CÓDIGO SEGURO DE VERIFICACIÓN (CSV): CCM0012JFLAF5yu0KA5n4l8sxir01HcIc=
URL de verificación: https://sede.camaradecuentasmadrid.org

Cámara de Cuentas
Comunidad de Madrid

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES PARA LA CONTRATACIÓN DE LA RENOVACIÓN DEL HARDWARE DEL CENTRO DE PROCESO DE DATOS

CÓDIGO SEGURO DE VERIFICACIÓN (CSV): CCM0012JFLAF5yu0KA5n4l8sxir01HcIc=
URL de verificación: https://sede.camaradecuentasmadrid.org

CÓDIGO SEGURO DE VERIFICACIÓN (CSV): CCM0012JFLAF5yu0KA5n4l8sxir01HcIc=
URL de verificación: https://sede.camaradecuentasmadrid.org

INDICE

1.- NECESIDAD Y OBJETO DE LA CONTRATACIÓN 5

1.1.- OBJETO DEL CONTRATO 5

1.2.- SITUACIÓN ACTUAL 5

2.- PROPUESTA TÉCNICA 5

2.1.- CARCTERÍSTICAS TÉCNICAS 5

2.2.- CARACTERÍSTICAS FUNCIONALES 7

2.3.- SUMINISTRO DE 50 CLIENTES VPN-ZTNA 11

2.4.- VIGENCIA DE LAS LICENCIAS 12

2.5.- SERVICIOS ADICIONALES 12

3.- PLANIFICACIÓN, CONTROL Y SEGUIMIENTO 13

3.1.- PLANIFICACIÓN 13

3.2.- CONTROL Y SEGUIMIENTO DEL PROYECTO 13

4.- CONDICIONES GENERALES DE REALIZACIÓN 14

4.1.- CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS 14

4.2.- SUBCONTRATACIÓN 14

4.3.-PERSONAL.. 14

4.4.- AUDITORÍAS 15

5. CRITERIOS DE VALORACION 15

6. PRESUPUESTO BASE DE LICITACIÓN 15

7. FORMA DE PAGO 15

CÓDIGO SEGURO DE VERIFICACIÓN (CSV): CCM0012JFLAF5yu0KA5n4l8sxir01HcIc=
URL de verificación: https://sede.camaradecuentasmadrid.org

CÓDIGO SEGURO DE VERIFICACIÓN (CSV): CCM0012JFLAF5yu0KA5n4l8sxir01HcIc=
URL de verificación: https://sede.camaradecuentasmadrid.org

1.- NECESIDAD Y OBJETO DE LA CONTRATACIÓN

1.1.- OBJETO DEL CONTRATO

El objeto de este contrato es el suministro de dos firewalls con sus correspondientes licencias del software de gestión.

Se incluyen también los servicios de migración y puesta en marcha de la solución ofertada.

1.2.- SITUACIÓN ACTUAL

En la actualidad , la Cámara de Cuentas de la Comunidad de Madrid cuenta con dos firewalls Fortigate 100D que finalizan su vida útil en julio de 2022.

Los firewalls se encuentran configurados en modo "activo-pasivo" para asegurar la alta disponibilidad en los accesos a internet, la alta disponibilidad es un requerimiento de los proyectos de mejora de seguridad en las comunicaciones que se encuentran implementados en nuestra institución.

En paralelo en cada portátil de la organización se encuentra instalado el software forticlient que asegura la conectividad de los equipos externos a la red con los requisitos exigidos para garantizar la seguridad perimetral.

2.- PROPUESTA TÉCNICA

2.1.- CARCTERÍSTICAS TÉCNICAS

Se presentan las características técnicas de los equipos solicitados.

- Instalación en alta disponibilidad, permitiendo tanto modo activo-activo, activo-pasivo o clustering, para lo que se requiere el suministro de dos sistemas con idénticas características técnicas.
- Rendimiento del servicio Firewall (IPv4, IPv6, UDP): 27 Gbps (1518 / 512 bytes), 11 Gbps (64 bytes).
- Latencia máxima Firewall (64 bytes, UDP): 4,78 µs.
- Rendimiento Firewall (paquetes por segundo): 16,5 Mpps.
- Rendimiento IPS (Enterprise Mix) (*): 5 Gbps.
    - (*) Rendimiento medido con registro habilitado.
- Rendimiento del servicio NGFW (**): 3,5 Gbps.
    - (**) Rendimiento medido con firewall, IPS, control de aplicaciones y registro habilitados.
- Rendimiento del servicio de protección de amenazas (***): 3 Gbps.

CÓDIGO SEGURO DE VERIFICACIÓN (CSV): CCM0012JFLAF5yu0KA5n4l8sxir01HcIc=
URL de verificación: https://sede.camaradecuentasmadrid.org

  - (***) Rendimiento medido con firewall, IPS, control de aplicaciones, protección malware y registro habilitados.
- Rendimiento del servicio IPSec VPN (512 bytes, AES256-SHA256): 13 Gbps.
- Rendimiento del servicio SSL-VPN: 2 Gbps.
- Túneles IPSec VPN:
  - Gateway-to-Gateway: 2.000
  - Client-to-Gateway: 16.000
- Usuarios concurrentes SSL-VPN (modo túnel): 500
- Rendimiento CAPWAP (HTTP 64K): 20 Gbps.
- Rendimiento Inspección SSL (sesiones HTTPS de diferentes suites de cifrado): 4 Gbps.
- Rendimiento Control de Aplicaciones (HTTP 64K): 13 Gbps.
- Máximo número de AP (Total / Modo Túnel): 256 / 128.
- Capacidad mínima de gestión de conexiones (TCP): 3.000.000 de sesiones concurrentes, permitiendo como mínimo 280.000 sesiones por segundo.
- Los equipos propuestos deberán garantizar los rendimientos solicitados mediante el uso de procesadores específicos para el tratamiento correcto del tráfico.
- Número mínimo de interfaces:
  - 2 x 10 GE SFP+ Slots.
  - 16 x GE RJ45 Interfaces.
  - 8 x GE SFP Slots.
  - 1/1 x GE RJ45 Puertos de Gestión / HA.
  - 1 x Puerto USB.
  - 1 x RJ45 Puerto de Consola.
- Número máximo de Dominios virtuales: 10.
- Número máximo de políticas de firewall: 10.000.
- Almacenamiento interno: 1 disco SSD de 480 GB.
- Tamaño máximo por equipo enracable: 1 RU.
- Fuentes de alimentación: Principal y redundante (integradas).
- Los equipos deben tener las funcionalidades integradas de UTM Protection (24x7 IPS, AV, Web Filtering and Antispam, Sandbox Cloud). No se acepta ningún acuerdo OEM con terceros, es decir, todas estas funcionalidades tienen que ser del propio fabricante de seguridad. El licenciamiento de las funcionalidades ha de basarse por equipo, no por usuario.

CÓDIGO SEGURO DE VERIFICACIÓN (CSV): CCM0012JFLAF5yu0KA5n4l8sxir01HcIc=
URL de verificación: https://sede.camaradecuentasmadrid.org

- El cortafuegos propuesto debe tener las certificaciones de Internet Computer Security Association (ICSA): ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; USGv6/IPv6.

2.2.- CARACTERÍSTICAS FUNCIONALES

A continuación, se presentan las características funcionales de los servicios que deberán proporcionar los sistemas requeridos.

- Servicio Firewall.
  - 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.
- Servicio VPN (Virtual Private Network).
  - Protocolos soportados: PPTP, IPSec y SSL.
  - Encriptación y autenticación: DES, 3DES y AES. SHA1 y MD5.
  - Integración con firma electrónica.
  - Modo de funcionamiento cliente/servidor y punto a punto.
  - Cliente VPN propietario que asegure la 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 para sistemas operativos IOS y Android.
- Servicio Antivirus y Antispyware.
  - Protocolos que se requieren analizar: HTTP/HTTPS, POP3/POP3S, FTP, SMTP/SMTPS, IMAP/IMAPS, mensajería instantánea.
  - Posibilidad de configurar por parte del administrador de la plataforma el funcionamiento en modo proxy (fichero) o en modo stream (flujo).
  - Posibilidad de bloqueo de ficheros por tipo y tamaño.

CÓDIGO SEGURO DE VERIFICACIÓN (CSV): CCM0012JFLAF5yu0KA5n4l8sxir01HcIc=
URL de verificación: https://sede.camaradecuentasmadrid.org

- Posibilidad de gestión de archivos en cuarentena.
- Servicio de actualización de firmas de virus al menos 3 veces al día.

- Servicio IPS (Intrusion Prevention System).
  - Análisis de tráfico e inspección IPS basado en los estándares de los diferentes protocolos.
  - Debe disponer de más de 8.000 firmas de IPS.
  - Deben actualizarse las firmas al menos 2 veces por semana.
  - Posibilidad de creación y edición de firmas personalizadas.
  - Escaneo de vulnerabilidades programable de servidores basado en las propias firmas de IPS.
- Servicio de Filtrado Web.
  - Protocolos a analizar: HTTP/HTTPS.
  - Categorización de contenidos web con más de 78 categorías con más de 50 millones de páginas categorizadas.
  - Creación de patrones para la definición de listas URL.
  - Bloqueo de contenidos web.
  - Posibilidad de fijación de cuotas de navegación por categoría.
  - Servicio de actualización en tiempo real de categorización de URL.
- 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, 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.
- Servicio de Protección de Fugas de Información (DLP).
  - Soporte de los siguientes protocolos: HTTP/HTTPS, correo y mensajería instantánea.
  - Identificación y control de información corporativa sensible.
  - Análisis de los tipos de ficheros más utilizados (Microsoft Office y PDF).
  - Definición de patrones a nivel binario y de poder calcular el hash de los documentos a proteger para controlar su salida del perímetro.

CÓDIGO SEGURO DE VERIFICACIÓN (CSV): CCM0012JFLAF5yu0KA5n4l8sxir01HcIc=
URL de verificación: https://sede.camaradecuentasmadrid.org

- Posibilidad de marcar documentos a proteger mediante una marca de agua identificable para evitar su salida de la organización.

- Servicio Antispam.
  - Protocolos a analizar: SMTP/SMTPS, POP3/POP3S e IMAP/IMAPS.
  - Gestión de listas negras RBL.
  - Posibilidad de bloqueo a nivel de dirección IP.
  - Posibilidad de filtrado por palabras y expresiones.
- Otras funcionalidades que otorgan valor añadido a la solución requerida:
  - Integración con Active Directory y con RADIUS/802.1X, pudiendo aplicar QoS a nivel de usuario o grupo de usuarios.
  - Licencias de usuario ilimitadas.
  - Capacidad de integrar, sin coste adicional, la funcionalidad de controlador de redes WiFi pudiendo aplicar políticas de control de aplicaciones, filtrado de URL, antivirus, IPS y calidad de servicio (QoS) a tráfico WiFi. Dispondrá de la posibilidad de suministro de Access Points adicionales, tanto de interior como de exterior, con varias antenas para la detección de Rogue Access Points. Dispondrá de una herramienta gratuita para la planificación de cobertura.
  - Disponibilidad de certificaciones reconocidas en la industria (NSS Labs, ICSA Labs).
  - Soporte del protocolo GRE, para el establecimiento y finalización de túneles en el mismo equipo.
  - Balanceo de líneas de acceso a internet con monitorización basado en IP origen o en anchos de banda.
  - Balanceo de carga a granjas de servidores.
  - Funcionamiento en modo proxy explícito.
  - Nat 64 y 46.
  - Control de ancho de banda basado en IP, usuarios y/o aplicaciones.
  - Capacidad de aplicar perfiles de protección específicos (WAF) para entornos y aplicaciones web.

La solución propuesta deberá por tanto contemplar:

- Rendimiento: Además del tratamiento del tráfico de seguridad, este tráfico deberá ser cursado también por procesadores específicos que ofrecen un gran rendimiento a todo tipo de redes realizando tareas de red, seguridad, sandboxing e inspección SSL.

CÓDIGO SEGURO DE VERIFICACIÓN (CSV): CCM0012JFLAF5yu0KA5n4l8sxir01HcIc=
URL de verificación: https://sede.camaradecuentasmadrid.org

- Balanceo de todo tipo de líneas: Deberá permitir configurar todos sus puertos como líneas WAN y crear múltiples túneles IPSec en cada una. Además, permitirá también conectar directamente módems USB 3G/4G para conectar redes de backup o adicionales.
    - Podrá definir dos tipos de SLA:
        - Best quality. Elige solo el mejor camino posible.
        - Minimum quality. Elige todos los caminos que cumplan con el SLA establecido.
        - Múltiples SLAs definidos para cada política de SD-WAN.
        - QoS (Entrada y Salida) y optimización WAN.
- Deberá poder realizar traffic shaping basado en porcentajes y balanceo de SD-WAN basado en capa 7 de aplicación (usando más de 3.000 firmas de aplicación) además de combinarlo con ISDB.
- Balanceo inteligente por aplicación: Deberá permitir balancear tráfico de Internet, aplicaciones SaaS y aplicaciones corporativas de forma inteligente mediante umbrales de latencia, jitter, ancho de banda disponible, para asegurar que la VoIP o videoconferencia y las aplicaciones críticas siempre vayan por la línea óptima en cada momento.
- VPN Inteligente: Tendrá que disponer de ADVPN (Auto Discovery VPN) para realizar túneles IPSec automáticos entre sedes. Esto permitirá optimizar las redes SD-WAN, crear caminos de baja latencia y mantener todas las ventajas de una red unificada bajo entorno IPSec centralizado.
    - Compatibilidad total con BGP (actualización de rutas, varios caminos usables en BGP, fusión entre ADVPN y SD-WAN…).
- Panel de gestión único: Al tener que estar 100% integrado con el sistema de Administración Centralizada existente, se puede gestionar todo el entorno SD-WAN desde un único punto, pudiendo controlar los túneles IPSec, el estado de todas las líneas, amenazas, incidencias de red, ofreciendo una completa visibilidad en tiempo real e informes personalizados desde un único punto central.
- VDOM SD-WAN y Red: Pudiendo gestionar VLANS, Routing Dinámico, Routing Estático, NAT Avanzado, IPSec, QoS, ADVPN, DNS, DHCP y conectividad WiFi.
- Deberá tener la funcionalidad de Auto-fallback, entre líneas SD-WAN.
- VDOM Seguridad L7: Permitiendo gestionar IPS, AppCtrl, firewall L4, AV, Sandboxing, Filtrado web, autenticación con AD y Gestión.
- Despliegue alta disponibilidad y zero-touch: La solución deberá ser desplegada en un único equipo, ofreciendo un despliegue zero-touch real.
- Deberá además contar con APIs, con las que es posible la integración con

CÓDIGO SEGURO DE VERIFICACIÓN (CSV): CCM0012JFLAF5yu0KA5n4l8sxir01HcIc=
URL de verificación: https://sede.camaradecuentasmadrid.org

cualquier Orquestador (Nuage, HP, OpenStack…).

- Permitirá el uso de soluciones de autenticación de doble factor, del mismo fabricante sin suscripción asociada. Estos podrán ser usados en formato físico y en versión software para Smartphone.
- No se acepta ningún acuerdo OEM con terceros, es decir, todas estas funcionalidades tienen que ser del propio fabricante de seguridad.
- El licenciamiento de las funcionalidades ha de basarse en licenciamiento por equipo, no por usuario.

2.3.- SUMINISTRO DE 50 CLIENTES VPN - ZTNA

Se requiere, dentro de esta licitación, la adquisición de **50 licencias de cliente VPN – ZTNA** compatible con la plataforma hardware solicitada anteriormente con las siguientes características técnicas.

Garantiza un acceso remoto seguro con funcionamiento continuo, SSL/Ipsec VPN que respalda la segmentación de la red, admisión condicional e integración con plataformas de inicio de sesión único y autenticación de múltiples factores

Seguridad de confianza cero: La edición ZTNA del cliente ofrece los requisitos para que un trabajador remoto se conecte a la red con un mínimo nivel de control. Esta edición habilita túneles cifrados ZTNA y VPN, al igual que filtrado de URL y control de dispositivos USB. Se incluye la gestión central a través de la plataforma EMS.

Administración central a través de EMS:

- Implementación y aprovisionamiento centralizado: Permite a los administradores implementar software de punto final de forma remota y realizar actualizaciones controladas. Hace que la implementación de la configuración del cliente en múltiples endpoints sea una tarea fácil con solo un clic en un botón.
- Panel de Vulnerabilidad: Ayuda a gestionar la superficie de ataque de una organización. Todos los puntos finales vulnerables se identifican fácilmente para una acción administrativa.
- Integración de Windows AD: Ayuda a sincronizar la estructura AD de una organización en EMS para que las mismas unidades de organización (OU) puedan usarse para la administración de endpoints. El estado de los endpoints en tiempo real proporciona siempre información actualizada sobre la actividad de los endpoints y los eventos de seguridad.

Registro de generación de informes central:

- Simplifica la elaboración de informes de cumplimiento y el análisis de seguridad mediante cualquier producto SIEM.

Conector dinámico Security Fabric:

CÓDIGO SEGURO DE VERIFICACIÓN (CSV): CCM0012JFLAF5yu0KA5n4l8sxir01HcIc=
URL de verificación: https://sede.camaradecuentasmadrid.org

- EMS crea grupos virtuales basados en postura de seguridad del endpoint. Estos grupos virtuales son recuperados por los dispositivos de seguridad y utilizados en la política firewall para el control del acceso dinámico. Los grupos dinámicos ayudan a automatizar y simplificar el cumplimiento de las políticas de seguridad.

Agente de vulnerabilidad y corrección:

- Asegura la higiene de los endpoints y los fortalece para reducir la superficie de ataque. Identifica los endpoints vulnerables y prioriza las vulnerabilidades del software y del sistema operativo no parcheadas con opciones de parches flexibles que incluyen parches automáticos.

SSL (Secure Socket Layer) VPN (Virtual Private Network) con MFA:

- Permite un túnel cifrado fácil de usar que atravesará casi cualquier infraestructura

Ipsec VPN con MFA:

- Permite un túnel cifrado fácil de usar proporcionando mayor capacidad de proceso VPN

Filtrado web:

- Supervisa todas las actividades del navegador web para aplicar la política de uso aceptable y seguridad web con más de 75 categorías. Funciona en todos los sistemas operativos compatibles y funciona con SafeSearch de Google. El perfil de Filtrado web del endpoint se puede sincronizar desde el dispositivo de seguridad para la aplicación coherente de las políticas. Los administradores pueden configurar listas negras y blancas, políticas dentro y fuera de la red e importar políticas de filtrado web del dispositivo de seguridad para una aplicación consistente.
- Compatible con un complemento de filtrado web que mejora la detección y el cumplimiento de las reglas de filtrado web en sitios HTTPS con tráfico cifrado.

Control de dispositivos USB:

- Evita que dispositivos USB no autorizados accedan al host

Túnel dividido:

- Respaldado por túneles ZTNA y VPN, el túnel dividido permite una experiencia de usuario optimizada

2.4.- VIGENCIA DE LAS LICENCIAS

La vigencia de las licencias y su soporte técnico será de tres años desde la fecha de puesta en marcha.

2.5.- SERVICIOS ADICIONALES

Se requieren los servicios de instalación, actualización, puesta en marcha y configuración en alta disponibilidad (en su caso) de los nuevos equipos, así como de migración de las

CÓDIGO SEGURO DE VERIFICACIÓN (CSV): CCM0012JFLAF5yu0KA5n4l8sxir01HcIc=
URL de verificación: https://sede.camaradecuentasmadrid.org

configuraciones de los cortafuegos FortiGate 100D actuales a los nuevos equipos para la potenciación y renovación del equipamiento actualmente dedicado a la seguridad perimetral. Dada la visibilidad, la efectividad de la seguridad de la información y de la criticidad que representa para Cámara de Cuentas el tiempo de parada de los sistemas de protección de red, esta actividad se llevará a cabo atendiendo a una planificación conjunta elaborada entre la empresa adjudicataria y los responsables técnicos en Cámara de Cuentas, donde Cámara de Cuentas propondrá la ventana más adecuada para llevar a cabo estas tareas de migración.

Asimismo, se requieren los servicios de configuración inicial y puesta en marcha de la plataforma EMS asociada a los clientes VPN – ZTNA requeridos.

3.- PLANIFICACIÓN, CONTROL Y SEGUIMIENTO

3.1.- PLANIFICACIÓN

En los siete días posteriores a la formalización del contrato se cerrará la planificación del cambio de infraestructura y migración de los servicios. Se fija como objetivo que los servicios no se vean interrumpidos entre las 7:00 y las 17:00 de lunes a viernes.

La confirmación de la planificación se realizará por parte del Director del Proyecto (Responsable del Contrato) designado por la Cámara de Cuentas y del Gestor del Proyecto de la empresa.

3.2.- CONTROL Y SEGUIMIENTO DEL PROYECTO

Se realizará por parte del Director del Proyecto designado por la Cámara de Cuentas y del Gestor del Proyecto de la empresa.

La Gestión de Proyectos tiene como finalidad principal el seguimiento y control de las actividades y de los recursos humanos y materiales que intervienen en las distintas fases. Como consecuencia de este control, será posible conocer en todo momento qué problemas se produzcan y resolverlos o paliarlos lo más pronto posible, con el fin de evitar desviaciones temporales y económicas.

Todas las modificaciones sobre el alcance del proyecto se deberán plantear y resolver en esta fase de control y seguimiento, correspondiendo la potestad decisoria al Director del Proyecto designado por la Cámara de Cuentas.

CÓDIGO SEGURO DE VERIFICACIÓN (CSV): CCM0012JFLAF5yu0KA5n4l8sxir01HcIc=
URL de verificación: https://sede.camaradecuentasmadrid.org

4.- CONDICIONES GENERALES DE REALIZACIÓN

4.1.- CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS

El adjudicatario deberá cumplir con la Política de Seguridad de la Cámara de Cuentas, adoptada por Acuerdo del Consejo de la Cámara de Cuentas de 29 de noviembre de 2017.

Esta obligación de confidencialidad subsistirá aun después de la realización del trabajo encomendado o de la finalización del contrato, por cualquier causa, tratándose por tanto de una obligación indefinida.

4.2.- SUBCONTRATACIÓN

De conformidad con el art. 215.2 los licitadores deberán indicar en la oferta la parte del contrato que tengan previsto subcontratar, señalando su importe y el nombre o perfil empresarial, definido por referencia a las condiciones de solvencia profesional o técnica, de los subcontratistas a los que se vaya a encomendar su realización.

Si con posterioridad a la adjudicación del contrato y, a más tardar, cuando inicie la ejecución de este, si resultase necesaria la subcontratación de algún servicio que no se hubiese indicado según el párrafo anterior, el adjudicatario deberá comunicarlo por escrito y solicitar la previa autorización de la Cámara de Cuentas. Si la Cámara de Cuentas autorizase dicha subcontratación, el adjudicatario procederá a establecer con la empresa subcontratista un contrato con las mismas especificaciones del presente, del cual remitirá una copia a la Cámara de Cuentas.

4.3.-PERSONAL

El adjudicatario deberá incluir en su oferta la designación de la persona o personas que, sin perjuicio de la responsabilidad propia de la empresa, estarán autorizadas para las relaciones con la Institución, a efectos del uso correcto del material y de la información a manejar. Se adjuntará una descripción de su perfil profesional y si, con posterioridad a la adjudicación del contrato, resultará necesaria su sustitución, esta será comunicada con suficiente antelación al Director del Proyecto.

Antes de iniciarse la ejecución del contrato, el adjudicatario se compromete a informar de la identidad del personal designado para desarrollar tales servicios, que se atendrá al cumplimiento de las normas, especificaciones y procedimientos de seguridad y acceso establecidos por la Cámara de Cuentas.

En particular, el adjudicatario se compromete a impartir, a todas las personas a su cargo, las instrucciones precisas para el efectivo conocimiento de las responsabilidades y el obligado cumplimiento de las medidas de seguridad que asumen en virtud del presente contrato, sobre confidencialidad y secreto. En este sentido, el adjudicatario realizará cuantas advertencias y suscribirá cuantos documentos sean necesarios con sus empleados, con el fin de asegurar el cumplimiento de tales obligaciones.

El adjudicatario responderá frente a la Cámara de Cuentas si tales obligaciones son incumplidas por sus empleados.

CÓDIGO SEGURO DE VERIFICACIÓN (CSV): CCM0012JFLAF5yu0KA5n4l8sxir01HcIc=
URL de verificación: https://sede.camaradecuentasmadrid.org

4.4.- AUDITORÍAS

La Cámara de Cuentas se reserva la capacidad de realizar las verificaciones y/o auditorías, que estime precisas, para asegurar el cumplimiento de las medidas técnicas y organizativas establecidas por la normativa aplicable.

5. CRITERIOS DE VALORACION

El único criterio de valoración será el precio.

6. PRESUPUESTO BASE DE LICITACIÓN

El presupuesto base de licitación del contrato asciende a 54.000€ correspondiendo 44.628€ al principal y 9.372€ al IVA. El desglose presupuestario máximo estimado, por elementos unitarios, se inserta a continuación:

Producto	Importe
Firewalls	41.140 €
Licencias VPN ZTNA	7.260 €
Instalación y migración	5.600 €
	54.000 €

Dicho presupuesto será imputado al subconcepto 63600 del Programa 911O, del Presupuesto General de la Comunidad de Madrid para el año 2022.

Dicho contrato no se divide en lotes al contar la Cámara de Cuentas con un único CPD, lugar donde se encuentran los firewalls a configurar, administrar y gestionar.

En ningún caso, el importe de licitación podrá ser rebasado por las ofertas que se presenten.

7. FORMA DE PAGO

Se efectuará el pago a la entrega del suministro y a su correspondiente instalación y migración, previa presentación de la factura y certificación de conformidad emitida por el responsable del contrato designado por la Cámara de Cuentas

DILIGENCIA: Para hacer constar que en el día de hoy, ha sido aprobado el pliego de prescripciones técnicas particulares por el Presidente de la Institución.

Madrid, a fecha de firma
LA OFICIAL MAYOR

Firmado digitalmente por MARÍA OTILIA ARMIÑANA VILLEGAS
Organización: CÁMARA DE CUENTAS DE LA COMUNIDAD DE MADRID
Fecha: 06/05/2022 12:58:31