CONSULTA PRELIMINAR DE MERCADO

DENOMINACIÓN DEL CONTRATO SOBRE EL QUE SE HACE CONSULTA PRELIMINAR.

Seguridad TIC Perimetral

OBJETO DEL CONTRATO A LICITAR

El objeto del presente contrato es cubrir el ámbito perimetral en la seguridad TIC (Tecnologías de la Información y las Comunicaciones) que son gestionados por el Servicio de Informática y Telecomunicaciones (en adelante, Servicio IT) de la Diputación Provincial de Málaga (en adelante, Diputación), y por los que también se beneficiarán los Ayuntamientos de menos de 20.000 habitantes (en adelante, Ayuntamientos) en muchos de los servicios a contratar al existir una centralización de los mismos.

Al haber múltiples aspectos que afectan a la seguridad y se factible el suministro o la prestación del servicio de forma individualizada sin afectar a la gestión y seguimiento de los contratos, esta contratación se divide en lotes, teniendo en cuenta que toda la infraestructura y elementos serán integrados en una arquitectura en Diputación gestionada y administrada por los técnicos que operan en el Servicio IT. Dentro de los diversos ámbitos de la Seguridad TIC, los lotes que ocupan este contrato son de la esfera “perimetral”, al estar relacionados con la protección en el perímetro en la organización.

Los lotes y una descripción del objeto de cada uno se describen a continuación, detallando las Medidas de seguridad asociadas del Real Decreto 3/2010, de 8 de Enero, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS).

FINALIDAD DE LA CONSULTA PRELIMINAR

Al amparo de lo establecido en el art. 115.1 LCSP, y para una mejor preparación de los pliegos que han de servir de base a la licitación del nuevo contrato, se eleva esta consulta a todos los operadores económicos activos con el fin de que éstos aporten sus respuestas y propuestas.

INFORMACIÓN TÉCNICA.

La prestación a contratar se concreta en los siguientes lotes:

LOTE 1. Servicio de Renovación y Mantenimiento de la Plataforma de Cortafuegos Perimetral.

El objeto de este lote es renovar el licenciamiento de la plataforma de protección perimetral por cortafuegos (*firewalls*) en Diputación, basada en Palo Alto. Esto permitirá mantener la necesaria protección de seguridad sobre los activos, redes y servicios TIC, dejando transitar los flujos de datos previamente autorizados y de un modo seguro, en especial con las redes externas como Internet y sobre la que se usarán túneles VPN (*Virtual Private Network*), y mejorar el rendimiento de su funcionamiento y la velocidad de las interfaces.

Además de ello, permitirá cumplir con las Medidas de seguridad dentro del Real Decreto 3/2010, de 8 de Enero, por el que se regula el ENS, referidas a Perímetro seguro y a la Protección de la confidencialidad.

1.1 ALCANCE.

El alcance de este Lote es la plataforma de cortafuegos (*firewalls*) perimetrales del Servicio IT, formada por 2 equipos Palo Alto, para dar cobertura a las necesidades de Diputación en este nivel de seguridad.

1.2 DESCRIPCIÓN DEL ENTORNO ACTUAL.

El entorno actual está formado por 2 equipos cortafuegos Palo Alto PA-3260, cuyo final de soporte es en Abril de 2021.

1.3 CARACTERÍSTICAS.

El adjudicatario procederá a realizar las siguientes tareas:

a) Renovación de la plataforma de cortafuegos Palo Alto:

Se deberá renovar el licenciamiento de la plataforma de cortafuegos Palo Alto compuesta por 2 equipos PA-2360 en configuración de alta disponibilidad A-P (Activo-Pasivo) y que se usa como protección perimetral de los servicios que se publican desde el Servicio IT.

Por tanto se deberá disponer de los siguientes componentes durante el tiempo de duración del contrato:

- ✓ 2 x cortafuegos Palo Alto PA-3260 en alta disponibilidad, que incluya soporte 24x7 de tipo “Premium” con el fabricante, con NBD para RMAs (*Return Merchandise Authorization*).
- ✓ Funcionalidades para: “Threat Prevention”, “URL filtering”, “Wildfire” y “Global Protect”, todo ello con el licenciamiento correspondiente, con soporte 24x7.

Esta renovación de licenciamiento, deberá permitir disponer de un soporte con el

fabricante durante el tiempo de duración del contrato con los siguientes servicios:

- ✓ Atención en castellano, desde territorio la Unión Europea.
- ✓ Resolución de incidencias por prioridad, con intervenciones remotas si es necesario.
- ✓ Acceso a actualizaciones de seguridad, *workarounds* (soluciones temporales), *hotfixes* (actualizaciones urgentes), actualizaciones mayores como *service* packs o descargas de nuevas versiones.
- ✓ Acceso a foros y base de datos de conocimiento de problemas, configuraciones, etc.
- ✓ Descarga de ficheros de firmas e información actualizada para la plataforma de forma periódica (diaria, mensual, urgentes) para mantener actualizados todos los componentes de la plataforma y así recoger las últimas protecciones.
- ✓ Sustitución de componentes o equipos (RMA) de la plataforma de cortafuegos ante averías que lo requieran.

La renovación constará de las siguientes subtareas a realizar por el adjudicatario:

- ✓ Registro de las licencias a nombre de la Diputación en el portal oficial del fabricante e instalación de las mismas en la plataforma de cortafuegos renovada.
- ✓ Actualización de los componentes a la última versión estable del fabricante.
- ✓ Pruebas, comprobación de funcionamiento y entrega de documentación técnica y de arquitectura de la plataforma renovada.

El adjudicatario realizará esta renovación en un plazo de 1 mes desde la formalización del contrato.

b) Soporte avanzado de protección de cortafuegos perimetral.

Este soporte permitirá tener a disposición de la Diputación un soporte en modalidad 8x5 NBD para el que deberá ser *partner* "Integrador Innovator" o superior, con personal técnico cualificado por parte del adjudicatario.

Realizará las siguientes tareas relacionadas con la protección de cortafuegos perimetral durante el tiempo de duración del contrato, y sin coste adicional:

- ✓ Realizar actualizaciones una vez al año al menos, de *software* y *firmware* a la versión recomendada por el fabricante, así como aplicación de parches de seguridad, conservando las configuraciones y operatividad de la plataforma.
- ✓ Tareas de revisión ante brechas de seguridad.
- ✓ Emisión de informes ante brechas de seguridad graves.
- ✓ Dirigir al personal de soporte que realice actuaciones, impartiendo al

efecto las órdenes e instrucciones necesarias para la ejecución de las mismas.
- ✓ Intermediación con el soporte del fabricante cuando sea necesario.

El medio de contacto será a través del sistema de gestión de incidencias usado por el Servicio IT, estableciéndose comunicaciones por correo y teléfono en caso necesario.

El adjudicatario proporcionará este soporte a demanda cuando sea necesario desde la firma del contrato.

1.4 ÓPTICAS Y CABLEADO.

El adjudicatario deberá suministrar los siguientes conectores SFPs y cableado por cada equipo:

- ✓ 10 x SFP+ 10GE y 10 x latiguillo FO 2 metros y 2 x latiguillo FO 7 metros.
- ✓ 1 x SFP+ 10GE (para HA) y 1 x latiguillo FO 1 metro (para HA).
- ✓ 2 x latiguillo FO 1 metro (para HA).
- ✓ 5 x latiguillo cobre CAT6 2 metros.
- ✓ 5 x latiguillo cobre CAT6 1 metro.

El adjudicatario deberá suministrarlos en un plazo de 1 mes desde la formalización del contrato.

LOTE 2. Servicio de Renovación y Mantenimiento de la Plataforma de Acceso Remoto Perimetral.

El objeto de este lote es renovar el mantenimiento de la plataforma que permite el acceso remoto seguro perimetral a equipos de Diputación. El acceso remoto permite a proveedores externos con los que se tiene un contrato de soporte, conectarse a equipos y dispositivos con un nivel de control y seguridad máximos, permitiendo un registro pormenorizado de las conexiones y el tiempo empleado en acceder a los distintos recursos.

Además de ello, permitirá cumplir con las Medidas de seguridad del Real Decreto 3/2010, de 8 de Enero, por el que se regula el ENS, referidas a Acceso remoto (*remote login*).

Por último, de acuerdo al Plan de Mejora de la Seguridad de la Información de la Diputación, la medida: “P03.03-192 Renovación de equipos sin Soporte Técnico”, quedaría atendida con esta contratación.

2.1 ALCANCE.

El alcance de este Lote será la plataforma de acceso remoto perimetral del Servicio IT, formada por 2 equipos Pulse Secure, para dar cobertura a las necesidades de Diputación en acceso remoto seguro perimetral.

2.2 DESCRIPCIÓN DEL ENTORNO ACTUAL.

El entorno actual está formado por 2 equipos VPN-SSL Junos Pulse PSA5000, con licencia para 250 sesiones concurrentes cada uno, cuyo final de soporte es en Abril de 2021.

2.3 CARACTERÍSTICAS.

El adjudicatario procederá a realizar las siguientes tareas, donde se especifican las características del contrato:

A) Renovación y mantenimiento de la plataforma de dispositivos VPN-SSL Pulse Secure:

Se deberán renovar la plataforma de acceso remoto Pulse Secure compuesta por 2 equipos Junos Pulse PSA5000 en configuración de alta disponibilidad A-P (Activo-Pasivo), y que se usan en los accesos remotos por parte de empresas que dan soporte técnico o por usuarios/as que necesitan acceder de forma remota a recursos en la infraestructura de Diputación.

Por tanto se deberá disponer de los siguientes componentes durante el tiempo de duración del contrato:

- ✓ 2 x dispositivos VPN-SSL Pulse Secure PSA5000 en alta disponibilidad, con soporte Platinum 24x7 y para dispositivo en alta disponibilidad PSA5000, con NBD para RMAs.
- ✓ Licenciamiento para 250 sesiones concurrentes de tipo “Essentials” durante el tiempo de duración del contrato para dispositivo en alta disponibilidad PSA5000, con soporte 24x7.

El mantenimiento con el fabricante permitirá disponer de:

- ✓ Atención en castellano, desde territorio la Unión Europea.
- ✓ Resolución de incidencias por prioridad, con intervenciones remotas si es necesario.
- ✓ Acceso a actualizaciones de seguridad, *workarounds* (soluciones temporales), *hotfixes* (actualizaciones urgentes), actualizaciones mayores como *service* packs o descargas de nuevas versiones.
- ✓ Acceso a foros y base de datos de conocimiento de problemas, configuraciones, etc.
- ✓ Descarga de ficheros de firmas e información actualizada para la plataforma de forma periódica (diaria, mensual, urgentes) para

mantener actualizados todos los componentes de la plataforma y así recoger las últimas protecciones.
- ✓ Sustitución de componentes o equipos (RMA) de la plataforma de acceso remoto ante averías que lo requieran.

Este servicio consta de las siguientes subtareas a realizar por el adjudicatario:
- ✓ Registro de las licencias a nombre de la Diputación en el portal oficial del fabricante e instalación de las mismas en la plataforma de acceso remoto renovada
- ✓ Actualización de los componentes a la última versión estable del fabricante.
- ✓ Pruebas, comprobación de funcionamiento y entrega de documentación técnica y de arquitectura de la plataforma renovada.

El adjudicatario realizará este servicio en un **plazo máximo de 1 mes** desde la formalización del contrato.

B) Soporte avanzado para el servicio de acceso remoto.

Este soporte exigido en este PPT permitirá tener a disposición de la Diputación, de un servicio en modalidad 8x5 NBD para el que deberá ser partner "Prefered" o superior, con personal técnico cualificado por parte del adjudicatario.

Realizará las tareas relacionadas con el acceso remoto de dispositivos VPN-SSL durante el tiempo de duración del contrato, y sin coste adicional:
- ✓ Realizar actualizaciones una vez al año al menos, de *software* y *firmware* a la versión recomendada por el fabricante, así como aplicación de parches de seguridad, conservando las configuraciones y operatividad de la plataforma.
- ✓ Tareas de revisión ante brechas de seguridad.
- ✓ Emisión de informes ante brechas de seguridad graves.
- ✓ Dirigir al personal de soporte que realice actuaciones, impartiendo al efecto las órdenes e instrucciones necesarias para la ejecución de las mismas.
- ✓ Intermediación con el soporte del fabricante cuando sea necesario.

El medio de contacto será a través del sistema de gestión de incidencias usado por el Servicio IT, estableciéndose comunicaciones por correo y teléfono en caso necesario.

El adjudicatario proporcionará este servicio **a demanda cuando sea necesario** desde la firma del contrato.

2.4 CABLEADO

El adjudicatario deberá suministrar el siguiente cableado:

- ✓ 3 x latiguillo cobre CAT6 5 metros.

El adjudicatario deberá suministrarlos en un **plazo máximo de 1 mes** desde la adjudicación del contrato.

LOTE 3. Servicio y Mantenimiento de protección WAF.

El objeto de este lote es suministrar y disponer de mantenimiento para la plataforma de Protección WAF que permita disponer de una alta seguridad en portales y aplicaciones web alojadas en Diputación y publicadas en internet. Esta protección permitirá frenar posibles ataques e infecciones de las web, y mejorar el acceso a las mismas, ofreciendo una disponibilidad óptima del servicio.
Además de ello, permitirá cumplir con las Medidas de seguridad dentro del Real Decreto 3/2010, de 8 de Enero, por el que se regula el ENS, referidas a Perímetro seguro y a la Protección de servicios y aplicaciones web.

Por último, de acuerdo al Plan de Mejora de la Seguridad de la Información de la Diputación, aspectos de la medida: "P03.01-397 Data Integrity" y de acuerdo al *pentesting* último realizado, en relación al filtrado del tráfico que llegue a las webs para que no ejecuten actividades maliciosas, quedarían ambos puntos atendidos con esta contratación.

3.1 ALCANCE.

El alcance de este Lote es la plataforma WAF del Servicio IT, para dar cobertura a las necesidades de Diputación en protección de aplicaciones web.

3.2 CARACTERÍSTICAS.

El adjudicatario procederá a realizar las siguientes tareas, donde se especifican las características del contrato:

A) Servicio y mantenimiento de la Plataforma WAF:
Se deberá dar servicio desde una plataforma WAF en nube, y cuya funciones en resumen serían las de analizar el tráfico generado desde internet o la red interna hacia cada servidor web, protegiéndolo frente a diversos ataques específicos como SQL injection, Cross Site Scripting, ataques de denegación de servicio (DoS), ataques de denegación de servicio distribuido (dDoS), inclusive los de nivel 7, acceso ilegal a recursos, bots maliciosos, etc., dirigidos a los servidores web. Además el sistema WAF debe acelerar el rendimiento de las aplicaciones utilizando un sistema de cacheo, traduciéndose en menor tiempo de carga de las páginas, menor carga de trabajo del servidor web y un menor consumo de ancho de banda.

Esta plataforma WAF que se solicita con funcionamiento en la nube, cuenta con la ventaja de permitir una sencilla puesta en marcha e implantación, sin necesidad de realizar cambios hardware ni software en la infraestructura de la Diputación, ni cambios en el código de las aplicaciones, únicamente cambiando los registros DNS de las webs y portales que se protegen con este sistema. De esta forma, las peticiones se dirigirán a la plataforma WAF en la nube del proveedor, dónde serán inspeccionadas y filtradas de tráfico malicioso y, únicamente las peticiones legítimas seguras, son las que se redirigirán a la red de Diputación (a los servidores web de Diputación). En caso de que el WAF detecte que se está produciendo un ataque, lo frenará e informará en tiempo real a la Diputación vía email y desde la propia consola de gestión.

Deberá disponer de las siguientes prestaciones durante el tiempo de duración del contrato:

- ✓ Firewall de aplicaciones Web: Protección frente a ataques que explotan
  vulnerabilidades de aplicaciones web registradas en OWASP TOP 10, SQL injection (SQLi), cross site scripting (XSS), acceso ilegal a recursos e inclusión remota de archivos (RFI).
- ✓ Cacheo estático y dinámico del tráfico (servicio CDN o red de entrega de
- ✓ contenidos), para mejorar el rendimiento, optimizar el uso del ancho de banda y los tiempos de respuesta. Políticas de cacheo flexibles y personalizables por el administrador del sistema.
- ✓ Protección frente a ataques de denegación de servicio (DoS) a nivel de aplicación y a nivel de red.
- ✓ Protección frente a ataques de denegación de servicio distribuidos (DDoSdistributed denial of service) con un ancho de banda de hasta 1Gbps ampliable: Sloworis, inundaciones ICMP, TCP & UDP, GET flood, SYN flood, PINGs de la muerte y amplificaciones DNS, etc.
- ✓ Mitigación avanzada de ataques DDoS de capa 7.
- ✓ Compresión de datos, especialmente imágenes, para optimizar el uso del ancho de banda y los tiempos de respuesta.
- ✓ Protección frente a exploits y ataques día 0.
- ✓ Protección frente a bots maliciosos, distinguiendo entre consultas de humanos, bots legítimos (google, facebook) y bots maliciosos.
- ✓ Protección para servicios web: El sistema debe proporcionar protección frente a ataques XSS (cross site scripting).
- ✓ Protección del protocolo HTTP: El sistema debe detectar la manipulación del protocolo http con el fin de prevenir ataques basados en cifrado, buffer overflows y otros ataques específicos de la aplicación.

- ✓ El sistema debe permitir programar reglas personalizables por el administrador del sistema, de forma simple, utilizando el interfaz GUI.
- ✓ Protección WAF certificada por los estándares de seguridad PCI, para proteger los datos sensibles, incluyendo informes del estado de la seguridad y cumplimiento de normas.
- ✓ Prevención del blacklisting, para asegurar que los sitios web estén siempre accesibles.
- ✓ Administración basada en roles.
- ✓ Generación de informes y estadísticas sobre el acceso a las webs uso de las aplicaciones: por tipo de ataques en un rango de fechas, por severidad de los ataques en un rango de fechas y por origen de los ataques (IP).
- ✓ El sistema debe proporcionar información estadística en tiempo real sobre el tráfico y el rendimiento.
- ✓ Análisis geográfico. El WAF debe incorporar un módulo de análisis geográfico por IP, permitiendo bloquear el acceso desde determinados países o zonas geográficas.
- ✓ Servicio categorización y bloqueo por reputación de IPs, para bloquear ataques desde fuentes asociadas con ataques DDoS, ataques phishing o sitios web de phishing, proxies anónimos, fuentes de software malicioso o spammers.
- ✓ Debe aceptar un funcionamiento en los modos seguridad negativa y positiva.
- ✓ Servicio 100% en la nube, totalmente gestionado y con una consola web de configuración que sea fácilmente administrable.
- ✓ Monitorización permanente 24x7 de todos los sitios web protegidos, garantizando el mayor nivel de protección y visibilidad.
- ✓ Notificaciones automáticas por correo electrónico de todas las amenazas detectadas y solicitudes bloqueadas que pudieran suponer una amenaza para los sitios web.
- ✓ Gestión y respuesta proactivas a eventos de seguridad, en el momento que se descubra un comportamiento sospechoso o malicioso, o que uno de nuestros sitios web dejara de estar disponible.
- ✓ Aprendizaje automático: Ajuste automático de políticas de forma proactiva y gestión de la configuración para proporcionar una óptima protección contra amenazas a las aplicaciones y eliminar falsos positivos.
- ✓ Informes gráficos semanales demostrando las tendencias en el tráfico en nuestros sitios web, las amenazas y las mejoras en el rendimiento.
- ✓ Asistencia y asesoramiento 24x7 sobre seguridad web a cargo de los especialistas en seguridad del sistema.

- ✓ Atención en castellano, desde territorio la Unión Europea.
- ✓ Resolución de incidencias por prioridad.
- ✓ Se dispondrán de 20 websites bajo protección WAF (donde 1 website corresponde a 1 dirección IP pública o un certificado SSL).

El servicio debe prestarse desde Centros de Datos con las siguientes características:

- ✓ Centros de Datos TIER II al menos, y ENS Nivel Medio al menos.
- ✓ Disponibilidad del servicio del demostrable con presencia de varios centros de datos en territorio Europeo, que garanticen la citada disponibilidad.

Este servicio consta de las siguientes subtareas a realizar por el adjudicatario:

- ✓ Registro de las licencias del servicio de la plataforma WAF en nube a nombre de la Diputación en el portal oficial del fabricante e instalación de las mismas en la plataforma WAF en nube.
- ✓ Instalación, configuración y puesta en marcha de la plataforma WAF, con los datos de los websites indicados por técnicos del Servicio IT y activando las funcionalidades y características detalladas anteriormente, incluyendo las integraciones necesarias.
- ✓ Pruebas, comprobación de funcionamiento y entrega de documentación técnica y de arquitectura de la plataforma WAF en nube, con la interrelación de los portales web y aplicaciones que protegerá.
- ✓ Se deberán seguir las recomendaciones indicadas en en el documento del CCN-CERT 661 “Seguridad en firewalls de aplicación web” y aplicables a la plataforma de protección WAF.

El adjudicatario realizará este servicio en un **plazo máximo de 2 meses** desde la formalización del contrato.

B) Soporte avanzado para la plataforma WAF:.
Este soporte exigido permitirá tener a disposición de la Diputación, de un servicio en modalidad 24x7 para el que deberá ser partner, con personal técnico cualificado por parte del adjudicatario. Realizará las tareas relacionadas con la protección WAF durante el tiempo de duración del contrato, y sin coste adicional:

- ✓ Tareas de revisión ante brechas de seguridad.
- ✓ Emisión de informes ante brechas de seguridad graves.
- ✓ Intermediación con el soporte del fabricante cuando sea necesario.

El medio de contacto será a través del sistema de gestión de incidencias usado por el Servicio IT, estableciéndose comunicaciones por correo y teléfono en caso

necesario.

El adjudicatario proporcionará este servicio **a demanda cuando sea necesario** desde la firma del contrato.

LOTE 4. Servicio y Mantenimiento de Protección Perimetral del Correo.

El objeto de este lote es prestar un servicio y su mantenimiento de protección perimetral a la plataforma del correo que permita disponer de una alta seguridad ante ataques y técnicas maliciosas dirigidas al servidor y a los usuarios que usan el correo de Diputación. Esta protección permitirá detectar infecciones (virus, malwares, enlaces maliciosos) en los mensajes de correo, ofreciendo una disponibilidad óptima del servicio.

Además de ello, permitirá cumplir con las Medidas de seguridad dentro del Real Decreto 3/2010, de 8 de Enero, por el que se regula el ENS, referidas a Perímetro seguro y a la Protección del correo electrónico.

4.1 ALCANCE.

El alcance de este Lote es la plataforma de protección perimetral del correo del Servicio IT, para dar cobertura a las necesidades de Diputación en seguridad sobre el correo.

4.2 CARACTERÍSTICAS.

El adjudicatario procederá a realizar las siguientes tareas, donde se especifican las características del contrato:

A) Servicio y mantenimiento de Plataforma de protección del correo:
Se deberá dar servicio desde una plataforma de protección de seguridad sobre el correo en nube, y cuya funciones en resumen serían las de limpiar de malwares, virus y enlaces maliciosos analizando los mensajes de correo antes de que ingresen en los distintos buzones de los usuarios, aportando una capa de seguridad al correo. Además el sistema de protección del correo aportará protección ante pérdida de datos (DLP o Data Loss Prevention) y *Sandboxing* (pruebas y ejecución de adjuntos sospechosos en un entorno aislado antes de su entrega), traduciéndose en una mayor confiabilidad en la entrega y envío de los correos.

Esta plataforma de protección del correo que se solicita con funcionamiento en la nube, cuenta con la ventaja de permitir una sencilla puesta en marcha e implantación, sin necesidad de realizar cambios hardware ni software en la infraestructura de la Diputación, ni cambios en el código de las aplicaciones, únicamente cambiando los registros DNS de los servidores de correos que se

protegen con este sistema. De esta forma, las peticiones se dirigirán a la plataforma de protección del correo en la nube del proveedor, dónde serán inspeccionados y filtrados de adjuntos, enlaces (*urls*) maliciosos, *phishing* y, únicamente las peticiones legítimas seguras, son las que se redirigirán a la red de Diputación (a los servidores de correo de Diputación) o saldrán de la red de Diputación (de los servidores de correo de Diputación). En caso de que la protección del correo detecte que se está produciendo un problema de seguridad, lo frenará e informará en tiempo real a la Diputación vía email y desde la propia consola de gestión.

Deberá disponer de las siguientes prestaciones durante el tiempo de duración del contrato:

- ✓ Filtrado de correos de entrada y de salida.
- ✓ Protección antivirus, *malwares*.
- ✓ Protección ante "*clicks*" de los usuarios en enlaces maliciosos.
- ✓ *Sandboxing*.
- ✓ DLP o (*Data Loss Prevention*): prevención de pérdida de datos con políticas que permitan identificar tipos de ficheros, contenidos de mensajes y bloquear su envío al exterior.
- ✓ Sistemas de cifrado basado en identidad (IBE o *Identity-Based Encrytion*).
- ✓ Intercambio seguro de mensajes entre servidores (TLS).
- ✓ Integración con LDAP.
- ✓ Traceo (seguimiento) de los mensajes de entrada y de salida.
- ✓ Proporcionar los logs ante solicitudes de auditorías o ataques que pudieron iniciarse por correo.
- ✓ Permisividad en envíos masivos desde remitentes identificados, con políticas limitativas por número de envíos por hora y diarios al menos.
- ✓ Protección frente ataques de suplantación de personalidad.
- ✓ Entrega a los usuarios de ficheros sin elementos activos (macros, enlaces, ...).
- ✓ Análisis de ficheros protegidos con contraseña.
- ✓ Análisis post-entrega, permitiendo escaneos proactivos de buzones basado en políticas de seguridad.
- ✓ Uso de "*sandbox*" para análisis de ficheros que podrían formar parte de ataques de día cero.
- ✓ Servicio 100% en la nube, totalmente gestionado y con una consola web de configuración que sea fácilmente administrable.
- ✓ Monitorización permanente 24x7 de todos los servidores de correo protegidos, garantizando el mayor nivel de protección y visibilidad.
- ✓ Detección de entradas en *blacklists* con aviso de forma inmediata por correo electrónico a los técnicos de SIT.

- ✓ Capacidad de analizar enlaces incluidos en correos, y de detectar cuándo un usuario ha pulsado sobre el mismo.
- ✓ Administración basada en roles.
- ✓ Generación de informes y estadísticas sobre seguridad detectado en los mensajes de correo: por tipo de ataques en un rango de fechas, por severidad de los ataques en un rango de fechas y por origen de los ataques (IP).
- ✓ El sistema debe proporcionar información estadística en tiempo real sobre los correos filtrados y totalizaciones según tipo de incidencia.
- ✓ Análisis geográfico. La protección del correo debe incorporar un módulo de análisis geográfico por IP, permitiendo bloquear mensajes de correo desde determinados países o zonas geográficas.
- ✓ Servicio categorización y bloqueo por reputación de IPs, para bloquear ataques desde fuentes asociadas con ataques phishing y envíos masivos de spam.
- ✓ Notificaciones automáticas por correo electrónico de todas las amenazas detectadas y solicitudes bloqueadas que pudieran suponer una amenaza para los servidores de correo.
- ✓ Gestión y respuesta proactivas a eventos de seguridad, en el momento que se descubra un comportamiento sospechoso o malicioso, o que uno de nuestros servidores de correo dejara de estar disponible.
- ✓ Aprendizaje automático: Ajuste automático de políticas de forma proactiva y gestión de la configuración para proporcionar una óptima protección contra amenazas a los servidores de correo y eliminar falsos positivos.
- ✓ Informes gráficos semanales demostrando las tendencias en el número de correos con algún problema de seguridad o sospecha que han sido filtrados a o desde los servidores de correo de Diputación.
- ✓ Asistencia y asesoramiento 24x7 sobre seguridad en el correo a cargo de los especialistas en seguridad del sistema.
- ✓ Atención en castellano, desde territorio la Unión Europea.
- ✓ Resolución de incidencias por prioridad.
- ✓ Se dispondrán de un máximo de 5.750 buzones de correo bajo protección perimetral del correo.
- ✓ Media de escaneo de cada mensaje < 1 minuto.

El servicio debe prestarse desde Centros de datos con las siguientes características:

- ✓ Centros de Datos TIER II al menos, y ENS Nivel Medio al menos.
- ✓ Disponibilidad del servicio de 99,999% demostrable con presencia de varios centros de datos en territorio Europeo, que garanticen la citada disponibilidad.

Este servicio consta de las siguientes subtareas a realizar por el adjudicatario:

- ✓ Registro de las licencias del servicio de la plataforma de protección del correo en nube a nombre de la Diputación en el portal oficial del fabricante e instalación de las mismas en la plataforma de protección del correo en nube.
- ✓ Instalación, configuración y puesta en marcha de la plataforma de protección sobre el correo, con los datos de los servidores indicados por técnicos del Servicio IT y activando las funcionalidades y características detalladas anteriormente, incluyendo las integraciones necesarias.
- ✓ Pruebas, comprobación de funcionamiento y entrega de documentación técnica y de arquitectura de la plataforma de protección del correo en nube, con la interrelación de los servidores de correo que protegerá.
- ✓ Se deberán seguir las recomendaciones indicadas en en el documento del CCN-CERT 814 "Seguridad en correo electrónico" y aplicables a la plataforma de protección del correo.

El adjudicatario realizará este servicio en un **plazo máximo de 2 meses** desde la formalización del contrato.

B) Soporte avanzado para el servicio de protección perimetral del correo.
Este soporte exigido permitirá tener a disposición de la Diputación, de un servicio en modalidad 24x7 para el que deberá ser partner, con personal técnico cualificado por parte del adjudicatario.

Realizará las tareas relacionadas con la plataforma de protección del correo durante el tiempo de duración del contrato, y sin coste adicional:

- ✓ Tareas de revisión ante brechas de seguridad.
- ✓ Emisión de informes ante brechas de seguridad graves.
- ✓ Intermediación con el soporte del fabricante cuando sea necesario.

El medio de contacto será a través del sistema de gestión de incidencias usado por el Servicio IT, estableciéndose comunicaciones por correo y teléfono en caso necesario.

El adjudicatario proporcionará este servicio **a demanda cuando sea necesario** desde la firma del contrato.

LOTE 5. Suministro y Mantenimiento de la Protección de Metadatos.

El objeto de este lote es suministrar y disponer de mantenimiento para una solución de Protección de los metadatos que se incluyen en documentos e información publicada en internet. Esta protección permitirá frenar posibles exposiciones de información sensible desde los portales webs de Diputación.

Además de ello, permitirá cumplir con las Medidas de seguridad dentro del Real Decreto 3/2010, de 8 de Enero, por el que se regula el ENS, referidas a Limpieza de documentos.

5.1 ALCANCE.

El alcance de este Lote es la protección de los documentos con metadatos que son publicados en internet por parte de los distintos Servicios de la Diputación, y para dar cobertura a las necesidades de Diputación en seguridad sobre metadatos en los documentos.

5.2 CARACTERÍSTICAS.

El adjudicatario procederá a realizar las siguientes tareas, donde se especifican las características del contrato:

- Suministro y mantenimiento de protección de metadatos:

Se deberá suministrar una plataforma de protección de metadatos sobre los documentos publicados en internet, y cuya funciones en resumen serían las de prevenir la fuga de información sensible, de manera que no pueda ser usada por terceros para realizar acciones maliciosas comprometiendo la seguridad e imagen de la Diputación.

Además de ello el cumplimiento del RGPD se verá facilitado, entre otros aspectos en el de exigencia a derecho al olvido (hace que se elimine información de datos personales). Además protegerá los metadatos incluidos en documentos ofimáticos (tipo office, openoffice, pdf) y en ficheros de imágenes, audio y video incluso.

Deberá disponer de las siguientes prestaciones durante el tiempo de duración del contrato:

- ✓ Prevenir fuga de información sensible en metadatos y datos ocultos.
- ✓ Eliminar datos ocultos e información sensible de documentos Microsoft Office (Word, Excel, PowerPoint y Visio), Open Office (Documento de texto, Hojas de cálculo y Presentaciones), PDF y ficheros de imágenes, audio y vídeo.
- ✓ Limpiar automáticamente todos los documentos antes de que estos sean compartidos por cualquier de los medios disponibles (correo, redes sociales, servidores web o ftp, nubes locales repositorio de documentos) y todo esto de forma transparente para el usuario.

- ✓ Configuración y administración muy intuitiva.
- ✓ Multiplataforma: windows, linux, unix, mac os.
- ✓ Funcionalidad desde linea de comandos a ejecutar en servidores con documentos:
  - eliminar/modificar metadatos en todos los ficheros.
  - elimina datos ocultos e información personal (rutas de impresora, historial de modificaciones de documentos).
  - exportación de los metadatos a ficheros excel para estudios posteriores, informes con resultados de la ejecución.
  - sin requisito de instalar los respectivos productos cuyos documentos asociados supervisa.
- ✓ Funcionalidad de protección de documentos en servidores web:
  - cuando se navegue por los sitios web de Diputación y consulten los documentos publicados, se eliminarán automáticamente los metadatos de los ficheros seleccionados por el usuario mostrándose sin metadatos (para evitar fugas de información).
  - optimización en el acceso a documentos si otro usuario ha consultado previamente el mismo (ganando velocidad de acceso).
  - lanzamiento de tareas programadas.
- ✓ Funcionalidad de protección con adjuntos en mensajes de correo:
  - deberá procesar los metadatos de los archivos adjuntos de los correos electrónicos de los servidores Zimbra evitando la filtración de información y reduciendo el impacto reputacional derivado del uso malintencionado de los metadatos.
  - filtrado en correos enviados al exterior y en correos internos.
  - consumo mínimo de recursos.
  - configuración de dominios de exclusión en el boraddo de metadatos (por ejemplo que los mails internos no se modifiquen los metadatos de los ficheros enviados).
  - que pueda preguntar al usuario si desea o no modificar los metadatos en ficheros PDF firmados (para no invalidar la firma).
- ✓ Despliegue de componentes en equipos de usuarios por políticas de Directorio Activo.
- ✓ Atención en castellano, desde territorio la Unión Europea.
- ✓ Resolución de incidencias por prioridad.
- ✓ Se dispondrán de un máximo de 5.750 buzones de correo bajo protección de metadatos incluidos en documentos adjuntos de los mensajes de correo.

El suministro deberá realizarse en Diputación.

Este suministro consta de las siguientes subtareas a realizar por el adjudicatario:

- ✓ Registro de las licencias del servicio de la plataforma de protección de metadatos a nombre de la Diputación en el portal oficial del fabricante e instalación de las mismas en la plataforma de protección de metadatos.
- ✓ Instalación, configuración y puesta en marcha de la plataforma de protección sobre los metadatos, con los datos de los servidores que alojen documentos susceptibles de proteger indicados por técnicos del Servicio IT y activando las funcionalidades y características detalladas anteriormente, incluyendo las integraciones necesarias.
- ✓ Pruebas, comprobación de funcionamiento y entrega de documentación técnica y de arquitectura de la plataforma de protección de metadatos con la interrelación de los servidores que protegerá.
- ✓ Se deberán seguir las recomendaciones indicadas en en el documento del CCN-CERT 835 "Borrado de Metadatos en el marco del ENS" y aplicables a la plataforma de protección de metadatos, así como la normativa del RGPD.

El adjudicatario realizará este servicio en un **plazo máximo de 2 meses** desde la formalización del contrato.

El medio de contacto será a través del sistema de gestión de incidencias usado por el Servicio IT, estableciéndose comunicaciones por correo y teléfono en caso necesario.

FORMA DE PRESTACIÓN DEL CONTRATO.

LOTE 1. Servicio de Renovación y Mantenimiento de la Plataforma de Cortafuegos Perimetral.

La realización de los suministros se realizará *in situ* en las Oficinas Centrales. La realización de los servicios asociados se podrá realizar en remoto (resolución de incidencias, tareas de configuración y actualización) y las tareas de instalación y migración se realizarán *in situ*.

El adjudicatario garantizará, las horas de trabajo necesarias para cumplir correctamente la ejecución del contrato, ya sea dentro del horario de trabajo de las dependencias siempre que no ocasione interrupciones en el desarrollo de sus actividades, y/o bien fuera del mismo si se coordina y planifica convenientemente.

LOTE 2. Servicio de Renovación y Mantenimiento de la Plataforma de Acceso Remoto Perimetral.

La realización de los suministros se realizará *in situ* en las Oficinas Centrales. La realización de los servicios asociados se podrá realizar en remoto (resolución de incidencias, tareas de configuración y actualización) y las tareas de instalación y migración se realizarán *in situ*.

El adjudicatario garantizará las horas de trabajo necesarias para cumplir correctamente la ejecución del contrato, ya sea dentro del horario de trabajo de las dependencias siempre que no ocasione interrupciones en el desarrollo de sus actividades, y/o bien fuera del mismo si se coordina y planifica convenientemente.

LOTE 3. Servicio y Mantenimiento de protección WAF.
La realización de los suministros se realizará mayoritariamente en remoto, en la dependencias del adjudicatario. La realización de los servicios asociados también se podrá realizar en remoto (resolución de incidencias, tareas de configuración y actualización) así como las tareas de instalación y migración.

El adjudicatario garantizará las horas de trabajo necesarias para cumplir correctamente la ejecución del contrato, ya sea dentro del horario de trabajo de las dependencias siempre que no ocasione interrupciones en el desarrollo de sus actividades, y/o bien fuera del mismo si se coordina y planifica convenientemente.

LOTE 4. Servicio y Mantenimiento de Protección Perimetral del Correo.
La realización de los suministros se realizará mayoritariamente en remoto, en la dependencias del adjudicatario. La realización de los servicios asociados también se podrá realizar en remoto (resolución de incidencias, tareas de configuración y actualización) así como las tareas de instalación y migración.

El adjudicatario garantizará las horas de trabajo necesarias para cumplir correctamente la ejecución del contrato, ya sea dentro del horario de trabajo de las dependencias siempre que no ocasione interrupciones en el desarrollo de sus actividades, y/o bien fuera del mismo si se coordina y planifica convenientemente.

LOTE 5. Suministro y Mantenimiento de la Protección de Metadatos.
La realización de los suministros se realizará mayoritariamente en remoto, en las dependencias del adjudicatario. La realización de los servicios asociados también se podrá realizar en remoto (resolución de incidencias, tareas de configuración y actualización) así como las tareas de instalación y migración.

El adjudicatario garantizará las horas de trabajo necesarias para cumplir correctamente la ejecución del contrato, ya sea dentro del horario de trabajo de

las dependencias siempre que no ocasione interrupciones en el desarrollo de sus actividades, y/o bien fuera del mismo si se coordina y planifica convenientemente.

PROCEDIMIENTO DE ADJUDICACION

Dado el objeto del contrato a licitar así como el contenido de las prestaciones, se estima que el procedimiento más acorde con los principios de transparencia, igualdad y no discriminación, publicidad y libertad de acceso (ex art. 1 LCSP), es el **procedimiento abierto (art. 156 y siguientes LCSP)**, si bien con las particularidades de la **contratación sujeta a regulación armonizada (art. 22 LCSP)**, por ser su valor estimado superior al umbral legalmente establecido (Orden HFP/1298/2017, de 26 de diciembre).

INFORMACIÓN A SUMINISTRAR POR LOS OPERADORES

Los operadores económicos que deseen participar en esta consulta preliminar habrán de suministrar, en referencia a la prestación objeto de la misma, y por cada lote, la siguiente información (se acompaña cuadro adjunto):

a) Desglose de los costes directos e indirectos, gastos generales, gastos eventuales y beneficio industrial, aplicado al cumplimiento de la prestación (art.101.1 LCSP y art. 131.1 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). Estos conceptos, a los que se les aplicará el Impuesto sobre el Valor Añadido según el porcentaje en vigor, habrán de entenderse del siguiente tenor:

   - *costes directos*: integrados por todos aquellos que se derivan directamente de la ejecución material de la prestación del contrato, estando incluidos los costes laborales, que son aquéllos gastos salariales del personal que ejecuta de manera directa la prestación, teniendo en cuenta a estos efectos el Convenio Colectivo de directa aplicación;
   - *costes indirectos*: representan aquellos gastos en los que incurre la empresa que no son asignados inmediata y directamente a la ejecución de la prestación;
   - *gastos eventuales o imprevistos*: son aquellos gastos no habituales, incluyéndose los denominados costes inesperados;
   - *gastos generales*: son aquellos gastos estructurales de la empresa, tales como los costes de administración, financieros o comerciales u otros gastos generales tales como consumos, intereses bancarios, tributos, etc;
   - *beneficio industrial*: para el cálculo de este beneficio debe aplicarse, como mínimo, **el 6% sobre todos los costes y gastos, incluido los**

generales, tomando tal porcentaje en aplicación analógica del art. 131.1.b RLCAP, sumándosele el porcentaje de IVA correspondiente.

b) Convenio Colectivo del sector aplicable al personal adscrito a la ejecución de la prestación, con desagregación de género (H/M) y categoría profesional (arts. 100, 101.2.II, 102.3.II y 201 LCSP). Debe señalar expresamente el Convenio Colectivo del sector (provincial, autonómico o estatal), con indicación de la fecha de su publicación en el boletín oficial correspondiente (ejemplo.- ***Convenio Colectivo de _____, de fecha _____ (BOPMA/BOJA/BOE nº ___, de __ de _____).***

c) Posibilidad de incluir criterios medioambientales, ya sea como criterios de adjudicación (art. 145 LCSP) o como condiciones especiales de ejecución (art. 202 LCSP).

PLAZO DE EJECUCIÓN Y FORMA DE PAGO

El plazo de ejecución del contrato será de **TRES (3) AÑOS** a contar desde la formalización del mismo, prorrogable por una anualidad.

La facturación se realizará por mensualidades vencidas, estando el adjudicatario obligado a presentar la correspondiente factura (en cumplimiento del Real Decreto 1619/2012, de 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación), que habrá de ser en formato electrónico (art. 198.4 y DA 32ª LCSP), y a través del Punto General de Recepción de Facturas del Estado (FACe), cumpliendo los requisitos de formato y firma electrónica previstos en la Ley 25/2013, de 27 de Diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público, y demás normativa de desarrollo.

CONDICION ESPECIAL DE EJECUCION

La prestación del contrato a licitar lleva impuesta como condición especial de ejecución (art. 202.2.II LCSP), la siguiente:

Condición Social de estabilidad en el empleo*: la empresa se compromete a mantener, salvo causas de fuerza mayor adecuadamente documentadas, al personal que haya iniciado la ejecución del contrato, exigiéndose que el 50% de la plantilla que ejecute el servicio que se licita sea indefinida. La verificación de esta condición de estabilidad se realizará al final de cada año natural mediante la entrega, por parte de la empresa, al responsable del contrato, de copia de los contratos laborales y de la Relación Nominal de los Trabajadores (RNT).*

La vinculación de la presente condición con este contrato deriva directamente de los artículos 1.1 y 40 de la Constitución Española (CE), que proclaman el Estado social y democrático de Derecho y prescriben la obligación de los poderes públicos de promover las condiciones favorables para el progreso social y económico en el marco de una política de estabilidad económica, destacando que "de manera especial realizarán una política orientada al pleno empleo". La contratación administrativa, a través de la inclusión de cláusulas sociales, sirve de instrumento para llevar a cabo diferentes políticas públicas, entre las que destaca el pleno empleo. Por su parte, el artículo 2 del Tratado de la Unión Europea (TUE) establece entre sus fines la promoción de "un alto nivel de empleo y de protección social".

El incumplimiento de esta condición tendrá la consideración de infracción grave, lo que conllevará la imposición de las penalidades que se prevean en el PCAP (art. 202.3 LCSP), con las consecuencias establecidas en el art. 71.2.c LCSP.

FECHA LÍMITE PRESENTACIÓN DE RESPUESTAS A LA CONSULTA PRELIMINAR.

La fecha límite para presentación de las consultas preliminares es de **DIEZ (10) DIAS NATURALES** desde la publicación de la consulta preliminar en la Plataforma de Contratación del Sector Público –PCSP-.

Las respuestas deberán ser remitidas a la siguiente dirección de correo electrónico: *administracionit@malaga.es*, indicando en el asunto: "Respuesta a consulta preliminar sobre contrato "***Seguridad TIC Perimetral".*** Las mismas habrán de enviarse en formato *"pdf"*, y firmadas digitalmente por el representante legal de la empresa o entidad.

Para cualquier consulta técnica sobre el contenido de la presente los operadores se podrán dirigir a Don Luis Fernández Plaza, Jefe de Sección de Sistemas y Comunicaciones, en la dirección de correo electrónico *lfernandez@malaga.es*. Las consultas siempre se realizarán por escrito, haciéndose públicas tanto las consultas como las respuestas otorgadas, todo ello en aras de la igualdad de oportunidades para todos los operadores.

CONFIDENCIALIDAD DE LA INFORMACIÓN.

Los datos relativos a la información presentada por las distintas empresas serán tratados por el órgano de contratación para la elaboración de los pliegos y cláusulas que han de regir el procedimiento para la contratación del meritado

servicio, garantizándose la más estricta confidencialidad respecto de su contenido (art. 115.3.II y III LCSP).

INTERVENCION POSTERIOR EN EL PROCEDIMIENTO DE CONTRATACION

La participación de los distintos operadores económicos en la presente consulta preliminar no impedirá su posterior intervención en el procedimiento de contratación que en su caso se tramite (art. 115.3.IV LCSP), salvo en los casos en los que exista conflicto de interés (art. 64.2 LCSP) o se den las circunstancias de compatibilidad del art. 70 LCSP.

DATOS REQUERIDOS PARA ESTUDIO DE MERCADO:

- **RESPUESTA ESTIMACION PRECIO DE MERCADO**

LOTE __

TOTAL Presupuesto de licitación – sin IVA –	TOTAL IVA	TOTAL Presupuesto de licitación – con IVA –
€	€	€

Sistema de determinación del Presupuesto base: (se incluye el Coste de los salarios desagregados por Género y Categoría Profesional de las personas empleadas para la ejecución del contrato cuyo trabajo forma parte del precio total del contrato)	
Costes Directos (IVA Incluido)	€
Costes Indirectos (IVA Incluido)	€
Gastos Generales (13%) [1]	€
Gastos Eventuales	€
Beneficio Industrial (6%) [2]	€
TOTAL (incluido IVA) :	€

[1] Aplicado sobre **la totalidad de los costes, incluido los gastos eventuales**
[2] Aplicado sobre **todos los costes y gastos, incluido los generales**

DESGLOSE COSTE SALARIALES
Convenio Colectivo de _____, de _____, de fecha _____
(BOPMA/BOJA/BOE nº ___, de __ de _____)

GENERO	CATEGORÍA PROFESIONAL	COSTES SEGÚN CONVENIO
		€
		€
		€

Criterios Medioambientales

»

(Firmar digitalmente por el representante de la entidad mercantil)