VICTOR ABARCA BLANCO (1 de 1)
OPERADOR DE SISTEMAS
Fecha Firma: 26/01/2026
HASH: ea8a903a2d5f2c9d8f150fc6f94922bc

PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HAN DE REGIR LA CONTRATACION DEL SUMINISTRO, INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN MARCHA DE UNA 2ª BARRERA DE SEGURIDAD PERIMETRAL PARA EL CPD DEL AYUNTAMIENTO DE ALMUÑÉCAR.

Ayuntamiento de Almuñécar

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 1 de 26

1. OBJETO DEL CONTRATO

El contrato al que se refiere el presente pliego tiene por objeto la realización del suministro, instalación, configuración y puesta en marcha de una 2ª barrera de seguridad perimetral exigida por el ENS que comprende los siguientes servicios y equipamientos:

- **Dos firewalls físicos perimetrales (appliances),** activo-pasivo de fabricantes diferentes a los Firewall Sophos XGS 3300 que actualmente posee el Ayuntamiento que cumplan las especificaciones técnicas descritas de forma expresa en este pliego de prescripciones técnicas para la seguridad del CPD y equipos informáticos de la entidad para reducir vulnerabilidades comunes en productos del mismo fabricante, dichos equipos tienen que trabajar conjuntamente con los Firewall Sophos que ya posee el Ayuntamiento de Almuñécar para combatir las amenazas existentes.
- **Un servicio de WAF en la nube** para la protección de todos los portales web que posee el Ayuntamiento de Almuñécar en su infraestructura y que están expuestos al exterior.
- **Una solución XDR 24x7 gestionada** que monitorice y remedie cualquier tipo de incidencia de seguridad en todos los servicios informáticos protegidos que posee el Ayuntamiento de Almuñécar.

2. SITUACIÓN ACTUAL

Actualmente el Ayuntamiento de Almuñécar, cuenta con 2 firewalls perimetrales Sophos XGS 3300 para la seguridad de todos los equipos informáticos municipales de la propia entidad y de las sedes remotas interconectadas al Ayuntamiento, a los que hay que añadir **2 nuevos Firewall perimetrales activo-pasivo de diferente fabricante**, **un servicio WAF en la nube para la protección de las aplicaciones web publicadas en internet y una solución XDR 24x7 gestionada** que se encargue de monitorizar y remediar cualquier incidencia de seguridad en la infraestructura del CPD municipal, así conseguimos añadir una capa adicional de seguridad perimetral con equipos de diferente fabricante a los ya existentes.

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 2 de 26

3. FUNCIONALIDADES Y CARACTERÍSTICAS MÍNIMAS Y OBLIGATORIAS A CUMPLIR DE LOS FIREWALLS DE NUEVA GENERACIÓN (NGFW)

Se requiere el suministro, instalación y configuración total de otro clúster adicional al existente del Ayuntamiento de Almuñécar constituido por 2 equipos (NGFW) en alta disponibilidad, permitiendo tanto modo activo-activo como activo-pasivo, con las siguientes características técnicas mínimas en este caso:

- Rendimiento mínimo del servicio Firewall IPV4/IPV6 (con paquetes de 1518 bytes UDP): 39 Gbps
- Rendimiento mínimo del servicio VPN (IPsec): 35 Gbps.
- Rendimiento mínimo NGFW (IPS+control de aplicaciones, tráfico Enterprise Mix): 3 Gbps
- Rendimiento mínimo Threat Protection (IPS+control de aplicaciones+Antimalware, tráfico Enterprise Mix): 2.8 Gbps
- Rendimiento mínimo inspección SSL (IPS sobre HTTPS): 3 Gbps
- Rendimiento mínimo de la funcionalidad IPS: 5 Gbps
- Rendimiento mínimo control de aplicaciones (HTTP): 6.7 Gbps
- Capacidad mínima de gestión de conexiones: 3.000.000 sesiones concurrentes, permitiendo como mínimo 140.000 nuevas sesiones por segundo.
- Número mínimo de interfaces 10 GE SFP+: 4
- Número mínimo de interfaces GE SFP: 8
- Número mínimo de interfaces GE RJ45: 16
- Posibilidad de disponer de dos puertos específicos de gestión o puertos disponibles en el dispositivo para su uso con tecnologías Ethernet dedicado con el objetivo de garantizar que no consuma interfaces de servicio para esta tarea.
- Disco interno: 1 x 480 GB SSD.
- Dominios virtuales mínimos: 10.

Todas las características de rendimiento ofertadas en cumplimiento de lo solicitado en este pliego se deben indicar con referencia a medidas en condiciones reales, en las que se indique una mezcla de trafico de diferentes características, y no serán aceptables de ningún modo medidas realizadas en condiciones ideales.

Asimismo, los requisitos funcionales que deben cumplir estos equipos son los siguientes:

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 3 de 26

- **Funcionalidades:**
  - Inspección profunda de contenido
  - Múltiples modos de despliegue (modos mirror, transparente y NAT/PAT)
  - Capacidades de Routing estático, policy based routing y routing dinámico, soportando BGP, OSPF, Rip v2 y Multicast, tanto para IPv4 y IPv6.
  - Gestión de VLAN e integración de 802.1Q.
  - Autenticación basada en grupos de usuarios
  - Capacidad de securización de VoIP
  - Protección basada en la creación de perfiles aplicables a usuarios individuales y/o grupos.

- **Networking**
  - Es necesario que la solución disponga de capacidades de SD-WAN seguro, proporcionando capacidades de gestión avanzada de los accesos disponibles a redes públicas y privadas aplicando todas las capacidades de securización de dicho tráfico disponibles.
  - Estas funcionalidades deben estar disponibles en los equipos cortafuegos sin necesidad de ninguna licencia adicional.
  - Las funcionalidades SD-WAN mínimas requeridas son las siguientes:
    - Comunicaciones:
      - Posibilidad de emplear agregación de enlaces independientemente de la red de transporte asociada a los mismos. Esta agregación debe poder realizarse tanto a nivel de paquete como a nivel de sesión. El número mínimo de conexiones físicas y lógicas que se pueden añadir a la SD-WAN debe ser de al menos 4 líneas para balancear.
      - Las interfaces disponibles en los dispositivos de sede no deben limitar la funcionalidad de las mismas permitiendo asignar a las mismas el rol más adecuado en función de cada escenario (LAN, WAN, HA,).
      - Balanceo inteligente de conexiones físicas y lógicas, indiferentemente del tipo de conexión WAN (MPLS, 3G / 4G, FTTH, VPN, etc.).
    - **VPN:**
      - Los sistemas empleados deben permitir el establecimiento de redes privadas virtuales (VPNs). De cara a habilitar la comunicación sede a sede la solución debe contar con mecanismos para establecer de forma dinámica los túneles VPN entre sedes cuando la comunicación lo requiera.
    - **SLAs y calidad de servicio:**

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 4 de 26

- Los health-check necesarios para la monitorización de los servicios debe poder basarse en, como mínimo, Ping, DNS y HTTP.
- Los SLAs asociados a los diferentes servicios deben basarse en la definición de umbrales para parámetros estándar tales como latencia, jitter o pérdida de paquetes.

- **Balanceo WAN:**
  - Configuración de políticas de WAN Steering inteligentes que permitirán determinar la elección del enlace como mínimo en base a su origen (usuarios ó grupos de usuarios [integrable con AD] y dirección MAC ó IP), en el destino (dirección IP, aplicaciones y/o servicios de Internet), de forma que se envié el tráfico por la(s) línea(s) con mejor calidad de ese momento (basado en valores configurables de jitter, packet loss, latencia, tráfico de subida/bajada o ancho de banda, así como una combinación de las mismas mediante pesos) mediante criterios de cumplimiento de SLAs, mejor calidad y menor coste, como mínimo.
  - Debe permitir habilitar mecanismos de remediación WAN tales como Forward Error Correction y Packet Duplication.

- **Seguridad:**
  - La solución planteada debe ser capaz de aplicar los controles de seguridad requeridos en la sede para ofrecer un servicio de acceso directo a Internet (local breakout) completamente securizado sin la necesidad de contar con elementos adicionales al Gateway SD-WAN ubicado en la sede. Esta seguridad debe cubrir, como mínimo, las siguientes funcionalidades:
    - Antimalware
    - IPS
    - Control de Aplicaciones
  - Adicionalmente, deben poder aplicarse todas las capacidades de protección del sistema cortafuegos a todo el tráfico cursado por las líneas de datos (underlay) o por las VPNs (overlay), con independencia de su destino.
  - La solución debe ser capaz de realizar inspección SSL de cara a identificar en detalle las aplicaciones de la red y poder aplicar políticas de balanceo y control no sólo en base a la propia aplicación sino a las acciones llevadas a cabo en la misma. Por ejemplo, controlar WhatsApp y la posibilidad de enviar ficheros a través de WhatsApp.
  - La solución planteada debe poder emplear elementos externos como fuente de datos para el control de las potenciales amenazas. Dichas fuentes de datos externas permitirán la importación de direcciones IP, hashes de ficheros o nombres de dominio para ser empleados en las políticas de acceso correspondientes.

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 5 de 26

- **Gestión:**
    - La gestión de las políticas de seguridad y las del propio servicio SD-WAN debe llevarse a cabo desde una misma plataforma unificada.

- Es necesario que el puerto USB se pueda conectar un módem 4G/5G para usarlo como conexión a Internet o backup.
- Capacidades de VXLAN y VXLAN VTEP para la extensión de redes de nivel 2 entre redes de nivel 3.
- El sistema propuesto debe tener una funcionalidad integrada de Traffic Shaping, siendo capaz de reservar ancho de banda y marcar el tráfico con DSCP. Este traffic shaping debe basarse en aplicaciones y URLs.
- Soporte de protocolos RIP v1 / v2, OSPF, ISIS, BGP y Multicast para IPv4 e IPv6.
- Routing basado en política o PBR.
- Soporte Dual Stack IPv4 e IPv6 simultáneamente.
- Network address translation NAT IPv4, NAT64 y NAT66.
- DHCP server / DHCP Relay/ DNS Server / DNS Proxy / NTP Server.
- 802.1Q VLANs.
- Routing basado en contenidos: ICAP y WCCP.
- Point-to-Point Protocol over Ethernet (PPPoE).
- 802.3ad: capacidad de crear enlaces LACP por la agregación de puertos.
- La solución planteada debe permitir identificar un mínimo de 4.000 aplicaciones. Esta identificación podrá emplearse como parte de las políticas de WAN Steering, la monitorización de health-checks de los servicios y la aplicación de políticas de QoS.

- **VPN (Virtual Private Network):**
    - Protocolos soportados: PPTP, IPSec.
    - Cifrado y autenticación: DES, 3DES y AES. SHA1 y MD5.
    - Modo de funcionamiento cliente/servidor y punto a punto.
    - Cliente VPN que asegure la mejor integración con los sistemas ofertados.
    - Modo proxy inverso que permita la publicación mediante portal web de aplicaciones tipo WEB, RDP, SSH, Acceso a carpetas y VNC.
    - Cliente VPN incluido para sistemas operativos IOS y Android.
    - Funcionalidad integrada del mismo fabricante de doble factor de autenticación vía token móvil, así como por SMS y correo electrónico, integrado en la misma

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 6 de 26

plataforma de seguridad. Este token también se debe poder utilizar para el acceso seguro de administración a la GUI de los equipos cortafuegos.

- **Inspección de tráfico cifrado:**
  - Soporte para TLS 1.3.
  - La solución propuesta ha de ser capaz de inspeccionar tráfico SSL y SSH, sin que el descenso de rendimiento sea superior al 30%.

- **Protección Antimalware:**
  - Protocolos a analizar: HTTP/HTTPS, POP3/POP3S, FTP, SMTP/SMTPS, IMAP/IMAPS, MAPI y mensajería instantánea.
  - Posibilidad de bloqueo de ficheros por tipo y tamaño.
  - Posibilidad de gestión de archivos en cuarentena.
  - Servicio Antibotnet.
  - Posibilidad de eliminar contenido dinámico de los ficheros analizados.
  - Posibilidad de controlar infecciones de virus entre actualizaciones de las firmas del fabricante.
  - Posibilidad de envío de cierto tipo de ficheros (parametrizables por el administrador) a una plataforma de sandboxing para la detección de ataques de día cero y amenazas persistentes avanzadas (APTs).

- **Servicio IPS (Intrusion Prevention System):**
  - Análisis de tráfico e inspección IPS basado en los estándares de los diferentes protocolos.
  - Debe disponer de más de 10.000 firmas de IPS.
  - Deben poder configurarse por parte de los administradores en función de los elementos a proteger (cliente, servidor, tecnología, …).
  - Deben actualizar las firmas al menos 2 veces por semana.
  - Posibilidad de creación y edición de firmas personalizadas.
  - Debe soportar la funcionalidad de One-Arm IDS (modo sniffer)

- **Servicio de Filtrado Web**
  - Protocolos a analizar: HTTP/HTTPS.
  - Categorización de contenidos web basado en diferentes categorías.

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 7 de 26

- Creación de patrones para la definición de listas URL.
- Bloqueo de contenidos web.
- Posibilidad de fijación de cuotas de navegación (tiempo y volumen de tráfico) por categoría.
- Servicio de actualización en tiempo real de categorización de URL.
- Posibilidad de solicitar la recategorización de páginas web.

- **Servicio de Control de Aplicaciones:**
  - Control de más de 3.000 aplicaciones con independencia de los puertos y protocolos utilizados.
  - Identificación y control de aplicaciones categorizadas por tipo y funcionalidad.
  - Posibilidad de aplicar QoS por aplicación o grupo de aplicaciones, así como a nivel de usuario o grupo de usuarios, permitiendo tanto limitar el ancho de banda como fijar un ancho de banda garantizado.
  - Posibilidad de solicitar la identificación de nuevas aplicaciones.
  - Disponibilidad de un servicio de actualizaciones de nuevas aplicaciones.

- **Controladora integrada**
  - El sistema debe ser capaz de actuar como controladora de puntos de acceso Wireless, así como de switches del mismo fabricante.
  - Esta funcionalidad no requerirá licencia adicional.
  - La gestión los APs y switches se hará desde la misma interfaz gráfica y CLI desde la que se gestiona el Firewall.
  - A nivel de Wifi las funcionalidades que al menos debe de realizar serán:
    - Soporte de un amplio catálogo de APs, tanto indoor como outdoor, como switches, incluyendo rugged, sin que ninguna de esas funcionalidades requiera costes adicionales.
    - Gestión completa de la seguridad de la plataforma wireless, incluyendo la protección frente a rogue APs, WIDS, monitorización (tanto de parámetros operativos como del medio radioeléctrico, incluyendo un análisis gráfico del espectro) y reporting
    - Soporte para APs 802.3az WAVE2 y WiFi6
    - Autenticación de SSID: WPA2-Personal, WPA2-Enterprise, WPA3 (SAE, SAE transition, Enterprise), Open. Múltiples PSK para WPA Personal.

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 8 de 26

- Soporte integrado o externo para portales cautivos, 802.1x, y preshared keys.
- Soporte para topologías wireless: Fast roaming, balanceo de carga entre APs, Wireless Mesh y bridging.
- Balanceo entre controladoras en caso de fallo.

○ A nivel de Switch al menos deberá de realizar:

- Funcionalidades configurables y monitorizables por puerto desde la consola centralizada (GUI y línea de comandos):
  - PoE (en los dispositivos compatibles)
  - DHCP blocking e IGMP snooping
  - STP (estado, BPDU, root guard)
  - LLDP, IGMP, sFlow y Dynamic ARP inspection (DAI)
  - Port mirroring
- Políticas de seguridad por puerto:
  - 802.1x (en modos "basado en puerto" y "basado en MAC")
  - Restricción del tipo de trama permitida a través de los puertos IEEE 802.1Q
  - Soporte para RADIUS accounting
  - MAC authentication bypass configurable
  - EAP pass-through
- Posibilidad de implementar políticas de NAC, empleando información de usuarios o información de los dispositivos detectada automáticamente (como el tipo de dispositivo o el sistema operativo, entre otros) para ubicar el tráfico en una VLAN específica o aplicar determinadas configuraciones de puertos.

- **Integración con Active Directory.**

- Los cortafuegos suministrados deben incorporar la capacidad de ampliar sus capacidades de conectividad con elementos adicionales, administrados y monitorizados desde el mismo equipo mediante su controladora integrada de switches, que incrementen la densidad de puertos disponibles.

- Los cortafuegos suministrados deberán contar con un procesador independiente del flujo directo del tráfico para la realización de las tareas de seguridad computacionalmente intensivas como:

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 9 de 26

- IPS
- Inspección SSL
- Descarga de cifrado y descifrado

- **Licencias de usuario ilimitadas.**

- **Posibilidad de activación de funcionalidad de proxy explícito.**

- **Control de ancho de banda basado en IP, usuarios y/o aplicaciones.**

- **La solución propuesta deberá proporcionar visibilidad en tiempo real de:**
  - Topología física
  - Topología lógica
  - Top fuentes de tráfico
  - Top destino de tráfico
  - Top de políticas más usadas
  - Países
  - Todas las sesiones
  - Top de aplicaciones más empleadas
  - Top de sitios web más visitados
  - Top de amenazas detectadas
  - Mapa de amenazas
  - VPN
  - Eventos de sistema
  - Interfaces

- La solución propuesta debe ser reconocida como líder en el último Cuadrante Mágico de Gartner para Network Firewall.

- La solución propuesta debe estar incluida en el Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación del Centro Criptológico Nacional, Guía de Seguridad de las TIC CCN-STIC 105. Dado que el proceso de actualización de este catálogo requiere unos plazos temporales amplios, se admitirán variaciones de los modelos ya existentes en dicho catálogo (como, por ejemplo, versiones actualizadas aún no recogidas en el mismo).

Esta solución de Firewall de contener una solución de Protección del puesto de trabajo y control de Acceso seguro con las siguientes características y requerimientos:

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 10 de 26

3.1.2 Garantía mínima de los equipos

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

3.1.3 Soporte y mantenimiento de los equipos

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

4. SERVICIO WAF EN LA NUBE PARA PROTECCIÓN DE APLICACIONES WEB

4.1 Introducción

El presente documento detalla las especificaciones técnicas del Web Application Firewall (WAF) para la protección de 30 aplicaciones web del Ayuntamiento. Este sistema proporcionará seguridad avanzada contra amenazas comunes y ataques de denegación de servicio, asegurando la integridad y disponibilidad de las aplicaciones.

4.2 Alcance

El WAF será implementado para la protección de todas las aplicaciones web del Ayuntamiento, incluyendo portales de servicios al ciudadano, plataformas de tramitación electrónica y sistemas internos de gestión municipal. Su despliegue abarcará:

- Seguridad perimetral y detección de amenazas en tiempo real.
- Protección de API y aplicaciones críticas.
- Integración con la infraestructura de red y seguridad existente.
- Monitoreo y reporte de incidentes de seguridad.
- Soporte para la escalabilidad de servicios municipales digitales.

4.3 Capacidades de Seguridad

- Modo "solo detección" y "prevención" configurable por elementos específicos de la aplicación.
- Bloqueo de conexiones mediante reinicio, respuesta de error personalizada, redirección o bloqueo de IPs maliciosas.

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 11 de 26

- Permitir bloquear conexiones por país, conexiones satelitales, accesos por redes TOR, proxies anónimos, fuentes conocidas de ataques; pudiendo generar excepciones por IP.
- Todas las respuestas y acciones posteriores deben ser parametrizables por cada tipo de ataque, permitiendo una parametrización fina.
- Funcionalidad de reescritura HTML y manipulación de cabeceras y URL.
- Restricción de métodos HTTP y WEBDAV.
- Aplicación de restricciones a niveles de aplicación, URL, parámetros, cabeceras y cookies.
- Cloaking de errores para ocultar información sensible.
- Análisis y bloqueo de patrones sensibles como números de tarjetas de crédito.
- Modelos de seguridad negativa (detección por regex) y positiva (whitelist).
- Protección contra ataques OWASP Top Ten (SQLi, XSS, CSRF, etc.).
- Prevención de ataques de fuerza bruta contra autenticaciones y sesiones.
- Protección de cookies mediante firma, cifrado y prevención de ataques de repetición.
- Inspección de archivos cargados en busca de malware.
- Integración con tecnologías de navegación blindada.
- El servicio debe permitir la integración con el servicio de SOC gestionado incluido en la propuesta
- El servicio debe permitir generar certificados con let's encrypt y automatizar la renovación automática de los mismos.
- El servicio permitirá separar protocolo y cyphers utilizados entre el cliente de los utilizados en los servidores.

4.4 Gestión de Bots y Protección contra DDoS

- Protección contra Web Scraping, spam en formularios y comentarios sin licencias adicionales.
- Identificación de bots mediante perfiles de tráfico y mecanismos de puntaje de riesgo.
- Limitación de tasa de acceso a bots y acción mediante CAPTCHA o tarpit.
- Capacidad de control de bots por categoría incluyendo categorías de IAs generativas.
- Generación de firmas digitales por conexión generando huellas dactilares que permitan identificar BOTs independientemente del origen y con trazabilidad de las acciones.

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 12 de 26

- La solución debe permitir detectar comportamientos similares entre BOTs para detección de campañas.
- Capacidad de generar protecciones específicas por URL y/o parámetro, por ejemplo, en el control de fuerza bruta, credential spraying o stuffing.

4.5 Capacidades de Gestión

- Registro detallado de ataques, accesos y auditorías administrativas.
- Exportación de logs en formatos comunes (W3C, NCSA) y a SIEMs como Splunk y Azure Sentinel, tanto del tráfico bloqueado como del tráfico consumido.
- Análisis de falsos positivos con mitigación fácil mediante logs interactivos y ejecutables.
- API REST JSON para configuración y gestión automatizada con herramientas como Ansible y Terraform.
- Control de acceso basado en roles con perfiles de usuario personalizados y RBAC con capacidad de limitar por aplicación.
- Integración con herramientas de escaneo de vulnerabilidades tanto incluido en el servicio como externos.
- Generación de informes personalizables y programables.
- Capacidad de crear snapshots tanto manuales como automáticos de configuraciones para tener un control de versiones.

4.6 Protección de APIs

- Seguridad para APIs basadas en JSON contra ataques específicos.
- Validación de payloads JSON y autenticación con JWT.
- Descubrimiento automático de endpoints API y generación de perfiles de seguridad de forma manual o automática de forma administrable.

4.7 Entrega de Aplicaciones

- Balanceo de carga de capa 7 con persistencia.
- Verificación del estado de servidores backend y reruteo inteligente.
- Caché de respuestas y compresión de contenido.
- Infraestructura integrada de CDN y DNS gestionado sin coste añadido.
- Capacidad de despliegue de inspección remota en contenedores Docker en caso necesario.

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 13 de 26

- Offloading de SSL y redirección automática HTTP a HTTPS.
- Pooling de conexiones para optimización del rendimiento de la aplicación.

4.8 Soporte

- El soporte debe estar incluido en la solución SaaS y proporcionar soporte técnico 24 horas al día, 7 días a la semana a través de teléfono, chat en directo, portal en línea y correo electrónico y debe estar limitado a contactos autorizados por parte del ayuntamiento para asegurar la privacidad y seguridad del servicio. Debe incluir:

- Acceso al portal de comunidades
- Teléfono, correo electrónico, canales de soporte web
- Mantenimiento de firmware
- Resolución de cuestiones técnicas
- Consulta de incidencias de software
- Acceso a la documentación del producto
- Guía de configuración
- Solicitudes de características
- Acceso al software en versión preliminar a través de los programas de Public Preview
- Casos de asistencia ilimitados para Contactos Autorizados

4.9 Conclusión

El WAF ofrece un nivel de seguridad robusto, con capacidades avanzadas de detección y mitigación de amenazas, gestión centralizada y optimización del rendimiento de aplicaciones web. Su integración con herramientas de automatización y análisis de datos lo convierte en una solución idónea para la protección de las aplicaciones del Ayuntamiento de Almuñécar.

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 14 de 26

5. SOLUCIÓN XDR GESTIONADA PARA EL AYUNTAMIENTO DE ALMUÑÉCAR

5.1 INTRODUCCIÓN

Este documento presenta la memoria técnica para la implementación de la solución XDR (Extended Detection and Response) en el Ayuntamiento de Almuñécar. El objetivo es proporcionar una protección integral para endpoints, servidores y redes, garantizando un entorno seguro frente a amenazas avanzadas. La solución contempla monitorizar, **300 buzones de M365**, **200 endpoints de puestos de usuarios con Sophos Central Endpoint**, **correlando los logs con un servicio EDR avanzado en 80 servidores con administración, monitorización de los eventos de 13 servidores con identidad propia, monitorización y respuesta a incidentes incluidas, junto con la monitorización de firewalls y redes con remediación automática de alertas en los firewalls existentes del fabricante Sophos y la solución perimetral incluida en la propuesta.**

5.2 ALCANCE DEL PROYECTO

La solución XDR incluirá:

- Monitorización y respuesta de **300 buzones de M365.**
- Monitorización avanzada de Endpoints con integración en **Sophos para 200 endpoints de usuario.**
- Implementación de EDR avanzado para la protección de **80 servidores**, con remediación automática, y gestionada por el equipo de SOC, de las alertas de seguridad.
- Monitorización de los eventos originados en **13 servidores con identidad propia**: AD,DB,etc
- Monitorización y respuesta automática para firewalls y redes, con remediación automática de alertas en firewalls Sophos que ya posee el Ayuntamiento de Almuñécar y la nueva solución de protección perimetral de Firewall incluida en la presente licitación.
- Monitorización del servicio de WAF incluida en la licitación.
- XDR Collector Appliance para la recogida de logs de los todos los Firewalls y los Switches de Core junto con su mantenimiento correspondiente y sustitución del dispositivo hardware en caso de fallo durante toda la vigencia del contrato.
- Gestión centralizada de eventos de seguridad.
- Generación de reportes a medida y threat advisories.

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 15 de 26

5.3 CARACTERÍSTICAS DE LA SOLUCIÓN

5.3.1 Servicio general

- Servicio de SOC 24x7 TIP y SOAR en modalidad follow de sun. Quedaran excluidos todos aquellos servicios de SOC que den servicio desde una sola ubicación, aunque sea en formato 24x7.

- El equipo de especialistas debe contar con Blue Team, Green Team, Purple Team, Red Team y White team con presencia regional en Europa.

- El servicio SOC debe tener la capacidad de orquestar cambios de forma automática en los firewalls cada vez que detecte un intento de ataque, por ejemplo, una regla de bloqueo automática a IP. Debe integrarse con el máximo de marcas posibles de firewall NextGen, incluida la solución actual de Sophos y de la solución que se ofrezca en esta licitación. Estas respuestas automáticas generarán una alerta al equipo del ayuntamiento y serán revisadas por el equipo del SOC.

- El servicio SOC debe poder recibir los logs del perímetro (firewall) y el tráfico del switch core y enviarlo al SIEM externo del servicio sin costes adicionales, sin límite de logs, licenciándose por equipo activo enviando logs, independiente de tráfico y/o usuarios, permitiendo así la escalabilidad futura de estos equipos.

- Así mismo debe poder observar los intentos de manipulación en los controladores de dominio para una rápida respuesta y el mantenimiento de datos relevantes de auditoría del dominio.

- El servicio de SOC debe tener su propio desarrollo basado en IA/ML para una primera capa de detección y orquestación antes de escalar al resto de funcionalidades y equipos del servicio.

- El servicio debe disponer de las siguientes certificaciones: CISSP, CISA, CSAP, ISO, 27001, AWS Security, GCIH, C|EH, GIAC, and_CySA+, Security+, Network+

- El servicio debe incluir el administrar el riesgo de varios servicios nube como pueda ser Microsoft 365 y Microsoft Azure (EntraID) con capacidades de orquestación, detección y mitigación avanzada de amenazas, con respuesta automática contra accesos no autorizados a los elementos Cloud, suspendiendo así de forma automática los usuarios con comportamiento malicioso. El servicio debe licenciarse por usuarios, sin límite en los orígenes a monitorizar, permitiendo así que el ayuntamiento pueda añadir en el futuro nuevos servicios Cloud como pueden ser soluciones de MFA como Okta o Duo.

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 16 de 26

- Las acciones automáticas además deben poder ser realizadas por el equipo del ayuntamiento desde las propias alertas del servicio.

- Las capacidades del SOC + SIEM + TIP + SOAR de última generación deben tener más de 10 mil millones de indicadores de compromiso, más de 800 detecciones basadas en ML, mapeo directo al marco de referencia MITRE ATT&CK, laboratorios de ataque y defensa automatizada contra amenazas.

-
- Licenciamiento por NGFW activo a monitorizar con ingesta ilimitada de logs.

- No debe existir ningún límite en la cantidad de consultas a realizar al SOC, tanto por correo, como por teléfono y/o a través de la consola.

- El servicio debe permitir programar reportes de estilo QBR, que incluyan tanto las métricas de detecciones y actuaciones como threat advisories de forma parametrizable.

- Los listados de contactos deben poder ser gestionados por el equipo informático del ayuntamiento de Almuñécar, pudiendo establecer diferentes contactos según criticidad de la alerta, así como por horario.

- El servicio debe permitir hacer búsquedas en los logs mediante un buscador de lenguaje natural, permitiendo así la trazabilidad de los logs de forma sencilla.

5.3.2 Protección de M365

- Integración con M365 para la monitorización de los 300 buzones de los usuarios.
- Integración con Microsoft M365 para permitir que XDR supervise sus registros e investigue y alerte sobre posibles riesgos de identidad, correo electrónico y otros riesgos encontrados en la nube, incluidos los inicios de sesión sospechosos y más. Telemetría avanzada y análisis de amenazas mediante SOC del fabricante de la solución ofertada.
- Integración con Microsoft Azure Entra ID para permitir que XDR supervise los registros de su Event Hub e investigue y notifique sobre los posibles riesgos de identidad y activos, incluidos los riesgos de Active Directory, como las modificaciones de políticas, los cambios en los grupos y más.

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 17 de 26

5.3.3 Protección de Endpoints

- Integración con Sophos para la monitorización de los 200 endpoints de usuario.
- Telemetría avanzada y análisis de amenazas mediante SOC del fabricante de la solución ofertada
- Soporte para Windows y Linux.
- No se debe diferenciar costes independientemente del tipo de SO, cliente, servidor, servicio Docker.

5.3.4 Protección de Servidores

- Implementación de EDR avanzado en 80 servidores
- Implementación de la monitorización de 13 servidores con identidad propia.
- El servicio debe permitir la configuración de reglas STAR, Security Threat Automation Rules, que permitan al equipo de SOC establecer respuestas automatizadas, minimizando así el tiempo de respuesta.
- Servicio de respuesta a incidentes por parte del equipo de SOC en servidores integrado con el servicio de EDR.
- Monitorización de modificaciones en Active Directory, cambios en registros y actividad sospechosa en shell.
- Análisis correlacionado con otras fuentes de datos de XDR.
- Visibilidad en tiempo real con agentes para Windows y Linux.
- El servicio de EDR debe integrarse con el servicio de VSS del sistema operativo, no solo a nivel de ficheros, permitiendo asegurar el poder revertir el sistema operativo al último punto seguro.
- La respuesta a incidentes debe permitir matar procesos, desconectar el equipo de la red, poner en cuarentena los elementos infectados, limpiar los elementos infectados y hacer un rollback del sistema operativo para asegurar la no persistencia del ataque.

5.3.5 Seguridad de Red y Firewalls

- El servicio debe incluir un sistema de detección de intrusiones (IDS) para análisis de la red interna con la conexión con el switch Core de la red.
- Monitorización de todos los firewalls con detección y respuesta automática a alertas de seguridad.
- Suministro e Implementación de un dispositivo **físico** IDS del fabricante de la solución, que recoja todos los logs y eventos de los equipos de Switch Core y demás Firewalls del Ayuntamiento de Almuñécar.

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 18 de 26

- El sistema de respuesta automatizada debe permitir la creación automática de reglas en el FW para establecer un bloqueo permanente para las IPs origen del ataque.
- La consola de gestión de las alertas generadas por el SOC debe permitir generar bloqueos con un click, sin necesidad de acceder a la consola de gestión del FW, tanto de IPs externas como internas que estén involucradas en los incidentes.
- Compatibilidad con dispositivos de red de fabricantes como Fortinet, Palo Alto, Cisco, Checkpoint, Barracuda y Sophos.
- Detección de anomalías mediante Machine Learning para minimizar falsos positivos, detectar ofuscaciones y añadir información extendida en las alertas como reputación de IPs, detección de VPNs, proxies, etc. Añadiendo esta información en las alarmas y alertas para ofrecer una visibilidad extendida.

5.3.6 Integración y Arquitectura

La solución XDR ofertada se integrará con la infraestructura existente del Ayuntamiento de Almuñécar de la siguiente manera:

- Endpoints **(200 dispositivos)**: Monitorización de alertas de seguridad mediante integración con Sophos.
- M365: (**300 buzones de usuario).**
- Servidores **(80 equipos)**: Protección avanzada con EDR gestionado.
- Servidores **(13 equipos):** monitorización de los eventos generados en servidores críticos con identidad propia.
- **Firewall y Red:** Implementación de IDS físico y remediación automática de alertas en firewalls Sophos, en el nuevo firewall perimetral de este presente pliego y WAF incluidos en la propuesta.

5.3.7 Beneficios de la Solución

- **Visibilidad y correlación de amenazas:** La solución XDR permite correlacionar eventos en diferentes capas de seguridad (nube, endpoint, red y servidores).
- **Automatización de respuestas**: A través de SOAR y respuestas automáticas en Microsoft 365, firewalls y endpoints.
- **Protección contra amenazas avanzadas**: Defensa contra ataques dirigidos, ransomware, APTs y amenazas basadas en inteligencia artificial.
- **Gestión centralizada:** Un único SOC (Security Operations Center) para la supervisión y respuesta a incidentes.
- **Gestión en los servidores**: Permitiendo de esa forma la respuesta completa a incidentes por parte del SOC.

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 19 de 26

5.3.8 Niveles de servicio

La solución XDR debe clasificar las alertas en base a su criticidad, estableciendo a su vez diferentes niveles de servicio.

- **Alertas de nivel alto.** Cualquier actividad maliciosa que tenga el potencial de generar un importante daño al entorno del ayuntamiento. Por ejemplo: malware o ransomware, escalación de privilegios o detección de herramientas de hackeo.
  SLA: 20 minutos
  Método de contacto: llamada telefónica, correo y alerta en el dashboard.

- **Alertas de nivel medio.** Cualquier actividad que requiera una acción pero que normalmente no causaría un impacto sustancial como evento aislado. Por ejemplo: eventos de login sospechosos, intentos de fuerza bruta o coincidencias de inteligencia sobre amenazas.
  SLA: 1 hora
  Método de contacto: correo y alerta en el dashboard.

- **Alertas de nivel bajo.** Cualquier actividad que ofrezca un valor el ser informado, pero que posiblemente no requiera de ninguna acción. Por ejemplo: creación de una cuenta de usuario, actividad de escaneo o cambio de contraseña.
  SLA: 8 horas
  Método de contacto: correo y alerta en el dashboard.

5.3.9 Conclusiones

La implementación de la solución XDR proporcionará al Ayuntamiento de Almuñécar una plataforma de seguridad robusta y escalable. La integración con Sophos para endpoints, EDR gestionado para servidores y la monitorización de firewalls garantizará la protección contra amenazas avanzadas, permitiendo una gestión eficiente de la seguridad TI municipal.

6. INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE TODOS LOS DISPOSITIVOS Y SERVICIOS LICITADOS

La empresa adjudicataria, se encargará de los siguientes servicios:

SOLUCIÓN XDR:

- Jefatura de proyecto
- Onboarding
- Instalación XDR Collector Appliance
- Integración con los nuevos Firewall Sophos existente del Ayuntamiento
- Configuración SOAR para remediación de alertas de seguridad en Firewall Sophos
- Integración con los nuevos Firewalls perimetrales

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 20 de 26

- Configuración SOAR para remediación de alertas de seguridad de los nuevos Firewalls.
- Integración con la consola existente de Sophos para Endpoints
- Integración con la consola de M365
- Integración con la consola de WAF del fabricante
- Instalación XDR Collector en 21 servidores
- Despliegue XDR con su agente correspondiente en 80 servidores
- Configuración reglas de remediación automática para los agentes
- Formación en la consola de XDR para revisión, remediación y cierre de alertas con SOC
- Documentación
- Cualquier otra configuración en la infraestructura existente del Ayuntamiento de Almuñécar que se requiera.

SERVICIO CLOUD WAF

- Jefatura de proyecto
- Onboarding
- Configuraciones necesarias en los Firewall Sophos existentes y equipos de red
- Análisis aplicaciones a proteger (total 30 aplicaciones)
- Configurar aplicaciones en modo monitoring
- Habilitar políticas de seguridad
- Protección contra OWASP Top 10 (XSS, SQLi, CSRF, etc.).
- Validación de solicitudes HTTP y URLs.
- Configurar reglas de inspección de tráfico.
- Configurar DDoS Protection y Rate Limiting.
- Configurar filtrado de IPs y geolocalización p ara restringir accesos desde ubicaciones
- específicas
- Configurar alertas y reportes vía correo o syslog
- Realizar pruebas y ajustes
- Ajustar reglas de firewall y seguridad basadas en el resultado de las pruebas
- Configurar aplicaciones en modo bloqueo una vez realizados todos los ajustes
- Formación en la consola WAF del fabricante para revisión y gestión de alertas
- Documentación
- Coordinación trabajos y actuación en Campo
- Cualquier otra configuración en la infraestructura existente del Ayuntamiento de Almuñécar que se requiera.

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 21 de 26

- Servicios profesionales de Montaje, configuración y puesta en producción, se decidirá con el adjudicatario la mejor configuración e instalación de los nuevos Firewall junto a los Firewalls Sophos existentes del Ayuntamiento de Almuñécar.
- Creación de las políticas necesarias de los nuevos firewalls.
- Servicios profesionales de Configuración y puesta en producción de ZNTA.
- Formación al departamento de informática del uso de los nuevos firewalls.
- Cualquier otra configuración en la infraestructura existente del Ayuntamiento de Almuñécar que se requiera.

7. TIEMPO DE IMPLANTACIÓN Y CONFIGURACIÓN TOTAL

La empresa adjudicataria se encargará de la implantación, configuración, migración y todas las intervenciones necesarias para dejar funcionando correctamente todos los dispositivos y servicios licitados en este pliego.

El tiempo de duración de dicha implantación será como máximo de **30 días laborables**, en el caso de que se supere este plazo se podrá realizar una rescisión del contrato por superar el tiempo total de suministro e implantación completa.

8. 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.

9. 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 CPD 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.

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 22 de 26

10. CERTIFIACIONES OBLIGARORIAS POR PARTE DEL LICITADOR DE LOS DIFERENTES SERVICIOS

- **ENS Alta**
- **ISO 27001**
- **ISO 14001**
- **ISO 9001**
- **Preferred Partner del fabricante del WAF y XDR.**
- **Web Application Firewall – Foundation o similar.**
- **Web Application Firewall Certified Product Specialist o similar.**
- **XDR Certified Product Specialist o similar.**
- **Autorización directa del fabricante para la implantación del servicio WAF.**
- **Autorización directa del fabricante para la implantación de los Firewall.**
- **Certificado de network security del fabricante del Firewall.**

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

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

11. EXPERIENCIA MÍNIMA DE LOS LICITADORES

Los licitadores tendrán que contar con una la siguiente experiencia mínima en la implantación de este tipo de proyectos de 5 años:

- Firewalls perimetrales
- Servicio Cloud WAF
- XDR gestionado
- Switches gestionables Cisco.

12. BOLSA DE HORAS

Los licitadores tendrán que incluir una bolsa de 150 horas para realizar servicios de asistencia y configuración post instalación de todos los servicios incluidos en el presente pliego.

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 23 de 26

13. 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.

14. CUADRO DE PENALIZACIONES DE SOLUCIÓN SOC XDR

NIVELES DE INCIDENCIAS	DESCRIPCIÓN	TIEMPO DE RESOLUCIÓN MÁXIMO INCIDENCIA	PENALIZACIÓN
Alto	Alertas de nivel alto. Cualquier actividad maliciosa que tenga el potencial de generar un importante daño al entorno del ayuntamiento. Por ejemplo: malware o ransomware, escalación de privilegios o detección de herramientas de hackeo.	20 Minutos	15% del precio de adjudicación de contrato
Media	Alertas de nivel medio. Cualquier actividad que requiera una acción pero que normalmente no causaría un impacto sustancial como evento aislado. Por ejemplo: eventos de login sospechosos, intentos de fuerza bruta o coincidencias de inteligencia sobre amenazas.	1 Hora	10% del precio de adjudicación de contrato
Baja	Alertas de nivel bajo. Cualquier actividad que ofrezca un valor el ser informado, pero que posiblemente no requiera de ninguna acción. Por ejemplo: creación de una cuenta de usuario, actividad de escaneo o cambio de contraseña.	8 Horas	5% del precio de adjudicación de contrato

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 24 de 26

15. 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.

16. DURACIÓN DEL CONTRATO

La duración del contrato será de 3 años sin posibilidad de prórroga.

17. PRESUPUESTO DEL CONTRATO.

- El precio base de licitación de todo el suministro y servicios, 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 y servicios de seguridad junto con su instalación y puesta en marcha, está distribuido de la siguiente forma:

SUMINISTROS

	CANTIDAD SIN IVA	IVA	CANTIDAD CON IVA
PRIMER AÑO	37.343,61 euros	7.842,16 euros	45.185.77 euros
SEGUNDO AÑO	37.343,61 euros	7.842,16 euros	45.185.77 euros
TERCER AÑO	37.343,61 euros	7.842,16 euros	45.185.77 euros
TOTAL 3 AÑOS	112.030,83 euros	23.526,48 euros	135.557,31 euros

SERVICIOS

	CANTIDAD SIN IVA	IVA	CANTIDAD CON IVA
PRIMER AÑO	9.962,38 euros	2.092,10 euros	euros
SEGUNDO AÑO	9.962,38 euros	2.092,10 euros	euros
TERCER AÑO	9.962,38 euros	2.092,10 euros	euros
TOTAL 3 AÑOS	29.887,14 euros	6.276,3 euros	36.163,45 euros

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 25 de 26

SUMINISTRO + INSTALACIÓN

	TOTAL SIN IVA	IVA	TOTAL CON IVA
PRIMER AÑO	**47.305,99 euros**	**9.934,25 euros**	**57.240,24 euros**
SEGUNDO AÑO	**47.305,99 euros**	**9.934,25 euros**	**57.240,24 euros**
TERCER AÑO	**47.305,99 euros**	**9.934,25 euros**	**57.240,24 euros**
TOTAL 3 AÑOS	**141.917,97 euros**	**29.802.75 euros**	**171.720,72 euros**

Firmado electrónicamente al margen

Cód. Validación: 7WZKC46YSST7K5KQGMKERZWT3
Verificación: https://almunecar.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 26 de 26