



metro bilbao

**Pliego de Prescripciones Técnicas para la contratación
del Servicio de "Implantación de un Sistema para la
gestión y reducción del riesgo de ciberataques"**

24-LG-DC-166

Versión 2
06/08/2024



Cuadro de Características

1. Objeto del contrato:

Contratación de la implantación y de las licencias de uso por un año de un sistema software que simule ataques informáticos y realice una priorización de actuaciones desde el punto de vista del riesgo para corregir ordenadamente los problemas de seguridad detectados.

2. Pliego de Prescripciones Técnicas:

24-LG-DC-124

3. Pliego de Cláusulas Administrativas:

20-LG-DC-016

4. Volumen del contrato:

El volumen de contrato en ningún caso será superior a 50.000 € para un (1) año de duración del contrato.

5. Normas específicas:

No procede.

6. Duración del contrato:

Un (1) año.

7. Fecha de Inicio:

Diciembre de 2024.

8. Requisitos de solvencia:

Se definen los siguientes requerimientos mínimos:

- Los participantes deberán acreditar su **solvencia económica y financiera** mediante:
 - Declaración sobre el volumen global de negocios, referido al mejor de los últimos tres ejercicios disponibles en función de la fecha de creación o de inicio de actividades del empresario, en la medida de que disponga de las referencias de dicho volumen de negocios, de **al menos setenta y cinco mil euros anuales (75.000 €/anuales)**. Deberán especificar el importe facturado anualmente en este tipo de suministros.



- Los licitadores deben acreditar su **solvencia técnica** en base al cumplimiento de todos los requisitos que se enumeran a continuación a través de los medios que se señalan en cada caso:
 - Relación servicios similares ejecutados en el curso de los últimos tres años avalados por certificados de buena ejecución. Estos certificados indicarán las fechas y el lugar de ejecución de los servicios y se precisará si se llevaron normalmente a buen término; en su caso dichos certificados serán comunicados directamente al órgano de contratación por la autoridad competente. **Se aportarán certificados de buena ejecución** de servicios similares al objeto del contrato, que acrediten haber realizado al menos un proyecto de implantación del mismo sistema, emitidos por las empresas correspondientes, acreditando un **volumen de al menos 50.000 € en el mejor de los últimos tres ejercicios disponibles**.
 - Las empresas licitadoras deberán acreditar estar certificadas en el **Esquema Nacional de Seguridad mínimamente a nivel medio**.

Metro Bilbao se reserva el derecho de comprobar la validez de las referencias, por lo que se deberá incluir un interlocutor y un teléfono/correo electrónico de contacto en los certificados de buena ejecución entregados.

Nota importante:

Las **acreditaciones del cumplimiento de los requisitos** solicitados en el punto 8 deben incluirse en el **sobre nº1** de la oferta (Documentación administrativa). En aquellas ofertas que no lo hagan así, no se abrirán el resto de los sobres.

Los citados requisitos podrán ser inicialmente presentados mediante declaración responsable (DEUC), que se incluye en la convocatoria del procedimiento. Posteriormente, al adjudicatario se le solicitará acreditación documental de todos los extremos declarados.

Caso de solicitarse expresamente la presentación física de ofertas, será obligatorio presentar **copia en formato electrónico** de la oferta **en cada uno de los sobres** presentados, según lo indicado en el Pliego de Cláusulas Administrativas.

En caso de empate en la puntuación TOTAL, se otorgará un (1) punto extra a la oferta que, al vencimiento del plazo de presentación de ofertas, incluya medidas de carácter social y laboral que favorezcan la igualdad de oportunidades entre hombres y mujeres, disponer y acreditar; y sistemas auditables de Responsabilidad Social Corporativa (RSC), disponer y acreditar.

9. Fecha límite de presentación de ofertas:

Las 12:00 h del 29 de octubre de 2024.



10. Criterios de valoración de las ofertas:

Criterios evaluables mediante fórmula: 100 puntos

✓ **Criterio 1: Oferta económica. 100 puntos**

Como valor de la oferta de la empresa licitadora (O_{lic}) se utilizará el Total Oferta especificado en el Anexo-1.

$$P_{lic} = (O_{min} / O_{lic}) \times P_{tot}$$

Siendo:

P_{lic} : Puntuación que obtiene la empresa licitadora.

O_{min} : Oferta mínima de las presentadas y admitidas.

O_{lic} : Oferta de la empresa licitadora.

P_{tot} : Puntuación total máxima del criterio evaluable mediante fórmula.

11. Presentación de la oferta económica:

De acuerdo al modelo del Anexo 1.

12. Revisión de precios:

No procede.

13. Fianza definitiva:

2.500 €.

14. Póliza de Responsabilidad Civil:

No procede.

15. Tratamiento de datos personales:

En el objeto de esta licitación no se realiza tratamiento de datos personales.



Índice

1. Objeto	6
2. Características del Proyecto	6
2.1 Antecedentes.....	6
2.2 Alcance	6
2.3 Requisitos que debe cumplir el nuevo sistema.....	6
2.4 Requisitos de seguridad que debe cumplir el sistema.....	11
2.5 Organización del Servicio.....	12
2.6 Soporte de la herramienta.....	12
2.7 Documentación de los trabajos.....	12
2.8 Composición del Equipo de Proyecto.....	12
2.9 Facturación.....	12
2.10 Propiedad Intelectual	13
2.11 Secreto y Confidencialidad.....	13
3. Elaboración de Propuestas	14
3.1 Información a incluir en el sobre 1 (oferta administrativa).....	14
3.2 Información a incluir en la Oferta Económica	14
4. Resolución.....	15
Anexo 1: Modelo de Propuesta Económica y Cuadro de Precios	16



1. Objeto

Definir un marco de actuación que nos permita establecer las condiciones tanto técnicas como económicas de cara a la contratación de la implantación, de las licencias de uso y del mantenimiento por un año de un sistema software que simule ataques informáticos y realice una priorización de actuaciones, desde el punto de vista del riesgo, para corregir cada problema de seguridad detectado.

2. Características del Proyecto

2.1 Antecedentes

Metro Bilbao requiere tener a su disposición en cada momento el conocimiento de su postura de seguridad para de esa forma poder minimizar sus riesgos y evitar que sus activos digitales más críticos sean alcanzados en un ciberataque.

2.2 Alcance

A efectos de esta licitación, se considerarán las siguientes tareas:

- ✓ Implantación del sistema. El adjudicatario deberá realizar todas las tareas necesarias para implantar el nuevo sistema e integrarlo en la infraestructura tecnológica y de seguridad de Metro Bilbao.
- ✓ Licencias de uso y mantenimiento del sistema por un año de duración.
- ✓ El sistema a implantar debe de gestionar el riesgo de mínimamente 100 servidores y 1.000 Workstation.

2.3 Requisitos que debe cumplir el nuevo sistema

La identificación del usuario debe de ser realizada por el directorio activo corporativo de Metro Bilbao, por lo que el sistema debe de estar integrado con dicho directorio activo.

La solución deberá soportar la autenticación multifactor (MFA) para verificar la identidad de un usuario requiriendo múltiples credenciales (por ejemplo, OTPs, TOTP, tarjetas inteligentes, dispositivos USB, otros dispositivos...).

Alcance de la Simulación

La solución deberá permitir implementar escenarios de simulaciones realistas alineados con los riesgos y el contexto de Metro Bilbao y confirmar qué amenazas pueden comprometer nuestros entornos.



La simulación del ataque debe hacerse de forma absolutamente segura, sin atacar ni comprometer la infraestructura de Metro Bilbao y sin generar alertas que impacten en las operaciones del SOC.

La simulación de ataques debe hacerse de manera continua (24x7) en el 100% de la infraestructura donde se haya desplegado.

La simulación del ataque deberá mostrar vectores de ataque basándose en:

- Vulnerabilidades
- Configuraciones erróneas: Credenciales almacenadas en memoria, Servicios habilitados, Puertos abiertos
- Actividades del usuario: Ejecuciones de archivos, Conexiones RDP, Cambios en la red

La simulación debe validar las condiciones del 100% de las técnicas y métodos de ataque conocidos cada vez que se ejecute

Posibilidades de configuración de la Simulación

La simulación de ataques debe permitir la creación de un número ilimitado de escenarios de ataque. Esos escenarios deben tener:

- Enfoque estático:
 - Desde un dispositivo/máquina específica a un dispositivo/máquina específica.
 - Desde un grupo específico de usuarios a un grupo específico de máquinas
- Dinámico: desde una máquina que sospechamos que puede estar comprometida a todos nuestros activos críticos

La simulación de ataque debe permitir definir los activos críticos. Estos pueden ser:

- Un servidor específico, una estación de trabajo
- Una subred específica
- Credenciales específicas, usuarios o grupos de usuarios
- Fichero específico
- Sistema operativo específico

La solución debe tener una interfaz totalmente visual que:

- Muestre todos los dispositivos del entorno



- Pueda reproducir los ataques simulados
- Se puede consultar el contexto de los dispositivos
- Muestra todos los pasos de una ruta de ataque

Simulación de ataques

Es necesario que la solución sea capaz de:

- Simular continuamente la actividad de un atacante real aprovechando la desconfiguración, la actividad del usuario y las vulnerabilidades sin interferir en las operaciones del SO
- Identificar y mapear los puntos de congestión en la red que tienen el mayor impacto en los activos críticos
- Descubrir en tiempo real nuevos problemas de seguridad que pongan en riesgo los activos críticos, por ejemplo: mostrar el movimiento lateral
- Proporcionar un desglose detallado de cada paso de la ruta de ataque y descubrir eventos que los grupos APT pueden aprovechar
- Simular continuamente vectores de ataque en entornos complejos, híbridos, multi-cloud y segmentados
- Simular el impacto de las medidas de corrección sugeridas
- Ejecutar de forma segura sin afectar a la continuidad del funcionamiento del entorno de producción mediante el control del consumo de recursos
- Simular un ataque basado en contenidos compartidos (infecciones de archivos, por ejemplo, exe, bat, dll, sh, pdf, scripts, office)
- Simular técnicas de ataque basadas en la actividad de los usuarios, como el secuestro de la sesión RDP, la navegación web o los medios de almacenamiento móviles
- Encontrar las causas fundamentales que afectan a la postura global de seguridad

Simulación de ataque específica para la nube

Para los entornos de nube, la solución debe concentrarse en

- Demostrar los riesgos de los usuarios/roles sensibles para los servicios críticos y la mejor manera de proteger a esos usuarios/roles
- Exponer los vectores de ataque del entorno on premise a la nube de forma continua



- Identificar el riesgo de las entidades de la nube con dirección pública y si sus perfiles pueden acceder a recursos sensibles en la nube
- Mostrar el entorno de la nube y las entidades automáticamente en un mapa de red interactivo

Informes

- Generar un informe continuo que muestre
 - Puntuación de riesgo global
 - Puntuación de riesgo para cada escenario definido
 - Número de activos críticos expuestos
 - Vectores de ataque que afectan a los activos críticos de Metro Bilbao
 - Tendencia de la evolución de la puntuación de riesgo para cada escenario en intervalos de tiempo configurables
- Debe disponer de diferentes niveles de informes dentro de la solución
 - Nivel ejecutivo
 - Nivel técnico
 - Informes y cuadros de mando personalizables
- El cuadro de mando necesita proporcionar:
 - Evaluación de los principales riesgos
 - Principales activos críticos en riesgo según su complejidad
 - Principales puntos de interés que influyen en los activos críticos
- Técnicas de ataque de mayor impacto en la infraestructura de Metro Bilbao
- Debe identificar y destacar los activos más débiles que se utilizan en los escenarios de ataque
- Priorizar la aplicación de parches a las vulnerabilidades en los activos más importantes
- Evaluar continuamente la postura de seguridad y su mejora

Remediación

La herramienta deberá de:



- Generar instrucciones prácticas de remediación adaptadas al entorno
- Proporcionar un enfoque en los consejos de remediación más eficaces para reducir el riesgo de manera efectiva
- Priorizar la aplicación de parches de vulnerabilidad en los puntos débiles más importantes que afectan a los activos críticos
- Priorizar la remediación en base a los riesgos para los activos críticos y centrar su atención en los pasos de remediación para garantizar que esos activos estén asegurados en primer lugar y luego centrarse en otras prioridades
- Simular el impacto de las acciones de remediación de forma anticipada
- Proporcionar un plan de acción paso a paso con las capturas de pantalla pertinentes y los KB externos

Supervisión continua de los controles de seguridad

La herramienta debe proporcionar:

- Una puntuación sobre las configuraciones de las herramientas de seguridad actuales usadas en Metro Bilbao y presentar el estado de optimización de esas herramientas basándose en las mejores prácticas de los fabricantes y en las recomendaciones del sector
- Una evaluación casi en tiempo real de todos sus dominios de seguridad y recomendaciones para mejorar en base a marcos reconocidos por la industria y controles de seguridad críticos. Los dominios de seguridad deben incluir
 - Gestión de cuentas
 - Defensa contra el malware
 - Seguridad de Red
 - Seguridad de aplicaciones
 - Seguridad de datos
 - Gestión de incidentes
- Proporcionar un programa continuo de ciberseguridad, un análisis de deficiencias y una gestión de la mitigación de riesgos para mejorar el entorno de seguridad de Metro Bilbao
- Proporcionar análisis y alertas continuas en caso de desviación del comportamiento normal aprovechando la supervisión de las herramientas y los dominios de seguridad



- Permitir una integración simple con las herramientas de seguridad e infraestructura más comunes a través de la API

Actualizaciones y mejoras

- La base de datos de vulnerabilidades se debe actualizar diariamente
- Las actualizaciones se deben publicar en correlación con las principales técnicas de ataque explotables desde campo
- Posibilidad de actualizar los componentes del producto de forma totalmente controlada .

2.4 Requisitos de seguridad que debe cumplir el sistema

El fabricante de la solución deberá estar certificado en la ISO 27001.

Sólo aquellos usuarios a los que se les haya concedido acceso de manera explícita tendrán acceso a la herramienta.

Se registrarán las actividades de los usuarios en el sistema, indicando quien realiza la actividad, cuándo la realiza y sobre qué información. Se incluye la actividad de los usuarios y, especialmente, la de los operadores y administradores en cuanto puedan acceder a la configuración y actuar en el mantenimiento del sistema.

Para la Identificación y prevención de posibles amenazas, el software deberá de disponer de una ubicación donde se publiquen las vulnerabilidades conocidas, así como de instrucciones de cómo subsanarlas o en su defecto cómo evitar que sean explotadas.

El sistema debe permitir realizar Copias de Seguridad del mismo de tal forma que ante cualquier eventualidad, Metro Bilbao sea capaz de restaurar a la última copia realizada.

En el caso de que la aplicación sea WEB, se garantizará la imposibilidad de acceder a la información obviando la autenticación, en particular tomando medidas en los siguientes aspectos:

- Se evita que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado
- Se previenen ataques de manipulación de URL
- Se previenen ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como "cookies"
- Se previenen ataques de inyección de código
 - Se previenen intentos de escalado de privilegios
 - Se previene ataques de "cross site scripting"



2.5 Organización del Servicio

Metro Bilbao tendrá un responsable del proyecto que deberá ser reportado por el adjudicatario de cualquier cambio en los parámetros generales de prestación del servicio. Además, Metro Bilbao nombrará una persona responsable de la coordinación del servicio que será responsable del seguimiento y control de las tareas objeto de la presente licitación.

Por su parte, la empresa adjudicataria deberá proponer sus estructuras operativas y de control para prestar su servicio y realizar el seguimiento y control del mismo basándose en una propuesta de reuniones / informes que se debe especificar en la oferta y que será consensuada posteriormente. En dicha oferta será imprescindible que mínimamente conste de un responsable del servicio que velará por el cumplimiento de las condiciones acordadas en el contrato y que se encargue de realizar el seguimiento de la correcta ejecución del servicio.

La interlocución entre Metro Bilbao y el equipo de trabajo designado por el adjudicatario se realizará en cualquiera de las lenguas oficiales de la Comunidad Autónoma del País Vasco.

2.6 Soporte de la herramienta

La empresa adjudicataria deberá de proporcionar todos los medios hardware y software necesarios para prestar adecuadamente el servicio requerido. Para ello el licitante deberá incluir el compromiso de soporte del fabricante de la herramienta.

2.7 Documentación de los trabajos

Se realizará una documentación detallada del sistema implantado, así como una sesión explicativa de dicha documentación al personal que Metro Bilbao designe.

2.8 Composición del Equipo de Proyecto

En la fase de adjudicación se fijará el Equipo de Proyecto propuesto por el proveedor en su oferta. Las modificaciones posteriores a la composición inicial del mismo deberán hacerse previo consenso entre las dos partes, sin que quede afectada la normal dinámica de trabajo adoptada.

2.9 Facturación

La empresa adjudicataria facturará el 50% del importe de implantación a la firma del contrato y el 50% restante al finalizar la implantación. Facturará el 100% del importe de las licencias y mantenimiento cuando se habilite la herramienta para su uso a Metro Bilbao.



2.10 Propiedad Intelectual

Toda la documentación, metodología, programas fuente y ejecutables a que la empresa adjudicataria tenga acceso a través de la prestación de los servicios contratados, tanto lo que exista en la actualidad, como lo que se genere durante la vigencia del contrato, es propiedad de Metro Bilbao y por tanto, se encuentra protegida por la legislación vigente en materia de propiedad intelectual. Se prohíbe la modificación, copia, reproducción, descarga, transmisión o cesión, distribución o transformación de todo ello, sin autorización expresa y por escrito de Metro Bilbao.

Queda asimismo prohibido descompilar, desensamblar, realizar ingeniería inversa, sublicenciar o transmitir de cualquier modo, traducir o realizar obras derivadas de los programas de ordenador de Metro Bilbao, así como realizar, respecto a todo o parte de tales programas, cualesquiera de los actos de explotación referidos en el párrafo anterior. La empresa adjudicataria deberá abstenerse en todo caso de suprimir, alterar, eludir o manipular cualquier dispositivo de protección o sistemas de seguridad que puedan estar instalados.

2.11 Secreto y Confidencialidad

Además de lo recogido en la legislación aplicable, Metro Bilbao podrá dictar otras directrices relativas a la seguridad y confidencialidad en la prestación de los servicios.

La empresa licitadora describirá en su oferta los métodos y procedimientos establecidos en relación a las medidas de seguridad adoptadas y el nivel de protección aplicado a la información relativa a Metro Bilbao.

Asimismo, la empresa licitadora se obliga a tomar todas las medidas necesarias para garantizar el secreto más absoluto sobre la información perteneciente a Metro Bilbao, sobre los trabajos realizados en el proyecto y, en general, sobre todos los servicios prestados a Metro Bilbao en virtud de este acuerdo. Dicha información sólo podrá ser comunicada a las personas designadas para el presente proyecto. El personal de la empresa licitadora deberá conocer y respetar dichas normas de secreto y confidencialidad.

Cualquier comunicación a personas distintas de las participantes en el proyecto estará supeditada a la autorización previa de forma expresa y por escrito de Metro Bilbao.

No está permitido sacar información en ningún tipo de soporte de las instalaciones de Metro Bilbao.

La empresa licitadora se compromete a mantener en secreto los términos y condiciones del presente acuerdo y a no reproducir, entregar, desvelar o poner a disposición de terceros cualquier información relativa al mismo.



La empresa licitadora estará obligada a guardar las normas vigentes sobre propiedad intelectual y documentación que por necesidades del contrato se vea obligado a manejar.

3. Elaboración de Propuestas

Durante el período de preparación de las ofertas, todas las dudas se remitirán al correo electrónico admin_mb@metrobilbao.eus.

Se facilitará el acceso de las empresas licitadoras que lo soliciten a las instalaciones de Metro Bilbao para obtener toda la información que consideren necesaria, no pudiendo alegarse posteriormente el desconocimiento de la misma, ni modificar por tal motivo su oferta o el correspondiente contrato en caso de adjudicación.

El licitante deberá presentar la documentación de las ofertas en:

<https://apps.euskadi.eus/appcont/lizitazioa>

En caso de problemas técnicos para cargar las ofertas solicitar ayuda en el tlf.: 945016298.

La propuesta deberá cumplimentarse de acuerdo a las especificaciones del presente pliego y del Pliego de Cláusulas Administrativas 20-LG-DC-017.

La empresa ofertante deberá presentar la documentación que se indica en los apartados siguientes.

3.1 Información a incluir en el sobre 1 (oferta administrativa)

Además de la solicitada en el pliego administrativo 20-LG-DC-016, se presentará una memoria técnica detallando el producto ofertado, de cara a poder verificar el cumplimiento de las características técnicas solicitadas en el presente pliego.

3.2 Información a incluir en la Oferta Económica

Se ofertará de acuerdo con el modelo de Propuesta Económica y Cuadro de Precios que se adjunta como Anexo 1.

El precio ofertado será un precio máximo y no modificable, en el que se habrán incluido todos los conceptos como traslados, portes, etc.

Valoración, si procede, del plan de transición del servicio propuesto.

El I.V.A. se facturará aparte.



4. Resolución

Metro Bilbao adjudicará el proyecto en base a la mejor oferta económica y técnica, según los criterios indicados en el cuadro de características, y condicionando la adjudicación a que la empresa suscriba y formalice la documentación contractual que Metro Bilbao redacte al efecto.

Una vez resuelta la adjudicación, se notificará el resultado de la misma a todas las empresas que hayan participado en el proceso.



Anexo 1: Modelo de Propuesta Económica y Cuadro de Precios



Modelo de Proposición Económica:

D./Dña..... con DNI.....en nombre de.....con domicilio a efectos de notificaciones en....., y CIF.....

DECLARO:

I.- Que he quedado enterado del procedimiento para la adjudicación del contrato que tiene por objeto la contratación del servicio de Implantación de un sistema para la Implantación de un Sistema para la gestión y reducción del riesgo ante ciberataques.

II.- Que igualmente conozco el Pliego de Prescripciones Técnicas, el Pliego de Cláusulas Administrativas y demás documentación que debe regir el presente contrato, que expresamente asumo y acato en su totalidad, sin salvedad alguna.

III.- Que la Empresa a la que represento cumple con todos los requisitos y obligaciones exigidos por la normativa vigente para su apertura, instalación y funcionamiento, y que en la elaboración de la oferta se han tenido en cuenta todas las obligaciones derivadas de las disposiciones vigentes en materia de protección de empleo, condiciones de trabajo y prevención de riesgos laborales y protección del medio ambiente.

IV.- Que en relación con la prestación de la presente oferta, propongo la realización de los trabajos según la tabla adjunta. Dichos importes incluyen todos los tributos, tasas, cánones de cualquier índole que sean de aplicación así como cualquier otro gasto que se derive de la prestación, o que se origine por el empresa adjudicataria como consecuencia del cumplimiento de las obligaciones contempladas en el presente pliego, **A EXCEPCION DEL IVA**, que no será incluido.

En....., a..... de..... de.....

Fdo:
D.N.I.:



Cuadro de Precios

Tabla de precios correspondiente al concurso 24-LG-DC-166

Concepto	Importe
Implantación e Integración en plataforma existente	0,00
Licencias de uso y Mantenimiento por 1 año	0,00
Total Oferta	0,00

El importe **máximo de licitación** es de **50.000 €**.
Todos los precios se ofertarán sin IVA.