CUADRO DE CARACTERÍSTICAS ADMINISTRATIVAS
Suministro de Servicios de ciberseguridad (Categoría 4 del SDA)

CARACTERÍSTICAS ADMINISTRATIVAS

1. **Objeto del contrato. Código CPV. Duración del contrato.**

Objeto: Nueva contratación del Sistema de protección antivirus y de seguridad de endpoints con capacidades EDR/XDR.

Código CPV: 48760000-3

Duración del contrato: 09/07/2024 – 08/07/2025

2. **Importe y presupuesto base de la licitación**.

Justificación del precio: se ha realizado una consulta a diferentes empresas del sector valorando las posibilidades.

El presupuesto base de la licitación es de un máximo de 21.607,09€ IVA incluido, siendo 17.857,10€ de base imponible y 3.749,99€ de IVA, teniendo en cuenta que la duración será de un año.

Concepto	**Cantidad**	**Precio unitario máximo**	**Total (IVA Excluido)**	**Total (IVA Incluido)**
Coste Licencias usuarios MS365	128	31,02€	3.970,56€	4.804,37€
Coste Licencias servidores	94	21,57€	2.027,58€	2.453,37€

Concepto	**Cantidad**	**Precio unitario máximo**	**Total (IVA Excluido)**	**Total (IVA Incluido)**
Servicio SOC 100 puestos y cuentas M365	1	5.653,20€	5.653,20€	6.840,37€
Servicios SOC Servidores	94	49,18€	4.622,92€	5.593,73€
Servicios SOC Usuario con Office 365	28	56,53€	1.582,84€	1.915,23€

3. Plurianualidades

Se contratará por un año

Año	Importe
2024	**8.928,55€**
2025	**8.928,55€**

4. Valor estimado del contrato

El valor estimado del contrato será de como máximo 17.857,10 € IVA excluido.

5. Garantía definitiva

De acuerdo con el artículo 107.1 segundo párrafo de la LCSP, el órgano de contratación puede exigir la constitución de garantía en los contratos específicos.

La adjudicataria deberá constituir una garantía definitiva correspondiente al 5% del presupuesto base de licitación del contrato, IVA excluido.

El plazo de garantía será de seis meses una vez finalizado el contrato de acuerdo con el artículo 111 de la LCSP.

La devolución de la garantía definitiva tendrá lugar durante los dos meses siguientes a que finalice el plazo y una vez haya firmado el acta de conformidad.

6. Lugar y forma de pago

Previa presentación de la factura, se abonará de la siguiente manera al adjudicatario:

- Primer 50% de la factura al inicio del contrato
- Último y segundo 50% a la entrega del proyecto

7. Criterios de valoración.

Mediante precio: se otorgará la máxima puntuación a las proposiciones que ofrecen el precio más bajo. El resto será de manera proporcional teniendo en cuenta las siguientes fórmulas:

<u>Coste Licencias usuarios MS365:</u>

$$Punts = \frac{Oferta\ més\ econòmica}{Oferta\ que\ es\ puntua} * 22\ punts$$

Coste Licencias servidores

$$Punts = \frac{Oferta\ més\ econòmica}{Oferta\ que\ es\ puntua} * 11\ punts$$

Servicio SOC 100 puestos y cuentas M365

$$Punts = \frac{Oferta\ més\ econòmica}{Oferta\ que\ es\ puntua} * 32\ punts$$

Servicios SOC Servidores

$$Punts = \frac{Oferta\ més\ econòmica}{Oferta\ que\ es\ puntua} * 26\ punts$$

Servicios SOC Usuario con Office 365:

$$Punts = \frac{Oferta\ més\ econòmica}{Oferta\ que\ es\ puntua} * 9\ punts$$

CARACTERÍSTICAS TÉCNICAS

1. Características técnicas.

La presente solicitud técnica tiene como objetivo seleccionar un proveedor que suministre un Sistema de Detección y Respuesta Ampliada (XDR) con capacidades de Detección y Respuesta ante Amenazas (EDR) para fortalecer la postura de seguridad. La solución debe incluir los servicios de despliegue, operación de un Centro de Operaciones de Seguridad (SOC), análisis de la postura de seguridad, funcionalidades XDR y protección de endpoint para usuarios y servidores.

La solución presentada debe cubrir:

- Software necesario (licencia anual) que comprenda diversos sistemas operativos (Windows desktop y server, Linux).
- Despliegue sustituyendo otras soluciones anteriores.
- Servicios gestionados de la solución XDR y acción según planes de contingencia específicos en caso de amenazas (SOC).
- Cumplimiento de la legislación vigente en España y Europa.

Requerimientos Específicos

La solución proporcionada deberá cubrir los siguientes puntos:

Servicios de Desarrollo de la Solución:

- Inicialización de la consola de gestión y configuración.
- Creación de políticas según perfiles de usuarios y servidores.
- Despliegue de nuevos agentes y sondas. En el caso de los servidores de producción de manera no automatizada.
- Formación en el equipo de administración.

Servicios SOC:

- Monitorización de seguridad 24/7.
- Servicio CERT para respuesta ante incidentes.
- Generación de informes mensuales de estado de seguridad.

Análisis de la Postura de Seguridad:

- Índice de riesgo desglosado por categorías.
- Representación gráfica en un cuadro de mando.
- Generación de informes ejecutivos de riesgos.
- Integración de información en la plataforma XDR.

Funcionalidades XDR:

- Detección y correlación avanzada de eventos de seguridad.
- Capacidad de investigación de alertas.
- Threat hunting automatizado.
- Ejecución de acciones de respuesta desde la plataforma.

Protección de Endpoint:

- Antimalware avanzado.
- Análisis de reputación web.
- Firewall de host.
- Control de USBs.

- Monitorización de integridad.
- Compatibilidad con el software.
- Compatibilidad con las VPN.

Requisitos de expansión

- Alojamiento de servidores dentro de la Unión Europea.
- Almacenamiento de telemetría y eventos de auditoría mínimo de 30 días.
- API para la gestión programática del producto.
- Integración con servicios de terceros y gestores de identidades.
- Integración y obtención de datos de amenazas a nivel global.
- Soporte para sistemas operativos y aplicaciones específicas (Linux, Windows desktop, Windows Server).
- Integración con el Active Directory.

Requisitos de la Consola de Gestión

La consola de gestión debe cumplir con los siguientes requisitos:

- Autenticación mediante SAML.
- Acceso basado en roles y doble factor de autenticación.
- Integración nativa con vCenter, y opcionalmente, Azure.
- Personalización de cuadros de mando e informes automatizados.

Requisitos de Seguridad

- Detección avanzada de malware y análisis de comportamiento.
- Protección contra ransomware y exploits.
- Análisis de reputación web a nivel de kernel.
- Firewall de host con reglas configurables.

Requisitos de Apoyo y Mantenimiento

- Soporte técnico 24/7 a través de plataforma online y sistema de ticketing
- Actualizaciones regulares de firmas y software.
- Capacidades para el equipo de administración.
- Garantía de disponibilidad y rendimiento.

Otros criterios

Aplicar los principios de seguridad y cumplir con los requisitos de un Esquema Nacional de Seguridad (ENS) en el contexto de una solución XDR (Detección y Respuesta Ampliada) o EDR (Detección y Respuesta a Amenazas) implica adaptar estos aspectos específicos a la naturaleza y las funciones de estas tecnologías, la solución debe tener algunas funciones habituales:

1. **Clasificación de la información**: Clasificar los datos según su nivel de sensibilidad e importancia para la seguridad. Esto puede ayudar a priorizar las alertas y las respuestas a amenazas según su impacto potencial.
2. **Política de seguridad**: Establecer políticas de seguridad específicas para la monitorización, la detección y la respuesta a amenazas mediante XDR/EDR. Esto puede incluir la configuración de reglas de alerta, la definición de procedimientos de respuesta a incidentes y la gestión del acceso a las funcionalidades de la solución a realizar en un equipo conjunto entre IL3-UB y la empresa a partir de los procedimientos habituales y experiencia de la empresa adjudicataria
3. **Gestión del acceso**: Controlar los privilegios de acceso al sistema XDR/EDR para garantizar que sólo los usuarios autorizados puedan visualizar y tomar acciones sobre las amenazas detectadas.
4. **Gestión de las identidades**: Implementar autenticación de dos factores (2FA) u otros mecanismos fuertes de autenticación para proteger el acceso a las consolas de gestión de XDR/EDR.
5. **Cifrado y protección de datos**: Asegurar que los datos almacenados y transmitidos por la solución XDR/EDR estén adecuadamente cifrados para protegerlos del acceso no autorizado.
6. **Gestión de riesgos**: Realizar evaluaciones periódicas de los riesgos de seguridad asociados con la solución XDR/EDR y tomar medidas para mitigarlos.
7. **Monitorización y detección de incidencias**: Configurar las políticas de alerta para detectar actividades sospechosas o potencialmente maliciosas en la infraestructura monitorizada. Además, implementar funcionalidades de respuesta automatizada o guiada para acelerar la mitigación de amenazas.
8. **Formación y concienciación**: Proporcionar formación del funcionamiento de la herramienta a los equipos encargados de gestionar la solución XDR/EDR para garantizar que estén capacitados para utilizar adecuadamente sus funcionalidades e interpretar las alertas generadas. La formación se hará una vez implementada la solución aprovechando las incidencias que se den.
9. **Gestión de continuidad del negocio**: Desarrollar planes de contingencia y de recuperación para asegurar la disponibilidad continua de la solución XDR/EDR en caso de incidentes o fallos del sistema.
10. **Auditoría y revisión**: Realizar auditorías semestrales de la configuración y el uso de la solución XDR/EDR para garantizar el cumplimiento de las políticas de seguridad establecidas e identificar áreas de ampliación o mejora.

Características del servicio de Centro de Operaciones de Seguridad (SOC)

Servicio	Descripción
Monitorización de seguridad	Supervisión constante de los sistemas, la red y las aplicaciones para detectar y responder a amenazas en tiempo real
Análisis de incidencias	Investigación y análisis de las amenazas e incidentes de seguridad para determinar el alcance y la gravedad.
Respuesta a incidentes	Acciones inmediatas para responder a amenazas activas e incidentes de seguridad para minimizar su impacto.

Gestión de vulnerabilidades	Identificación, evaluación y corrección de las vulnerabilidades en los sistemas y aplicaciones.
Análisis forense	Recopilación y análisis de pruebas digitales para comprender el origen y el impacto de los incidentes de seguridad.
Seguridad de la red	Implementación de medidas para proteger la infraestructura de red contra ataques como DDoS o intrusiones.
Seguridad del endpoint	Protección de los dispositivos finales contra amenazas como malware y ransomware
Auditoría de seguridad	Revisión y evaluación de las políticas de seguridad, los controles y las prácticas para garantizar el cumplimiento de los estándares.

Estos servicios ayudan a proteger a las organizaciones contra una amplia gama de amenazas cibernéticas y a responder eficazmente a los incidentes de seguridad cuando se producen.

Certificaciones del producto

GDRP	CC
ENS Alta	CSA Level 2
ISO27001	C5
SOC 2 Type II	FedRAMP

Se acreditarán con una declaración responsable del licitador propuesto adjudicatario.

2. Obligaciones del adjudicatario.

El adjudicatario deberá contar con la capacidad de re vender o contratar a nombre de terceros (distribuidor oficial) el producto solicitante. El producto debe cumplir con los requerimientos de la tabla de características técnicas. Se acreditarán con una declaración responsable del licitador propuesto adjudicatario.

El adjudicatario deberá tener la solvencia contrastada en el cuadrante Gartner EPP 2023 en la zona de Leaders. Se acreditarán con una declaración responsable del licitador propuesto adjudicatario.

Sr. Ruben Colon
Responsable que promueve la necesidad
Reponsable Departamento de TIC

D. Martin Madueño
Responsable del presupuesto
Director Departamento de TIC