Ortuella
Udala

PLIEGO DE CONDICIONES TÉCNICAS PARA LA CONTRATACIÓN, MEDIANTE CONCURSO ABIERTO DE LA PRESTACIÓN DEL SERVICIO DE ALOJAMIENTO EN CLOUD Y APLICACIONES DEL AYUNTAMIENTO DE ORTUELLA, 2024-27

1. Introducción

Las Tecnologías de la Información y la Comunicación (TIC) agrupan los equipamientos y servicios usados en el tratamiento y la transmisión de la información, principalmente la informática, Internet y las telecomunicaciones.

En los últimos años, las TIC han tomado un papel importantísimo en nuestra sociedad y se utilizan en multitud de actividades. Las TIC forman ya parte de todos los sectores: educación, robótica, empleo, empresas, salud, etc., y son un eje fundamental y esencial en la Administración Pública.
Es indudable que, para afrontar los futuros retos, la evolución y sostenibilidad de la Administración Local (Smart City, Administración Electrónica, ahorro energético y sostenibilidad, cercanía a los ciudadanos, cero papeles, aumento de eficiencia y eficacia, …) hay que hacerlo a través de las TIC, y por eso, este Ayuntamiento de Ortuella viene apostando desde 2014 por la mejora del equipamiento y servicios necesarios para agilizar y proporcionar nuevas prestaciones TIC a la ciudadanía.

En definitiva, el buen uso de las TIC en la Administración Local maximiza la utilización de los recursos que maneja y aumenta el valor de la actividad pública en su conjunto, lo que supone un ahorro de costes internos para la Administración y para ciudadanos y empresas.

Hoy en día, el Ayuntamiento de Ortuella, en adelante Ayuntamiento, tiene alojados en dos Datacenters de un proveedor privado todos sus servicios informáticos, en modalidad Cloud, pago por uso. Además, el Ayuntamiento dispone de un Datacenter ubicado en uno de sus edificios, donde aloja un servidor de Directorio Activo.

Entre las ventajas observadas del servicio en nube ya existente destacan la seguridad, la estabilidad, la posibilidad de ajustar la capacidad necesaria a la demanda en cada momento, amplio acceso a la información y servicios desde cualquier lugar a través de redes mediante todo tipo de dispositivos, la agregación y compartición de recursos, la flexibilidad en la asignación de recursos y un ahorro económico significativo, entre otros. La atención directa, la monitorización y control a tiempo completo, en proximidad y altamente especializada en la aplicación que provisionan constituyen, en nuestro caso, unas de las características clave que llevaron a contemplar un alojamiento externo del servicio.

Por finalización del actual contrato del servicio Cloud y servicios asociados TIC, se hace preciso iniciar un nuevo expediente de licitación para la continuación y ampliación de estos por un nuevo período.

Ortuella
Udala

Se detallan en el presente pliego los aspectos técnicos del nuevo servicio a contratar, con el fin de que cualquier empresa interesada pueda presentar su propuesta de acuerdo con las condiciones necesarias.

Se requiere de la empresa adjudicataria la dotación, instalación, configuración, puesta en marcha, gestión y mantenimiento de lo definido en el presente pliego, garantizando su plena operatividad durante todo el período de vigencia del contrato.
El contratante asumirá todos los servicios de migración del pool de servidores actual a los Datacenters ofertados, sin cargo adicional para el Ayuntamiento y con la menor parada e impacto posible en el servicio para los trabajadores del Ayuntamiento.

La empresa adjudicataria deberán cumplir con la normativa vigente de la Unión Europea y española en lo referente a sus aspectos ergonómicos, salud laboral, medioambientales, de ahorro energético, de compatibilidad electromagnética, de reducción de radiación emitida y protección de datos.

La empresa adjudicataria estará obligada al cumplimiento de todas las clausulas en materia de igualdad entre mujeres y hombres: incorporará la perspectiva de género, adoptará medidas de igualdad entre mujeres y hombres y aplicará medidas de conciliación entre la vida, personal, laboral y familiar. La empresa adjudicataria durante la vigencia del contrato, en cumplimiento de lo establecido en el artículo 48 de la Ley Orgánica 3/2007, deberá promover condiciones de trabajo que eviten el acoso sexual y el acoso por razón de sexo, así como arbitrar procedimientos específicos para su prevención y para dar cauce a las denuncias o reclamaciones que puedan formular quienes hayan sido objeto de este. Dicho compromiso implica el deber de difundir las estas medidas y acciones entre el personal adscrito a la ejecución del contrato y entre las personas usuarias o beneficiarias.

2. Objeto del contrato

El objeto de este expediente son los servicios de provisión, alojamiento y operación de la plataforma tecnológica del Ayuntamiento en modalidad de Cloud que da soporte a los sistemas del Ayuntamiento y otros servicios que requieren disponibilidad de 24x7.

Los servicios demandados son los siguientes:

1. Servicio de Centro de Proceso de Datos en Cloud.
2. Servicio de SGBD Oracle.
3. Servicio de SGBD Microsoft SQL Server.
4. Servicio de virtualización de aplicaciones.
5. Servicio de seguridad y antivirus.
6. Servicio de Recuperación ante Desastres para servicios corporativos (CPD secundario)
7. Servicio de Correo electrónico, Almacenamiento compartido (Exchange Online).

Queda fuera del alcance del contrato cualquier actividad relacionada con desarrollos, sobre las aplicaciones de negocio del Ayuntamiento, a excepción de la asistencia al respecto de

compatibilidades con configuraciones relacionadas con los Sistemas Operativos, Sistemas Gestores de Base de Datos (en adelante SGBD), y otro software de base objeto de este pliego.

3. Presupuesto de licitación

El presupuesto de licitación asciende a 443.834,26 € (IVA no incluido)

No procede la división en lotes que se pudieran adjudicar a distintos proveedores dado que el sistema debe considerarse como un todo ya que todas las aplicaciones se encuentran integradas entre sí.

4. Duración del servicio

El plazo de ejecución será de 4 años, con opción a 1 de prórroga, contados a partir de la fecha de firma del contrato.

La duración de la fase de migración será de un máximo de dos meses.

5. Situación actual

En la actualidad el Ayuntamiento, tiene sus datos y aplicaciones alojados en dos Datacenters externos, desde los cuales se presta servicio a los usuarios para la realización del trabajo diario, usando una infraestructura compartida de servidores.

Asimismo, existe un Datacenter ubicado en el edificio Horno, donde se aloja un servidor de Directorio Activo.

El número de usuarios actuales del cloud es de 43 ubicados en las siguientes dependencias municipales:

- Edificio Ayuntamiento (próximamente habrá una reubicación de un departamento municipal en nuevos locales)
- Edificio el Horno
- Casa de cultura OKE
- Edificio Servicios Sociales

En la Biblioteca, edificio OKE, existen, además, 5 ordenadores para uso público, su función es ofrecer acceso a la ciudadanía a esta herramienta.
Además, se da mantenimiento a 3 ordenadores sitos en el Juzgado de Paz y 1 ordenador del servicio de Intervención Socioeducativa.

Los servidores necesarios para dar soporte a las aplicaciones de gestión y trabajo diario son:

- Servidor1 – Controlador de dominio y servidor de ficheros.
  - 4 vCPU.

- 16 GB de RAM.
- 1.300 GB de disco duro.

➢ Servidor2 – Controlador de dominio y base de datos SQL.
- 4 vCPU.
- 16 GB de RAM.
- 800 GB de disco duro.

➢ Servidor3 – Base de datos Oracle.
- 4vCPU
- 12 GB de RAM.
- 1,2 TB de disco duro.

➢ Servidor4 - Aplicaciones Servicios Sociales.
- 4 vCPU.
- 16 GB de RAM.
- 100 GB de disco duro.

➢ Servidor5 – Aplicación Administrador de aplicaciones.
- 4 vCPU.
- 16 GB de RAM.
- 210 GB de disco duro.

➢ Servidor6 – Aplicación Gestión de expedientes (web).
- 4 vCPU.
- 16 GB de RAM.
- 120 GB de disco duro.

➢ Servidor7 – Aplicación Gestión de expedientes (procesos).
- 4 vCPU.
- 16 GB de RAM.
- 100 GB de disco duro.

➢ Servidor8 – Aplicación Estadística.
- 4 vCPU.
- 16 GB de RAM.
- 100 GB de disco duro.

➢ Servidor9 – Aplicación Secretaría.
- 4 vCPU.
- 16 GB de RAM.
- 80 GB de disco duro.

➢ Servidor10 – Aplicación Portal externo.

- 2 vCPU.
- 8 GB de RAM.
- 100 GB de disco duro.

➢ Servidor11 – Gestión virtualización de aplicaciones.
- 4 vCPU.
- 16 GB de RAM.
- 70 GB de disco duro.

➢ Servidor12– Virtualización de aplicaciones.
- Unidades = 5
- 8 vCPU.
- 36 GB de RAM.
- 100 GB de disco duro.

➢ Servidor13 – Servidor T-Systems
- 2 vCPU.
- 4 GB de RAM.
- 75 GB de disco duro.

➢ Servidor14 – Virtualización de aplicaciones T-Systems
- 6 vCPU.
- 20 GB de RAM.
- 115 GB de disco duro.

➢ Servidor15 – Acceso externo virtualización de aplicaciones.
- 2 vCPU.
- 2 GB de RAM.
- 20 GB de disco duro.

➢ Servidor16 – Acceso doble factor de autenticación.
- 2 vCPU.
- 2 GB de RAM.
- 20 GB de disco duro.

➢ Servidor17 – Servidor apache para aplicaciones web.
- 2 vCPU.
- 8 GB de RAM.
- 100 GB de disco duro.

➢ Servidor18 – Servidor controlador de dominio (servidor físico a suministrar por el adjudicatario, para instalar en el Ayuntamiento).
- 2 procesadores Intel Xeon 8 cores.
- 32 GB de RAM.

- 600 GB de disco duro en RAID 1.
- Tendrá garantía durante toda la vigencia del contrato

Las aplicaciones que están en uso actualmente son:

Sede Electrónica	
AYTOS: @ccede (3.0.10)	AYTOS BERGER LEVRAULT
Gestión documental y contabilidad.	
Firmadoc BPM, versión 20.6.33	AYTOS BERGER LEVRAULT
APP FirmadocMobile	
AytosSecretaria	
SicalWin, Sistema de Información Contable, versión 8.82.11	
Tramitación factura electrónica.	
eF4aktur v.5.3.1. (PCs)	IZENPE
AYTOS: @ccede (3.0.10) - Extranet Proveedor (Aplicación On-Line).	AYTOS BERGER LEVRAULT
Tramitación de subvenciones	
AYTOS: @ccede (3.0.10)	AYTOS BERGER LEVRAULT
Gestión tributaria, recaudación, multas, etc...	
GT/WIN (TAO 1.0) versión base de datos 5.0.0. y versión PTF 098,	TAO S.A.
Acces 2003.	MICROSOFT
WinGT v. 4,25,11	AYTOS BERGER LEVRAULT
APP Multas APP	
AytosAnalytics	
Sistemas integrados de gestión bibliotecaria (SIGB)	
AbsysNet. versión 2.2.	BARATZ SERVICIO DE TELEDOCUMENTACIÓN S.A.
Firma electrónica	
Kit Izenpe – Id@zki Desktop	IZENPE
Egoitza Tarjeta Virtual profesional	
Card Manager	
Padrón municipal	
AYTOS: @ccede (3.0.10)	AYTOS BERGER LEVRAULT

Aplicaciones ofimáticas	
Word, Excel, Publisher, Power Point, Outlook 2013	MICROSOFT
Acceso web correo electrónico	
OUTLOOK WEB ACCES (OWA)	MICROSOFT
Lectura y edición de documentos PDF	
Adobe Acrobat Reader v.2021,011,20039 / 2023.003.20244.	ADOBE
Cianoplan JS (Une y Separa páginas de PDF)	CIANOPLAN
Impresoras PDF	
AdobePDF Creator v.2.2.	pdfforge GmbH
BulzipPDF printer v.11,13,0,2823	BULLZIP
Compresor/descompresor archivos	
7zip	WinRAR
Gestión de albaranes de Correos	
WinSCP v. 5,19,6	
Ganes 22,01,00,00	CORREOS
Aplicación Servicios Sociales	
Gestión Unificada de la Información para la Acción Socio Laboral (GUIAS)	ADOS INFORMATICA
Software croquis para la Policía	
Croquis de Accidentes con Word v.1.0.0.	By Salva
Software para confeccionar nóminas	
Iberper Nómina y Administración de Personal, Iberper 9.50.00.9 (201810-8). (PCs)	IBERMÁTICA S.A.
Software para inventario municipal.	
Inventario	ADOS INFORMATICA
Navegadores de internet	
Microsoft Internet Explorer 1607	MICROSOFT
Google Chrome. v. 97.0.4692.71	GOOGLE
Mozilla Firefox. v. 97,0,1	MOZILLA
Visores de imágenes	

Microsoft Office Picture Manager. V.11.8161.8405.	MICROSOFT
Paint. (versión 1607).	
Visualizador de fotos de Windows.	
Editores de imágenes	
Irfanview. V 4.54.	IRFANSKILJAN
GIMP (GNU Image Manipulation Program) v.2.10.	GIMP
Reproductor multimedia	
Windows Media Player	MICROSOFT
VLC Media Player v. 3,08	

Además, el Ayuntamiento dispone de un servicio de correo electrónico alojado en Office 365.

El número de asientos contratados actualmente es de 46 del plan Exchange Online.

El Ayuntamiento dispone de los siguientes dominios de internet, cuyo mantenimiento forma parte de esta licitación, durante toda la vigencia del contrato:

Dominio	Fecha de renovación
ortuella.eus	10/03/2024
ortuellaguretzat.eus	03/04/2024
aytoortuella.net	15/11/2024
ortuella.biz	12/10/2024

6. Especificaciones técnicas del servicio

Este proyecto, además de las soluciones tecnológicas, requiere de un proveedor especializado que garantice el funcionamiento de los sistemas informáticos asumiendo la responsabilidad de su mantenimiento y continuidad 24x7.

En cualquier caso, la solución técnica tendrá que ser adecuada a la situación actual de la tecnología y deberá aportar garantías de adaptación a la evolución tecnológica de los próximos años.

El pliego define los requerimientos mínimos que debe presentar la solución técnica aportada, especificando estrictamente los productos o servicios a suministrar, siendo esta adecuada a la situación actual de la tecnología y deberá aportar garantías de adaptación a la evolución tecnológica de los próximos años.

En los apartados siguientes se presentará la relación de los objetivos a cubrir y los requisitos de toda índole, tanto generales como específicos, para alcanzar el fin del proyecto.

La empresa adjudicataria realizará todos los trabajos necesarios en orden a conseguir los objetivos fijados en este documento. Como resultado final, el sistema implantado quedará totalmente operativo, cumpliendo todas las características definidas en este documento e integrándose completamente en la plataforma tecnológica que se describe, bajo las características y los estándares fijados para la misma.

En el presupuesto de licitación se incluyen tanto la parte de migración e instalación y configuración de todos los sistemas tecnológicos del Ayuntamiento, incluyendo tanto aplicativos, datos y programas de gestión que se realizará al inicio del proyecto, como las mensualidades/cuotas de mantenimiento y soporte a usuarios.

7. Prestación del servicio

Se deberán prestar los servicios desde dos centros de proceso de datos (Datacenter) propios y deberá disponer en todo momento de la documentación relacionada con la prestación del servicio en caso que sea requerida por el Ayuntamiento a través de una auditoría o cualquier otra petición.

El Datacenter principal deberá estar certificado TIER III o superior, por el Uptime Institute en diseño y construcción, o certificación equivalente de organismo acreditado. Se deberá aportar copia de la certificación al respecto.

Adicionalmente, se deberá disponer de un Datacenter de respaldo, en el que se realizarán las copias de seguridad y desde el que se deberá prestar servicio en caso de contingencia del Datacenter principal.

El Datacenter de respaldo deberá cumplir las especificaciones TIER III o superiores establecidas por el Uptime Institute, o certificación equivalente de organismo acreditado.

En la actualidad los elementos gestionados se encuentran en un Datacenter externo, por ello el licitador deberá incluir en su oferta un plan detallado de migración desde estas instalaciones al nuevo Cloud planteado en este pliego, con fases e hitos e identificando los principales riesgos y las medidas propuestas para minimizarlos o eliminarlos.

La solución ofertada deberá ser escalable para permitir atender demandas crecientes en el futuro, añadiendo nuevos componentes sin introducir cuellos de botella. El licitador deberá incluir una descripción detallada de las principales características de los Datacenter en los que alojará los sistemas del Ayuntamiento.

El proveedor del servicio deberá asegurar la continuidad de éste, disponiendo de un mecanismo de respaldo para posibles contingencias en el Datacenter de respaldo.

Asimismo, se deberá realizar el backup en dicho centro de respaldo para una mayor garantía de custodia de los datos del Ayuntamiento.

El proveedor del servicio, deberá asegurar el restablecimiento del servicio en los tiempos establecidos, según los niveles de servicio correspondientes para el Datacenter principal y para el Datacenter de respaldo

8. Conectividad

Se deberá establecer una conexión VPN redundante en ambos extremos entre las sedes del Ayuntamiento y los dos Datacenters del proveedor de servicio.

En el extremo del Ayuntamiento se podrán utilizar para tal fin las líneas de conexión a Internet disponibles en la actualidad con Euskaltel.

El ancho de banda total de las líneas actuales del Ayuntamiento es de 100 Mbps simétricos, divididos entre las diferentes sedes.

En el extremo del proveedor del servicio Cloud se deberán utilizar dos o más proveedores diferentes de ancho de banda en cada Datacenter, para garantizar la redundancia.

El ancho de banda de la VPN será el necesario para la prestación del servicio en condiciones óptimas de rendimiento, pudiendo llegar hasta un máximo de 100 Mbps bidireccionales, capacidad máxima actual de las líneas del Ayuntamiento.

9. Migración

En su solución para la migración desde el Datacenter actual al Datacenter del adjudicatario, los licitadores deben considerar como un factor clave minimizar o eliminar si es posible, todos los riesgos desde un punto de vista operacional, especialmente la integridad y continuidad del servicio a los usuarios finales.

El licitador debe detallar su metodología de transformación, desde la elaboración de la estrategia hasta su ejecución, incluyendo el proceso de validación y seguimiento global.

Se requiere que la transformación esté totalmente finalizada y, por lo tanto, todos los elementos completamente operativos desde el Datacenter del adjudicatario en el menor tiempo posible. Los licitadores deberán acompañar un plan para el traslado del Datacenter que tenga en cuenta las siguientes fases de ejecución:

Fase 1. Definición de la estrategia de transformación. Definición de una estrategia de migración y confirmación del alcance y servicios a alojar en el Datacenter, con análisis de la criticidad de los servicios, su situación actual, para definir los criterios para la estrategia más adecuada y de menor riesgo.

Fase 2. Creación del plan de migración. Consiste en la definición detallada de las actividades que son necesarias para trasformar los servicios desde el Datacenter donde actualmente se encuentran alojados, hasta el Datacenter propuesto por el adjudicatario, conforme a la estrategia definida con anterioridad.
En esta fase el adjudicatario realizará y documentará un análisis de riesgos y planes para su mitigación.

Fase 3. Ejecución de la migración. Preparación y configuración de todos los elementos a trasformar y de la infraestructura necesaria para realizar la migración del servicio. Se realizarán la definición de los planes de "marcha atrás" y sus pruebas, para el caso de que se presenten problemas durante la migración, así como la ejecución, el seguimiento y la realización de las pruebas que servirán para validar que la migración del servicio se ha ejecutado correctamente.
Una vez realizada la migración de los sistemas al nuevo Datacenter en su estado actual, el adjudicatario tendrá que realizar la actualización de todos los sistemas operativos, así como sus aplicaciones y bases de datos para adaptar los sistemas del Ayuntamiento a las nuevas versiones.

El plazo de migración no se dará por finalizado hasta que el Ayuntamiento compruebe que todos sus aplicativos y sistemas están en últimas versiones y funcionando de forma adecuada.

10. Trabajos adicionales a realizar

Una vez, finalizado el proceso de migración al nuevo Cloud del adjudicatario, será necesario realizar las siguientes migraciones/implantaciones:

- Actualización de Directorio Activo: Actualmente existe un controlador de dominio en versión Windows Server 2003 y 2008, por necesidades de las aplicaciones. Es necesario realizar la migración de la base de datos actual y despromocionar dicho controlador, para elevar el nivel funcional y promocionar DCs en sistema operativo Windows Server 2019.
- Actualización de servidor de ficheros a última versión disponible de Windows Server. Configuración de rol y migración de todos los datos y permisos.
- Mantener la configuración doble factor de autenticación en acceso externo a aplicaciones y escritorios mediante código OTP, iniciada en julio 2023.
- Actualización de plantilla de servidor de virtualización de aplicaciones/escritorios a última versión de sistema operativo estable, reinstalando todas las aplicaciones y configuraciones necesarias.
- Actualización de todos los servidores de aplicaciones a ultimo sistema operativo (Berger Levrault) y soporte a la instalación por parte del fabricante. El adjudicatario asumirá los servicios de instalación del fabricante dentro de este contrato.
- Activación de doble factor de autenticación para correo electrónico.

11. Servicio de Datacenter

Se deberá prestar el servicio desde dos Centros de Proceso de Datos (Datacenter Principal y de Respaldo) propiedad del licitador.
Ambos Datacenters deberán cumplir las siguientes especificaciones:

- La ubicación física de los Datacenters deberá estar en España.
- Doble acometida eléctrica, protegida por un mínimo de dos grupos electrógenos dispuestos en configuración N+1 y protegida por un mínimo de dos SAIs dispuestos en configuración N+1, de tal forma que en todos los armarios rack se disponga de dos unidades de distribución de potencia (PDU) alimentadas cada una de una acometida diferente.
- Doble circuito de climatización de la sala técnica, con un mínimo de dos equipos de refrigeración externos e internos al Datacenter, dispuestos en configuración N+1.
- Doble acometida de comunicaciones, con operadores diferentes y medios físicos y canalizaciones totalmente independientes hasta los armarios de comunicaciones del Datacenter.
- El Datacenter Principal deberá disponer, como mínimo, de la acreditación TIER III Certification of Constructed Facility según el estándar ANSI/TIA-942.
- El Datacenter secundario deberá cumplir las especificaciones de TIER III, en el que se realizarán las copias de seguridad y desde el que se deberá prestar servicio en caso de contingencia del Datacenter principal.
- El servicio de Datacenter deberá estar monitorizado por un SOC que controle a nivel de infraestructura común y accesos, las posibles intrusiones. El Centro de Operaciones de Ciberseguridad estará ubicado y operado desde España. La empresa encargada de la explotación de éste deberá formar parte de la comunidad CSIRT.ES y de la Red Nacional de SOC. Esta información se contrastará con el Centro Criptológico Nacional (CCN).

Por ello, el licitador deberá incluir en su oferta un plan detallado de migración desde el actual adjudicatario a su nueva ubicación, con fases, hitos e identificando los principales riesgos y las medidas propuestas para minimizarlos o eliminarlos.
La solución ofertada deberá ser escalable para permitir atender demandas crecientes en el futuro, añadiendo nuevos componentes sin introducir cuellos de botella. El licitador deberá incluir una descripción detallada de las principales características de los Datacenters donde se alojarán los sistemas municipales.

12. Equipamiento

El adjudicatario es responsable de proveer la potencia (CPU, RAM) y almacenamiento SSD para dar servicio a los servidores indicados en el apartado 5, necesarios para el buen funcionamiento de las aplicaciones del Ayuntamiento. Durante la vigencia del contrato se podrá solicitar la ampliación de los servidores y/o recursos, licencias en base a nuevas necesidades.

El licitador propondrá una lista de precios unitarios para las ampliaciones de recursos, licencias o servicios que deberá mantener durante todo el periodo de vigencia del contrato, para eventuales necesidades adicionales de equipamiento o prestación de servicios, que se

facturarán con cargo al importe variable en caso de ser necesarios. Estos precios se detallarán como anexo a la oferta económica, aunque no serán objeto de valoración.

El equipamiento deberá cumplir los siguientes requisitos:

- Las vCPU deberán corresponderse, como mínimo, con un core físico en hyperthreading (no podrá haber sobresuscripción).
- Servicio de electrónica de red, incluyendo conmutadores, routers, firewall perimetral, etc.
- Snapshot de cabina, que garantice la posibilidad de recuperar el estado de las máquinas virtuales a un punto en el tiempo. El servicio deberá incluir puntos de recuperación cada 4 horas, almacenando 12 puntos de restauración y puntos de recuperación cada día, almacenando 1 día. Dichos snapshots de cabina deberán estar protegidos de forma inmutable, de tal manera que no puedan ser eliminados, cifrados o modificados.
- El almacenamiento de backup en equipamiento físico independiente del almacenamiento de producción, será el necesario para realizar la copia de seguridad de toda la información del Ayuntamiento con la política de copia de seguridad requerida.
- Se deben cumplir, al menos, los siguientes valores de recuperación de servicio:
    - RTO<30
    - RPO=0

Será, pues, responsabilidad del adjudicatario la instalación, mantenimiento, actualización y gestión de la configuración de los elementos hardware del Datacenter.

El adjudicatario será el responsable de la gestión de la arquitectura técnica del centro de datos para dar la respuesta adecuada a las necesidades planteadas por este pliego.

El adjudicatario será el responsable de la gestión de las comunicaciones dentro del Datacenter, de la VPN que conecte con la LAN del Ayuntamiento y de la salida a Internet, por lo que proveerá al Ayuntamiento de:

- Ancho de banda para la conexión a internet con un mínimo de 100Mbps.
- Direcciones IPs públicas necesarias para la puesta en marcha del sistema de información.
- Gestión del firewall perimetral de red, con doble barrera de firewall de diferente fabricante.

13. Licenciamiento software

Se deberán proporcionar las licencias de software, su instalación y la configuración necesaria para que el equipamiento del Datacenter funcione de forma correcta para la prestación del servicio.

Se migrarán los sistemas operativos de Windows a últimas versiones siempre que el aplicativo instalado sobre ellos lo permita.

En este sentido deberá incluir al menos:

- Licencias de sistema operativo Microsoft Windows Server para todos los servidores mencionados en el apartado 5.
- Licencia Oracle Database Standard 2 para un único procesador, sobre una plataforma que esté 100% certificada y soportada por Oracle.
- Licencia de SQL Server Standard para 4vCPUs.
- Licencias de hipervisor para alojar todas las máquinas virtuales mencionadas.
- Licencias de virtualización de aplicaciones y desktops con sus correspondientes licencias de Microsoft Remote Desktop para todos los usuarios del Ayuntamiento, que serán 51.
- Licencias para habilitar el acceso externo con doble factor de autenticación a las aplicaciones para todos los usuarios del Ayuntamiento.
- Licencias de Exchange Online para todos los usuarios del Ayuntamiento durante la vigencia del contrato:
    - 57 licencias EO P1
    - Durante la vigencia del contrato es probable que se necesiten modificar las ediciones en base al consumo, se regularizará mediante los precios unitarios de la modificación de contrato.
- Licencias de Microsoft Apps for Enterprise para 51 usuarios.
- Licencia para las herramientas de monitorización.
- Licencia para las herramientas de backup.
- Licencias de antivirus para todos los servidores descritos en el apartado 5; y PCs y ordenadores portátiles, sumando estos dos últimos un total de 53, lo que hace un total de 71.
- Licencias de antivirus para todos los móviles/tablets corporativos (22 unidades).
- Herramientas de seguridad perimetral (sistema de detección de intrusiones, navegación, etc.).

Será, pues, responsabilidad del adjudicatario la instalación, mantenimiento, actualización y gestión de la configuración de los sistemas operativos y de software de terceros instalado en el hardware del Datacenter.

La empresa adjudicataria gestionará las renovaciones de licencias y garantías de cada solución activa que requiera continuidad dentro de la organización. Para ello la empresa adjudicataria dispondrá de una aplicación para la gestión y seguimiento de caducidades de productos y soluciones del Ayuntamiento de Ortuella.

La infraestructura completa deberá estar certificada por los fabricantes hardware y software implicados en la solución.

14. Virtualización de aplicaciones

En lo que se refiere a la virtualización de aplicaciones, la empresa adjudicataria deberá suministrar y realizar la configuración, instalación y puesta en marcha del conjunto de herramientas necesarias habilitadas a tal fin, aportando un sistema tolerante a fallos y de alta

disponibilidad. Estas deberán ofrecer un contexto robusto, seguro, escalable y de alta disponibilidad para las soluciones de virtualización del puesto de trabajo

Se deberá suministrar los servidores necesarios para alojar un servicio de virtualización de aplicaciones y escritorio remoto para todos los usuarios del Ayuntamiento. En ellos será necesario instalar todas las aplicaciones que el Ayuntamiento necesite para trabajar en su día a día.

Se crearán usuarios, perfiles, scripts y, en general, cualquier labor necesaria para dicha virtualización, bajo las recomendaciones del sistema de virtualización seleccionado, siguiendo las políticas establecidas en el Ayuntamiento.

Se suministrará un servicio de virtualización de aplicaciones para acceso remoto de forma segura y óptima a los recursos locales, permitiendo una forma de trabajo que garantice una experiencia de usuario mejorada desde ubicaciones remotas, con un rendimiento adaptado a los accesos desde redes WAN. Se plantea conseguir:

- Optimizar los recursos en infraestructura tanto en inversión como en mantenimiento.
- Poseer una infraestructura fiable.
- Contar con una solución de acceso remoto segura con doble factor de autenticación.
- Crear una infraestructura común para los puestos de trabajo.
- La optimización de los recursos, por medio de un acceso seguro a los sistemas tanto internamente como externamente.
- Disponer de una arquitectura de futuro sobre la que basarse para acometer todos los proyectos necesarios.

La empresa adjudicataria dotará de licencias o sistemas para cubrir las necesidades expuestas, además de los certificados públicos que ello le requiera.

Se consideran incluidos dentro del presente pliego todos aquellos productos, licencias o servicios necesarios para la puesta en marcha y correcto funcionamiento del servicio y que deberán ser detallados en la oferta técnica.

El adjudicatario deberá hacerse cargo de todos los costes de instalación de todos los servidores del proyecto, instalación de aplicaciones, migración de datos y todos aquellos derivados del traspaso de información del actual adjudicatario a la infraestructura a la nueva, instalación de aplicaciones de escritorio, migración de las bases de datos, traspaso de datos de usuario, perfiles, buzones, etc.

Será responsabilidad del adjudicatario contactar con los proveedores de aplicaciones y prestarles el soporte necesario para que puedan instalar y configurar sus aplicativos en el nuevo Cloud.

15. Backup

El licitador incluirá en su oferta servicios de backup para todos los servidores virtuales y físicos que conforman el entorno del Ayuntamiento, que aseguren la salvaguarda diaria y recuperación de la información en ellos almacenada. Las condiciones mínimas del servicio de backup son las siguientes:

- Copias de seguridad de las máquinas virtuales completas con una periodicidad semanal e incremental diaria, que será como mínimo:
  - Backup máquina virtual completa diario cada 24h, aprox. a partir de las 21:00 de L a D.
  - Periodo de retención mínimo exigible es de 30 días.
- Backup mensual en cinta con retención 12 meses de todos los servidores y copia anual durante la vigencia del contrato.
- Incluye el espacio de almacenamiento requerido en función del número de servidores, el dimensionamiento de disco de estos y el periodo de retención mínimo establecido.
- Incluye la posibilidad de gestionar hasta un máximo de 6 solicitudes de recuperación mensuales.

El licitador deberá especificar la tecnología empleada, así como las capacidades de recuperación y reportes incluidos.

16. Monitorización

Se realizará la monitorización de los sistemas alojados en el Datacenter con el objeto de facilitar las tareas de gestión de fallos e incidencias mediante los procedimientos de escalado y resolución adecuados.

En este sentido se examinarán los procesos en tiempo real y los recursos de los sistemas para reaccionar ante problemas en el menor tiempo posible y para detectar cuellos de botella. En concreto, se realizará:

- Monitorización de los dispositivos de los servidores y de los elementos de almacenamiento. Deberán proporcionarse mecanismos de monitorización de los componentes de los sistemas de gestión de base de datos.
- Monitorización de infraestructura, incluyendo seguridad perimetral y VPN.
- Monitorización no intrusiva de servicios sin necesidad de instalar ningún software adicional en los sistemas supervisados.

Las herramientas de monitorización deberán estar separadas del resto de sistemas y el acceso físico a las mismas deberá estar restringido exclusivamente al personal del equipo de trabajo dedicado a estas tareas.

Se realizará la configuración inicial de los agentes de monitorización y su mantenimiento, así como la actualización de las versiones de las herramientas de monitorización y el

mantenimiento y actualización de los procedimientos de atención de las alertas técnicas. El licitador deberá incluir en su oferta el detalle de los procedimientos que vaya a utilizar.

17. Antivirus

Las nuevas amenazas del ciberespacio, tales como el ransomware, hacen necesaria la incorporación de nuevos elementos de detección y respuesta (EDR) que complementen la protección clásica de los antivirus basados en firmas.

Por ello, el Ayuntamiento propone modernizar la seguridad de puesto con una solución que cumpla los siguientes requisitos mínimos:

- La solución ofertada deberá aparecer como certificada en la Guía de Seguridad de las TIC CCN-STIC-105 del CCN CERT (https://www.ccncert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-lacomunicacion/),conforme a Esquema Nacional de Seguridad. En caso de estar en proceso de certificación, se admitirá igualmente, debiendo aportarse la documentación necesaria para justificación de este punto.
- La existencia de un único agente para EPP y EDR, sin necesidad de agentes adicionales
- Para minimizar el consumo de recursos, el producto debe permitir la instalación de módulos personalizada (por ejemplo, instalación del módulo de antimalware sin el módulo de firewall).
- Para ofrecer una mejor protección contra Ransomware la solución debe incluir “Ransomware Vaccine” que inmunizará los servidores y actuará como una capa de bloqueo contra el proceso de cifrado.
- Ransomware Vaccine será actualizada por el proveedor utilizando el mismo proceso de actualización que está siendo desarrollado por el módulo antimalware.
- La solución deberá poder proteger específicamente los endpoints contra los ataques ransomware bloqueándolos antes de que puedan dañar los sistemas.
- La solución debería poder bloquear los ataques basados en Ransomware tanto de forma local a los endpoints como de forma remota (debe proteger los recursos compartidos de red accesibles desde el exterior de los sistemas).
- La solución incluirá algoritmos Machine Learning utilizados contra ataques Zero-Day o Advanced Exploit (directional).
- La solución incluirá un módulo de gestión del riesgo capaz de identificar y proporcionar remediación automática o manual para una gran categoría de indicadores de riesgo relaciones con red y Sistema Operativo que pueden afectar a la funcionalidad y comprometer la seguridad del endpoint.
- El módulo de gestión de riesgo debe proporcionar un Dashboard con el estado de riesgo del cliente.
- El módulo de gestión de riesgo debe proporcionar una separación entre configuraciones incorrectas, vulnerabilidades de aplicaciones y comportamiento humano.

- Esta tecnología también será utilizada para detectar APTs (Advanced Persistent Threats), archivos o tráfico de red sospechoso con la capacidad de establecer al menos 3 umbrales de protección para cada tipo de actividad/archivo sospechoso: permisivo, normal o agresivo.
- La tecnología deberá ser capaz de reportar, bloquear, desinfectar, eliminar o enviar a cuarentena cada uno de los archivos sospechosos y dar la opción al administrador de la solución de bloquear o reportar cada categoría (incluyendo la capacidad de reportar actividad/archivos que deberían haber sido bloqueados en un umbral más alto que el actualmente en uso).
- El módulo Sandbox tendrá la capacidad de bloquear o monitorizar los archivos actualmente enviados para analizar. En el modo monitorización, el archivo enviado deberá ser accesible en el endpoint durante la detonación mientras que el modo bloqueo el acceso al archivo enviado será bloqueado hasta que la detonación se haya completado y se decide realice una acción específica en el archivo enviado.
- La solución Sandbox deberá ser capaz de analizar URLs.
- La solución Sandbox deberá ser capaz de analizar archivos protegidos por contraseña.
- La solución incluirá un módulo Endpoint Detection and Response, capaz de identificar ataques avanzados que se estén llevando a cabo en tiempo real (fase de ejecución).
- El módulo EDR tendrá la capacidad de filtrar incidentes desde la consola de administración utilizando varios criterios: puntuación, fecha, estado, ID de la alerta, nombre del endpoint, tipo de ataque, número de alertas, técnicas ATT&CK, IP del endpoint, MD5, SHA256, nombre del nodo, nombre de usuario
- El módulo EDR permitirá la visualización con gran detalle de cada incidente incluyendo detalles específicos de cada endpoint afectado, proceso especifico, cronología y también actuar en cada paso del incidente con un conjunto de acciones que se pueden utilizar para investigar más a fondo (Sandbox, Virus Total, Google search) o simplemente matar el proceso, aislar el equipo, realizar una conexión remota con el equipo, instalar parches o añadir una excepción de URL (dependiendo del tipo de amenaza evaluada en cada paso del incidente).
- El módulo EDR podrá añadir excepciones para archivos no maliciosos para parar cualquier investigación en ellos o puede añadir a una lista negra un conjunto de archivos maliciosos conocidos para prevenir movimientos laterales.
- El módulo EDR permitirá conexión remota al endpoint potencialmente comprometido para hacer posible una rápida investigación y remediación directamente en el endpoint desde la consola. Un conjunto específico de comandos a nivel de kernel están disponibles para minimizar el tiempo de remediación o recoger datos adicionales.
- La solución deberá incluir un módulo Host IPS capaz de bloquear varias amenazas en la capa de red incluyendo la prevención de movimientos laterales para varias categorías de malware.
- La solución EDR trabajará con la solución EPP para crear incidentes de seguridad para todo el malware detectado en los endpoints.
- La solución de antivirus contemplará la instalación en dispositivos móviles propiedad del Ayuntamiento.

18.Servicio de evolutivos

Se requiere de un servicio gestionado de monitorización, gestión y control de actualizaciones y parches que permita centralizar la administración en un único punto.

La plataforma como servicio estará mantenida y actualizada por el adjudicatario, que aplicará las actualizaciones y medidas de seguridad necesarias para una adecuada prestación del servicio.

El adjudicatario deberá proveer una solución integral que permita:

- Gestionar de forma centralizada y ágil los activos informáticos, con sistemas operativos Windows y Linux.
- Capacidad de resolución de problemas sin intervención por parte del usuario final.
- Gestión integral y centralizada de actualizaciones de los sistemas operativos.
- Despliegue fácil y sencillo de aplicaciones o actualizaciones de estas dentro de los activos.
- Capacidad de automatizar tareas que permitan realizar acciones desatendidas a modo de optimizar el tiempo operativo.
- Identificación centralizada de problemas, como así también la notificación de alertas vía correo electrónico.
- Gestión remota de los activos en caso de requerimiento técnico.
- Gestión de aplicaciones de actualizaciones de forma programada.
- Proveer calendario de actualizaciones gestionado en base a los sistemas operativos, que permita mantener los servidores en las últimas versiones garantizando funcionalidad y seguridad.
- Gestión y monitorización en tiempo real que permita identificar el software instalado en los activos informáticos.

Además, la solución deberá ser capaz de:

- Desplegar de forma rápida y sencilla la solución adoptada en los diferentes activos.
- Gestionar perfiles administrativos basado en roles, que garantice la autenticidad y trazabilidad de las conexiones.
  Generar informe de las actualizaciones realizadas si se requiere.

19.Administración

El adjudicatario será responsable de la administración de la infraestructura hardware y software alojada en el Datacenter:

- Gestión de red del Datacenter.
- Mantenimiento y gestión y de infraestructura común del Datacenter, así como la gestión de configuraciones de elementos del Datacenter y seguimiento del uso de los recursos, incluyendo la configuración de dispositivos en el sistema, el mantenimiento, administración y optimización del almacenamiento y el mantenimiento del sistema de ficheros.

- Gestión de fallos e incidencias, incluyendo las actividades de detección, aislamiento y corrección de errores, recuperación de la red, gestión de las alarmas reportadas en monitorización y mantenimiento preventivo.
- Gestión del rendimiento de los sistemas y las aplicaciones, detección de cuellos de botella, dimensionamiento y cumplimiento de los niveles de servicio.
- Gestión de la seguridad, mediante el establecimiento de la ejecución técnica de políticas de seguridad, auditorías internas de seguridad, gestión de la seguridad perimetral, gestión de firewalls, gestión de los antivirus y sistemas de detección de intrusiones, y control de accesos y de la seguridad física. El adjudicatario deberá realizar también la administración de los elementos de seguridad para permitir el acceso privado y seguro desde las instalaciones del Ayuntamiento a las aplicaciones y servicios alojados en el Datacenter y deberá distribuir la información sobre seguridad y privacidad de datos al responsable del servicio del Ayuntamiento.
- Gestión del entorno de producción alojado en el Datacenter, incluyendo la virtualización de recursos y la elaboración de los procedimientos de despliegue en el Datacenter.
- Gestión de copias de seguridad y restauración de datos de los sistemas incluyendo las operaciones manuales, conforme a la política de seguridad que apruebe el Ayuntamiento.

El licitador deberá describir en la oferta una propuesta de política de seguridad, y que deberá contemplar al menos copia de seguridad diaria de todos los servidores del Ayuntamiento. Las copias de seguridad se realizarán por una red específica, independiente y aislada de la red de datos del servicio en producción, y se realizarán en una ubicación distinta a la que contiene los datos de producción.

20. Soporte

Además de las actuaciones de mantenimiento de la infraestructura alojada en el Cloud, la empresa adjudicataria se encargará del mantenimiento de todos los puestos de trabajo del Ayuntamiento de Ortuella (virtualizados o no), con los siguientes servicios:

- Solución de problemas hardware.
- Solución de problemas software.
- Configuraciones básicas de sistemas operativos.
- Configuraciones de periféricos.
- Procedimientos y políticas de seguridad.
- Implementación de nuevas aplicaciones, versiones o nuevas funcionalidades.
- Soporte a los usuarios en el uso de los equipos y de las aplicaciones base.
- Soporte funcional de aplicaciones corporativas, salvo las de Berger Levrault.
- Soporte remoto a usuarios.
- Reinstalaciones de sistemas operativos.
- Incidencias relacionadas con virus y/o antivirus, sin incluir la recuperación del servicio en caso de incidente grave de seguridad.
- Soporte “in situ” a todas las incidencias que no puedan ser resueltas de forma remota, averías en los equipos de microinformática.

- Atención de peticiones de servicio de los usuarios (cambios de PCs, instalación de nuevas aplicaciones, instalación de nuevos componentes hardware, actualización de aplicaciones, etc..).
- Gestión y actualización del inventario.
- Remitir un informe mensual con las acciones realizadas

La empresa adjudicataria deberá:

- Ejecutar un control permanente del inventario software/hardware en los servidores y en los PCs.
- Recopilar y mantener para su análisis la documentación sobre las tareas realizadas
- En caso de averías en el CPD y/o en los servidores si su resolución precisa de la intervención de técnicos ajenos a la empresa adjudicataria, su intervención será supervisada por un técnico de la empresa adjudicataria.
- Garantizar la sustitución de los técnicos que asisten la instalación en su periodo de vacaciones con técnicos del mismo nivel.

El adjudicatario será responsable de ejecutar las actividades habituales para proporcionar un soporte adecuado, asumiendo la responsabilidad y la coordinación de los problemas relativos al servicio de Cloud hasta su resolución, incluyendo:

- Soporte de primer nivel. Servicio de atención personal 24x7 para asegurar cobertura continúa del servicio de Cloud durante 24 horas al día, 365 días al año. Este servicio incluirá la recepción, clasificación, escalado, seguimiento, cierre y reporte de incidencias. Este servicio será un soporte de primer nivel de interlocución para todo lo relacionado con el Cloud.
- Soporte de segundo nivel. Servicios de operación y explotación que incluyen tareas de gestión y supervisión de sistemas, usuarios y cambios, así como diagnóstico y resolución de incidencias. En caso de que la incidencia sea de un tercero (como puede ser un fabricante) se realizará el escalado y seguimiento de las incidencias hasta su resolución, actuando como interlocutor.
  La previsión de soporte en remoto de segundo nivel es de 240h/año, a facturar únicamente por el servicio consumido.
- Soporte presencial: Personal dependiente de la empresa adjudicataria estará presente tres horas semanales, todas las semanas del año, a convenir, en las instalaciones de este Ayuntamiento, donde, con carácter de exclusividad, dará cobertura a problemas, dudas, cambios, actualizaciones, intermediación con el CPD, formación, auditorias de recursos, propuestas de mejora, …, y todos aquellos relacionados con la informática municipal que fueran necesarios, de manera transversal y siempre orientados a la mejora del rendimiento actual y futuro.

21. Comunicación de incidencias

El adjudicatario pondrá a disposición del Ayuntamiento una herramienta de comunicación de incidencias internas que permita realizar reportes entre las personas designadas a tal fin por el Ayuntamiento y la empresa adjudicataria.

Las características deseables que dicho software deberá cumplir, entre otras, serán:

- Carácter multidispositivo.
- Posibilidad de tipificar las incidencias.
- Cumplimiento de los estándares exigidos en materia de LOPD.
- Generación de informes.
- Certificada en ENS.

Mensualmente el adjudicatario deberá enviar informes al Ayuntamiento con las incidencias producidas, así como su estado y los tiempos de resolución.

22. Metodología y plan de trabajo

En la oferta se detallará la metodología y procedimiento a seguir para la gestión y seguimiento del proyecto.

Se presentará un plan de trabajo, en el que se definirán las tareas a realizar, los responsables de su ejecución, el tiempo estimado y los resultados a obtener.

Si existe una modificación en el plan de trabajo, dicha modificación deberá ser documentada, validada y aceptada por ambas partes.

Todas las labores deberán realizarse de tal forma que el impacto para la organización sea mínimo y garantizando la transparencia de dichos cambios para el usuario.

La empresa adjudicataria nombrará un responsable del Servicio, que se encargará del seguimiento y control de los trabajos a realizar por el personal de su empresa, así como de verificar su nivel de calidad. Dicho responsable será el interlocutor de seguimiento del servicio entre dicho responsable y el Ayuntamiento, con objeto de analizar las incidencias detectadas.

El licitador deberá estar en posesión de las siguientes certificaciones relacionadas con la prestación del servicio:

- ENS nivel medio: Esquema Nacional Seguridad de nivel medio para los Servicios de Cloud y los servicios de instalación, y soporte a infraestructuras de Tecnologías de la Información y las Comunicaciones – TIC.

El equipo de trabajo asignado al proyecto deberá disponer, al menos, de las siguientes certificaciones técnicas:

- Oracle Database Administration 2019 Certified Professional (OCP).
- Citrix Certified Expert - Virtualization (CCE-V).

23. Plan de contingencias

La empresa adjudicataria deberá elaborar un Plan de Contingencias, con el fin de dar respuestas y/o soluciones a posibles interrupciones graves de los servicios que dependan de los elementos

objeto de este pliego. Dicho plan de contingencias deberá hacer mención del tiempo de respuesta ante un evento concreto.

En el caso de que se produzca una incidencia en el Datacenter principal, el servicio deberá poder levantarse en el Datacenter de respaldo en un tiempo inferior a 30 minutos.

Esta posible contingencia no debe suponer pérdida de datos para el Ayuntamiento (replicación síncrona y consistente).

24. Obligaciones del adjudicatario y Devolución del servicio

El licitador deberá especificar claramente en su propuesta un plan de retorno del servicio de Cloud de manera que, una vez alcanzado el plazo máximo de prestación, se facilite una hipotética transferencia o traslado de la infraestructura objeto de la licitación a un nuevo proveedor.

Las actividades propuestas por el licitador, en el plan de retorno del servicio, se entienden todas ellas incluidas dentro del importe económico ofertado en el presente procedimiento pudiendo, por tanto, y llegado el momento, ser todas ellas exigidas por el Ayuntamiento sin posibilidad de facturación adicional por parte del licitador.

Dichas actividades deberán de planificarse y ejecutarse con la antelación suficiente que permita completar el traslado de la infraestructura a un nuevo proveedor con anterioridad a la fecha de finalización de los servicios objeto de la presente convocatoria.

Además de las obligaciones contractuales el adjudicatario deberá:

- Comunicar cualquier alteración que afecte al servicio.
- Controlar y mantener informado periódicamente al Ayuntamiento del estado general de sus instalaciones informáticas.
- Asesorar al Ayuntamiento en todos los aspectos informáticos.
- Poner a disposición una herramienta de comunicación de incidencias.
- Documentación: será parte de las tareas a realizar por el Adjudicatario la realización de los siguientes manuales y documentación:
    - Memoria con la arquitectura, así como la información relativa a la arquitectura física y lógica de la plataforma instalada y configurada.
    - Memoria del sistema con la descripción de sus funcionalidades, su implantación y su funcionamiento y operativa.
    - Memoria con el código fuente de los posibles desarrollos que se puedan realizar para la consecución de los trabajos.
    - Manual de configuración con la información relativa a la parametrización realizada.
    - Manual de administración con los procedimientos de administración, los accesos, los permisos, los parámetros configurables, así como un plan de contingencia ante eventuales fallos en el sistema.

- Manual de mantenimiento con la información relativa a las tareas y acciones de mantenimiento preventivo a realizar, así como para el seguimiento de todas las acciones preventivas y correctivas realizadas. Se incluirán en este apartado los manuales de monitorización para el correcto funcionamiento de la plataforma, los procedimientos de parada y de arranque de cada componente o módulo funcional.
- Manual de usuario con la información relativa al uso de la plataforma para cada uno de los perfiles de trabajo, así como todo aquel material utilizado en las acciones formativas indicadas en el plan de formación
- Una vez finalizado el proceso de instalación, se considera necesario, como parte del proceso de validación, la acreditación por parte de la empresa adjudicataria del plan de pruebas realizado, considerando la prestación de servicios como completada cuando, una vez realizadas todas las pruebas de funcionamiento.

Por otra parte, toda la documentación generada por el Adjudicatario en el período de ejecución del contrato será propiedad exclusiva del Ayuntamiento, sin que el contratista pueda conservarla ni obtener copia de esta o facilitarla a terceros sin la expresa autorización. Se remitirá copia en papel y digital de la misma al Ayuntamiento de Ortuella.

Por otra parte, durante la ejecución de los trabajos objeto del contrato, el Adjudicatario se comprometerá a facilitar en todo momento a las personas designadas por el Ayuntamiento, a tales efectos, la información y documentación que éstas soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan surgir en su evolución futura, y de las tecnologías, métodos y herramientas disponibles para resolverlos.

Los solicitantes indicaran si su empresa tiene Plan de seguridad que recoja los principios y acciones contempladas en la RGPD. El adjudicatario queda 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 pliego, ni tampoco ceder a otros ni siquiera a efectos de conservación. El adjudicatario quedará obligado al cumplimiento de Reglamento General de Protección de Datos en vigor. El oferente incluirá en su oferta la memoria descriptiva de las medidas de seguridad que adoptará para asegurar la disponibilidad, confidencialidad e integridad de los datos manejados y de la documentación facilitada.

El adjudicatario se compromete a cumplir las siguientes normas de comportamiento respecto a los sistemas de información:

- No introducir software microinformático ajeno al Ayuntamiento.
- No divulgar la estructura de ficheros, la existencia de estos ni las funcionalidades de los aplicativos desarrollados o de los que se tuviera conocimiento.
- No difundir ni publicar los sistemas de seguridad de la información.
- Acceso exclusivo a la información necesaria para el desempeño de las funciones encomendadas.

En cuanto a la RGPD la empresa adjudicataria asesorará técnicamente ante la toma de decisiones y mecanismos de implantación, tanto obligatorios como complementarios, como lo puede ser la firma digital, técnicas de encriptación, etc.
El licitador acepta expresamente que los derechos de explotación de cualquier aplicación informática y de los programas desarrollados al amparo del presente pliego corresponden únicamente al Ayuntamiento, con exclusividad y a todos los efectos.

En caso de rescisión del contrato por cualquier causa sobrevenida el adjudicatario se compromete a la entrega de toda la documentación e información propiedad del Ayuntamiento, en el plazo máximo de 1 mes desde la notificación de esta. Y, en cualquier caso, todas aquellas incluidas en el Esquema Nacional de Seguridad y en el Reglamento General de Protección de Datos.

25. Contenido de la oferta

La oferta técnica deberá incluir, como mínimo, la siguiente información:

- Sobre "Criterios sujetos a valoración subjetiva"
  - Características generales de la empresa.
  - Descripción de los DataCenters desde los que se prestará servicio.
  - Relación de clientes significativos de servicios de Cloud.
  - Arquitectura de la solución técnica propuesta:
    - Plataforma Cloud.
    - Conectividad.
    - Centro de respaldo.
  - Plan de migración.
  - Plan de devolución del servicio.
  - Planteamiento del servicio:
    - Periodo de atención.
    - Sistema de recepción de avisos.
    - Tiempo de respuesta.
    - Tiempo de resolución normalizado.
    - Tiempo de resolución incidencias críticas.
- Sobre "Criterios sujetos a valoración objetiva"
  - Documentación certificaciones.
  - Documentación oferta económica.
  - Precios unitarios.

26. Otros requisitos

Requisitos de seguridad de la información

Al objeto de dar unos servicios al ciudadano seguros, que protejan los datos personales, su intimidad, la integridad de la información, que eviten ataques, y que garanticen el cumplimiento

de la normativa vigente en materia de seguridad TIC, el adjudicatario deberá cumplir una serie de requisitos en materia de seguridad en distintas áreas de TIC relacionadas con los diferentes servicios pedidos en el presente pliego. Se exige que el adjudicatario ofrezca unos servicios de seguridad de carácter horizontal a todos los demás servicios exigidos en este pliego, y en particular que se articule en las áreas contempladas en el presente apartado.

Todos los sistemas de información del Ayuntamiento se conforman dentro del ámbito de aplicación del Reglamento General de Protección de Datos (RGPD) y del Esquema Nacional de Seguridad (ENS), por lo que las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración Electrónica.

En este sentido los sistemas de alojamiento deberán implantar, al menos, las medidas de seguridad que el ENS establece para los sistemas de información de categoría media.

SLA - Acuerdo de nivel de servicio

En el plazo máximo de tres meses desde la firma del contrato, la empresa adjudicataria y este Ayuntamiento firmarán un Acuerdo de Nivel de Servicio según el estándar ITIL más actual.

27. Criterios de valoración

1.- Criterios objetivos (75 puntos)

a.- Oferta económica 30 puntos

Valoración oferta económica = 30 x (oferta más económica / oferta a valorar)

b.- Certificaciones (35 puntos)

b.1. certificaciones empresa

- ISO 22301: Sistema de Gestión de Continuidad de Negocio 5 puntos
- ISO 27017: Sistema de Gestión de la Seguridad en la Nube 5 puntos
- ISO 27018: Sistema de Gestión de Protección de la información en Cloud 5 puntos

b.2.- certificaciones de técnico

- Microsoft Certified Solutions Associate: SQL Database Administration 6 puntos
- VMware Certified Professional – Data Center Virtualization (2022) 6 puntos

b.3.- ENS nivel alto: Esquema Nacional Seguridad de nivel alto para los Servicios de Cloud y los Servicios de instalación y soporte a infraestructuras TIC. 8 puntos

c.- Plazo de migración (compromiso de ejecución en menos de 30 días) 10 puntos

2.- Criterios subjetivos (25 puntos)

- Arquitectura de la solución técnica propuesta. 10 puntos
- Plan de migración. 7 puntos
- Plan de devolución del servicio. 3 puntos
- Planteamiento del servicio 5 puntos
  - Periodo de atención.
  - Sistema de recepción de avisos.
  - Tiempo de repuesta.
  - Tiempo de resolución normalizado.
  - Tiempo de resolución incidencias críticas