MEMORIA JUSTIFICATIVA PARA LA CONTRATACIÓN DE LA SUSCRIPCIÓN A UN PRODUCTO SOFTWARE PARA LA REALIZACIÓN DE PRUEBAS DE PENETRACIÓN AUTOMATIZADAS (PENTESTING) EN LOS PUESTOS DE USUARIO, SERVIDORES, EQUIPAMIENTO DE COMUNICACIONES Y ELECTROMÉDICO DEL SERVICIO ANDALUZ DE SALUD.

1.- ANTECEDENTES

La creciente complejidad y sofisticación de los ataques cibernéticos, combinado con el aumento de la importancia de los datos confidenciales que se manejan en las instituciones sanitarias, hacen que éstas estén cada vez más en riesgo de sufrir violaciones de seguridad. En este contexto, la progresiva complejidad de los sistemas hace que la gestión de las vulnerabilidades, la evaluación de las medidas de seguridad necesarias y el aseguramiento del cumplimiento normativo sea una tarea cada vez más compleja.

En sus inicios, los test de penetración diseñados para determinar el alcance de los fallos de seguridad de un sistema, denominados pentesting, eran principalmente un proceso manual, que requerían una gran cantidad de tiempo y esfuerzo para identificar y explotar las vulnerabilidades en un sistema. Ante esta situación, el mercado tecnológico ha proporcionado una nueva categoría de herramientas que vienen a mitigar la problemática expuesta. Estas herramientas, conocidas como herramientas de pentesting automatizado, son relativamente recientes en su concepción, pero están alcanzando un alto grado de aceptación en la industria, ayudando a identificar vulnerabilidades conocidas, escanear redes y sistemas en busca de fallos de seguridad y realizar pruebas de intrusión controladas. Se están desarrollando herramientas cada vez más avanzadas que pueden simular ataques sofisticados, como inyecciones de código, ataques de fuerza bruta y escalada de privilegios, y permiten a los expertos en seguridad evaluar la resistencia de un sistema a una amplia gama de ataques sin la necesidad de realizar cada prueba manualmente.

Así, desde el punto de vista operativo, el uso de las herramientas de pentesting supone los siguientes beneficios:

- Detección automatizada de vulnerabilidades que podrían pasar desapercibidas, ayudando a mejorar la seguridad de los sistemas, haciéndolos más sólidos ante ataques malintencionados.
- Incremento en la completitud y sistematización de las pruebas.
- Ahorro en esfuerzos de personal especializado tanto para la realización de pruebas como para la identificación de las vulnerabilidades y de las medidas de mitigación de éstas, así como de la identificación de falsos positivos.
- Incremento de la capacidad para resistir los ataques malintencionados de las infraestructuras y sistemas informáticos.
- Establecimiento de un círculo virtuoso continuo de detección, remediación y validación.

Estas herramientas ayudan al cumplimiento normativo, ya que, de acuerdo con la política de seguridad TIC

del Servicio Andaluz de Salud, en su Resolución del 8 de abril de 2021, de la Dirección Gerencia del Servicio Andaluz de Salud, que aprueba la Política de Seguridad de las Tecnologías de la Información y la Comunicación del Servicio Andaluz de Salud, el SAS expresa su compromiso con la gestión de la seguridad TIC para responder a la obligación recogida en el artículo 10 del Decreto 1/2011, modificado por el Decreto 70/2017, cumpliendo además a las obligaciones establecidas por el Esquema Nacional de Seguridad (ENS).

El objetivo último de la Política de Seguridad TIC es garantizar la calidad de la información y la prestación continuada de los servicios para que el SAS pueda cumplir sus objetivos. Para ello, y según el *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad*, en las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

I. Seguridad integral, entendida como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el Sistema.
II. Gestión de riesgos, donde el análisis de éstos será parte esencial del proceso de seguridad, y cuya gestión dará lugar al mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables.
III. Prevención, reacción y recuperación, para evitar que las amenazas sobre el mismo no se materialicen y no afecten gravemente a la información que maneja o a los servicios que se prestan.
IV. Líneas de defensa, estableciendo una estrategia de protección constituida por múltiples capas de seguridad;
V. Reevaluación periódica de las medidas de seguridad y actualización permanente de las mismas.
VI. Función diferenciada, donde la responsabilidad de la seguridad TIC estará diferenciada de la responsabilidad del sistema y por tanto de la responsabilidad sobre la prestación de los servicios.

2.- OBJETO DEL CONTRATO

2.1. Objeto del contrato: El objeto de esta contratación lo constituye la suscripción durante doce meses a un producto software para la realización de pruebas de penetración automatizadas (pentesting) para, al menos, 5.000 equipos testeables simultáneamente, estos son, dispositivos de puesto de usuario (PCs, thin clients, terminales móviles y tablets), servidores y equipamiento de comunicaciones y electromédico del Servicio Andaluz de Salud, asegurando que, durante la vigencia del contrato, este producto tiene cubiertos sus requisitos en cuanto a actualización a nuevas versiones del software, acceso a parches y hotfixes, y resolución de las incidencias del producto.

En el art. 16 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, se definen como contratos de suministro aquellos que tienen por

objeto la adquisición, el arrendamiento financiero, o el arrendamiento, con opción a compra o sin ella, de productos o bienes muebles. Y más concretamente, en relación con los productos informáticos, la letra b) del apartado 3 considera que, en todo caso, son contratos de suministro:

"Los que tengan por objeto la adquisición y el arrendamiento de equipos y sistemas de telecomunicaciones o para el tratamiento de la información, sus dispositivos y programas, y la cesión del derecho de uso de estos últimos, en cualquiera de sus modalidades de puesta a disposición, a excepción de los contratos de adquisición de programas de ordenador desarrollados a medida, que se considerarán contratos de servicios".

La Comisión Consultiva de Contratación Administrativa de la Junta de Andalucía en su informe 10/2009, consideró que:

"La adquisición del derecho de actualizaciones y soporte software de las licencias del producto, y la entrega y acceso a los parches y correcciones de errores relativas a dicho software así como el acceso a las nuevas versiones liberadas, entrarían dentro del concepto de suministro".

Por otro lado, la Junta Consultiva de Contratación Pública del Ministerio de Hacienda y Función Pública (JCCAMEH), en su informe 4/16, haciendo referencia a las prestaciones que se suelen incluir en el servicio de garantía de soporte consideró lo siguiente:

"(...) la actualización de un programa estandarizado no conlleva ningún tipo de actuación compleja sino tan sólo la mejora, el parcheado o la corrección de fallos (bugs fixing) en el mismo. Esto forma parte del desarrollo normal de cualquier programa estandarizado del que se venden licencias de uso tales como sistemas operativos, paquetes de procesamiento de textos, tablas de cálculo, etc."

Dado que las prestaciones del contrato no incluyen labores de actualización complejas adicionales, propias de un contrato de servicios, cabe concluir que este expediente es un contrato de suministro, al amparo lo mencionado en el artículo 16.3.b) de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

El Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público, aun habiendo sido derogada por la Ley 9/2017 de Contratos de Sector Público siendo la norma vigente, no determina expresamente la calificación jurídica de los contratos de actualización de software estandarizado.

2.2. CPV: 48517000-5 Paquetes de software de TI

2.3. Determinación del tipo de suministro: suministro por cuantía determinada, al amparo del artículo

16.3.b) de la Ley 9/2017, de 8 noviembre, de Contratos de Sector Público.

2.4. División en lotes: dada la naturaleza indivisible del objeto del contrato se justifica su no división en lotes, de acuerdo con el artículo 99.3 de la Ley 9/2017, de 8 noviembre, de Contratos de Sector Público.

El objeto del presente contrato se constituye como una actuación global e integrada, definiéndose como una única prestación la suscripción a una herramienta de una única tipología, por lo que no es procedente ni adecuado la división por lotes en tanto en cuanto el objeto se circunscribe a un único tipo de suministro, de forma que no hay tareas o partes de la prestación que puedan hacerse de forma separada sin poner en riesgo la correcta ejecución del mismo. Dado que es un único producto a suministrar, por su naturaleza y tipificación, su división dificultaría la correcta coordinación de las actividades necesarias para la gestión de su activación y eventuales incidencias que pudieran producirse. Si cada una de las licencias se adjudicara a diferentes personas licitadoras, la administración y gestión de ellas se complicaría sensiblemente, pudiendo tener incluso fechas diferentes de validez de unas a otras. Además, siendo un único proveedor, se obtienen mejores precios por volumen de venta, produciéndose así una racionalización del gasto del sector público. Por otra parte, la no división en lotes no se efectúa ni en perjuicio ni en beneficio arbitrarios de alguna persona licitadora o tipo de licitador, y tampoco se restringe injustificadamente la competencia.

2.5. Necesidades administrativas a satisfacer e idoneidad del objeto: Este contrato es necesario para garantizar que los sistemas informáticos del SAS puedan ser testeados automáticamente de forma simultánea, aumentando su seguridad y mejorando la velocidad de detección de vulnerabilidades, de manera que, la información en general y los sistemas TIC en particular, estén protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Además, debe asegurarse el cumplimiento de las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, realizando un seguimiento continuo, analizando las vulnerabilidades reportadas y preparando una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

En caso de no contar con esta herramienta, los sistemas seguirán siendo testeados de manera manual, por lo que tendrán falta de consistencia en las pruebas que implicaría variabilidad en los resultados. Adicionalmente, los sistemas cuyas vulnerabilidades no hayan sido correctamente identificadas pueden ser puerta de entrada a ciberdelincuentes y poner en riesgo el resto de los sistemas informáticos del SAS y, por ende, la continuidad asistencial y la seguridad del paciente.

A tal efecto, el objeto, el contenido y procedimiento elegido, mediante el contrato proyectado, son los idóneos para su satisfacción.

2.6. Centros vinculados al contrato: Todos los centros del Servicio Andaluz de Salud.

3.- FORMA DE ADJUDICACIÓN

3.1. Procedimiento de licitación: Según el artículo 116.4.a) de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, el procedimiento de licitación utilizado será el abierto, porque los suministros contemplados en este expediente de contratación pueden ser realizados por distintos operadores/proveedores del mercado. Así, todo empresario que cumpla los requisitos establecidos podrá presentar oferta, lo que a su vez favorecerá la consecución de una mejor relación calidad/precio obtenida como consecuencia de la concurrencia y libre competencia de distintos proveedores.

3.2. Tipo de tramitación: ordinaria.

4.- PLAZO DE DURACIÓN DEL CONTRATO Y DE EJECUCIÓN DE LA PRESTACIÓN

4.1. Fecha de inicio del contrato: desde la formalización.

4.2. Duración del contrato: 1 mes desde su formalización.

4.3. Plazos parciales: no.

5.- PRESUPUESTO BASE DE LICITACIÓN Y VALOR ESTIMADO

5.1. Sistema de determinación del precio: La determinación del precio del suministro objeto de esta contratación se realizará a tanto alzado.

5.2. Presupuesto base de la licitación (IVA incluido): 212.960,00 €
IVA (21 %): 36.960 €

5.3. Resumen de los costes directos e indirectos y otros eventuales gastos calculados para la determinación de los precios de licitación. Adecuación a precios de mercado.

Atendiendo a lo estipulado en la Instrucción 1/2023, de 4 de mayo de 2023, de la Agencia Digital de Andalucía sobre perfiles, precios de referencia y desglose de costes en contratos de bienes y servicios TIC, cuyo objetivo principal es determinar la información de referencia para la elaboración de la documentación de licitación de bienes y servicios TIC por parte de las entidades incluidas en su ámbito de aplicación, a continuación, se determina el desglose del precio de las partidas de las que se compone el presente contrato de suministros de bienes de naturaleza TIC.

Metodología utilizada

Para obtener el desglose del presupuesto base de licitación diferenciando los costes directos, indirectos y

otros eventuales gastos, conforme a lo preceptuado por el artículo 100.2 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, se considera la metodología definida en el libro "La determinación del precio en los contratos públicos con base en el coste"[1] para estimar los Gastos Generales y el Beneficio Industrial de una empresa en función de su sector de actividad.

Para ello, se tienen en cuenta los datos de las ratios sectoriales publicados por la Central de Balances del Banco de España (CenBal)[2], concretamente las siguientes:

- R01: valor añadido/cifra neta de negocios (margen bruto en %)
- R02: gasto de personal/cifra neta de negocios (en %)
    - Se estimará en cada caso un peso para los gastos de personal directamente imputables a la ejecución del contrato según su tipología (gpd).
- R03: resultado económico bruto/cifra neta de negocios (en %)
- R14: inmovilizado material/total activo fijo (en %)

Con estas ratios se calculan los datos necesarios aplicando las siguientes fórmulas establecidas en la citada metodología:

Beneficio Industrial = R03
Gastos Generales de Estructura = 100 – Costes Directos – beneficio industrial.
Costes Directos = ((100 – R01) x (1 – R14 /100)) + (gpd x R02)

Cálculo para el desglose de costes en suministros TIC

Para aplicar la metodología descrita a las contrataciones de suministros TIC y obtener los parámetros aplicables a la estructura de costes y margen de beneficio industrial de las empresas licitadoras de este tipo de contratos se han tenido en cuenta las ratios sectoriales publicadas por la Central de Balances del Banco de España (CenBal) para el sector de actividad "G465: Comercio al por mayor de equipos para las tecnologías de la información y las comunicaciones" para el año 2021, incluyendo todos los volúmenes de facturación agregados. Para cada ratio empleada en el cálculo se ha tomado el valor Q2, que se corresponde con la mediana de la serie estadística.

[1] Juan Carlos Gómez Guzmán. 2018. "La determinación del precio en los contratos públicos con base en el coste". Editorial Wolters Kluwer.

[2] Disponibles en Internet para descarga libre y gratuita a través de la URL http://app.bde.es/rss_www/Ratios

Ratio	Nombre de Ratio	Q2
R01	Valor añadido/Cifra neta de negocios	21,07 %
R02	Gastos de personal/Cifra neta de negocios	15,84 %
R03	Resultado económico bruto/Cifra neta de negocios	3,65 %
R14	Inmovilizado material/Total activo fijo	4,63 %

Tabla. Ratios consideradas para el cálculo del desglose de costes en contratos de suministros TIC

Se considera que, del total de gastos de personal de la empresa (RO2 = 15,84% sobre el total de la cifra de negocio), la proporción directamente imputable a la ejecución del contrato es únicamente del 40% (gpd=0,4) de dichos gastos, al ser los suministros una actividad poco intensiva de mano de obra (transporte -en su caso-, instalación y garantía).

De este modo, se obtiene la siguiente estructura de costes:

- **Gastos Generales de Estructura**: 14,74% del presupuesto de ejecución material.
- **Beneficio Industrial**: 3,65% del presupuesto de ejecución material.

Los **costes directos** supondrán, por tanto, un 81,86%.

Las tablas siguientes muestran los cálculos realizados en base a la metodología descrita:

Cifra de ventas:		
Actividad G465 Comercio al por mayor de equipos para las tecnologías de la información y las comunicaciones		
	%	(€)*
(a) Valor de las ventas = (b)+ (c) + (d)	**100%**	**176.000,00 €**
R01: Valor añadido / cifra neta de negocios	21,07%	37.083,20 €
R02: Gastos de personal / cifra neta de negocios	15,84%	27.878,40 €
R02 directa = 0,40 x R02	6,34%	11.158,40 €
R02 indirecta = 0,60 x R02	9,50%	16.720,00 €
(b) Total coste de ventas = costes directos + GGF ((a)-R01)	**81,61%**	**143.636,31 €**
(c) Gastos generales de estructura = (a)-(b)-(d)	**14,74%**	**25.939,69 €**
(d) R03 Resultado de explotación/beneficio industrial	**3,65%**	**6.424,00 €**

* Valores IVA no incluido

Respecto a la estructura de costes en directos e indirectos, y sin que las cuantías cambien, se ha considerado el siguiente desglose:

Concepto	Total
Costes directos (81,86%)	**144.073,60 €**
- Costes directos de personal (6,34%)	11.158,40 €
- Otros costes directos (75,52%)	132.915,20 €
Costes indirectos (14,49%)	**25.502,40 €**
- Costes indirectos de personal (9,5%)	16.720,00 €
- Otros costes indirectos (4,99%)	25.939,69 €
Beneficio industrial (3,65%)	**6.424,00 €**
Total (IVA no incluido)	**176.000,00 €**

A partir de estos datos, los importes desglosados son los que se indican en el siguiente cuadro:

ARTÍCULO	Costes Directos *	Costes indirectos*	Resultado de la explotación / Beneficio industrial *	% de IVA	Importe IVA	Importe (IVA incluido)
Suscripción Pentesting	144.073,60 €	25.502,40 €	6.424,00 €	21	36.960,00 €	212.960,00 €

* Valores IVA no incluido

La estructura de costes viene dada por los siguientes conceptos:

- Costes directos:
  - Coste de la herramienta.
  - Coste de nuevas versiones del software, parches y hotfixes.
  - Mano de obra de los trabajadores que se dedican a los servicios de garantía y asistencia técnica multicanal del producto.
  - Dietas y otros gastos directos asociados.
- Costes indirectos (tanto los costes indirectos de producción como los estructurales):
  - Seguros (responsabilidad civil, incendios, vehículos, etc.).
  - Apoyo de personal de dirección, técnico y/o administrativo.
  - Gasto de las oficinas centrales/delegación.
  - Servicios bancarios.
  - Publicidad.
  - Impuestos.
- Beneficio industrial.

5.4.- Valor estimado (presupuesto base licitación, IVA excluido): 176.000,00 €, que se corresponde con el presupuesto base de licitación, IVA excluido, de conformidad con lo establecido en el artículo 101 de la Ley,

9/2017, de 8 noviembre, de Contratos de Sector Público.

CONCEPTO	PRESUPUESTO BASE DE LICITACIÓN (IVA EXCLUIDO)	TOTAL
Suscripción a una herramienta de Pentesting automatizado	176.000,00 €	176.000,00 €
TOTAL, VALOR ESTIMADO (IVA no incluido)		**176.000,00 €**

El jefe del servicio de informática
Fdo.: Rafael Pastor Saénz