PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HAN DE REGIR LA CONTRATACION DEL SUMINISTRO, INSTALACIÓN, MIGRACIÓN Y PUESTA EN MARCHA DE DOS FIREWALL FÍSICOS (APPLIANCES) PARA LA SEGURIDAD PERIMETRAL DEL CPD DEL AYUNTAMIENTO DE ALMUÑÉCAR.

Ayuntamiento de Almuñécar

1. OBJETO DEL CONTRATO

El contrato al que se refiere el presente pliego tiene por objeto la realización del suministro, instalación, migración y puesta en marcha de dos firewalls físicos perimetrales (appliances), es decir, misma marca y modelo entre ellos que cumplan las especificaciones técnicas descritas de forma expresa en este pliego de prescripciones técnicas para la seguridad del CPD y equipos informáticos del Ayuntamiento de Almuñécar.

2. SITUACIÓN ACTUAL

Actualmente el Ayuntamiento de Almuñécar, cuenta con 2 firewalls perimetrales para la seguridad de todos los equipos informáticos municipales de la propia entidad y de las sedes remotas interconectadas al Ayuntamiento, dicho equipamiento actual ya no satisface las necesidades actuales de esta entidad (velocidad, rendimiento, fiabilidad, consumo, etc), además de que es equipamiento antiguo y en un futuro cercano el fabricante ya no podrá mantenerlo por lo tanto, se requiere nuevo equipamiento en el ámbito de la seguridad informática perimetral con su mantenimiento activo por parte del fabricante que cubra las necesidades del Ayuntamiento de Almuñécar.

3. FUNCIONALIDADES Y CARACTERÍSTICAS MÍNIMAS A CUMPLIR DE LOS FIREWALLS.

3.1. Arquitectura

Con el fin de obtener el mayor rendimiento en el procesado de tráfico, la arquitectura de la solución será una arquitectura de procesamiento dual en la que se permita un tratamiento independiente para el plano de control y el plano de datos.

En el caso de optar por una solución en formato appliances, los equipos ofertados incluirán la capacidad de aprovechar esta arquitectura DUAL asignando recursos físicos independientes al plano de control y al plano de datos, consiguiendo así una aceleración hardware en el tratamiento del tráfico de aplicaciones. Esta arquitectura estará formada por la combinación de CPUs (Core processing unit) multicore y procesadores de flujo o NPUs (Network Processing Unit) con el fin de minimizar latencias y maximizar el rendimiento.

Arquitecturas que no contemplen este procesado DUAL, como por ejemplo las arquitecturas simplemente multicore, no serán válidas debido a la gran diferencia de rendimiento real respecto al indicado en los datasheet.

Con el fin de evitar problemas derivados de este tipo de entornos, las arquitecturas donde es necesario instalar un software de gestión de los appliances tampoco serán válidas.

3.2. Funcionalidades mínimas.

3.2.1. Alta disponibilidad

Se deberá proponer la redundancia en los componentes para asegurar una disponibilidad del 99,9% en la producción.

Se planteará doble equipamiento: principal y backup, pudiéndose definir tanto como Activo-Activo, Activo-Pasivo.

3.2.2. Autenticación

- Deberá integrarse con el Directorio Activo
- Gestión centralizada de usuarios.
- Identificación de aplicaciones, usuarios e integración con Active Directory y dispositivos.
- Autenticación transparente para usuarios, de manera que podamos utilizar reglas de usuario (la llamada “capa 8”) para las siguientes funcionalidades.
    - Firewall
    - Navegación
    - Control de aplicaciones
    - Calidad de Servicio

- Identificación de sesión en usuarios conectados a través de equipos multiusuario como servidores RDP.
- Local users
- Active Directory
- eDirectory
- LDAP
- TACACS+
- RADIUS
- X.509v3 certificates
- Métodos de autenticación:
    - Single Sign On con Windows y Mac.
    - Compatibilidad con NTLM y Kerberos.
    - Portal Cautivo al que se redireccionen las conexiones a una web, donde el usuario debe introducir sus credenciales o logarse como usuario invitado.
    - Sólo mediante direcciones IP.
    - Identificación del usuario sin necesidad de colector externo mediante integración con la solución de protección de endpoint instalado en los PCs.

3.2.3. Administración

- Gestión y creación de roles de administración pudiendo restringir el acceso a determinadas partes de la configuración.
- El firewall deberá poder ser accesible desde una plataforma en el Cloud sin coste adicional mediante conexión cifrada entre el equipo y la plataforma, la cual incluirá medidas de seguridad como autenticación de doble factor
- Posibilidad de gestión de backups en cloud, en la misma plataforma de administración.
- Posibilidad de creación de reglas de firewall y configuraciones comunes a varios equipos a la vez
- Gestión de objetos dinámicos aplicables en las configuraciones de grupos de dispositivos.
- Se debe poder generar un fichero de configuración desde la consola de gestión cloud para poder instalar un firewall desde cero a través de un pendrive
- La plataforma de gestión incluirá también capacidades de orquestación del apartado SD-WAN de los equipos.
- Posibilidad de añadir a la herramienta de gestión centralizada, mediante el licenciamiento necesario:
  - Capacidad de generar, programar y exportar informes
  - Visualización de logs de hasta 1 año de antigüedad
  - Capacidad de visualización de reportes multi-dispositivo.
- Posibilidad de licenciamiento y actualización de firmas offline
- El servicio de administración, configuración de las reglas de firewall y visualización de logs, debe ir incorporado en el propio equipo sin necesidad de instalar software adicional.
- La configuración y cambios de políticas y objetos se hará en tiempo real sobre el propio equipo no siendo admitidas acciones de compilación de políticas o similar.
- Herramienta buscadora de configuraciones en la propia consola de administración para facilitar las tareas de configuración
- Gestión de certificados.
  - Posibilidad de incluir certificado de CA de terceros
  - Posibilidad de hacer inspección HTTPS con certificados CA de terceros
  - Autogenerado de certificado de usuarios para validación VPN SSL
- Compatibilidad con SNMPv3 para monitorización del equipo
- Posibilidad de cambiar el puerto de administración
- Sistema con doble partición de firmware mediante el cual poder hacer un rollback o marcha atrás de versión simplemente arrancando desde una u otra partición.

3.2.4. Firewall

- **IDS/IPS**
  - Posibilidad de creación de reglas IPS personalizadas
  - Filtro IPS con al menos 60 categorías
  - Firmas específicas para entornos SCADA y control de aplicaciones ICS (Industrial Control System)
- **Capacidades SD-WAN sin coste adicional**
  - VPN (site to site, y acceso remoto)
  - Policy Routing and forwarding IPv4 y IPv6 en base origen, destino, usuario, aplicación ...)
  - Selector de mejor camino mediante la creación de perfiles SD-WAN que permitan elegir la mejor calidad entre varios enlaces (en base a SLAs personalizables como jitter, perdida de paquetes o latencia) (v19)
  - Monitorización en tiempo real de la calidad de los enlaces

- **Posibilidad de enrutar tráfico por:**
  - IP/Red Origen
  - IP/Red Destino
  - Servicio
  - Aplicación
  - Usuario
- Soporte de Jumbo Frames
- LACP – 802.3ad
- DNAT, SNAT y PAT
- IPV4 e IPV6
- Protocolos de enrutamiento RIP, OSPF, BGP y estático.
- Inspección de certificados y tráfico SSL.
- Motor DPI (Deep Packet Insepction) agnóstico al puerto utilizado.
- Posibilidad de crear reglas de inspección SSL en base al tipo de cifrado, protocolo y características del certificado.
- Compatibilidad con TLS 1.3 sin downgrade.
- Protección ataques DOS y DDOS.
- Clasificación del tráfico.
- Balanceo de enlaces de Internet entre 2 o más accesos.
- Definición de políticas de firewall por Zonas
- Gestión de ancho de banda según usuario, grupo de usuarios, VLAN, IP, puerto, horarios,
- zonas sean internas o externas y aplicación.
- Detección de APT
- Identificación de aplicaciones
- GeoIP Database (mapeo de IPs por país dinámico) para creación de reglas de firewalls por países

3.2.5. Accesos Remotos

- Compatibilidad con dispositivos de tunelización remota Zero-touch para sedes pequeñas.
- Portal de usuario desde el que descargar el cliente SSL y los clientes de autenticación.
- Capacidades SD-WAN.
- VPN Site to Site usando protocolos IPSec, SSL y Amazon VPC.
- Posibilidad de crear túneles IPSec tanto basados en políticas como basados en rutas (Routed Based VPN).
- Compatibilidad con IKEv2.
- Cliente VPN para Android y iPhone.
- Portal HTML5 para acceso VPN sin cliente (Web Mode). Con compatibilidad al menos con los protocolos: RDP, TELNET, SSH, FTP, FTPS, SFTP, VNC, SMB.
- Configuración de túneles IPSec por Wizard.

- Cliente vpn compatible tanto con SSL como con IPsec incluido en la licencia sin límite de usuarios compatible con Windows y MacOS

    - Autenticación via pre-shared key (PSK), PKI (X.509), smartcards, tokens, XAUTH
    - Encriptación: AES (128/192/256), 3DES (112/168), Blowfish (128/448), RSA (up to 2048 Bit), MD5, SHA-256/384/512, GCM y Suite-B
    - Split-tunneling
    - Soporte NAT-Traversal
- Compatible con Accesos remotos L2TP y PPTP

3.2.6. Control de aplicaciones

- Control de accesos a nivel de aplicación.
- Control de aplicaciones por firmas incluidas en el propio appliance.
- Identificación automática de nuevas aplicaciones desconocidas o que se comuniquen por HTTPS mediante la comunicación con el endpoint, sin necesidad de romper el túnel seguro.
    - Deberá de proporcionar el Path local de la aplicación no identificada para poder clasificarla.
- Gestión de ancho de banda por aplicación.

- Funcionalidades CASB: Identificación de tráfico generado por aplicaciones cloud.
- Clasificación de aplicaciones identificadas.
- QoS.

3.2.7. Filtrado Web

- Protección contra sitios web maliciosos mediante filtrado por reputación.
- Protección contra amenazas web con análisis de malware avanzado.
- Filtrado URL con más de 100 categorías.
- Antivirus de doble opinión o dual. Sumando la protección de un segundo motor. AV de otro fabricante distinto integrado en el propio appliance.
- Forzado de búsquedas seguras "SafeSearch" en Google, Yahoo y Bing.
- Cacheo web para reducir el consumo de ancho de banda.
- Detección y bloqueo de proxies anónimos.
- Filtrado HTTPS con análisis de tráfico cifrado.
- Establecimiento de acciones disponibles dentro de aplicaciones (Facebook, Twitter, gmail, etc…).
- Filtrado ficheros no autorizados.
- Filtrado web por palabras incluidas en el propio site.
- Detección de tipos de fichero real (True File Type).
- Detección de APT (con informa de equipos sospechosos).
- Soporte de dispositivos móviles.
- Soporte de accesos para invitados y equipos compartidos.
- Integración con Directorio Activo y eDirectory para la creación de reglas por usuario.
- Autenticación flexible vía SSO (Single Sign-On) o portal cautivo.
- Políticas flexibles por usuario o grupos de usuarios con o sin AD o eDirectory
- Cuotas de navegación.
  - Cuotas de Navegación cíclicas y no cíclicas.
  - Cuotas de Navegación por días, semanas, meses y años.

3.2.8. QoS

- Catalogación de aplicaciones y servicios y aplicación de parámetros de QoS limitando los caudales máximos, garantizando caudales mínimos y prioridades.
- QoS por usuario, aplicaciones, URL y reglas.
- Deberá permitir limitar un ancho de banda o garantizarlo.
- La limitación podrá ser por usuario individual o compartida entre varios.
- Se podrá seleccionar la prioridad.
- Podremos seleccionar ancho de banda de subida y de bajada
- Se podrá añadir una programación en la que el QoS será aplicado.
- Gestión de ancho de banda independiente del sentido de la comunicación.

3.2.9. Auto-remediación

- Integración con el driver de red de la solución de protección antivirus de endpoint y servidores instalada en los equipos.
- El equipo debe poder bloquear automáticamente los accesos DESDE una máquina cuando su estado de salud no sea el requerido o no reporte su estado.
- El equipo debe poder bloquear automáticamente el acceso HACIA una máquina cuando su estado de salud no sea el requerido o no reporte su estado.
- El equipo debe poder prevenir los movimientos LATERALES de malware dentro de un mismo segmento de red, mediante la comunicación con el agente de los endpoint no comprometidos.

3.2.10. Portal de usuario

- Accesible desde la propia GUI del Firewall en un puerto seleccionable.
- Desde el portal de usuario se podrá gestionar.

    - Tickets para accesos WIFI.
    - Accesos VPN html5.
    - Cuarentena de email de usuario.
    - Creación de vouchers de bypass del filtrado web.
    - Descarga del cliente VPN.
    - Configuración del doble factor de autenticación

3.2.11. Web Application Firewall (WAF)

El equipo debe incluir, al menos, las siguientes protecciones en el apartado de protección de aplicaciones Web.:

- Form hardening.
- Escaneo Dual de antivirus, tanto para subidas como descargas.
- Cookie signing.
- Static URL hardening.
- Bloquea clientes con mala reputación.
- Protocol Violations.
- Protocol Anomalies .
- Request Limits.
- HTTP Policy.
- Bad Robots
- Generic Attacks.
- SQL Injection Attacks.
- XSS Attacks.
- Tight Security.
- Trojans.
- Outbound.
- Creación de formularios personalizados de autenticación.
- Limitar la sesión del usuario.

- Timeout.
- Lifetime

3.2.12. Informes y logs

- Los informes serán inbox, en el propio equipo.
- Posibilidad de integración y envío de log a un SIEM.
- Compatibilidad con Secure Syslog.
- Monitor de flujo en tiempo real, que permita conocer que IPs, Usuarios y aplicaciones están consumiendo el ancho de banda en todo momento.
- Informes de usuarios UTQ, coeficiente de amenazas de usuario, que asigne una puntuación a los usuarios conflictivos, unificando en el mismo informe alertas de firewall como del endpoint si lo hubiera.
- Visor de log en raw que permita visualizar varios módulos de logeado al mismo tiempo, así como aplicar filtros de visualización.
- Policy tester o simulador de políticas que permita saber si un tráfico debería estar siendo permitido o bloqueado.
- Anonimización de logs y reportes que permita la ocultación de nombres de usuario, direcciones IP, MAC y direcciones email con el objetivo de preservar la privacidad de los usuarios aplicando el concepto de 4 ojos.

3.2.13. Sandboxing

- La solución debe estar integrada en el panel de control del producto y aportar un informe de amenazas avanzado con todos los detalles sobre las amenazas bloqueadas (conexiones, procesos, capturas de pantalla, reputación, etc)
- Debe de utilizar tecnología Deep Learning con baja tasa de falsos positivos.
- El servicio de Sandbox debe correr en la nube y no localmente en el equipo para minimizar el consumo de recursos.
- Debe analizar, al menos:
    - Ejecutables de Windows (incluyendo EXE, COM y DLL).
    - Documentos Word (incluyendo .doc, .docx, docm and .rtf).
    - Documentos PDF.
    - Archives containing any of the file types listed above (ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet.
    - Dynamic malware behavior analysis and deep learning runs files in real environments.
    - In-depth malicious file reports and dashboard file release capability Average analysis time less than 120 seconds Flexible user and group policy options on file type, exclusions, and actions on analysis Supports one-time download links.
- Además, debe contar con técnicas anti-evasión.

3.2.14. Firewall Manager

Se debe incluir en la solución la gestión centraliza desde una plataforma en cloud de todos los firewalls de la red, pudiendo administrar políticas y configuración desde una única consola.

La solución ofertada deberá ser compatible con el actual equipamiento de seguridad de antivirus del que dispone el Ayuntamiento actualmente.

Requisitos mínimos:

- Capacidad de administrar un número de equipos ilimitado.
- Doble factor de autenticación para el acceso.
- Solución alojada en el cloud.
- Capacidad para almacenar de forma centralizada los logs por al menos 30 días, sin ningún tipo de coste adicional.
- Creación de plantillas que puedan ser reutilizadas para configurar diferentes firewalls.
- Administración basada en Roles.
- Control de cambios.
- Posibilidad de funcionar como servidor gestor de actualizaciones.
- Monitorización del estado de salud de los dispositivos gestionados, así como su conectividad y versión de firmware instalada.
- Posibilidad de creación y envío de alertas.
- Gestión de objetos dinámicos aplicables en las configuraciones de grupos de dispositivos.
- Posibilidad de filtrar equipos en base a grupos, número de serie, modelo o versión.
- Se debe poder generar un fichero de configuración desde la consola de gestión cloud para poder instalar un firewall desde cero a través de un pendrive.
- Visor de registros del firewall con posibilidad de realizar búsquedas sobre ellos.
- Posibilidad de exportar los informes en PDF, CSV o HTML.
- Selección al gusto de columnas en la vista de logs con más de 100 opciones de datos visualizables.
- Vista de amenazas y eventos bloqueados geográfica, es decir, situando el origen o destino de la amenaza en un mapa.
- Integración nativa con algún sistema de administración centralizado del mismo fabricante con el que contar con la gestión centralizada no solo de los dispositivos firewalls sino también del resto de soluciones del fabricante.

3.3. Características mínimas de cada uno de los 2 Firewalls.

3.3.1. Especificaciones técnicas

Montaje	**Montaje en bastidor 1U (2 orejas de montaje en bastidor incluidas) en rack de 19”**
Dimensiones Máximas Ancho x Altura x Profundidad	**438 x 44 x 405 mm**

3.3. Entorno

Fuente de Alimentación	**Alcance automático interno de CA-CD 100-240 VCA, 3-6 A @50-60 Hz**
Consumo de energía	**201 W / 686,68 BTU/h (máx.)**
Adición de PoE habilitada	**76 W / 260 BTU/h (máx.)**
Temperatura en funcionamiento	**0 a 40 °C (en funcionamiento) -20 a +70 °C (almacenamiento)**
Humedad Máxima	**10-90 %, sin condensación**

Posibilidad de despliegue en entornos Cloud Azure y Amazon Web Services

3.3.3. Certificaciones del Firewall

Certificaciones	**CB, CE, UKCA, UL, FCC, ISED, VCCI, KC, RCM, NOM, Anatel, CCC, BSMI, TEC, SDPPI**

3.3.4. Rendimiento

FIREWALL	**58.000 Mbps**
INSPECCIÓN TLS	**3.130 Mbps**
IMIX FIREWALL	**27.000 Mbps**

IPS	**14.000 Mbps**
VPN IPSEC	**31.100 Mbps**
NGFW	**12.500 Mbps**
PROTECCIÓN CONTRA AMENAZAS	**3.000 Mbps**
LATENCIA (UDP DE 64 BYTES)	**4 µs**
CONEXIONES SIMULTÁNEAS	**13.7 Millones**
CONEXIONES NUEVAS/SEG	**257800**
TÚNELES SIMULTÁNEOS VPN IPSEC	**6500**
TÚNELES SIMULTÁNEOS VPN SSL	**6500**
CONEXIONES SIMULTÁNEAS DE SSL/TLS DE XSTREAM	**102400**

3.3.5. Conectividad

INTERFACES ETHERNET (FIJAS)	**8 x GE cobre 2 x SFP fibra 4 x SFP+ 10 GE fibra 4 interfaces de cobre a 2.5Gbps 4 Interfaces GbE PoE 4 interfaces 2.5 GbE Poe**
PARES DE PUERTOS DE OMISIÓN (FIJOS)	**1**
MÁX. DENSIDAD DE PUERTOS (INCL. MÓDULOS)	**20**
INTERFACES DE ADMINISTRACIÓN	**1 x RJ45 MGMT 1 x COM RJ45 1 x COM Micro-USB**
OTRAS INTERFACES E/S	**2 x USB 3.0 (frontal) 1 x USB 2.0 (trasero)**
MÁX. POE (USANDO MÓDULO FLEXI PORT)	**1 módulo: 4 puertos, 60 W máx.**
2ª FUENTE DE ALIMENTACIÓN REDUNDANTE	**SI**

El adjudicatario tendrá que suministrar 8 Cables Twinax de cobre de conexión directa pasivo (DAC) compatible con los modelos de firewalls a suministrar 10G SFP+ 4m.

El precio ofertado para el suministro de dos firewalls tendrá que contar con un mantenimiento de 36 meses en todas sus licencias por parte del fabricante, parte hardware y software incluyendo el soporte remoto para cualquier incidencia y el

cambio del dispositivo in situ por parte del fabricante en caso de avería sin coste alguna para el Ayuntamiento de Almuñécar**.**

4. INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE FIREWALLS.

La empresa adjudicataria, se encargará de:

- De la dirección del proyecto y toma de datos.
- De la instalación, enracado, configuración y migración de políticas de los Firewalls actuales a los nuevos Firewalls.
- Saneamiento de políticas existentes sin utilidad.
- Pilotaje y pruebas.
- Pase a producción.
- Formación especializada y Documentación el para el Departamento de Informática del Ayuntamiento de Almuñécar en el manejo de los suministros licitados.

5. TIEMPO DE IMPLANTACIÓN, CONFIGURACIÓN, MIGRACION DE ANTIGUOS DISPOSITIVOS ETC.

La empresa adjudicataria se encargará de la implantación, configuración, migración y todas las intervenciones necesarias para dejar funcionando correctamente todos los dispositivos licitados en este pliego.
El tiempo de duración de dicha implantación será como máximo de **30 días naturales**, en el caso de que se supere este plazo se podrá realizar una rescisión del contrato por superar el plazo total de suministro e implantación completa.

6. LUGAR DE ENTREGA DEL SUMINISTRO Y SERVICIOS.

El lugar de entrega de suministros objeto del contrato será en la sede del Ayuntamiento de Almuñécar, Plaza de la Constitución, nº 1, Almuñécar, CP 18690 (Granada), 1ª Planta, CPD.

7. REQUISITOS LOGÍSTICOS EXIGIDOS A LOS LICITADORES.

La empresa adjudicataria dispondrá un sistema logístico que garantice la entrega efectiva y eficiente del material en la planta de Proceso de Datos donde está alojado el cpc de acuerdo a las necesidades del Departamento de Informática del Ayuntamiento de Almuñécar.
Asimismo, el Departamento de Informática, podrá solicitar en todo momento tanto la planificación de los envíos como información actualizada del estado de los mismos.

8. RECONOCIMIENTOS DE TERCEROS OBLIGATORIAS.

Con objeto de adquirir una solución de contrastada seguridad y garantías, se requerirán al menos los siguientes reconocimientos

En el caso de que los licitantes no los presenten se les excluirá del proceso de licitación:

- **Líder en el último courante Gartner de UTM (Unified Threat Management (Unified Threat Management).**

- **El equipo debe aparecer en el último cuadrante de Gartner de Network Firewalls.**
- **El equipo debe aparecer al menos dentro de la categoría de Strong Performers del último diagrama de Forrester Wave para Enterprise Firewalls.**

Además, se debe de contar con las siguientes certificaciones que demuestren la robustez de la solución:

- **Common Criteria (ISO 15408) EAL 4+**
- **ISO 9001**
- **FIPS 140 140-2**
- **ICSA Labs**
- **CB, CE, FCC, ISED (IC), VCCI, RCM, UL, CCC, BIS, ANATEL**

9. CERTIFIACIONES OBLIGARORIAS POR PARTE DEL LICITADOR

- **ENS Alta**
- **ISO 27001**
- **ISO 14001**
- **ISO 9001**
- **Certificado del fabricante de estar en posesión del más alto nivel de partnership, del fabricante ofertado, en el año en curso.**

***Si se presentan empresas en UTE o subcontratando, deberán tener ambas empresas, las certificaciones.**

En el caso de que los licitantes no los presenten se les excluirá del proceso de licitación.

10. DOCUMENTACION APORTADA POR LA EMPRESA ADJUDICATARIA.

La empresa adjudicataria deberá suministrar al Departamento de Informática del Ayuntamiento de Almuñécar la siguiente documentación:

- Inventario de todo el material suministrado, incluyendo: marcas, modelos, números de serie,
  características y descripción de cada equipo y sus componentes.

- Relación de licencias y claves de producto de todo el software suministrado o incluido con cada equipo.
- CD/DVD de todo el software suministrado, incluyendo sistema operativo y drivers, en el caso de ser necesario para la implantación de los nuevos sistemas.
- Hojas de producto y/o especificaciones de todo el equipamiento suministrado.
- Procedimiento de gestión/ejecución de la garantía.

11. GARANTÍA MÍNIMA

La garantía mínima completa de los firewalls será de **3 años tanto en la parte hardware somo software.**

12. SOPORTE Y MANTENIMIENTO

Soporte directo del fabricante 24x7. 8x5 en español tanto en la parte hardware como software.

13. CUADRO DE PENALIZACIONES

NIVELES DE INCIDENCIAS	DESCRIPCIÓN	TIEMPO DE RESOLUCIÓN MÁXIMO INCIDENCIA	PENALIZACIÓN
Baja	Incidencia donde los firewalls funcionan con normalidad, salvo algún error puntual, pero se puede trabajar sin problema en las tareas diaria y todos los servicios están activos.	48 horas	5% del precio de adjudicación de contrato
Media	Incidencia donde fallan como máximo 1 módulo protección de uno de los firewalls impidiendo que este modulo realice sus tareas de protección.	36 horas	10% del precio de adjudicación de contrato
Alta	Incidencia donde los firewalls presentan fallos que los dejan fuera de servicio totalmente.	24 horas	15% del precio de adjudicación de contrato

14. CONFIDENCIALIDAD

La documentación e información suministradas por este Ayuntamiento al adjudicatario, o aquella a la que este pueda acceder, tendrá carácter de confidencial y no podrá ser utilizada para fines diferentes de la estricta ejecución del contrato.

No se podrá transferir información alguna sobre los trabajos, su resultado, ni la información de base facilitada, a personas o entidades sin el consentimiento previo, por escrito, del Ilmo. Ayuntamiento de Almuñécar.

15. PRESUPUESTO DEL CONTRATO.

- El precio base de licitación de todo el suministro, junto con su instalación, configuración, migración y puesta en marcha total se ha obtenido de acuerdo a un estudio de las diferentes empresas en el sector que se encargan de suministrar este tipo de equipamiento de seguridad junto con su instalación y puesta en marcha es de:

  39.669,42 euros sin IVA incluido

  48.000 euros con IVA incluido