarse sin impacto perceptible en la operación, garantizando la continuidad de servicio mediante mecanismos de migración en caliente.

La infraestructura de red de la Agencia se apoya en tecnología Fortinet, por lo tanto, los switches que se incluyan han adecuarse a las necesidades indicadas y deberán estar certificados para integración con la infraestructura Fortinet existente, incluyendo compatibilidad con FortiManager y FortiLink cuando corresponda.

Por otro lado, para realizar las copias de seguridad se dispone de una solución de backup basada en el software de backup de CommVault. El adjudicatario deberá readecuar la configuración de los backups de máquina virtual a la nueva solución implantada. Así mismo, la solución propuesta por el adjudicatario deberá garantizar que los datos de backup existentes en la actualidad sean recuperables sobre la nueva infraestructura.

4.2 Diseño de la solución

4.2.1 Requisitos de arquitectura

La plataforma deberá cumplir obligatoriamente los siguientes requisitos.

Su incumplimiento será motivo de exclusión:

- El hardware no podrá encontrarse en estado End-of-Life ni End-of-Sale en la fecha de presentación de ofertas.
- Integrar cómputo y almacenamiento en los mismos nodos, mediante controladora virtual en cada host, gestionando la caché, la replicación de bloques, la localidad de datos y la coherencia del clúster de forma nativa.
- Implementar almacenamiento distribuido agregando discos locales de todos los nodos.
- No depender de cabinas SAN, Fibre Channel ni iSCSI externos.
- Basarse en un modelo Scale-Out real, donde el crecimiento se realiza añadiendo nodos.
- Disponer de autosanación automática ante fallos de discos o nodos.
- Utilizar una red interna de 25 Gbps dedicada al tráfico del clúster.
- El crecimiento de capacidad y rendimiento deberá realizarse añadiendo nodos, sin

reconfiguraciones complejas ni interrupciones.

- Estar certificada oficialmente por el fabricante del software HCI.
- Incorporar mecanismos nativos de protección frente a *ransomware* (*snapshots* inmutables, detección de patrones anómalos de IO, recuperación rápida por VM / grupo de VMs), gestionados desde la propia consola HCI.
- Soporte y mantenimiento oficial 24x7 durante al menos 60 meses del hardware

Requisitos de servidores (nodos físicos):

- Tres (3) nodos de computación para máquinas virtuales que, combinados, ofrezcan 96 cores licenciados para el software HCI
- Un (1) nodo dedicado a almacenamiento con 20 TB y 32 cores
- Todo el hardware deberá pertenecer a la misma familia y fabricante, con certificación oficial para el software hiperconvergente ofertado por parte del fabricante de hardware.
- El soporte 24x7 deberá incluir reemplazo de hardware en un máximo de 4 horas.

Requisitos mínimos por nodo

- Procesadores multinúcleo 2x16
- 256 GB RAM por nodo.
- Subsistema de almacenamiento híbrido:
 - SSD para tier de rendimiento.
 - HDD para tier de capacidad.
 - Capacidad gestionada distribuida mínima de 20 TB en el clúster.
 - Los SSD y HDD deberán formar parte de un subsistema híbrido oficialmente certificado por el fabricante para configuraciones NVMe + SAS/SATA simultáneas.
 - Cada nodo deberá incluir un mínimo de 2 SSD de alto rendimiento y un mínimo de 4 HDD destinados al tier de capacidad, formando parte del subsistema híbrido certificado.
 - El almacenamiento deberá mantener, como mínimo, dos réplicas completas de los datos distribuidas en nodos distintos del clúster.
- Conectividad:
 - 2x25 Gbps SFP28 para tráfico interno (almacenamiento/replicación).
 - 2x10 Gbps para gestión y servicios.
- Doble fuente de alimentación redundante.
- Chasis formato 2U, mínimo 24 bahías hot-swap, compatibles con SSD/HDD.
- Soporte para configuración híbrida NVMe + SAS/SATA oficialmente certificada.
- El sistema deberá permitir actualizaciones unificadas ("one-click upgrade") del software, del hipervisor y del firmware del hardware sin intervención manual y sin impacto en producción.
- Soporte para configuraciones agregadas de hasta 128 cores licenciados por nodo.
- El fabricante deberá aportar matriz oficial de compatibilidad del servidor con la plataforma HCI.

- Formato enrackable 19" estándar.

4.2.2 Requisitos del software hiperconvergente

El software deberá cumplir obligatoriamente los siguientes requisitos.

Su incumplimiento será motivo de exclusión.

- El software ofertado deberá encontrarse dentro de su ciclo de vida
- Permitir desplegar VMs sin herramientas externas.
- Disponer de interfaz única para computación, almacenamiento, red, snapshots, métricas y operaciones, sin necesidad de herramientas externas, plug-ins adicionales ni bases de datos independientes.
- Utilizar almacenamiento distribuido, entendiendo por almacenamiento distribuido aquel en el que los datos se fragmentan, replican y gestionan de forma nativa entre los nodos del clúster, sin arrays RAID por hardware y sin cabinas externas.
 - Sin RAID por hardware.
 - Con al menos dos copias de los datos en nodos distintos.
 - Con localidad de datos (IO preferente en el nodo donde reside la VM).
 - Con reconstrucción automática sin degradación significativa.
- El sistema deberá garantizar que el fallo completo de un nodo no provoca pérdida de servicio ni pérdida de datos, manteniendo la disponibilidad del clúster durante los procesos de reconstrucción.
- Ofrecer deduplicación, compresión y tiering en tiempo real.
- Permitir snapshots por VM, deberán ser consistentes y crearse sin impacto significativo en las cargas de trabajo, garantizando la consistencia de los datos en todas las máquinas virtuales incluidas en un mismo grupo.
- Permitir grupos de consistencia para snapshots simultáneos entre VMs de manera
- Ejecutar la controladora de almacenamiento en una VM dedicada por nodo.
- Ofrecer un entorno Kubernetes completamente integrado en la plataforma, que deberá desplegarse, gestionarse y actualizarse desde la consola nativa, sin necesidad de orquestadores externos, sin clústeres adicionales y con soporte oficial del fabricante de la plataforma de hiperconvergencia.
- La solución deberá permitir extender el mismo stack HCI a nubes públicas, manteniendo hipervisor, gestión y políticas, sin rediseñar las VMs ni la arquitectura, incluyendo como mínimo compatibilidad con las principales nubes públicas del mercado.
- Permitir actualización unificada ("one-click") del software de la plataforma, del hipervisor y del firmware del hardware, incluyendo BIOS, controladoras, discos y componentes, de forma orquestada desde la consola de gestión y sin impacto en producción.
- Incluir un hipervisor nativo completamente integrado en la propia plataforma de hiperconvergencia, sin necesidad de licencias externas ni dependencias de terceros.
- Disponer de consola única para virtualización, almacenamiento, red, automatización, snapshots y analítica.
- Integrar motor de analítica avanzada con ML para detección de anomalías.
- Permitir modelo de licenciamiento mixto (por capacidad gestionada + cores).
- Soporte y mantenimiento oficial 24x7 durante al **menos 12 meses**

4.2.3 Requisitos de la red para hiperconvergencia

A nivel de red, se deberá cumplir obligatoriamente los siguientes requisitos.

Su incumplimiento será motivo de exclusión.

Incluir dos switches redundantes, certificados para entornos HCI con 25/100 GbE; que además soporten telemetría avanzada, auditoría integrada, automatización por API y gestión centralizada en una plataforma nativa del fabricante.

El hardware de red ofertado no podrá encontrarse en estado End-of-Life ni End-of-Sale en la fecha de presentación de ofertas.

Hardware y capacidades

- 48 puertos 25 GbE SFP28 para interconexión entre nodos.
- Puertos uplink 100 GbE QSFP28 (mínimo 8 nativos) sin módulos adicionales.
- Puertos adicionales 10 GbE SFP+.
- Doble fuente de alimentación redundante.

Funciones de red

- Soporte completo para LACP, MLAG/MCLAG, STP y routing capa 2/3.
- Controlador de red centralizado nativo del fabricante.
- Integración nativa con la plataforma de seguridad de red:
 - Políticas unificadas de red y seguridad desde una única consola.
 - Gestión integrada de switching y seguridad.
- Gestión desde la consola principal, sin sistemas externos.
- El fabricante deberá aportar matriz oficial de compatibilidad de sus switches para HCI 25/100 GbE.
- Las actualizaciones del sistema operativo de los switches deberán poder realizarse sin interrupción del servicio mediante mecanismos ISSU (In-Service Software Upgrade) o equivalente.

Compatibilidad requerida, aportando:

- Documentación oficial de compatibilidad con el hardware de hiperconvergencia ofertado.
- Compatibilidad de switches para 25/10/100 Gbps en clúster HCI.
- Soporte y mantenimiento oficial 24x7 durante al **menos 36 meses**.

4.2.4 Licenciamiento y capacidades

Se deben cumplir obligatoriamente los siguientes requisitos a nivel de licenciamiento y capacidad e incluir todas las funciones descritas en este pliego sin necesidad de adquirir licencias adicionales.

Su incumplimiento será motivo de exclusión.

- 128 cores para virtualización, gestión y computación.
- 20 TB de capacidad/almacenamiento gestionado distribuido.
- Consola de gestión empresarial integrada, unificada para computación, almacenamiento, red y seguridad, sin plugins externos.
- Hipervisor nativo integrado, sin licencias adicionales y con soporte completo.

- Posibilidad de modelo de licenciamiento mixto según producto (capacidad y/o cores).
- API REST para automatización.
- Herramientas de operación
- Panel unificado de salud del entorno.
- Integración nativa con AD/LDAP.
- Alerta y diagnóstico proactivo mediante analítica avanzada.
- Soporte oficial del fabricante durante al menos 12 meses.
- ITAM del fabricante tras puesta en producción por 6 meses
- Formación técnica oficial para dos personas.
- El adjudicatario deberá aportar, antes de la puesta en producción, un documento de arquitectura final que refleje el diseño de la solución, los parámetros configurados y las políticas aplicadas. Asimismo, deberá presentar un plan de migración detallado que incluya prerequisites, fases, pruebas, validación final y mecanismos de rollback ante incidencias.

4.2.5 Actualización de características

En el caso que durante el periodo de vigencia del contrato, el porfolio del fabricante se actualice con nuevos productos por una renovación tecnológica, o se produzca un cambio de denominación y los "part numbers" que se suministraron conforme a la adquisición inicial se descataloguen o se vean superados por otros más modernos se actualizara en consecuencia y las adquisiciones sucesivas se harían de esos nuevos modelos de la última generación disponible siempre que cumplan o superen las características solicitadas y manteniéndose también los precios ofertados.

4.3 Suministro de la infraestructura

El adjudicatario deberá suministrar todo el equipamiento tanto hardware como software, incluyendo licencias, que sea necesario para la implantación y el correcto funcionamiento de la infraestructura descrita en el presente pliego.

El equipamiento suministrado deberá cumplir con los requisitos establecidos en el presente pliego de condiciones técnicas.

El adjudicatario desplegará su solución en la Sala Técnica de la Agencia ubicada en el Parque Tecnológico de Álava.

4.4 Mantenimiento de la solución

4.4.1.1 Garantía y mantenimiento de fabricante

Todos los componentes, tanto hardware como software, incluidos en la propuesta deberán disponer de un contrato de mantenimiento con el fabricante correspondiente durante al menos el periodo indicado en la siguiente tabla:

Suministro	Periodo de mantenimiento
Hardware (tres nodos HCI + nodo de storage)	5 años
Switches de red	3 años
Licencias Nutanix + soporte oficial	1 año

Dicha contratación deberá garantizar al menos una cobertura en modalidad 24x7 con un tiempo de respuesta no superior a 4h. En el caso de la sustitución hardware ésta deberá realizarse como máximo en modalidad NBD.

Para la apertura y seguimiento de los casos la Agencia dispondrá de un punto único de contacto para cualquier tipo de necesidad, los escalados necesarios se realizarán de forma transparente.

4.4.1.2 Software y licencias

La propuesta deberá incluir todo el software y las licencias necesarias para las diferentes funcionalidades propuestas durante al menos los 12 primeros meses.

La no inclusión en la propuesta de cualquier concepto de licencia asociado tanto al hardware como al software de la plataforma y que sea necesario para el completo funcionamiento de esta, podrá dar lugar a la exclusión de la oferta.

4.4.1.3 Mantenimiento del equipamiento

- Garantía y soporte de fabricante de acuerdo con los requisitos descritos en el pliego de prescripciones técnicas.
- Software y licencias necesarias para las diferentes funcionalidades y tecnologías propuestas.
- Soporte técnico especializado durante el periodo establecido.

4.5 Servicios profesionales

El adjudicatario deberá prestar al menos los siguientes servicios¹:

Servicios	Periodo
Nutanix ITAM	6 meses
Formación oficial NCP x 2	No aplica
Servicios profesionales avanzados:	1 año
• Instalación, migración y puesta en marcha	
• Mantenimiento de la solución	

4.5.1 Implantación de la solución

- Revisión de la solución final, del plan de trabajo y de la metodología establecida para validación por parte de la Agencia.
- Instalación, configuración y puesta en marcha del equipamiento en la Sala Técnica de la Agencia de acuerdo con la arquitectura de solución propuesta y validada.
- Elaboración y ejecución de un plan de pruebas que certifique la adecuada puesta en marcha de la solución.

4.5.2 Migración de los sistemas y servicios existentes

- Migración de las máquinas virtuales desde el entorno actual a la nueva plataforma.
- Adecuación de la configuración de los backups y de la monitorización a la nueva solución

¹ Servicios comercializados "en paquete" por fabricante.

implantada.

- Formación a la Agencia sobre las soluciones y tecnologías desplegadas.
- Documentación de la solución desplegada.

4.5.3 Servicios profesionales de mantenimiento

Servicios profesionales avanzados prestados por el adjudicatario durante 12 meses desde la formalización del contrato con el fin de mantener en óptimas condiciones la solución desplegada y de adecuar la nueva infraestructura a las necesidades de integración que puedan surgir a futuro. Dichos servicios profesionales deben cubrir al menos los siguientes conceptos:

- Al comienzo y al final del servicio:
 - Revisión del estado de salud y de la configuración de la plataforma.
 - Actualización anual de todos los elementos que compongan la solución desplegada.
- De manera continua:
 - Aprovisionamiento de parches.
 - Soporte ante incidencias, apertura, seguimiento y solución de casos con el fabricante.
 - Soporte on-site en caso de necesidad.
 - Desarrollos para automatización e integraciones de la plataforma con nuevos elementos o necesidades que puedan surgir en la Agencia.

4.5.4 Servicios profesionales del fabricante de las licencias del software HCI

A la fecha de formalización del contrato se proporcionarán los siguientes servicios por parte del fabricante de las licencias del producto HCI (sin opción a adquirir servicios adicionales a posteriori):

- Acceso a formaciones regladas del fabricante de las licencias del producto HCI para poder optar a la Nutanix Certified Professional (NCP) para dos personas
- Servicio de un ITAM del fabricante de las licencias del producto HCI por 6 meses

4.6 Requisitos de los servicios profesionales

4.6.1 Organización y equipo de trabajo

El adjudicatario deberá aportar y describir los conocimientos, metodologías, herramientas y equipo humano en el que se apoyará para asegurar el resultado óptimo del proyecto.

La empresa adjudicataria deberá comunicar por escrito la designación de una persona de su organización, encargada de ejercer las facultades de responsable del proyecto en lo referente al proyecto contratado, siendo el interlocutor y responsabilizándose frente a la Agencia de las personas que prestan el servicio.

El equipo de trabajo a incorporar tras la formalización del contrato para la ejecución de los trabajos deberá ser el detallado en la oferta adjudicataria y consecuentemente valorado.

Dicho equipo o la empresa debe contar con experiencia demostrable en las tecnologías implicadas, para ello debe disponer de las certificaciones:

- Hardware: Máximo nivel de certificación en servicios y soporte del fabricante ofertado.
- Infraestructura: Nivel superior de asociación técnica en la plataforma de infraestructura propuesta.
- Virtualización: Máximo rango de alianza comercial y técnica del fabricante de virtualización.

- Especialización: Acreditación de competencia técnica avanzada en diseño y despliegue de Centros de Datos.

4.6.2 Implantación de la solución

4.6.2.1 Planificación

Tras la formalización del contrato la empresa adjudicataria se ceñirá al **plan de implantación** incluido en la oferta técnica consistente en una propuesta inicial detallando la solución final, el plan de trabajo y la metodología establecida para la ejecución del proyecto para su validación por parte de la Agencia. Dicho plan detallará también el modo en el que se propone abordar el despliegue de la solución propuesta.

4.6.2.2 Despliegue de la solución

El despliegue de la solución consiste en el traslado, suministro, instalación, configuración y puesta en marcha de la solución técnica propuesta y validada.

La instalación del equipamiento se realizará en la sala técnica de la Agencia en el Parque Tecnológico de Álava sobre bastidor en formato rack de 19" ya existente. El adjudicatario deberá aportar todos los elementos hardware y software con sus licencias correspondientes, accesorios, cableados y materiales que sean necesarios para la implantación de la solución propuesta, que deberán ser necesariamente nuevos. Así mismo deberá destinar al proyecto el personal técnico adecuado para la realización de los trabajos.

El reciclaje de los embalajes, así como la retirada del equipamiento actual correrá por cuenta del adjudicatario y deberá estar incluido en la propuesta. El adjudicatario deberá garantizar un borrado seguro de los datos.

El adjudicatario llevará a cabo todas las tareas necesarias para que la solución técnica quede completamente operativa, incluyendo la configuración y puesta en marcha del equipamiento incluido en el contrato. La configuración final de la nueva infraestructura deberá replicar todas las configuraciones existentes en la plataforma actual sin perjuicio de que el adjudicatario pueda plantear configuraciones alternativas que mejoren el rendimiento o las prestaciones actuales. La Agencia deberá validar y aprobar la configuración final antes de su implementación.

4.6.2.3 Plan de pruebas

El adjudicatario elaborará un **plan de pruebas** que permita confirmar que la solución es completamente operativa y certificar la adecuada puesta en marcha de la solución, así como la prestación de todas las funcionalidades solicitadas.

Se incluirán también pruebas de contingencia contemplando al menos los siguientes escenarios: rotura de disco (HDD y SSD), caída de nodo y caída de switch.

El plan de pruebas será ejecutado por el adjudicatario y, en caso de considerarlo necesario, por personal de la Agencia. Los resultados obtenidos serán validados por parte de la Agencia y condicionarán el cierre del proyecto. En el caso de que los resultados del plan de pruebas evidencien que la solución implantada no cumple con los requisitos establecidos, el adjudicatario deberá realizar todos los cambios y/o correcciones necesarias hasta lograr el cumplimiento de la totalidad de los requisitos establecidos sin que esto suponga un incremento en los costes del proyecto.

4.6.3 Migración de los sistemas y servicios existentes

4.6.3.1 Migración desde el entorno actual

El adjudicatario deberá realizar la migración de las máquinas virtuales que actualmente se ejecutan en la plataforma existente a la nueva solución implantada. Dicha migración deberá realizarse garantizando la continuidad del servicio, valorándose que el tiempo de indisponibilidad de los sistemas sea el menor posible.

La propuesta deberá describir de forma detallada el plan de migración propuesto indicando como se realizará la migración de las máquinas virtuales desde el entorno actual a la nueva plataforma.

4.6.3.2 Adecuación de la infraestructura de backup

El adjudicatario deberá reconfigurar la infraestructura de backup existente para adaptarla a la nueva solución implantada.

Los backups se realizan diariamente, la migración de las máquinas y readecuación del entorno de backup deberá realizarse de forma coordinada garantizando que todas las máquinas se siguen respaldando a diario incluso durante esta fase de transición.

Así mismo, la solución propuesta por el adjudicatario deberá garantizar que los datos de backup existentes en la actualidad sean recuperables sobre la nueva infraestructura.

4.6.3.3 Traspaso del conocimiento

El adjudicatario deberá incluir en su propuesta un plan de formación en la solución implantada. El objetivo de dicha formación no será obtener un conocimiento generalista del equipamiento, sino traspasar al personal de la Agencia el conocimiento y las particularidades de la infraestructura tecnológica implantada.

A continuación, se indican algunos de los aspectos mínimos que se desean tratar en la sesión de traspaso del conocimiento del proyecto:

- Familiarización con los distintos componentes de la infraestructura con el objetivo de conocer la arquitectura y las configuraciones realizadas.
- Administración de la consola de gestión de la solución implantada.
- Monitorización de la nueva plataforma.

4.6.3.4 Documentación

Tras la implantación de la nueva solución y la migración de los sistemas y servicios actuales el adjudicatario deberá entregar en un plazo no superior a 7 días la documentación completa de la misma incluyendo en ella toda la información relevante y necesaria para su posterior administración y gestión por parte de la Agencia.

Entre la documentación a aportar, no debe faltar la siguiente:

- Inventario del equipamiento instalado, con número de serie, modelo y marca de los equipos.
- Documentación de la configuración de la plataforma a nivel de arquitectura y conectividad.
- Configuraciones realizadas en todos los equipos: IP's, configuración del software, parametrización, contraseñas y demás.
- Guía de comandos útiles y/o de uso habitual.
- Guía de resolución de problemas comunes.
- Pruebas de validación realizadas y los resultados obtenidos.
- Documentación del fabricante y garantía, incluyendo manuales.

5 Control y seguimiento

El seguimiento y supervisión del servicio se realizará de forma continuada en el marco de la gestión ágil del trabajo. Adicionalmente, se establecerá un modelo de seguimiento de carácter ejecutivo, basado en informes periódicos y reuniones de revisión, orientado a evaluar el grado de cumplimiento del contrato y de los compromisos adquiridos.

Cada una de las partes designará los participantes que estime oportunos, debiendo el adjudicatario designar, al menos, un Coordinador del Servicio responsable de asegurar la correcta ejecución del contrato, actuando como el canal de comunicación directo y único con la empresa adjudicataria. Sus funciones principales incluyen la supervisión de los equipos de trabajo, el control estricto del cumplimiento de los Niveles de Calidad del Servicio (SLA) y la resolución inmediata de incidencias operativas, garantizando en todo momento la continuidad, eficiencia y optimización de las tareas asignadas., .

Cyberzaintza podrá solicitar reuniones de seguimiento adicionales cuando lo considere necesario.

El licitador deberá presentar un modelo tipo de los entregables identificados.

La falta de adopción efectiva de las prácticas descritas en este apartado podrá considerarse un incumplimiento metodológico del servicio.

6 Anexo I – Políticas de Seguridad para personal de empresas proveedoras

https://www.ejie.euskadi.eus/contenidos/informacion/ejie2016_contratacion_presenta/es_def/adjuntos/Politicas-de-seguridad-para-proveedores-v4.2.pdf