FICHA DE ESPECIFICACIONES TÉCNICAS PARA ADQUISICIONES POR ÍNFIMA CUANTÍA

CUADRO RESUMEN

Objeto de la contratación:	Adquisición de Equipo de Seguridad Perimetral para la Empresa Pública Metropolitana Mercado Mayorista de Quito.
Funcionario del Área Requirente Responsable De La Contratación:	Ing. Andrés Alejandro Bravo Sandoval
Teléfono de Contacto:	0982375980
Correo Electrónico:	a.bravo@mmqep.gob.ec
Fecha Límite para la entrega de Proformas:	3 días contado a partir del primer día hábil de la publicación de la invitación en el SOCE.

1. INFORMACIÓN ADICIONAL PARA PROFORMAS.

De acuerdo a la Circular Nro. SERCOP-SERCOP-2021-0013-C de fecha 23 de mayo de 2021 suscrita por la Econ. Laura Silvana Vallejo Páez Directora General Del Servicio Nacional De Contratación Pública "Herramientas informáticas para publicación de Necesidades de Ínfimas Cuantías y Convenios de pago y cualquier instrumento jurídico que genere afectación presupuestaria, provenientes de la aplicación del numeral 2 del artículo 117 del Código Orgánico de Planificación y Finanzas Públicas".
Para lo cual se solicita lo siguiente:

Adicionalmente se solicita que las proformas deben contener la siguiente información:

- ✓ Nombre, Razón Social y Ruc
- ✓ Vigencia de la Oferta
- ✓ Tiempo de Entrega
- ✓ Forma de pago
- ✓ Detallar si los productos ofertados llevan o no llevan IVA (subtotal 0% / subtotal 12% / IVA12% y total)
- ✓ Dirección y teléfono de proveedor
- ✓ Correo Electrónico

2. OBJETIVO DE LA COMPRA

Realizar la adquisición de equipo de seguridad perimetral para la Empresa Pública Metropolitana Mercado Mayorista de Quito con el fin de asegurar la red, asegurar la navegación y garantizar niveles de seguridad, disponibilidad y confiabilidad

3. ESPECIFICACIONES TÉCNICAS

MARCA:	ESPECIFICAR
MODELO:	ESPECIFICAR
CANTIDAD:	1

Equipo nuevo de fábrica no re manufacturado	Si, Obligatorio
Características generales del Dispositivo	El fabricante del Gateway de seguridad, debe ser Líder del cuadrante mágico de Gartner para Firewalls Empresariales de Red de al menos los cuatro últimos años
	El dispositivo debe ser un equipo de propósito específico, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux
	El fabricante de hardware y del software de seguridad, debe ser el mismo
	El Gateway y su administración, deben permitir adicionar nuevas funcionalidades a través de plugins o blades, sin necesidad de realizar un upgrade completo de software o hardware
	El appliance debe poder incluir Firewall, VPN, IPS, Control de aplicaciones e identificación de usuarios a través de directorio activo, todas en un solo hardware con la posibilidad de ejecutar todas las funcionalidades al mismo tiempo
	El sistema operativo debe estar totalmente integrado con IPv4.
	El equipo debe ser accesible a través de SSH y de interfaz Web usando SSL
	Soportar al menos 200 VLANs
Caracteristicas minimas de hadware del dispositivo	El throughput debe ser al menos 7000 Mbps para firewall texto claro y 4000 Mbps para VPNs, según conste en el Datasheet público del fabricante.
	El throughput del IPS activo, dentro de la misma plataforma con tráfico mixto debe ser de al menos 5000 Mbps con un perfil recomendado de seguridad, según conste en el Datasheet público del fabricante.
	El throughput de Threat Prevention, dentro de la misma plataforma con tráfico mixto debe ser de al menos 1900 Mbps con un perfil recomendado de seguridad, según conste en el Datasheet público del fabricante.
	Debe ser capaz de manejar al menos 2,000,000 sesiones concurrentes y 64,000 conexiones por segundo
	Debe tener al menos 16 interfaces 10/100/1000Mbps RJ-45 LAN interfaces
	Debe tener al menos 2 interfaces 2.5 GB RJ-45
	Debe tener al menos 1 interfaces 10/100/1000Mbps RJ-45 WAN interface
	Debe tener al menos 1 interface 10 GB base RJ-45/ 10 GB SFP DMZ interface. No se requiere incluir el transceiver.
	Debe tener un puerto para la consola por USB/RJ-45
	El equipo debe incluir dos (2) fuentes de poder redundantes de 110 a 240 VAC

	La capacidad del disco duro deberá ser de al menos 240 GB SSD
	Capacidad Emmc 32 GB
Firewall	El gateway debe estar basado en la tecnología conocida como “Stateful Inspection”, el cual realiza un análisis granular de los estados de las comunicaciones y aplicaciones, para controlar el flujo del tráfico pasando a través del gateway, y de esta manera abrir dinámicamente y de una forma segura, puertos y un gran rango de protocolos.
	Debe proveer seguridad a implementaciones de VoIP, soportando al menos el protocolo SIP
	Debe incluir la posibilidad de crear NATs dinámicos (N-1 o Hide) y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete y en una sola regla
	Debe permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo
	Debe soportar DHCP en modos server
	El Gateway debe soportar redundancia a enlaces, sin la necesidad de una licencia adicional o software / Hardware de terceros
	La política puede ser ejecutado en un rango de tiempo configurado
	Soporte para limitar el tráfico de subida y bajada basado en una política
IPsec VPN	Deben ser soportados 3DES y AES-256 para las fases I y II de IKE
	Debe soportar al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit).
	Debe soportar integridad de datos con md5 y sha1
	Debe incluir soporte a las topologías VPNs site-to-site: Full Meshed (todos a todos), Star (Oficinas Remotas a Sitio Central) y Hub and Spoke (Sitio remoto a través del sitio central hacia otro sitio remoto)
	Soporte a VPNs client-to-site basadas en IPSEC
	Debe tener la posibilidad de realizar VPNs SSL sin cliente para acceso remoto para 500 usuarios, sin necesidad de instalar un cliente.
	Debe incluir un método simple y central, de crear túneles permanentes entre gateways del mismo fabricante
	Debe poder establecer VPNs con gateways con direcciones IP dinámicas pública
IPS	El IPS integrado, debe incluir al menos los siguientes mecanismos de defensa. Engine settings: Protecciones que contienen ajustes que alteran el comportamiento de otras protecciones. Anomalías de Protocolo: grupo de protecciones que identifican cuando el tráfico no cumple con los estándares del protocolo. Firmas: grupo de protecciones que identifica el tráfico que intenta explotar una vulnerabilidad específica
	El administrador debe poder configurar la inspección, solo para el tráfico interno.

	Para cada protección se debe incluir la siguiente información: Tipo de protección (cliente o server), severidad de la amenaza, Impacto en el desempeño, y nivel de confidencia.
	Debe detectar y bloquear ataques de red y de aplicación, protegiendo al menos los siguientes servicios: Email, DNS, FTP, servicios de Windows (Microsoft Networking) y SNMP.
	Debe incluir protecciones para los protocolos POP3 e IMAP.
Filtrado URL y Control de Aplicaciones	La solución debe integrar reglas de filtrado de URL y control aplicaciones en la misma licencia y contar al menos con 4500 aplicaciones y 96 millones de sitios web agrupados en categorías
	La administración debe centralizar las políticas de seguridad del control de aplicaciones y filtrado URL en la misma consola.
	Debe contar con un repositorio en línea para identificar URLs y aplicaciones no clasificadas
	Debe tener un servicio de clasificación basando en la nube que permita categorizar dinámicamente el tráfico Web.
	Debe ser posible definir nuevas aplicaciones y sitios web, así como categorías y grupos que no estén definidos dentro de la base de datos.
	Debe ser posible integrar la solución con Directorio Activo u Open LDAP para crear reglas de control de aplicaciones y filtrado URL basadas en: usuarios, grupos de Usuarios, maquinas, dirección IP, redes y todas las opciones combinadas
Antivirus & Anti-Malware	El Gateway antivirus debe realizar scan de virus y bloquearlos en al menos los siguientes protocolos: SMTP y HTTP.
	Se pueden generar excepciones basadas en IP, URLS o tipos de archivo
	El módulo de Antivirus & antimalware debe hacer escaneo en tiempo real tanto de antivirus como de antimalware.
	Debe incluir la posibilidad de bloquear a través de IP reputación, y evitar de esa forma los falsos positivos.
	La solución debe incluir capacidades de emulación en la nube del fabricante de archivos desconocidos para prevenir ataques de día cero.
	Debe permitir la creación de listas blancas y negras que pueden ser encontradas también como block list y allow list.
AntiBot	La solución debe proveer una herramienta que haga descubrimiento de bots dentro de la red institucional. Dicha herramienta debe bloquear la comunicación que intenten establecer los bots con los atacantes.
	La solución debe poder detectar host infectados con bots, analizando el tráfico de la red utilizando una tecnología multicapa.
	La herramienta antibot debe analizar al menos 250 millones de direcciones para descubrimiento de bots, que incluyan al menos, direcciones de: IP de Command and Control, URL y DNS.
	Debe incluir al menos 2000 patrones de comunicación de botnets.
	La solución debe utilizar tecnología de inspección multicapas.

	La herramienta debe contar con una base de datos en la nube para para la actualización de las firmas.
Funciones Avanzadas de Red y Clustering	Debe poderse definir limites en el ancho de banda, para restringir aplicaciones no criticas de red.
	Debe soportar Alta Disponibilidad y Balanceo de Carga de links de al menos 2 ISP, sin depender del uso de enrutamientos dinámicos o equipos externos dedicados.
Identificación de usuarios	La solución debe proveer tres métodos para obtener las identidades de los usuarios: Sin agente haciendo búsquedas al directorio activo o portal cautivo.
	Cuando se detecte que los usuarios no se han autenticado, la solución tiene que re direccionarlos a un portal cautivo, a través del protocolo http
	La solución debe poder integrarse con el directorio activo sin la necesidad de instalar un agente en el servidor de dominio o en los equipos de los usuarios finales.
	Con la finalidad de crear reglas de acceso por usuario, debe poder integrase con otras soluciones como: control de aplicaciones y filtrado de URL
Logging & Status	Debe incluir un log interno y la posibilidad de enviar los logs a un servidor central utilizando syslog
	Debe proveer diferentes logs para los eventos regulares y los de seguridad
	Debe contar con reportes estándares en la misma plataforma
Monitoreo	Debe incluir una interface gráfica de monitoreo que provea acceso fácil a monitorear el estado del Gateway
	Debe proveer la siguiente información del sistema: estado de las Interfaces, uso de CPU y uso de memoria
	Debe indicar el estado de cada uno de los componentes del gateway como firewall, vpn, antivirus, etc
	Debe indicar la cantidad de conexiones y túneles VPN activos
	Monitoreo del tráfico de las conexiones activas.

SERVICIOS
INSTALACIÓN DE SOLUCIÓN DE SEGURIDAD PERIMETRAL
DESCRIPCIONES GENERALES
Instalación y configuración de la solución de seguridad perimetral
Configuración de Logs y Reportería
Configuración Básica
Configuración de Interfaces y Zonas
Configuración de acceso de administración
Configuración de control de aplicaciones y filtrado URL

Configuración de Antibot y Antivirus
Configuración de IPS
Configuración de FW

SOPORTE TECNICO	
CARACTERÍSTICAS DEL SOPORTE	
DESCRIPCIONES GENERALES	
CARACTERÍSTICA	DETALLE
HORAS DE SOPORTE	El oferente deberá incluir en su oferta un paquete mínimo de 10 horas de soporte de la solución instalada durante todo el período garantía técnica (1 año)
Número de Incidente	El oferente deberá poseer una mesa de ayuda designada para este proyecto la cual proporcionará un número de incidente (ticket), y solución ofertada
	El oferente deberá proporcionar los contactos para la comunicación a la mesa de ayuda vía telefónica, vía mail o vía web y los niveles de escalamiento, para los incidentes de hardware y software
	Para la apertura de casos, el oferente deberá poner a disposición de la Empresa un número telefónico
	Adicionalmente el oferente contar con soporte directo con el fabricante, para el tema de incidentes en el hardware y software
Horario de Atención	El horario de atención por parte del fabricante será en esquema 7x24
Oficina Local	El oferente deberá entregar adjunto a la proforma una copia de un certificado de que acredite mantener por lo menos una oficina en la ciudad de quito, para brindar soporte técnico local.
Garantías y Suscripciones	
Descripciones Generales	
Característica	Detalle
Descripciones Generales	Reposición de partes y piezas ante defectos de Fabricación y/o Mantenimientos. El hardware ofertado tendrá soporte brindado directamente por el fabricante del equipo durante el período de vigencia de las suscripciones que es de un (1) año, y cada año que se renueve las suscripciones deberán proporcionar la garantía sobre el hardware, hasta que finalice el soporte por el fabricante, el mismo que deberá cubrir el reemplazo de partes y piezas originales sin ningún costo adicional para la INSTITUCIÓN
Cobertura, reemplazo y provisión de los repuestos.	El reemplazo de partes y/o piezas por daño será realizado por el oferente y/o canal de servicios autorizado por el fabricante para el Ecuador si costo adicional.

Período de la Suscripción de los módulos o blades, solicitados en las especificaciones técnicas	Los equipos deberán poseer suscripción de un (1) año, durante este tiempo la Empresa podrá acceder a todas las actualizaciones de versiones, parches de software que el fabricante libere y soporte directo del fabricante, para el software y hardware provisto en este proceso, sin ningún costo adicional
Garantía de los equipos	Los equipos y el software ofertados deberán tener garantía y soporte de fábrica por todo el periodo de la suscripción contratada en este caso de (1 año) partir de la entrega de los equipos en las oficinas de la institución

Para el presente proyecto y la correcta ejecución del mismos es necesario contar con personal calificado en la solución propuesta, es por ello que se requiere contar con los siguientes perfiles.

PERSONAL TÉCNICO MÍNIMO

Cantidad	Función	Nivel de Estudio	Titulación Académica
2	Soporte técnico	Tercer nivel con título	Ingeniería en Sistemas o Telecomunicaciones o Electrónica, o carreras afines, que cuenten con certificaciones a nivel experto y master vigentes (Adjuntar hoja de vida, registro Senescyt)

EXPERIENCIA MÍNIMA DEL PERSONAL TÉCNICO

PERSONA / FUNCIÓN	DESCRIPCIÓN	TIEMPO DE PARTICIPACIÓN EN EL PROYECTO	NÚMERO DE PROYECTOS	MEDIOS DE COMPROBACIÓN
SOPORTE TÉCNICO	Implementación y soporte técnico en productos de la marca ofertada	5 días	2 proyectos	• Certificado del oferente o certificado del cliente del oferente en el cual se indique la participación que tuvo el personal técnico en el proyecto de soporte técnico en la plataforma ofertada. • En el caso que se incluya **Certificados** deberá especificarse claramente; el nombre de la contratante, con sus respectivos teléfonos de contacto, el periodo de

				contratación, detalle del servicio prestado y, firma y cargo del empleado de la empresa privada o pública que emitió el documento

EXPERIENCIA ESPECÍFICA MÍNIMA DEL OFERENTE

TIPO	DESCRIPCIÓN	TEMPORALIDAD AÑOS	NUMERO DE PROYECTOS SIMILARES	VALOR DEL MONTO MÍNIMO (SUMATORIA DE CONTRATOS)	MEDIOS DE COMPROBACIÓN
Experiencia Específica	Adquisición, renovación o Soporte técnico objeto de la plataforma ofertada	Durante los últimos 5 años previos a la publicación del procedimiento	1	$ 150,00	• Copias de actas de entrega/recepción definitiva, contratos o certificados emitidos por los clientes del oferente. • En el caso que presente Certificados deberá especificarse claramente; el nombre de la contratante, con sus respectivos teléfonos de contacto, el periodo de contratación, detalle del servicio prestado y su monto de contratación, firma y cargo del empleado de la empresa privada o pública que emitió el documento

OTROS PARÁMETROS

- Certificado de ser canal autorizado de la marca ofertada, con un nivel de socio de negocios por lo menos 3 estrellas y sea partner autorizado para comercializar los productos en el territorio ecuatoriano.
- Que cuente con certificación (CCSP) que lo autoriza a brindar soporte de primera línea, mantenimiento preventivo y correctivo de la marca.

4. PLAZO DE EJECUCIÓN: Parciales y/o total

El plazo de entrega es de 60 días calendarios una vez notificada o entregada la Orden de Compra, por la totalidad de las partes y piezas, y para los casos de entregas parciales, donde se detalla el cronograma establecido.

5. FORMA Y CONDICIONES DE PAGO

El pago se realizará 100% Contra Entrega

6. LUGAR Y FORMA DE ENTREGA

El lugar de entrega del bien o servicio será en la Empresa Pública Metropolitana Mercado Mayorista de Quito – MMQ-EP, ubicado en Ayapamba s/n y Teniente Hugo Ortiz.

7. GARANTÍAS

De acuerdo a lo establecido en los ART .74, 75, 76 LOSNCP. *Garantía Técnica, en los casos que aplique.*

8. MULTAS

Por cada día de retardo en la ejecución de las obligaciones contractuales por parte del contratista, se aplicará la multa de 1 por 1.000 del total de la orden de compra.
En caso de que el valor total de las multas supere el 5% del valor total del contrato, se podrá dar por terminado anticipadamente y unilateral el contrato. (El porcentaje para el cálculo de las multas lo determinará la entidad en función del incumplimiento y de la contratación). Ref. Art. 71 de la Ley Orgánica del Sistema Nacional de Contratación Pública.

9. VIGENCIA DE LA OFERTA.

Vigencia de la oferta será de 90 días.

10. FIRMAS DE RESPONSABILIDAD

Quito, 6 de agosto de 2021

Acción	Funcionario	Puesto	Firma
Elaborado por:	Ing. Andrés Alejandro Bravo Sandoval	**JEFE DE DESARROLLO TECNOLÓGICO**	Firmado electrónicamente por: ANDRES ALEJANDRO BRAVO SANDOVAL