VERSIÓN PÚBLICA - ART. 30 LAIP

MINISTERIO DE CULTURA

GOBIERNO DE EL SALVADOR

UNIDAD DE ADQUISICIONES Y CONTRATACIONES INSTITUCIONAL (UACI)

ORDEN DE COMPRA PARA OBRAS, BIENES Y SERVICIOS

LUGAR Y FECHA:	Alameda Juan Pablo II, Calle Guadalupe Edificio A-5, Plan Maestro, Centro de Gobierno, San Salvador 07 de noviembre de 2022	**ORDEN No.:** OC/266/2022
REFERENCIA:	"SUMINISTRO DE GESTOR UNIFICADO DE AMENAZAS, CON LICENCIAMIENTO DE UN AÑO DE FIREWALL, PARA EL MINISTERIO DE CULTURA".	
RAZÓN SOCIAL DEL SUMINISTRANTE		**NIT**
JARET NAUN MORAN SORTO		[redacted]

No.	CÓDIGO ONU	CÓDIGO PRESUPUESTARIO	CANTIDAD	UNIDAD DE MEDIDA	DESCRIPCIÓN TÉCNICA	PRECIO UNITARIO (CON IVA)	VALOR TOTAL (CON IVA)
1	43210000	61104	1	Unidad	**"SUMINISTRO DE GESTOR UNIFICADO DE AMENAZAS, CON LICENCIAMIENTO DE UN AÑO DE FIREWALL, PARA EL MINISTERIO DE CULTURA".** (Según especificaciones técnicas requeridas en el numeral 2.2.1 de los Términos de referencia y Anexo a la Orden de Compra.)	$ 35,000.00	$ 35,000.00
					MONTO TOTAL (CON IVA)		$ 35,000.00

MONTO TOTAL EN LETRAS: TREINTA Y CINCO MIL 00/100 DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA.

JUSTIFICACIÓN: Debido a la necesidad para mantener en línea los servicios informáticos que se ofrecen tanto a personal interno como externo del Ministerio de Cultura, protección de Correo Electrónico, protección de red interna (LAN edificio central y sus dependencias), se requiere adquirir una herramienta especializada que tenga a cargo proveer la seguridad y filtrado web, que se adapte a la infraestructura tecnológica que posee la institución. Esto con el propósito de garantizar un servicio adecuado y administrado de forma centralizada que proporcione componentes de seguridad ante ataques de virus, SPAM, Phishing, ataques DOS, malware, ramsomware, etc.

FINANCIAMIENTO: FONDOS GOES

GARANTÍA: Según anexo a la orden de compra.	**TIEMPO DE ENTREGA:** Según anexo a la orden de compra.	**FORMA DE PAGO**: Se realizará un solo pago. **Crédito a 60 días calendario**, posteriores a la emisión del quedan.

LUGAR DE ENTREGA: El suministro será entregado en las instalaciones de la **Unidad de Informática y Sistemas,** ubicado en Alameda Juan Pablo II y Calle Guadalupe, Centro de Gobierno, Plan Maestro, Edificio A-5, 3ra. Planta, San Salvador.

DOCUMENTOS DE COBRO: El Suministrante para la emision del Quedan, deberá presentar en los 5 días hábiles siguientes a la recepción del suministro, los documentos que se detallan a continuación: **Factura de Consumidor Final** (duplicado-cliente), a nombre del MINISTERIO DE CULTURA, NIT 0614-170118-113-6, **fotocopia de Nota de Garantía de Buen Servicio, Funcionamiento o Calidad de Bienes y Acta de Recibido de conformidad.**

ADMINISTRADOR DE ORDEN DE COMPRA: Con base a las facultades que otorga el Acuerdo N° 020/2022 de fecha 16 de mayo de 2022, en el cual se ratifica el Acuerdo N° 037/2019 de fecha 21 de junio de 2019, se nombra como Administrador de esta Orden de Compra al [redacted]

DOCUMENTOS. Forman parte de esta orden: a)Solicitud de bien, obra y servicio, b)solicitud de disponibilidad, c)Términos de referencia, d)Ofertas de las empresas, e)cuadro comparativo (si aplica), f)Opinión Técnica de la unidad solicitante (si aplica), g)Resolución de Adjudicación , Resolución Razonada (si aplica), Anexos (si aplica).

MODIFICACIÓN UNILATERAL. Queda convenido por ambas partes que cuando el interés público lo hiciera necesario, sea por necesidades nuevas, causas imprevistas u otras circunstancias, El Ministerio de Cultura podrá modificar de forma unilateral la presente orden, emitiendo al efecto la Resolución correspondiente, la cual formará parte integral de esta orden.

TOMAR EN CUENTA LAS SIGUIENTES INDICACIONES

1º Antes de realizar la entrega, el Suministrante deberá comunicarse con la persona designada como Administrador de esta Orden, al **Tel. 2501-4413** con el objeto de coordinar la entrega del suministro referido.

2º - El Ministerio de Cultura no se hace responsable por documentos que no se presenten a cobro transcurridos dos semanas después de haberse recibido el suministro de conformidad.

3º - Si el suministrante incumpliere en cualquiera de las condiciones de esta Orden, se aplicará el artículo 85 de la LACAP.

[redacted]

DESIGNADO

[redacted]

Vo. Bo. JEFA UACI

[redacted]

SUMINISTRANTE

ELABORADO POR: [redacted]

FORMULARIO AUTORIZADO PARA LA LIBRE GESTIÓN UAC

[redacted]

10:08 Am

15/11/2022

[redacted]

[redacted]

[redacted]

ANEXO A LA ORDEN No. OC/266/2022

1° OBJETO

El Suministrante **JARET NAUN MORAN SORTO,** se compromete a entregar el **"SUMINISTRO DE GESTOR UNIFICADO DE AMENAZAS, CON LICENCIAMIENTO DE UN AÑO DE FIREWALL, PARA EL MINISTERIO DE CULTURA",** de acuerdo a las Especificaciones Técnicas requeridas en el numeral 2.2.1 de los Términos de Referencia, a su Oferta Técnica – Económica presentada al Ministerio de Cultura y según el siguiente detalle:

2° DESCRIPCIÓN DE ESPECIFICACIONES TÉCNICAS.

A. Características Técnicas del hardware:

Firewall Througput	**40 Gbps**
NGFW Througput	**12 Gbps**
Threat Protection Throughput	**6 Gbps**
Máximo Sesiones Concurrentes	**8 Millones**
Sesiones Nuevas	**310,000**
IPS Througput	**20 Gbps**
AV througput	**9.4 Gbps**
IPSec througput	**12 Gbps**
SSL Proxy Throughput	**2 Gbps**
SSL VPN usuarios	**8000**
IPSec tuneles	**20,000**
Puertos	**14 ethernet**
Almacenamiento Local	**8 Gb**
Fuente de Poder Redundante	

B. Otras características

- ✓ Módulo de Detección de comportamiento anormal y detección avanzada de malware.
- ✓ Detección de programas maliciosos conocidos y desconocidos, incluyendo virus, desbordamiento, gusanos, troyanos, etc.
- ✓ Detección y prevención de malware desconocido.
- ✓ Detección y prevención de intrusiones en la red.
- ✓ Detección y prevención de virus y malware conocidos.
- ✓ Clasificación y prevención del spam en tiempo real.
- ✓ Descubrir botnets en intranet y conexiones maliciosas tipo C&C.
- ✓ Identifique y filtre el tráfico de las IP de riesgo.
- ✓ Categorías de URL y filtrado por flujo de amenazas web maliciosas.
- ✓ Reportería Granular.
- ✓ Zero Trust Network Address.

C. Servicios de Red

- ✓ Enrutamiento dinámico, estático
- ✓ Rutas controladas por la aplicación
- ✓ DHCP, NTP, Servidor DNS y proxy DNS incorporados
- ✓ Modo Tap - se conecta al puerto SPAN
- ✓ Modos de interface: sniffer, puerto agregado,
- ✓ loopback, VLAN (802.1Q y Trunking)
- ✓ Conmutación y enrutamiento de L2/L3

D. **Firewall**
- ✓ Modos operativos: NAT/ruta, (puente) transparente, y modo mixto
- ✓ Objetos de política: predefinidos, personalizados y por agrupación de objetos
- ✓ Política de seguridad basada en la aplicación, geolocalización.
- ✓ Soporte y Configuración de NAT, SNAT, DNAT
- ✓ Soporte de los siguientes protocolos HTTP/HTTPS, POP3, IMAP, SMTP y FTP
- ✓ Soporte de los siguientes protocolos PE, ZIP, RAR, Office, PDF, APK, JAR y SWF
- ✓ Soporte de Transferencia de Archivos y Control de tamaño de Archivos
- ✓ Proporciona un informe completo sobre el análisis del comportamiento de los archivos maliciosos
- ✓ Prevención de Intrusiones
- ✓ Detección de anomalías de protocolo, detección basada en tasas, firmas personalizadas, actualización manual o automática de firmas.
- ✓ Listado de amenazas integrada
- ✓ Acciones IPS: por defecto, monitoreo, bloqueado,
- ✓ Reinicio (IP de los atacantes o de la víctima, interfaz de entrada) con tiempo de caducidad
- ✓ Opción de registro de paquetes
- ✓ Selección basada en filtros: gravedad, destino, sistema operativo, aplicación o protocolo
- ✓ Modo rastreo IDS
- ✓ Protección DoS basada en tasas IPv4 e IPv6 con configuración de umbral contra inundaciones de TCP Syn, escaneo de puertos TCP/UDP/SCTP, Barrido de ICMP, inundación de sesiones TCP/UDP/SCIP/ICMP (origen/destino)
- ✓ Bypass activo con interfaces de bypass
- ✓ Configuraciones de prevención predefinidas

E. **Anti-Virus**
- ✓ Manual, actualización automática de firmas
- ✓ Antivirus basado en flujos: protocolos que incluyen HTTP, SMTP, POP3, IMAP, FTP/SFTP
- ✓ Escaneo de virus en archivos compreso
- ✓ Antispam

F. **Defensa contra Ataques**
- ✓ Defensa contra ataques de protocolo anormal
- ✓ Anti-DoS/DDoS, incluyendo SYN Flood, defensa contra inundación de consultas DNS
- ✓ Defensa contra ataques ARP

G. **Filtrado por URL**
- ✓ Inspección de filtrado web basado en el flujo
- ✓ Filtrado web definido manualmente basado en URL, contenidos web y por cabecera MIME
- ✓ Filtrado web dinámico con base en datos de categorización en tiempo real, basados en la nube
- ✓ Características adicionales del filtrado web: Filtrado de Applets de Java, ActiveX o de cookies Bloqueo a Posteos HTTP
- ✓ Registro de palabras clave de búsqueda
- ✓ Anulación del perfil web de filtrado: permite que el administrador asigne temporalmente diferentes
- ✓ perfiles de usuario/grupo/IP
- ✓ Filtro Web para categorías locales y anulación de categorías calificadas.

H. **Reputación de IP**
- ✓ Bloqueo del IP del servidor Botnet con base de datos IP de reputación global.

I. **Descifrado SSL/TLS**
- ✓ Identificación de la aplicación para el tráfico cifrados ssl
- ✓ Habilitación IPS para el tráfico cifrado SSL
- ✓ Habilitación AV para el tráfico cifrado SSL
- ✓ Filtro URL para tráfico cifrado SSL
- ✓ tráfico cifrado SSL y lista blanca
- ✓ Modo proxy por descarga SSL.

J. **Control de Aplicaciones**
- ✓ Filtrado de aplicaciones por nombre, categoría, subcategoría, tecnología y por riesgo
- ✓ Cada aplicación contiene una descripción, sus factores de riesgo, dependencias, puertos típicos
- ✓ utilizados, y las URL de referencia adicionales
- ✓ Acciones: bloqueo, reinicio de la sesión, monitoreo, modulación del tráfico
- ✓ Identifica y controla aplicaciones en la nube

- ✓ Proporciona monitoreo multidimensional y estadísticas para las aplicaciones en la nube, incluyendo la categoría de los riesgos y sus características.

K. Calidad de Servicio (QoS)

- ✓ Número máximo de túneles/ancho de banda garantizados o por IP/usuario
- ✓ Asignación de túnel basada en dominio de seguridad, interfaz, dirección, usuario/grupo, servidor/grupo de servidores, app/grupo de apps.
- ✓ Ancho de banda asignado por hora, prioridad, o reparto equitativo del ancho de banda
- ✓ Asignación de prioridades de ancho de banda restante
- ✓ Número máximo de conexiones simultáneas por ip

L. Balanceo de Carga en Enlaces

- ✓ Equilibrio de carga del enlace bidireccional
- ✓ Inspección del enlace con ARP, PING, y DNS

M. VPN

- ✓ VPN IPSec
- ✓ Soporte IKEv1 e IKEv2 (RFC 4306)
- ✓ Método de autenticación: certificado y una clave pre-compartida
- ✓ Configuración a modo de IKE (como servidor o cliente) DHCP por IPSec
- ✓ Caducidad de clave cifrada IKE configurable, NAT transversal para mantener viva la frecuencia
- ✓ Cifrado propuesto para Fase 1/Fase 2: DES, 3DES, AES128, AES192, AES256
- ✓ Autenticación propuesta para Fase 1/Fase 2: MD5, SHA1, SHA256, SHA384, SHA512
- ✓ Soporte Diffie-Hellman para Fase 1/Fase 2: 1,2,5
- ✓ Política de seguridad para inspección de redundancias
- ✓ Debe proveer vpn gratuito para al menos 500 usuarios.

N. IPv6

- ✓ Gestión sobre IPv6, logueo IPv6 y HA
- ✓ Túneles IPv6, DNS64/NAT64 etc.
- ✓ Protocolos de enrutamiento IPv6, enrutamiento estático, enrutamiento por política, ISIS, RIPng, OSPFv3 y BGP4
- ✓ IPS, identificación de aplicaciones, control de acceso, defensa contra ataques ND.
- ✓ Soporte Modo Alta Disponibilidad Activo/Activo y Activo/Pasivo
- ✓ Notificación de fallas
- ✓ Base de datos de usuario local
- ✓ Autenticación de usuario remoto: TACACS +, LDAP, Radius, Active
- ✓ Single-Sign-on: Windows AD
- ✓ Autenticación de 2 factores: Apoyo a terceros, servidor de contador integrado con token físico y SMS
- ✓ Políticas de usuario y por dispositivo
- ✓ Sincronización de grupos de usuarios basada en AD y LDAP.

3º <u>OTRAS CONDICIONES:</u>

El suministrante deberá cumplir cada una de las siguientes condiciones:

a) **Brindar Garantía, plazo del soporte y asistencia técnica mínimo de 1 año.**
b) Entregar documentación que respalde el período de contratación del licenciamiento del gestor unificado de amenazas.
c) Proveer soporte local y de forma directa con el fabricante del producto.
d) Brindar soporte en la modalidad 24 x 7 y un plazo de atención en sitio no mayor a 5 horas, después de solicitada la asistencia correspondiente.
e) Proveer acceso ilimitado vía Web hacia alguna base de datos generalizada sobre problemas conocidos, incidentes, manuales, White Paper, configuraciones acerca de modos de operación y tecnologías implantadas en ellos.
f) Proporcionar asistencia de soporte personalizada en caso de cambios de configuración, actualización de versiones de software o depuración de fallos, pudiéndose llevar a cabo en horarios que no afecten las labores de la institución y sin costo adicional al contratado.
g) Generar reportes granulares de consumo por segmento de red, dirección IP, aplicaciones, amenazas, sin discriminación de horario o fecha, si la licencia ofertada no los provee, entregar software adicional de reportes que si lo genere con **vigencia para un año (la vigencia de las licencias deberá ser para un año).**
h) **Asignar 2 (dos) Técnicos Certificados en la herramienta o solución suministrada.**

i) Auxiliar al contratante, en caso de que sea solicitado por este último, encaminadas a la gestión de incidentes de seguridad de la información, asociadas con los servicios contratados y derivados de actividades de hackers.
j) Crear todas las configuraciones necesarias para el correcto funcionamiento de los equipos ofertados, sin ningún cargo extra para la institución.
k) Jornadas de capacitación de las herramientas de seguridad para al menos 3 usuarios y 12 horas como mínimo.
l) En caso de daño de hardware, sustituir el equipo con uno de igual o superiores características técnicas.

4° TIEMPO Y FORMA DE ENTREGA:

A. **TIEMPO DE ENTREGA: 5 días Calendarios**, los cuales iniciarán el día hábil posterior a la fecha que el Suministrante reciba copia de la Orden de Compra autorizada.

B. **FORMA DE ENTREGA**: El suministrante deberá realizar **una sola entrega** de la herramienta informática, además se coordinarán con el Administrador de la Orden de Compra, al menos **3 jornadas de capacitación en el uso de la misma**.

5° NOTA DE GARANTÍA DE BUEN SERVICIO, FUNCIONAMIENTO O CALIDAD DE BIENES

El suministrante se compromete a presentar una **Nota de Garantía de Buen Servicio, Funcionamiento o Calidad de Bienes** a favor del MINISTERIO DE CULTURA, con una vigencia mínima de **UN AÑO**, la cual deberá estar firmada por el Representante Legal, Gerente o persona autorizada para emitirla, y la empresa se debe comprometer a responder por cualquier desperfecto de fábrica y mal funcionamiento, en caso de daño de hardware, sustituir el equipo con uno de igual o superiores características técnicas, así como también deberá garantizar el plazo del soporte y asistencia técnica durante una vigencia mínimo de un año. **Este documento deberá de entregarse en la UACI en un tiempo máximo de un día después de firmar el Acta de recepción.**

CONFORME.

[redacted]
DIRECTOR GENERAL DE ADMINISTRACIÓN
MINISTERIO DE CULTURA

[redacted]
SUMINISTRANTE

[redacted]