PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES

SUMINISTRO DE LA INFRAESTRUCTURA DE CONECTIVIDAD CON ASEGURAMIENTO DE ESTÁNDARES DE CIBERSEGURIDAD DEL AYUNTAMIENTO DE SESTAO 2021-2025

AYUNTAMIENTO DE SESTAO

En Sestao a xx de xxxx de 2021

ÍNDICE

1. - OBJETO.....3
2. - ALCANCE.....3
3. - REQUISITOS ESPECÍFICOS DE LA SOLUCIÓN DE SEGURIDAD Y SD-WAN.....8
4. - REQUISITOS ESPECÍFICOS PARA LA CONSULTORÍA DE CERTIFICACIÓN ENS.....13
5. - REQUISITOS ESPECÍFICOS DE LA HERRAMIENTA DE PROTECCIÓN DE SERVIDORES ANTE ATAQUES RANSOMWARE.....14
6. - REQUISITOS ESPECÍFICOS DE LA SOLUCIÓN DE CONECTIVIDAD INALÁMBRICA Y CABLEADO PARA LAS SEDES DEL AYUNTAMIENTO Y EL EDIFICIO CASTAÑOS.....14
7. - ENTORNO TECNOLÓGICO.....17
8. - METODOLOGÍA PARA LA EJECUCIÓN DEL CONTRATO:.....17
9. - DURACIÓN DEL CONTRATO.....18
10. - PRESUPUESTO Y VALOR ESTIMADO.....18
11. - PROPOSICIÓN ECONÓMICA.....19
12. - CRITERIOS DE ADJUDICACIÓN.....19

1. - OBJETO

El objeto del presente Pliego de Prescripciones Técnicas (en adelante PPT) es establecer las condiciones técnicas a las que debe ajustarse la licitación, contratación y desarrollo del presente contrato de Suministro, y servicio residual, con prestaciones vinculadas entre sí, que consiste en el:

Suministro de:

- Plataforma de firewalls para la renovación de la defensa perimetral.
- Plataforma SD-WAN
- Plataforma de gestión, análisis y reportes.
- Herramienta de protección de endpoints ante ataques Ransomware
- Plataforma WiFi
- Instalación y configuración de plataforma WiFi y estudio de cobertura
- Migración y configuración de la plataforma de firewall actual
- Implantación y configuración de la plataforma SD-WAN

Servicios de:

- Servicio de consultoría de cumplimiento del Esquema Nacional de Seguridad
- Servicio de Mantenimiento preventivo y correctivo de hardware, software y licencias para los 4 primeros años
- Bolsa de horas
- Formación

CPV Principal: 30200000-1
CPV Secundarios: 48000000-8, 71316000-6

2. - ALCANCE

En este apartado se describen los suministros, actividades y tareas que deberán ser realizados por el adjudicatario.

- El suministro será en régimen de compra, de los elementos necesarios para garantizar la conectividad y seguridad de la red de datos de cara al exterior y también la seguridad de las comunicaciones entre las diferentes ubicaciones del Ayuntamiento de Sestao. En los puntos 4 a 8 se describen las características mínimas de la que debe cumplir la nueva instalación.

- Se trata por tanto de una prestación de suministro y servicio “llave en mano”, por la que el adjudicatario deberá proveer todos los elementos técnicos y humanos, el conocimiento, el hardware, el software, las licencias y las configuraciones necesarias de tal forma que el conjunto quede listo para su plena utilización.

- Dado que el Ayuntamiento de Sestao debe cumplir el ENS, se valorará que la empresa adjudicataria disponga de certificación del ENS en niveles medio o alto.

- Los trabajos incluirán la instalación de todos los elementos y la realización de las configuraciones necesarias para su integración en la red del Ayuntamiento. De modo no exhaustivo se detallan las siguientes tareas:

a. Migración de los cortafuegos actuales
   - Ajuste de nuevas reglas según criterios del Ayuntamiento de Sestao
   - Pruebas de validación
   - Integración con herramientas de logs y alarmas.

b. Seguridad IT. Instalación de cortafuegos en el resto de las ubicaciones (descritas en el apartado 5)
   - Definición de firmas de aplicación o IPS personalizadas en aquellas ubicaciones que sea necesario.
   - Parametrización de reglas en cada ubicación según requerimientos de cada uno de los diferentes servicios del Ayuntamiento de Sestao.
   - Pruebas de validación y verificación de correcto funcionamiento del servicio según la configuración definida para cada servicio, en cada ubicación.

c. SD-WAN
   - Análisis de tráfico de cada ubicación para definición de matriz de comunicaciones.
   - Configuración de las políticas aplicadas a las conexiones mediante SD-WAN

d. Plataforma de gestión e. Plataforma de analítica
   - Configuración de todos los equipos en la misma.
   - Configuración de métricas y reportes según indicaciones del Ayuntamiento de Sestao.

f. Plataforma Wireless
   - Instalación de una nueva plataforma Wireless formada por puntos de acceso WiFi 6 y con controlador integrado en el firewall.
   - Instalación de nuevo cableado desde el CPD hasta los puntos de acceso distribuidos por las diferentes plantas de dos edificios.

g. Servicio de Consultoría de Adecuación a ENS
   - Evaluación del estado de cumplimiento en materia de gestión de la seguridad de la información de acuerdo a los requerimientos aplicables en el ENS.
   - Preparación del organismo para abordar de una forma racional el cumplimiento en materia de seguridad de la información de acuerdo a los requerimientos del ENS.

h. Herramienta de protección de servidores ante ataques Ransomware

   Instalación y puesta en marchas de una herramienta para la protección de 3 servidores Microsoft ante ataques Ransomware

- Para facilitar la gestión centralizada, los equipos Firewall, Wireless y de monitorización deberán ser del mismo fabricante.

- El servicio de mantenimiento correctivo de 4 años de duración, se aplicará a la resolución de incidencias (in situ o en remoto) generadas por problemas o mal funcionamiento de los equipos incluidos en contrato, incluyendo las tareas necesarias hasta conseguir la restauración del servicio y otras asociadas a la gestión de incidencias y mejora continua, como pueden ser:
  a. Reparación y/o sustitución de elementos averiados para lo que debe incluir el servicio de soporte del fabricante en formato 24x7x365 durante 4 años.
  b. Trabajos de reconfiguración de equipos.
  c. Instalación de software por: fallo, vulnerabilidades publicadas que afecten, necesidad de actualización detectada en el mantenimiento preventivo o por indicación del fabricante.
  d. Pruebas para verificación de la reposición del servicio.
  e. Escalado a fabricantes.

f. Soporte técnico avanzado propio y soporte especializado experto del fabricante en el ámbito de la incidencia. Acceso al Centro de Asistencia Técnica del fabricante para la resolución de problemas.
g. Servicio de atención y gestión de incidencias para la gestión de averías, reemplazos, gestión de stock y de garantía, así como para la apertura de casos con el fabricante.
h. Asistencia y soporte remoto y telefónico que permita resolver incidencias, aunque no impliquen fallos graves del servicio.
i. Sustitución del equipamiento averiado.
j. Actualización de las versiones del software de los equipos y acceso a parches para la resolución de fallos.
k. Registro, seguimiento y documentación de la incidencia hasta su resolución.

- El mantenimiento preventivo (proactivo) será anual y conllevará la realización de propuestas orientadas a mejorar el rendimiento y/o disponibilidad de la red e incluirá un análisis de las versiones software en los equipos, buscando el reducir el número de incidencias a futuro en la red, la revisión hardware, obsolescencia tecnológica y fechas de fin de vida. En cada informe preventivo, se reflejarán las acciones sobre el hardware/software que se consideren necesarias:
    i. Propuesta.
    ii. Ventajas/inconvenientes de la migración.
    iii. Inconvenientes de la no migración.
    iv. Estimación de esfuerzo e impacto sobre el servicio
    v. Observaciones si las hubiera.

- Para el desarrollo de los servicios de mantenimiento, el centro de soporte del adjudicatario debe apoyarse en procedimientos reglados por las recomendaciones y cumplimientos obligados y teniendo en consideración las buenas prácticas recomendadas por ITIL V3, debiendo disponer de manera obligatoria de las siguientes certificaciones o equivalentes:
    - UNE-EN ISO 20000 Certificado de Sistemas de Gestión de Servicio de Tecnologías de la Información
    - ISO 27001 de Gestión de la Seguridad de la Información

- Renovación de las garantías de equipos. Se renovarán las garantías de los equipos objeto de contrato hasta el periodo de validez del contrato indicado.

- Se definirán unos acuerdos de nivel de servicio (SLA) que serán de aplicación para todos los servicios indicados en el pliego. No obstante, a lo indicado a continuación, el adjudicatario podrá describir en su propuesta otros acuerdos de nivel de servicio, respetando en todo caso los mínimos establecidos en el presente pliego.

- Los niveles de servicio propuestos por el adjudicatario, deberán ser validados por el Ayuntamiento de Sestao al inicio del contrato, quien se reserva el derecho de modificarlos si no los considera adecuados para asegurar la calidad del servicio prestado.

- El acuerdo de nivel de servicio mínimo que deberán prestar por el adjudicatario para el mantenimiento correctivo es el siguiente:
    a. Horario de prestación del servicio: 24x7.
    b. Tiempo de atención de incidencias:
        - No urgente 12 horas
        - Normal 4 horas
        - Severa 2 horas
    c. Tiempo de resolución (restauración del servicio en remoto):
        - No urgente 24 horas

- Normal 8 horas
- Severa 4 horas

d. Devolución del equipo averiado.

- Con el fin de cumplir los acuerdos de nivel de servicio mínimos, el adjudicatario dispondrá de los acuerdos y contratos de soporte y mantenimiento necesarios con el fabricante, de los cuales aportará los correspondientes certificados del fabricante donde se especificará el detalle de base instalada cubierta.

- El Ayuntamiento de Sestao dispondrá de una bolsa de horas a utilizar durante los cuatro años siguientes a la fecha de inicio del contrato para actualización de la configuración tras la puesta en marcha en cualquiera de las plataformas objeto del contrato de una duración de 40 horas en total.

- El adjudicatario proporcionará la formación necesaria a los administradores del Ayto. de Sestao sobre la nueva infraestructura de seguridad, SD-WAN y WiFi desplegada, con una duración mínima de 84 horas lectivas.

- Esta formación estará encaminada a que los administradores de sistemas del Ayuntamiento de Sestao puedan obtener las certificaciones del fabricante. En concreto, el adjudicatario deberá ofrecer la formación oficial del fabricante y asesoramiento necesarias para que dos personas del equipo de Informática obtengan el primer nivel técnico de certificación en ciberseguridad de este fabricante y otra alcance el máximo nivel técnico de certificación en ciberseguridad del fabricante.

- A efectos de valoración de la oferta técnica, se presentará un documento descriptivo del planteamiento global y un plan de implantación completo de la solución propuesta. También se incluirá un plan de formación, dirigido al personal responsable de la administración de las plataformas instaladas, con indicación de tiempos previstos para cada tipo de formación y su contenido.

- Ámbito territorial

  El ámbito territorial para el desarrollo de los trabajos, cuando estos precisen una realización in-situ, comprenderá la totalidad de la zona de servicio del Ayuntamiento de Sestao.

  Expresamente se mencionan:

  - En Oficinas Generales del Ayuntamiento.
  - En Sede de Policía Local
  - En el Euskaltegi Municipal
  - En el Edificio de Jardinería
  - En la Residencia Municipal

- Propiedad de los trabajos

  Todo trabajo desarrollado por el adjudicatario durante la vigencia del presente contrato, incluyendo la documentación correspondiente, será propiedad exclusiva del Ayuntamiento de Sestao. El adjudicatario no podrá conservar copia en ningún soporte, ni facilitarlo a terceros sin la expresa autorización del Ayuntamiento de Sestao

- Horario de los trabajos

  El horario habitual de prestación de servicios para el Ayuntamiento de Sestao será durante todo el año de lunes a viernes, desde las 8:00 hasta las 15:30 horas.

- Con independencia de la organización que el licitador oferte para el desarrollo de los trabajos, se estima que, por circunstancias del servicio, un 5 % de las horas anuales de trabajo estimadas habrán de ser realizadas fuera del indicado horario habitual.

- El licitador habrá de tener en cuenta esta circunstancia para confeccionar su oferta, puesto que sólo se admitirá un único precio unitario por hora de trabajo en relación con los componentes del equipo.

- Para todos los servicios y trabajos, con presencia in-situ, el licitador deberá cumplimentar toda la documentación requerida por el técnico de Prevención de Riesgos Laborales, además de entregar la documentación que se le solicite al respecto sobre los aparatos instalados (fichas de riesgos,…).

- Ubicación

  Durante la ejecución del contrato, salvo indicación expresa del Ayuntamiento de Sestao el adjudicatario realizará los servicios correspondientes en sus propias instalaciones, corriendo con todos los gastos derivados de las líneas de telecomunicaciones necesarias, si se dieran. Sin embargo, el Ayuntamiento de Sestao podrá requerir la presencia in-situ del adjudicatario para labores de definición, seguimiento, implantación, puesta en marcha, correcciones urgentes o cualquier otro servicio que demande el Ayuntamiento de Sestao.

- Documentación

  Para todos los servicios y trabajos, además de su realización técnica, el adjudicatario deberá entregar, como parte intrínseca de dichos trabajos, toda la documentación generada durante la realización de los mismos, considerándose absolutamente imprescindible los análisis funcionales y técnicos y los manuales de usuario.

  Toda la documentación, tanto técnica, operativa o de usuario, generada durante la ejecución del contrato, será propiedad exclusiva del Ayuntamiento de Sestao sin que el adjudicatario pueda conservarla, ni obtener copia de la misma o facilitarla a terceros sin la expresa autorización del Ayuntamiento de Sestao.

  El adjudicatario deberá suministrar al Ayuntamiento de Sestao las nuevas versiones de la documentación que se vayan produciendo. También se entregarán, en su caso, los documentos sobre los que se haya basado el diseño de las operaciones, documentos de trabajo previos, etc.

- Condiciones de seguridad y propiedad de los trabajos

  Sin menoscabo de las leyes y normativas que sean de aplicación, el licitador deberá considerar y reflejar en su oferta de servicios los siguientes aspectos relacionados con la seguridad informática:

  • <u>Acceso a los Sistemas de Información</u>

    Los sistemas, aplicaciones o herramientas a los que el Ayuntamiento de Sestao facilite el acceso al adjudicatario para ejecutar sus trabajos, deberán ser utilizados únicamente con este fin. Todo el personal del adjudicatario que acceda a cualquiera de los sistemas del Ayuntamiento deberá hacerlo con el identificador facilitado para ello, que será personal e intransferible. Cada empleado del adjudicatario al que se provea de un identificador para la ejecución de trabajos relacionados con este pliego será responsable de mantener la confidencialidad de las contraseñas u cualesquiera otros métodos de autenticación.

  • <u>Acceso a los Datos</u>

    La información y datos que el adjudicatario deba utilizar para la realización de sus trabajos, o sea producida como consecuencia de los mismos, son propiedad del Ayuntamiento de Sestao y no podrán ser utilizados para otros fines que no sean la prestación de los Servicios, quedando prohibida su copia en cualquier

soporte, sin previa autorización. En caso de autorización para el uso o copia de cualquier información, el adjudicatario se comprometerá a destruirla físicamente, cualquiera que sea su formato, una vez finalizados los trabajos para los que fueron creados.

El adjudicatario deberá mantener secreto sobre los datos e información a los que haya podido tener acceso, obligación que persistirá incluso después de finalizado el contrato.

- Acceso Físico

  El adjudicatario deberá facilitar la lista de empleados que deban acceder a los recintos para la resolución de incidencias y problemas que requieran de actuaciones in-situ. Además, cuando para la realización de los proyectos y actuaciones sea necesario acceso a ciertas ubicaciones, el adjudicatario lo comunicará al Responsable del Contrato del Ayuntamiento con la antelación suficiente para que pueda revisar y autorizar la petición.

- Protección de Datos y Seguridad de la Información

  El adjudicatario queda obligado al cumplimiento de lo establecido en la legislación sobre Protección de Datos de Carácter Personal y sobre Seguridad de la Información en el marco de los servicios prestados.

3. - REQUISITOS ESPECÍFICOS DE LA SOLUCIÓN DE SEGURIDAD Y SD-WAN

El objetivo de la solución de seguridad descrita en este apartado es la de proporcionar una solución integral para proteger las ubicaciones detalladas del Ayuntamiento tanto en términos generales como en específicos de entornos IT.

Se instalarán cortafuegos de tres tipologías en las ubicaciones del Ayuntamiento de Sestao con las siguientes características mínimas, en base a la tipología de la ubicación. Las características mínimas de cada tipología se detallan en el punto 12 de este apartado.

TIPO DE EQUIPAMIENTO	UNIDADES
Cortafuegos Tipo 1	2
Cortafuegos Tipo 2	3
Cortafuegos Tipo 3	1
Consola de gestión centralizada	1
Consola de análisis de eventos	1

1. Con carácter general, todos los cortafuegos deberán tener las siguientes características:
   - Capacidad de configuración de proxy explícito por interfaz, pudiendo hacer proxy chaining en caso de ser necesario.
   - Visualización de número de usos y cantidad de tráfico de cada regla. Así como de la última vez que se ha utilizado.
   - Funcionalidad integrada de Traffic Shaping tanto de tráfico saliente como entrante siendo capaz de reservar ancho de banda y marcar el tráfico con DSCP.
   - Deberá permitir la creación de firmas específicas de IPS.
   - Controles por aplicación y usuario.
   - Deberá permitir trabajar con listas blancas y negras de urls.
   - Deberá incluir firmas específicas para proteger entornos industriales, incluidas al menos 1300 firmas para entornos OT.
   - Funcionalidades de acceso VPN con identificación por usuario/contraseña y certificado digital.
   - Protección ante pérdida de datos.
   - Balanceo de salidas en Internet de forma dinámica (sd-wan).

- Certificaciones de Internet Computer Security Association (ICSA): Cortafuegos, IPSec, IPS, Antivirus; y Common Criteria.

Adicionalmente, la solución debe tener las siguientes características avanzadas:

2. **IDENTIFICACIÓN DE USUARIOS**
   - Identificar usuarios, integrándose con Microsoft Active Directory y Novel eDirectory
   - Control de usuarios Citrix.
   - Control de usuarios de Microsoft Terminal Server.
   - Soporte de mensajes Radius Accounting para SSO.
   - Autenticación en servidores remotos mediante LDAP, RADIUS y TACACS+

3. **VISIBILIDAD**
   - Funcionalidad de consolidación de logs y diferentes niveles de agrupación (origen, destino, aplicación, amenaza, websites, etc) para su visualización.
   - Esta visualización tiene que ser tipo "Drill-down", es decir, poder seleccionar unos de los objetos agrupados e ir filtrando el resultado en base a esta selección, hasta saber el detalle completo.

4. **CONTROL DE APLICACIONES**
   - Capacidad para identificar un mínimo de 4000 aplicaciones activas actuales (incluyendo aplicaciones Web 2.0)
   - La solución debe clasificar las aplicaciones en diferentes categorías y subcategorías, para poder aplicar reglas de acuerdo con estas categorías / subcategorías (control granular dentro de la aplicación)
   - Aplicar técnicas de identificación de aplicaciones a todos los puertos TCP / UDP y no sólo en los más comunes.
   - Capacidad para identificar las aplicaciones bajo túneles HTTPS.

5. **SEGURIDAD**
   - Arquitectura basada en interfaces, para la aplicación de políticas de seguridad.
   - Capacidad para definir múltiples reglas de seguridad en las interfaces origen / destino, incluyendo "año".
   - Debe soportar varios modos de funcionamiento:
     - Modo transparente.
     - Modo routed y / o modo sniffer.
   - DLP: capacidad de búsqueda de patrones como DNI, tarjetas de crédito, etc., así como a asociaciones concretas. Más funcionalidades:
     - Posibilidad de definición de los tipos de dato en función de palabras clave, palabras clave ponderadas, expresiones regulares, atributos de archivo, diccionario, plantillas corporativas
     - Detección e identificación de documentos mediante "Fingerprint"
     - Posibilidad de añadir marcas de agua en los documentos de office.
   - Monitorizar y controlar la navegación web pudiendo trabajar con listas blancas y negras.
   - Funcionalidad integrada del mismo fabricante de doble factor de autenticación vía token hardware o software, asi como por SMS, integrado en la misma plataforma de seguridad.
   - Funcionalidad de reconocimiento del tipo de dispositivo del cliente (Iphone, Ipad, Android, etc...) y poder hacer políticas en función del tipo

de dispositivo, sin la instalación de ningún agente en el dispositivo remoto.

- Funcionamiento como IPS basado tanto en patrones (basado en firmas con más de 11000 firmas prestablecidas) como en "Rated based". Posibilidad de crear firmas de IPS customizadas.
- Session helpers y ALGs: dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS (Oracle)
- Soporte para tráfico VoIP: SIP/H.323 /SCCP NAT trasversal, RTP
- Soporte para diferentes tipos de protocolos: SCTP, TCP, UDP, ICMP, IP
- Definición de objetos para aplicación en políticas de seguridad, de diferentes tipos: IP, Subnet, intervalo de IPs, Geografia y FQDN
- Detección y bloqueo de botnets en base a listas de reputación globales
- Inspección de tráfico cifrado SSL

6. **VPN**

- El sistema propuesto deberá cumplir los estándares de la industria, sin el apoyo externo adicional de hardware o módulos:
  - IPSEC VPN (IPv4 e IPv6)
  - PPTP VPN
  - L2TP VPN
  - SSL VPN
  - GRE sobre IPSEC
  - ADVPN
- El sistema propuesto deberá soportar 3 modos de funcionamiento SSL VPN:
  - Sin cliente - Acceso web: para clientes remotos que sólo necesitan un navegador y no requiere la instalación de ningún agente, a fin de acceder vía web en: HTTP / HTTPS Proxy, FTP, Telnet, SMB / CIFS, SSH, VNC y RDP.
  - Modo túnel: para equipos remotos que ejecutan una variedad de aplicaciones de cliente y servidor
  - Modo Puerto Forwarding: utiliza un applet de Java que escucha en el puerto local en el ordenador del usuario. Cuando se recibe datos desde una aplicación de cliente, el puerto delantero cifra y envía los datos al dispositivo SSL VPN, que reenvía el tráfico en el servidor de aplicaciones.

7. **ALTA DISPONIBILIDAD**

- Failover Activo / Pasivo, Activo / Activo y clustering sin necesidad de licencia.
- Sincronización de configuración y sesiones.
- Interfaces reservados para gestión.
- Posibilidad de configurar interfaces HeartBeat redundantes.

8. **NETWORKING**

- Soporte de protocolos soportar RIP v1 y v2, OSPF, ISIS, BGP y Multicast para IPv4 e IPv6.
- Routing basado en política.
- Soporte Dual Stack IPv4 e IPv6 simulatáneamente.
- Network address translation NAT IPv4, NAT64 y NAT66.
- DHCP server / DHCP Relay
- DNS Server y DNS Proxy
- NTP Server
- 802.1Q VLANs
- Routing basado en contenidos: ICAP y WCCP

- Point-to-Point Protocol over Ethernet (PPPoE).
- Capacidades de virtualización: Los equipos deben disponer de al menos 10 dominios virtuales incluidos en el cortafuegos sin coste adicional.
- 802.3ad Capacidad de crear enlaces LACP para la agregación de puertos.
- Capacidad alanceo de servidores, con posibilidad de hacer SSL offloading para el tráfico HTTPS.

9. **GESTIÓN Y ADMINISTRACIÓN**

- Soporte de SNMP y sFlow.
- Exportación de logs vía SYSLOG, FTP, SCP y TFTP.
- Administración por GUI y CLI directamente en el equipamiento, sin necesidad de instalar un cliente en máquina externa al firewall para su administración y / o cualquier otra función del firewall.
- Creación de diferentes cuentas de administración con diferentes niveles de acceso.
- Aplicación de cambios de forma inmediata, sin ninguna espera en su aplicación.
- Adicionalmente se debe asegurar la gestión centralizada de todos los equipos que se desplieguen desde una plataforma de gestión centraliza, el número de equipos a gestionar en un futuro puede ascender a 100 por lo que se debe de tener en cuenta este número total de dispositivos.
- Por otro lado, se desea que exista una plataforma de gestión de logs centralizada para todos los equipos debiendo permitir esta plataforma el almacenamiento de 6 gb al día y 3 tb de capacidad.

10. **SD-WAN**

- Los cortafuegos deben tener integrado un sistema SD-WAN (SD-WAN con seguridad integrada) que proporcione una selección de ruta dinámica entre las opciones de conexión de cada sede con capacidad de identificación de la aplicación.
- El sistema debe ser capaz de realizar un balanceo de carga de los enlaces de Internet de forma dinámica con métodos opcionales de:
    - Para ip de origen
    - Ponderado
    - Weighted-based
    - Spill-over (también llamada basada en el uso)
    - Para calidad de la linea de internet para latencia y jitter (de forma dinámica)
    - El sistema debe de ser capaz de balancear al menos 5 líneas.
    - El sistema debe ser capaz de proporcionar redundancia de enlaces WAN monitorizando el estado de las líneas
- El sistema debe garantizar una administración y orquestación centralizadas y unificada con la operativa de red y seguridad. Ante la posibilidad de crecimiento en el número de conexiones, deberá tener capacidad de aprovisionamiento sin intervención.

11. **FUNCIONALIDADES (licenciamiento incluido)**

El sistema deberá tener licencias para las siguientes funcionalidades durante toda la duración del contrato

- Control de aplicaciones
- IPS, con firmas para protección de entornos industriales

- Antivirus
- Threat protection
- Ip reputation & antibotnet security
- Filtrado de contenidos
- Antispam
- Sandbox cloud
- Mobile Security
- Capacidad para eliminar contenidos dinámicos de un documento para poder analizarlo entregando al usuario un primer archivo sano, sin contenido dinámico.
- Herramienta integrada de auditoria donde se pueda evolucionar un rating de seguridad de firewall.
- Comprobación de firmas de AntiVirus en tiempo real contra una base de datos de inteligencia global del fabricante, sin esperar a recibir el paquete de actualización de firmas
- Doble factor de autenticación integrado en la misma plataforma y del mismo fabricante
- La solución debe proveerse en alta disponibilidad física.

12. **A continuación, se describen las características mínimas** que deberían tener los cortafuegos a instalar en cada ubicación:

IMPORTANTE:
En el caso de que el fabricante ofrezca varias mediciones de rendimiento para la misma máquina, se considerará únicamente la que ofrezca menor rendimiento Todas las tipologías deben de compartir sistema operativo, así como mismas funcionalidades.

	TIPOLOGIAS		
	1	**2**	**3**
Rendimiento para paquetes de 64 bytes Gbps	24	6	5
Rendimiento para paquetes de 1518 bytes Gbps	32	10	5
Sesiones concurrentes	4.000.000	700.000	700.000
Nuevas sesiones por segundo	450.000	35.000	35.000
Latencia para paquetes 64 byte UDP (µs)	2,14	3,3	2.97
Rendimiento IPS Mbps	7.800	1.400	1.000
Threat protection Mbps	5.000	700	600
Inspección SSL Mbps	4.800	630	310
Rendimiento de VPN SSL Mbps	4.500	900	490
Rendimiento IPSec (paquetes 512 bytes). Gbps	20	6.5	4.4
Usuarios simultáneos VPN SSL sin licencia adicional.	5.000	200	200
Puerto de consola	1	1	1
Puertos USB	2	1	1
Puertos GE RJ45	16	5	3
GE RJ45 MGMT/HA Ports	2	0	0
GE SFP Slots	16	0	0
GE RJ45 WAN Ports		2	1
GE RJ45 DMZ Port		1	0
GE RJ45 HA Ports		2	1

13. **Consola de gestión centralizada**

El adjudicatario deberá proveer al ayuntamiento de una consola de gestión centralizada de toda la solución con capacidad de gestionar todos los elementos que la conforman. No se admitirán soluciones en nube.

Las licencias necesarias deberán tener una validez de 4 años.

14. **Consola de Análisis y eventos** La solución deberá disponer de una herramienta de correlación de logs con capacidad de hacer búsquedas sobre logs almacenados en los dispositivos involucrados en la solución (al menos de Firewall y SDWAN) y generar acciones automáticas de remediación. La solución deberá proveerse en formato virtual, con capacidad de 6 GB/Dia de Logs y 3Tb de capacidad de almacenamiento. GB/Day ilimitados cuando se use solo en modo colector.

Las licencias necesarias deberán tener una validez de 4 años.

4. - REQUISITOS ESPECÍFICOS PARA LA CONSULTORÍA DE CERTIFICACIÓN ENS

El adjudicatario deberá proporcionar un Servicio Profesional de Consultoría de Evaluación y Soporte para cumplimiento en materia de Seguridad de la Información, de los requisitos establecidos en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración.

Los objetivos generales de este servicio de consultoría son proporcionar al Ayuntamiento de Sestao una visión global de su nivel de cumplimiento actual, un plan de adecuación y servicios profesionales para ayudarle al cumplimiento.

- Evaluar el estado de cumplimiento en materia de gestión de la seguridad de la información de acuerdo a los requerimientos aplicables en el ENS.
- Preparar el organismo para abordar de una forma racional el cumplimiento en materia de seguridad de la información de acuerdo a los requerimientos del ENS.

Estos objetivos generales se desarrollan en objetivos específicos, que se pueden resumir en los siguientes:

- Analizar los procesos y la información gestionada para realizar la categorización del sistema.
- Desarrollar la Categorización del Sistema de acuerdo a los requisitos establecidos en el ENS.
- Definir la propuesta de Política de Seguridad de la Información de acuerdo a las guías de seguridad aplicables.
- Definir una propuesta de composición del Comité de Seguridad de la información y los criterios de funcionamiento.
- Realizar un análisis cumplimiento de las medidas de protección aplicables del ENS.
- Desarrollar un análisis de riesgos de acuerdo a los requisitos aplicables por el ENS.
- Detectar las carencias de materia de cumplimiento ENS.
- Elaborar un plan de adecuación con los proyectos más relevantes.
- Como producto del servicio se construirán diferentes entregables y un entregable principal denominado Plan de mejora ENS.

Este servicio se desarrollará a partir de una bolsa de mínimo 80 horas de un consultor que deberá tener al menos dos de los siguientes requisitos de titulación o equivalentes:

- ISACA: Certified Information Security Manager (CSIM)
- ISACA: Certified Information System Auditor (CISA)
- (S-0B) Especialista Implantador ISO 27001 SGSI
- (S-05) Auditor interno ISO 27001 SGSI

5. - REQUISITOS ESPECÍFICOS DE LA HERRAMIENTA DE PROTECCIÓN DE SERVIDORES ANTE ATAQUES RANSOMWARE

Con el objetivo de mejorar la capacidad de respuesta ante incidentes de ransomware, se requiere la provisión de una herramienta de remediación que ante un ataque de ransomware desconocido por el antivirus, permita la rápida recuperación de los sistemas soportados, para 3 servidores con sistema operativo Windows Server 2008 R2, 2012 y 2016 del Ayuntamiento durante 4 años. La herramienta debe proteger la información de los servidores de manera transparente y centralizada desde el Centro de soporte del licitador.
Requerimientos y funcionalidades:

- El software debe proteger el sector de arranque o inicio de la unidad para evitar que tipos agresivos de ransomware se hagan cargo del proceso de inicio y eviten que las aplicaciones escriban en el registro de inicio.

- Protección y supervisión del acceso directo al disco evitando que programas maliciosos destruyan datos en el disco duro o SSD.

- Recuperación del sistema dañado desde la interfaz de administración de la herramienta, así como de los archivos encriptados desde la interfaz de administración.

Funcionalidades:

- Mirror Shielding o tecnología equivalente
- Bloqueo de archivos
- Protección de disco en la nube
- Protección de arranque
- Protección contra borrado de disco
- Revisiones de archivos utilizando Data Engrams o tecnología equivalente
- Protección de carpeta personalizada
- Protección y recuperación de archivos de datos de manera rápida y sencilla con un clic
- Evitar que el ransomware se haga cargo del proceso de arranque
- Evitar que el malware borre datos en el disco duro
- Detectar y proteger contra amenazas conocidas y desconocidas
- Restaurar el sistema a un estado correcto, libre de amenazas
- Proteger las carpetas de unidades locales en la nube permitiendo que los datos destruidos o corruptos se recuperen rápidamente **sin conexión a Internet**. Debe admitir soluciones tipo OneDrive, Google Drive, DropBox y Box.com
- La solución de protección debe tener gestión en la nube
- Debe ser una solución multicapa con protección de archivos, arranque y disco
- Debe proteger los archivos evitando que se modifiquen los archivos originales:
  - Las aplicaciones ven una imagen espejo de los archivos protegidos
  - Recuperación instantánea

✓ Esta solución debe proteger a un total de **3 servidores** durante un periodo de 4 años y el licitador deberá estar certificado por el fabricante de la solución propuesta.

6. - REQUISITOS ESPECÍFICOS DE LA SOLUCIÓN DE CONECTIVIDAD INALÁMBRICA Y CABLEADO PARA LAS SEDES DEL AYUNTAMIENTO Y EL EDIFICIO CASTAÑOS

El objetivo es dotar a las sedes del Ayuntamiento y del Edificio Castaños de una nueva red WIFI, tanto para los empleados del ayuntamiento como para sus visitas, garantizando el aislamiento del tráfico de empleados con respecto al de los visitantes.
Es un servicio que impulsará la comodidad y las capacidades de comunicación e integración de forma exponencial.

El lugar de suministro, instalación y configuración de los componentes, así como de prestación de los servicios demandados, será la Sede Central del Ayuntamiento y en la sede del Edificio Castaños.

El proyecto es dotar de Red WIFI a estos dos edificios, los cuales actualmente no tienen infraestructura WIFI ni cableado apropiado para soportarla.
El licitante, cableará todos los APs necesarios para dotar de cobertura Wifi a cada centro. Tras el cableado, el cual se realizará en las diferentes plantas, los puntos se unificarán en un nuevo Switch en cada edificio, proporcionados por el licitador, los cuales se instalarán en la habitación de comunicaciones correspondiente donde están actualmente los RACKs en cada edificio. En los mismos existe espacio suficiente para la instalación de los puntos de parcheo y los dos nuevos Switches. Estos Switches serán configurados con las VLANs indicadas por el Ayuntamiento, para invitados o personal propio del centro y así organizar mejor las capacidades tanto en la parte de seguridad como en la gestión del ancho de banda.

Específicamente se habrán de suministrar como mínimo los siguientes equipos HW:

- 22 uds APs WiFi.
- 2 uds de Switches de 24 puertos, L2+ Gigabit Ethernet - PoE

Habrá de incluirse soporte y mantenimiento extendido durante 4 años.

Características Técnicas de los Switches:

Los Switches serán de 24 puertos Gigabit Ethernet y 4 puertos 10 GE SFP+. Deberá funcionar con los estándares de comunicación IEEE 802.3af y IEEE 802.3at. El modelo ha de gestionar 10G y tecnología PoE. La transferencia de datos se desarrollará a una velocidad mínima de 128 Gbit/s. El dispositivo deberá estar destinado para su montaje en bastidores.
La potencia mínima PoE deberá ser de al menos 370W con gran rendimiento, soporte PoE+ y conmutación inteligente para redes WIFI, totalmente gestionable a través de la plataforma de firewall.

Características mínimas de los Switches	
Puertos	24x GE RJ45 y 4x 10GE SFP+
Power over Ethernet Ports	24 (802.3af/at)
PoE Power Budget	370 W
Capacidad de switching (dúplex)	128 Gbps
Gestionable	Si
Nivel OSI	Nivel 2+

Características Técnicas de los Aps.

Dispositivos son para uso interno, con soporte de tecnología 802.11ax. El punto de acceso ofrecido habrá de admitir dual band y tecnología 2x2 MIMO en 5 GHz. También habrá de disponer de botón de reset en el AP, puertos de conectividad principal, puerto secundario, con un mínimo de velocidad de hasta 574 Mbps para una frecuencia de 2,4 GHz y de 1201 Mbps para 5 GHz. Deberá disponer du una tercera radio para realizar monitorización tanto en la banda de 2,4

GHz como en la de 5 GHz. El dispositivo se alimentará tanto a través de una fuente de alimentación dedicada o utilizando switches estándar PoE como los suministrados en la solución indicada con un consumo máximo de 17W.
Con el objeto de mejorar la seguridad del tráfico inalámbrico, los puntos de acceso deberán asociarse a un controlador que esté integrado en la plataforma firewall del edificio correspondiente.

Características principales
- Para uso en el interior de edificios
- Gran rendimiento
- Manejo intuitivo
- Tecnología 2x2 11AX MIMO
- Escalabilidad

Características de los puntos de acceso	
Estándar WiFi	802.11 AX (Wifi 6)
Número de radios	3 + 1 BLE
Número de antenas	3 Dual band Internal Wi-Fi + 1 BLE/ZigBee
Ganancia	4.5dBi para 2.4Ghz y 5.5dBi para 5GHz 4.5 dBi para antena BLE
MIMO radios de 2.4 y 5 GHz	2x2
Data Rate Radio 1 (2.4 GHz)	574 Mbps
Data Rate Radio 2 (5 GHz)	1201 Mbps
Puertos	2x 10/100/1000 Base-T RJ45 1x Type 2.0 USB 1x RS232 RJ45 Serial Port
Power over Ethernet	802.3at PoE. Consumo max. 17W
Protocolos y estándares soportados	EAP Type(s) EAP-TLS, EAPTTLS/MSCHAPv2, PEAPv0/EAPMSCHAPv2, PEAPv1/EAPGTC, EAP-SIM, EAP-AKA, EAP-Fast 802.11a, 802.11b, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11w, 802.11ac, 802.11ax, 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az
Autentificación	WPA™, WPA2™, and WPA3™ with 802.1x or Preshared key, WEP, Web Captive Portal, MAC blocklist & allowlist
Máxima potencia de transmisión	Radio 1: 2.4GHz: 23 dBm / 200 mW Radio 2: 5GHz: 22 dBm / 158 mW
Modo de trabajo	Modo túnel, Local-bridge y Mesh

El adjudicatario deberá instalar un nuevo trazado de cableado entre los switches instalados en el CPD y los puntos de acceso distribuidos por las diferentes plantas de cada edificio:

-Edificio Castaños consta de 5 plantas con al menos 13 puntos de acceso, ampliable a 20 puntos de acceso entre sus plantas.

-Edificio Central del Ayuntamiento consta de 4 plantas con al menos 9 puntos de acceso, ampliable a 12 puntos de acceso entre sus plantas.

En aquellas zonas en las que no se pueda hacer uso de la canalización existente, tanto vertical como horizontal, se priorizará realizar un nuevo trazado por falso techo, con canaleta de superficie hasta el puesto de trabajo.
El licitador deberá de proponer una solución de última generación instalando cableado de Categoría 6 o superior. Estas tomas servirán para la conexión de los APs de la nueva red WIFI.

Se solicitará material de cableado de tipo COMMSCOPE o similar, especializado en la fabricación e innovación de alta calidad de soluciones de cableado de red de alto rendimiento, el licitador deberá ofrecer 25 años de garantía en el cableado, debiendo ser instalados por técnicos Instaladores Certificados por COMMSCOPE, siguiendo las pautas de diseño, planificación e instalación del fabricante, se exige que tanto la empresa instaladora del cableado como la empresa que instale, suministre y configure los APs, sea la misma.

Para completar el proyecto, se habrán de incluir tanto la parte de canalizaciones, tubos y materiales adicionales necesarios para el correcto funcionamiento del sistema, todo ello de fabricantes de primer nivel de calidad utilizados habitualmente en el mercado español.

7. - ENTORNO TECNOLÓGICO

El Ayuntamiento de Sestao dispone de diversas ubicaciones conectadas mediante túneles VPN a través un operador de telecomunicaciones con las Oficinas Centrales.
Las Oficinas Centrales tienen 3 salidas WAN para proporcionar diferentes servicios.

A continuación, se relacionan dichas ubicaciones, agrupadas por "Tipología". Cuanto menor es el número de tipología, más importancia tiene dicha ubicación.

En la actualidad, el Ayuntamiento de Sestao dispone de un sistema redundante de cortafuegos en la Sede de Oficinas Centrales del fabricante PF-Sense que se usa exclusivamente para asegurar las comunicaciones hacia y desde Internet. Los cortafuegos a instalar en las Oficinas Centrales del Ayuntamiento deberán estar redundados en alta disponibilidad.

Tipología	Número de sedes	Ubicación	Localidad	Tipo Conexión
1	1	Ayuntamiento de Sestao (Oficinas Centrales)	Sestao	2 líneas de 1000Mbps 1 línea de 500Mbps
2	3	Residencia Euskaltegi Policía Municipal	Sestao	Línea de 500 Mbps Línea de 500 Mbps (se dotará de línea de 500 Mbps)
3	1	Brigada Jardinería	Sestao	Línea de 500 Mbps

8. - METODOLOGÍA PARA LA EJECUCIÓN DEL CONTRATO:

El licitador deberá presentar necesariamente en su propuesta técnica una Metodología para la ejecución del contrato.

1. Modelo de relación

El licitador deberá describir, de forma detallada, el modelo por el cual propone coordinar su relación con el Ayuntamiento. Se debe definir un modelo orientado al servicio, documentado y con plena trazabilidad de las decisiones tomadas y de los trabajos realizados.
Este modelo debería incluir, como mínimo, los siguientes extremos:

- Ámbitos de decisión y personas autorizadas.

- Detallar la organización del licitador de cara al Ayuntamiento de Sestao. Personas con poder de decisión que intervengan en el desarrollo del contrato.
- Fases del proyecto y actividades del mismo.
- Descripción y duración de las fases que debe comprender el proyecto, así como una descripción de las actividades a realizar en cada una.
- Formato y periodicidad de las reuniones de trabajo.
- Composición, si procede, de comités de trabajo.
- Definir los formatos de los diferentes tipos de reuniones.
- Documentación de las mismas.
- Documentaciones a producir.
- Formato de la documentación que garantice la plena transparencia y trazabilidad de todas las actuaciones realizadas, tanto en el aspecto técnico como en el administrativo.

2. Además de lo que el licitador pueda proponer más concretamente en su oferta, el Ayuntamiento considera que se deben observar las siguientes líneas básicas:
    - La fase de instalación, consistente en el periodo que va desde el inicio del contrato hasta la plena instalación y funcionamiento de la totalidad de la solución de seguridad demandada, no debe prolongarse más allá de 60 días naturales, marcando además, el 31 de diciembre de 2021, como fecha máxima para la implantación completa del sistema.
        - Estos tiempos podrán ser mejorados por el licitador en su oferta.
3. Equipo de trabajo:

La composición del equipo de trabajo que el licitador dedique al proyecto no es una característica valorable en la presente licitación. No obstante, el equipo de trabajo deberá estar plenamente formado y dispuesto para el inicio de su actividad en la fecha de inicio del Contrato

4. El licitador deberá acreditar su capacidad para dar respuesta positiva a los trabajos solicitados por el Ayuntamiento en los plazos y formas detallados en su oferta.
5. El licitador deberá estar certificado como partner con un nivel Advanced, Gold o equivalente en el fabricante de la solución propuesta.

9. - DURACIÓN DEL CONTRATO

El plazo de duración del contrato o contratos resultantes del presente pliego será de **CUATRO (4) AÑOS**, sin posibilidad de prórroga.

10. - PRESUPUESTO Y VALOR ESTIMADO

El presupuesto de licitación del presente contrato de servicios asciende a la cantidad total de ciento veinte y un mil seiscientos veintiocho euros (128.628,00 €) I.V.A. excluido.
El citado presupuesto tiene carácter de máximo y comprende, además del precio del contrato, todos los gastos, impuestos y tasas que puedan corresponder y resulten necesarias para la ejecución del servicio, con la única excepción del Impuesto sobre el Valor Añadido (I.V.A.). Para el cálculo del presupuesto se ha tenido en cuenta los valores de mercado y contrataciones similares realizadas por el Ayuntamiento de Sestao y otras Administraciones Públicas anteriormente.

Costes:

A continuación se detallan los COSTES DIRECTOS E INDIRECTOS y OTROS GASTOS calculados para la determinación del presupuesto base de licitación (importes con IVA incluido):

- Costes Directos (78 %): 121.399,11 €
- Costes Indirectos (15 %): 23.345,98 €
- Otros gastos (7 %): 10.894,79 €

Costes Directos: Integrados por todos aquellos que se derivan de la ejecución material del suministro, directamente relacionados con el contrato a imputarse dentro del período de ejecución

del mismo, incluyendo el coste de material inventariable y fungible dedicado al servicio, gastos de desplazamiento, gastos del personal y equipamiento.

Costes Indirectos: Los costes indirectos representan aquellos gastos en los que incurre la empresa que no son asignados directamente a la prestación del servicio, tales como los costes de administración, financieros o comerciales u otros gastos generales tales como consumos, amortizaciones de maquinarias, intereses bancarios, tributos, etc.

Otros gastos: otros eventuales gastos precisos para la ejecución del contrato.

11. - PROPOSICIÓN ECONÓMICA

Exclusivamente se admitirá UNA ÚNICA OFERTA por licitador. Dicha oferta deberá recoger la prestación de todos los servicios ofertados.

12. - CRITERIOS DE ADJUDICACIÓN

La determinación de la mejor oferta, se realizará mediante la valoración de los criterios cualitativos y económicos siguientes:
Criterios cualitativos cuantificables mediante juicios de valor: hasta 42 puntos
Criterios valorados mediante la aplicación de fórmula: hasta 58 puntos

Criterios cualitativos cuantificables mediante juicios de valor.
Propuesta técnica (hasta 42 puntos):
Se realizará una valoración basándose en los criterios objetivos relativos a aspectos técnicos, excluyendo el precio. La distribución de los puntos asignados a la proposición técnica (42 puntos) se realizará de la manera siguiente:

a) Planteamiento global de la solución
Peso o puntuación máxima en este criterio: 20 puntos En concreto se valorará:
Idoneidad de la solución: En este criterio medirá el grado de adecuación de la propuesta a los requisitos solicitados. Se tendrá en cuenta la coherencia y visión global, que la solución técnica descrita en la oferta se adecúe a los parámetros solicitados en el pliego, así como el detalle técnico y funcional que permita asegurar la prestación de los servicios con máxima calidad.

Valores añadidos: En este criterio se valorarán todos aquellos aspectos de la solución adicionales a los requeridos en el pliego que faciliten la implantación del servicio y su evolución o contribuyan a la mejora de la calidad del servicio.

b) Planes de implantación y de migración
Peso o puntuación máxima en este criterio: 15 puntos
Se valorará la organización, el detalle de tareas y los medios necesarios para llevar a cabo el plan de implantación, así como la duración, interrelaciones y dependencias entre dichas tareas, incorporando la migración de las plataformas existentes. Se tendrá en cuenta la identificación previa de necesidades y posibles riesgos, así su tratamiento.
En concreto se valorará:
Organización y detalle de tareas: Se valorará que el Plan de Implantación y el Plan de Migración incluyan detalles técnicos suficientes para acreditar cómo se llevará a cabo dicha la implementación del servicio de forma progresiva y no disruptiva.

c) Planes de Propuesta del servicio de Mantenimiento
Peso o puntuación máxima en este criterio: 7 puntos
Se valorará la organización, el detalle de tareas y los medios necesarios para llevar a cabo el plan de desarrollo del servicio de mantenimiento.

En concreto se valorará:

- Organización general del servicio
- Equipo de trabajo
- Plan de Trabajo: Fase de asimilación, fase de ejecución y fase de devolución del servicio.

La obtención de una puntuación inferior al 50% del máximo de puntos asignados a cualquiera de los apartados anteriores será motivo de exclusión, así como la obtención de menos de 21 puntos en total

Criterios valorados mediante aplicación de fórmulas (hasta 58 puntos):

a) Oferta económica (hasta 30 puntos)
La valoración económica de las ofertas se realizará aplicando la siguiente fórmula:
Px = 30 * (1 - 1/2 * (Oferta valorada – oferta más baja) / presupuesto base de licitación)

b) Certificaciones ENS (hasta 10 puntos)
Peso o puntuación máxima en este criterio: 10 puntos
Se valorará el nivel de certificación del adjudicatario en el Esquema Nacional de Seguridad para la entrega del servicio de soporte.
Criterio de valoración:

- Categoría Media: 5 puntos
- Categoría Alta: 10 puntos

c) Desarrollo del fabricante (hasta 8 puntos)
Se valorará el nivel de desarrollo de los fabricantes propuestos en las soluciones que son objeto de la oferta.

- Presencia de los fabricantes de la solución firewall en el “Magic Quadrant” de Gartner por, al menos, tres años atrás consecutivos: 2 puntos.
- Presencia de los fabricantes de la solución SD-WAN en el “Magic Quadrant” WAN EDGE INFRAESTRUCTURE de Gartner por, al menos, el último año atrás: 6 puntos.

d) Mejora de Bolsa de horas del Servicio de Consultoría de Certificación ENS (5 puntos)
Se valorará con 5 puntos el incremento de la bolsa de horas del Servicio de Consultoría de Certificación ENS en 80 horas adicionales a las indicadas en el pliego. Sólo se valorará este apartado a aquellas propuestas que incluyan este incremento de al menos 80 horas adicionales. Todas las propuestas que lo cumplan obtendrán la máxima puntuación en este apartado.

e) Mejora del número de puntos de acceso (5 puntos)
Se valorará con 5 puntos el incremento del suministro, cableado, configuración y mantenimiento del número de puntos de acceso ofertados en 10 unidades con respecto a los indicados en el pliego. Sólo se valorará este apartado a aquellas propuestas que incluyan este incremento de al menos 10 unidades con respecto a las indicadas en el pliego. Todas las propuestas que lo cumplan obtendrán la máxima puntuación en este apartado.

CAMPO SANCHEZ HAITZ - 35777175P

Firmado digitalmente por CAMPO SANCHEZ HAITZ - 35777175P
Fecha: 2021.09.29 12:47:54 +02'00'