INFORME TÉCNICO DE CUESTIONES CONTRACTUALES PARA LA CONTRATACIÓN DEL "SUMINISTRO DE LICIENCIAS SOLUCIÓN EDR/XDR/MDR (ENDPOINT DETECTION AND RESPONSE/EXTENDED DETECTION AND RESPONSE/ VIGILANCE MDR) PARA PREVENCIÓN DE CIBERATAQUES" Mediante Orden TER/836/2022, de 29 de agosto, se aprobaron las bases reguladoras y se efectuó la convocatoria correspondiente a 2022 de subvenciones destinadas a la transformación digital y modernización de las administraciones de las entidades locales, en el marco del Plan de Recuperación, Transformación y Resiliencia (BOE 1 de septiembre de 2022).

ÍNDICE

El objeto de este contrato persigue garantizar la prestación y calidad de los servicios y aplicaciones, así como otros servicios de valor añadido inherentes al Ayuntamiento, para lo que considera indispensable la implantación de una solución integrada de detección y respuesta ante amenazas. La implantación de este sistema engloba: el diseño, la configuración, la instalación, la puesta en marcha del servicio, la documentación, la gestión y el mantenimiento de todos sus elementos durante el tiempo de vigencia del contrato.

Las soluciones EDR-XDR (Endpoint Detection and Response - Extended Detectio and Response), están diseñadas para integrar y correlacionar datos de diferentes fuentes de seguridad, como puntos finales, redes y aplicaciones, lo que les permite detectar amenazas más reforzadas que podrían pasar desapercibidas para otras soluciones de seguridad.

La detección y respuesta gestionadas (MDR, por sus siglas en inglés) no es una tecnología independiente, sino más bien un servicio gestionado que comprende los beneficios de la EDR y la XDR en una solución cómoda. La MDR puede ayudar con la investigación de búsqueda de datos y la búsqueda de amenazas, el análisis de ingestión y los flujos de trabajo en toda la red, reducir la fatiga de alerta, mejorar el análisis de eventos centrados en amenazas y más.

La MDR anula la necesidad de contratar expertos externos en ciberseguridad. Dado que un proveedor externo experimentado creó la solución, puede obtener fácilmente el triaje de alertas para distinguir los falsos positivos de las amenazas reales. La mayoría de las veces, la MDR ofrece un enfoque integral de las funciones tradicionales de detección y respuesta. También puede acelerar el análisis de amenazas multidominio y beneficiar a los firewalls DNS, la supervisión en la nube, los sensores de red y más para proteger la infraestructura de TI de la empresa.

Las herramientas generales de detección y respuesta de puntos finales (EDR, por sus siglas en inglés) monitorean los puntos finales en tiempo real utilizando análisis de comportamiento (IOC e IOA), se basan en una base de datos y gráficos de amenazas, la contención de la red y presentan a los equipos de seguridad recomendaciones de remediación.

La MDR proporciona las mismas capacidades que la EDR, pero ofrece servicios administrados las 24 horas del día, los 7 días de la semana, para monitorear los puntos finales y eliminar y remediar las amenazas.

La XDR ofrece soluciones de análisis para tráfico de red centradas en las amenazas. Agiliza la ingesta de datos de seguridad de varias fuentes, mejora drásticamente la visibilidad de las amenazas, acelera el análisis de amenazas y reduce el riesgo de amenazas. La visibilidad mejorada de amenazas de XDR acelera las operaciones de seguridad, permite una investigación en profundidad del análisis de amenazas de

dominio y proporciona a los equipos herramientas de seguridad aisladas que unifican toda la estrategia de ciberseguridad de su empresa.

La vigencia de las licencias será de 3 años.

El contrato tiene como objeto las siguientes finalidades:

1. Proteger todos los puestos de trabajo de ataques que provoquen secuestro o pérdida de datos sin dejar de lado el resto de software malicioso, con la instalación, configuración detallada y puesta a punto de los agentes y plataforma de gestión con sus correspondientes licencias en modalidad de alquiler (SaaS), disponiendo, de este modo, de un servicio de ciberseguridad proactivo y reactivo de monitorización de todo el entorno para la detección, búsqueda de amenazas, investigación de incidentes y respuesta que no sólo identifique la amenaza o tome acción de las alertas, sino que interprete lo que está pasando en la red y presente un contexto de lo que se detectó.
2. Formación y coordinación con el departamento de Informática para la explotación y gestión del entorno de ciberseguridad que se oferte.

En definitiva, se trata disponer de un servicio capaz de reaccionar de forma eficaz ante las amenazas de ciberseguridad actuales y futuras de tal forma que nos ayude a entender de dónde proviene la amenaza, cómo se desarrolló, cuál es su causa raíz, escala, etc. y que nos ayude a tomar decisiones para la reparación y mejora continua de forma proactiva. Todo ello a través de un proceso de gestión de incidentes, con pasos como la identificación, la contención, la erradicación, la recuperación y el análisis para prepararnos para futuros ataques,

Por lo tanto, lo que se licita en este pliego es es una solución, junto con un servició de explotación que cuente con inteligencia de amenazas, correlación, herramientas de detección y respuesta que permitan detectar y responder de manera eficiente ante comportamientos extraños y posibles brechas que se encuentren en cualquier sistema y red de información del Ayuntamiento, proporcionando todas las herramientas, el personal y la experiencia necesaria para protegernos contra las ciberamenazas.

Con el fin de reducir los costes de mantenimiento y explotación de la solución, es requisito mínimo que la plataforma donde se aloje la infraestructura se encuentre fuera de nuestras instalaciones en un modelo SaaS en la nube, en el que no haya un inconveniente en el crecimiento y escalabilidad de la plataforma.

La justificación de la necesidad de la licitación de este contrato, según lo previsto en el artículo 28 y 116 de la LCSP, se encuentra en el hecho de que el Ayuntamiento de Ontinyent necesita adquirir un EDR basado en varios factores:

El Ayuntamiento provee de equipamiento tecnológico a sus empleados para el desarrollo de sus funciones y como tal, debe velar por la disponibilidad de estos.

Actualmente, la plataforma cliente del Ayuntamiento tiene como mecanismo de seguridad el software de antivirus avanzado ESET.

No obstante, los patrones de ataque y software malicioso actuales hacen conveniente la instalación de varias capas de seguridad que protejan tanto servidores como equipos cliente de tal forma que se complementen y doten a la organización de un sistema fiable y seguro. Las amenazas tanto externas como internas a que están sometidos los ordenadores personales de los usuarios, y los propios servidores corporativos, son cada día más numerosas y su capacidad destructiva mayor, a la par que la sofisticación en el desarrollo de estas herramientas de ataque hace más difícil su detección y eliminación. Particularmente peligrosos son las denominadas amenazas "Zero-day", del tipo ransomware, es decir, aquellas que aprovechan vulnerabilidades recién descubiertas y que por lo tanto no han sido incluidas aún en los ficheros de firmas tradicionales que utilizan los programas antivirus.

Las soluciones de antivirus tradicionales ya no son una buena barrera para detectar y eliminar multitud de amenazas que llegan a los equipos. Los ataques son cada vez más sofisticados y hacen uso de numerosas técnicas de evasión orientadas a pasar desapercibidos y no ser detectados por las distintas herramientas de seguridad. Existen en el mercado nuevas plataformas que complementan las funciones de los antivirus tradicionales: las llamadas soluciones EDR (Endpoint Detection and Response) y que han evolucionado a las plataformas XDR. Mientras que EDR recopila y correlaciona las actividades que se suceden en varios endpoints, XDR amplía el alcance de la detección con el fin de proporcionar detección, análisis y respuesta no solo en los endpoints, sino también en las redes, servidores, cargas de trabajo en la nube, SIEM, etc proporcionando una vista unificada de varias herramientas y vectores de ataque. Esta visibilidad mejorada contextualiza las amenazas para facilitar la clasificación, investigación y reparación. XDR recopila y relaciona automáticamente los datos de diversos vectores de seguridad, favoreciendo así una detección más rápida de las amenazas para que los analistas de seguridad puedan responder rápidamente antes de que se amplíe el alcance de la amenaza. Las integraciones listas para usar y los mecanismos de detección preestablecidos en varios productos y plataformas diferentes ayudan a mejorar la productividad, la detección de amenazas y el análisis forense.

Con el fin de poder cumplimentar la documentación será necesaria y obligada para la ejecución del PRTR sobre el cumplimiento de los hitos marcados en la solicitud de los fondos la redacción de un informe sobre los mismos y que trata de:

El presente proyecto de transformación digital y modernización se encuentra vinculado a los hitos 167 y 169 así como al objetivo 168 de la Propuesta de Decisión

de Ejecución del Consejo (CID), al contribuir con las líneas estratégicas de interoperabilidad y de infraestructuras digitales de la Inversión C11.I3 del PRTR, así como a la consecución de la transformación digital en términos de infraestructuras físicas, lógicas e informáticas del ayuntamiento.

El conjunto de actuaciones contempladas en este proyecto está encaminado a conseguir principalmente:

- *Fomentar la interoperabilidad entre administraciones publicas siguiendo el espíritu de la presente convocatoria, potenciando la interacción con las aplicaciones del estado.*

- *Facilitar y acompañar a la ciudadanía en la utilización de servicios públicos digitales, mediante la implementación de puntos físicos de acceso y soporte, para avanzar en la democratización del uso y el entendimiento de las herramientas tecnológicas de la administración digital.*

- *Dotar de infraestructuras tecnológicas adecuadas para la capacitación digital de empleados públicos que a su vez redundará en personal más preparado y con mejores recursos para ofrecer servicios públicos modernos a la ciudadanía.*

- *Mejorar la seguridad y la salvaguarda de los datos haciendo así que la administración sea más confiable cara a la ciudadanía e intentando evitar cualquier posible intrusión y perdida de datos.*

ESTOS HITOS VAN DIRECTAMENTE RELACIONADOS CON LAS CARACTERÍSTICAS REQUERIDAS EN LA ORDEN TER/836/2022

Con lo anteriormente descrito los hitos del proyecto que van directamente a cumplir con los hitos marcados en el Plan de Recuperación y que son el 167 y 169.

En el hito 167 Administración orientada al ciudadano, Operaciones inteligentes e infraestructuras digitales.

En el hito 169 Transformación digital en términos de infraestructuras físicas y lógicas y programas informáticos, Transformación digital en términos de proactividad, movilidad, experiencia del usuario y Transformación digital en términos de automatización y Administración Pública centrada en los datos.

Estos dos hitos tendrán una implantación a lo largo de ejecución del proyecto y tendrán una vigencia más duradera.

En nuestro proyecto, estos hitos están desarrollados como siguen:

- Contar con herramientas digitales modernas de comunicación, colaboración y difusión a partir de las infraestructuras tecnológias asociadas a los puestos de trabajo y a las labores que se desempeña por el ayuntamiento.

- Facilitar y acompañar a la ciudadanía en la utilización de servicios públicos digitales, mediante la implementación de puntos físicos de acceso y soporte, para avanzar en la democratización del uso y el entendimiento de las herramientas tecnológicas de la administración digital con la apertura de nuevas oficinas y puntos de acceso tanto para la ciudadanía como las empresas

- Dotar de infraestructuras tecnológicas adecuadas para la capacitación digital de empleados públicos que a su vez redundará en personal más preparado y con mejores recursos para ofrecer servicios públicos modernos a la ciudadanía.

- Dotar de infraestructuras tecnológicas adecuadas para expandir la administración electrónica por todo el municipio acercándola a toda la ciudadanía permitiendo una conectividad y control desde las oficinas centrales del ayuntamiento, de la misma manera que se dotará de la seguridad requerida por los estándares actuales para la protección de los datos, como se ha dicho anteriormente, tanto municipales como del ciudadano y las empresas de nuestro municipio.

Al mismos tiempo, los objetivos que se pretenden alcanzar en nuestro Proyecto dentro del Plan de Recuperación, Transformación y Resilencia, Componente 11, Inversión 3 han de ser los siguientes:

- Mejorar la accesibilidad de los servicios. El proyecto mejora la accesibilidad de los servicios de la administración modernizando y digitalizando sus servicios al proporcionar acceso digital a la ciudadanía en relación a los tramites que deben gestionar con la administración.

- Reducir la brecha digital. El proyecto es accesible a toda la ciudadanía facilitando el acceso a internet a las personas que, por sus circunstancias, no tiene acceso particular a internet.

- Mejorar la eficiencia y eficacia de los empleados públicos. Al poder gestionar trámites con la administración desde los puntos de acceso en cada sede facilita y mejora la eficacia de los empleados públicos al tener que gestionar menos trámites de forma presencial. Al mismo tiempo, la implementación de medidas informáticas de seguridad permitirán que el trabajo de los empleados públicos sea más seguro, evitando, en lo posible, que con los ataques informáticos se quede paralizada nuestra administración.

- Reutilizar los servicios y soluciones digitales construidas. El uso de oficinas que están en desuso en los barrios de la población permitirá una proximidad de la administración tanto a la ciudadanía como a las empresas del municipio, dando a estos barrios una oportunidad de desarrollo a partir de los nuevos servicios y locales puestos a su disposición.

Situación actual.

El Ayuntamiento de Ontinyent dispone, en la actualidad, de un sistema de protección de los puestos de trabajo basado en un antivirus tradicional pero que ya se ha comprobado, por los ataques recibidos por otras administraciones públicas de nuestro entorno, que no es suficiente. Además, nos encontramos en un momento en el que no se trata de saber si vas a ser atacado o no, sino de cuándo lo serás y qué alcance tendrá el ataque.

Ante esta situación se hace necesario reforzar la seguridad tanto en la protección ante código malicioso como con el secuestro o pérdida de datos.

Obligaciones del contratista.

Tratándose de un servicio cofinanciado por el Fondo Europeo de Desarrollo Regional (FEDER), el adjudicatario estará obligado a cumplir las obligaciones de información y publicidad establecidas en el anexo XII, Sección 2.2. del Reglamento (UE) 1303/2013, del Parlamento Europeo y del Consejo, de 17 de diciembre de 2013, y especialmente, las siguientes:

- Durante la ejecución del contrato, el adjudicatario deberá hacer constar en toda la información y publicidad que pudiera generarse con ocasión de la ejecución del contrato que el mismo se encuentra cofinanciado por el Fondo Europeo de Desarrollo Regional (FEDER), de acuerdo con lo dispuesto en el Reglamento (UE) 1303/2013.

- En los documentos de trabajo, así como en los informes y en cualquier tipo de soporte que se utilice en las actuaciones necesarias para el objeto del contrato, aparecerá de forma visible y destacada el emblema de la UE, haciendo referencia expresa a la Unión Europea y el Fondo Europeo de Desarrollo Regional.

- En toda difusión pública o referencia a las actuaciones previstas en el contrato, cualquiera que sea el medio elegido (folletos, carteles, etc...), se deberán incluir de modo destacado los siguientes elementos: emblema de la Unión Europea de conformidad con las normas gráficas establecidas, así

como la referencia a la Unión Europea y al Fondo Europeo de Desarrollo Regional, incluyendo el lema "Una manera de hacer Europa".

1. En relación a la insuficiencia de medios.

Para entender, analizar y proponer soluciones a los diferentes tipos de ataques que se producen a día de hoy, es necesario disponer de personal altamente especializado del cual no disponemos en la actualidad por lo que lo conveniente es licitar un servicio gestionado que automatice la prevención, detección, investigación y respuesta ante incidentes de seguridad que nos proporcione una mayor anticipación a los ataques dirigidos, un menor tiempo de exposición a incidentes de seguridad y una visibilidad completa de las amenazas.

Actualmente el Ayuntamiento de Ontinyent no dispone de personal propio que pueda encargarse de realizar el servicio.

2. En relación a la duración del contrato.

La duración del contrato será de 2 meses sin posibilidad de prórroga.

3. En relación al código CPV aplicable.

En cuanto a la codificación del objeto del contrato, el código correspondiente al presente contrato de acuerdo con Reglamento (CE) Nº 2195/2002, del Parlamento Europeo y del Consejo de 5 de noviembre de 2002, modificado por el Reglamento 213/2008, de la Comisión, de 28 de noviembre de 2007 por el que se modifica el Vocabulario Común de contratos públicos (CPV) será el indicado a continuación:

48760000 Paquetes de software de protección antivirus.

72253200 Servicios de apoyo a sistemas.

72251000 Servicios de recuperación en caso de catástrofe.

4. En relación a las condiciones especiales de ejecución.

Es obligatorio el establecimiento de al menos una condición especial de ejecución, relacionada estrictamente con el objeto del contrato, en los términos previstos en el art. 202 de la LCSP.

En relación a la eventual cesión de datos y finalidades del tratamiento; obligación esencial.

La cesión de datos conlleva necesariamente como condición especial de ejecución la obligación del contratista de someterse a la normativa nacional y de la Unió Europea en materia de protección de datos, advirtiéndose además al contratista de

que esta obligación tiene el carácter de obligación contractual esencial de conformidad con lo dispuesto en la letra f) del apartado 1 del artículo 211.

Cláusula ambiental.

En atención a los artículos 1.3, 28.2 y 145 de la LCSP, en relación al 145 del mismo cuerpo legal, se exige que los licitadores se comprometan a utilizar, en el desarrollo de las actividades del contrato, equipos con tecnología eficiente de bajo consumo energético como pantallas con iluminación LED o impresoras inteligentes, el uso de materiales consumibles reciclados como papel o la tinta de las impresoras y que las comunicaciones con el órgano contratante sean exclusivamente a través de medios electrónicos.

El cumplimiento de esta exigencia se acreditará mediante informe del responsable de la correcta ejecución del servicio a licitar y que tendrá que ser emitido en el término de un mes desde la formalización del contrato.

Antes del inicio del proyecto se deberá analizar los riesgos que tiene el proyecto en relación con posibles impactos significativos en el medioambiente, esto se deberá hacer utilizando lo especificado en el art 5 Orden HFP/1030/2021, de 29 de septiembre donde se deben cumplir los seis objetivos medioambientales definidos en el Reglamento (UE) n.º 2020/852 del Parlamento Europeo y del Consejo, de 18 de junio de 2020. Al fin de poder comprobar este cumplimiento se establecerá como documentación de inicio del proyecto cumplimentar el test establecido en el anexo II.B.4 de la citada Orden, así como tener en cuenta las referencias de gestión que proporciona el anexo III.B a fin de evitar impactos medioambientales no deseables.

El proyecto se deberá desarrollar al cumplimiento de las obligaciones asumidas en materia de etiquetado verde y etiquetado digital y los mecanismos establecidos para su control regulados en la Orden HFP/1030/2021, de 29 de septiembre en su art 4. Se establece que los efectos a computar se encuentran en el Reglamento del MRR anexo VII para digital "*Campo de intervención 4: Administración electrónica, servicios públicos digitales y ecosistemas digitales locales Dimensión 5 del DESI: Servicios públicos digitales 011 Soluciones de TIC para la Administración, servicios electrónicos, aplicaciones (6) 100 %,* 011 ter Implantación del sistema europeo de identidad digital para uso público y privado 100 %"

5. En relación al Análisis del Procedimiento.

Análisis de la ejecución por lotes.

En base al artículo 99.3.b, de la LCSP, dada la naturaleza de las prestaciones no es posible entender estas como una realización y aprovechamiento individual y funcional de las mismas que permitan se ejecutadas de forma independiente. Además, habría que exigir una coordinación y planificación global de los trabajos

para una correcta ejecución completa de las prestaciones que resulta desproporcionada para las finalidades de interés público que se persiguen en la ejecución de estas, todo lo cual permite concluir que las prestaciones no pueden ser ejecutadas de forma independiente sin menoscabar la correcta ejecución de los trabajos y una correcta asignación de los recursos públicos proporcionales a la finalidad requerida.

La realización independiente de las diversas prestaciones comprendidas en el objeto del contrato dificulta la correcta ejecución del mismo desde el punto de vista técnico: en este sentido, a naturaleza del contrato no permite su división por lotes puesto que las plataformas de seguridad EDR/XDR son plataformas todo-en-uno, desarrolladas para luchar contra el panorama de amenazas avanzadas, que proporciona protección contra ataques mediante la identificación y mitigación de conductas maliciosas a velocidad de máquina y no son soluciones modulares ni separadas sino integrales por lo que es imposible realizar una división por lotes.

6. En relación al presupuesto.

De conformidad con el precio de mercado, el valor estimado del contrato se determina por la agregación de los diferentes elementos que componen el objeto del contrato:

El importe total de este contrato es de 52.054,20 € más 10.931,38 € de IVA al 21%, **lo que equivale a un total de 62.985,58 € con iva incluido** y que estará dividido en las siguientes partes:

Para el cálculo de estos importes se han consultado las fuentes obrantes en internet, tanto de los fabricantes, distribuidores, empresas del sector y otros contratos ya adjudicados.

La duración del contrato será de 2 meses sin posibilidad de prórroga.

Estos presupuestos incluyen todos los servicios necesarios para su puesta en funcionamiento tal y como se prevé en el pliego de prescripciones técnicas.

El valor estimado del contrato, a los efectos que disponen el art. 101 y concordantes de la LCSP es de **52.054,20 €** cincuenta y dos mil cincuenta y cuatro euros con veinte céntimos – IVA no incluido.

Componente	Importe de licitación (IVA excluido)	Tipo IVA aplicable: 21% Importe IVA	Presupuesto base de licitación (IVA incluido)

1. 230 licencias ENDPOINT	27.326,30	5.738,52	33.064,82
2. 39 licencias SERVER	7.842,12	1.646,85	9.488,97
3. 269 licencias Vigilance MDR	11.830,62	2.484,43	14.315,05
4. Plataforma de gestión	1.665,16	349,68	2.014,84
5. Servicio iniciales de puesta a punto	3.390,00	711,90	4.101,90
TOTAL	**52.054,20**	**10.931,38**	**62.985,58**

7. En relación a las ofertas desproporcionadas o con valores anómalos.

Para determinar las ofertas desproporcionadas propongo utilizar los criterios establecidos en el artículo 85 del Real Decreto 1098/2001, de 12 de octubre, por el que se aprueba el Reglamento General de la Ley de Contratación de las Administraciones Públicas.

8. En relación a los criterios de adjudicación

El artículo 145 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, señala que la adjudicación de los contratos se realizará utilizando una pluralidad de criterios de adjudicación en base a la mejor relación calidad-precio, si bien, previa justificación en el expediente, los contratos se podrán adjudicar con arreglo a criterios basados en un planteamiento que atienda a la mejor relación coste-eficacia, sobre la base del precio o coste, como el cálculo del coste del ciclo de vida con arreglo al artículo 148.

Asimismo, la mejor relación calidad-precio se evaluará con arreglo a criterios económicos y cualitativos, según prevé el apartado segundo del artículo 145 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público -LCSP 2017-

Los criterios cualitativos que establezca el órgano de contratación para evaluar la mejor relación calidad/precio podrán incluir aspectos medioambientales o sociales, vinculados al objeto del contrato en la forma establecida en el artículo 145.6, que

podrán ser, entre otros, los siguientes: La calidad, incluido el valor técnico, las características estéticas y funcionales, la accesibilidad, el diseño universal o diseño para todas las personas usuarias, las características sociales, medioambientales e innovadoras, y la comercialización y sus condiciones

Por su parte, el artículo 145 Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público -LCSP 2017, establece en su apartado 3º que la aplicación de más de un criterio de adjudicación procederá, en todo caso, en la adjudicación de los siguientes contratos:

- Cuando el órgano de contratación considere que la definición de la prestación es susceptible de ser mejorada por otras soluciones técnicas o por reducciones en su plazo de ejecución.
- Contratos de servicios, salvo que las prestaciones estén perfectamente definidas técnicamente y no sea posible variar los plazos de entrega ni introducir modificaciones de ninguna clase en el contrato, siendo por consiguiente el precio el único factor determinante de la adjudicación.

Siendo así y puesto que esta es un contrato fundamentalmente de prestación de servicios, se establecen los siguientes criterios de valoración

Para seleccionar la oferta, propongo utilizar el criterio siguiente de valoración, siendo la puntuación total de 100 puntos:

a) Criterio de valoración matemática:

- Precio ofertado, de acuerdo con la siguiente fórmula: 90 puntos:

$$Vi = 90 \cdot \frac{Plicitación - Oi}{Plicitación - Oadmisible}$$

Vi= Puntuación obtenida por la oferta i.

Plicitación= Presupuesto de licitación sin IVA.

Oadmisible= Oferta más económica admisible sin IVA.

Oi=Importe oferta y sin IVA.

Por otra parte, será la oferta más económica admisible (Oadmisible) la cuantía por debajo de la cual las ofertas se consideren en presunción de temeridad de acuerdo con el artículo 85 del Real Decreto 1098/2001, de 12 de octubre, por el que se aprueba el Reglamento general de la Ley de Contratos de las Administraciones Públicas.

En el caso de que la mesa de contratación aceptara una o varias ofertas que fueran consideradas inicialmente en presunción de temeridad por quedar adecuadamente justificadas, en la fórmula se utilizará el valor de la oferta más económica aceptada, Oi más económica, en lugar de la oferta más económica admisible, Oadmisible.

Se propone exigir que la oferta económica esté detallada y desglosada especificando el coste de cada uno de los conceptos. La oferta debe ser coherente con la oferta desglosada.

- Se valorarán los siguientes apartados:

Mayor número de licencias ofertadas (hasta 10 puntos)

Por 10 licencias adicionales Complete Server:	5 puntos
Por 10 licencias adicionales Vigilance MDR:	5 puntos

Los criterios de adjudicación determinados están vinculados al objeto del contrato, en el sentido que se expresa a continuación:

- Han sido formulados de forma objetiva, con pleno respeto a los principios de igualdad, no discriminación, transparencia y proporcionalidad. Y no confieren al órgano de contratación una libertad de decisión ilimitada.

- Las ofertas serán evaluables en condiciones de competencia efectiva y permitirán comprobar de manera objetiva la información facilitada por los licitadores, con el fin de evaluar en que medida la oferta cumple los criterios de adjudicación.

Se comprobará de manera efectiva la exactitud de la información.

Se considera necesario y conveniente el incremento, tanto del número de licencias como de horas de asistencia, por la mejora en el servicio. Con el aumento del número de licencias podemos tener una reserva ante la posibilidad de aumento del número de trabajadores en nuestra administración. En cuanto al número de horas, evitamos aumentar el coste del servicio en caso de necesidad.

En relación a las fórmulas:

- Para la distribución de puntos de acuerdo con el criterio del precio se ha seleccionado la fórmula anterior por ser una distribución lineal directa que puntúa más a la oferta de precio más baja partiendo de que el máximo de puntos se inicia en el límite para ser considerada como baja temeraria, que otorga 0 puntos si no se produce ninguna baja, pero que no distribuye necesariamente todos los puntos a los efectos de evitar que pequeñas diferencias en el precio den lugar a puntuaciones muy diferentes. De esta forma, se otorga la mayor puntuación a la propuesta más ventajosa

económicamente para el Ayuntamiento d'Ontinyent. Respecto a la fórmula utilizada se han seguido los criterios establecidos por la Sindicatura de Comptes en diversos informes de auditoría de los expedientes de contratación de diversos ayuntamientos.

9. En relación al régimen de pagos.

Se propone incluir "Los pagos se realizarán una vez ejecutados la totalidad de los trabajos de acuerdo a la certificación que los servicios técnicos municipales expedirán una vez realizada la acta de recepción. Para las certificaciones se utilizarán los precios desglosados en la oferta económica. Los servicios no prestados no se certificarán y, por lo tanto, no se pagarán".

10. En relación a las ampliaciones o reducciones del contrato.

No se contemplan.

11. En relación a la eventual cesión de datos y finalidades del tratamiento; obligación esencial.

La cesión de datos conlleva necesariamente como condición especial de ejecución la obligación del contratista de someterse a la normativa nacional y de la Unió Europea en materia de protección de datos, advirtiéndose además al contratista de que esta obligación tiene el carácter de obligación contractual esencial de conformidad con lo dispuesto en la letra f) del apartado 1 del artículo 211.

12. En relación a posibles Penalidades.

Un retraso en la resolución de una incidencia sin existir una justificación explícita y real de la misma, implica un perjuicio para el Ayuntamiento y tendrá consideración de infracción.

Evitar la demora injustificada en la resolución de incidencias y conseguir la máxima eficiencia utilizando las aplicaciones objeto del presente contrato es cuanto se pretende conseguir mediante el presente régimen sancionador.

Así pues, la demora en la resolución de incidencias dará lugar a la imposición d penalidades y eventual resolución del contrato, en los términos previstos en los artículos 192 y 193 de la LCSP siendo de aplicación el mismo régimen de penalidades tanto en el caso del incumplimiento total como del incumplimiento parcial. En el caso del incumplimiento parcial el cálculo de las penalidades se referirá al importe del presupuesto del servicio parcialmente incumplido. Lo anterior se entiende sin perjuicio de la facultad de la Administración de proceder a la resolución del contrato y a la eventual reclamación de indemnización de daños y perjuicios.

En materia de prestación defectuosa de los mantenimientos, soportes y actualizaciones o de incumplimiento de los compromisos o de las condiciones especiales de ejecución del contrato, establecidas al amparo de los artículos 76.2 y 202.1 de la LCSP 2017, se impondrán penalidades en proporción a la gravedad del incumplimiento hasta los límites máximos del 10% o del 50% en los términos señalados en el artículo 192 de la LCSP 2017.

A los anteriores efectos se establecen:

- Penalidades por incumplimiento parcial o cumplimiento defectuoso. Serán del 10% del precio del contrato, por cada una de ellas con un límite del 50%

- Penalidades por demora en la ejecución. Dada la especial naturaleza del contrato, la perentoriedad de los plazos de ejecución del mismo y la imposibilidad de la recuperación de los retrasos en la ejecución, la penalidad será de 150 € diarios por día transcurrido entre la fecha máxima de entrega y la fecha en que efectivamente se realice el suministro.

Estas penalidades ser harán efectivas mediante deducciones de las cantidades que en concepto de pago total o parcial deban abonarse al contratista, o sobre la garantía conforme al artículo 194.2 de la LCSP.

Las penalidades por cumplimiento defectuoso se impondrán con independencia de la obligación que legalmente incumbe a la contratista en cuanto a la reparación de tales defectos.

La imposición de penalidad no excluye la indemnización por daños y perjuicios (art. 194 y 196 de la LCSP).

13. Ofertas con valores anormales o despropocionados.

Las ofertas económicas se considerarán desproporcionadas, anormalmente bajas o temerarias según lo dispuesto en el artículo 85 del RGLCSP, quedando por tanto fuera de la fórmula expuesta aquellas que así queden definidas y que no hayan sido debidamente justificadas según lo previsto en el artículo 149 de la LCSP.

14. En relación a la repercusión y efectos económicos que generará el contrato propuesto.

La actuación proyectada no generará nuevos gastos al provenir de la subvención basada en la Orden TER/836/2022, de 29 de agosto, se aprobaron las bases reguladoras y se efectuó la convocatoria correspondiente a 2022 de subvenciones destinadas a la transformación digital y modernización de las administraciones de las

entidades locales, en el marco del Plan de Recuperación, Transformación y Resiliencia (BOE 1 de septiembre de 2022).