



EMPRESA PÚBLICA MUNICIPAL DE TRÁNSITO DE EL GUABO

Creada mediante Ordenanza Municipal, sancionada el 15 de Diciembre del 2023



UNIDAD DE SISTEMAS

Oficio No 002-EPMT-G-US-2025-OF

El Guabo, 08 de enero del 2025

ASUNTO: ADQUISICIÓN, CAPACITACIÓN, CONFIGURACIÓN Y PUESTA EN MARCHA DE UN DISPOSITIVO DE SEGURIDAD PERIMETRAL PARA LA EMPRESA PÚBLICA MUNICIPAL DE TRÁNSITO DE EL GUABO.

Ab. José William Valle Chávez

GERENTE GENERAL

EMPRESA PUBLICA MUNICIPAL DE TRANSITO DE EL GUABO EPMT-G

Presente. -

De mi consideración:

Por medio de la presente, me permito dirigirme a usted en mi calidad de Jefe de la Unidad de Sistemas de la Empresa Pública Municipal de Tránsito de El Guabo, con el fin de solicitar formalmente la adquisición, capacitación, configuración y puesta en marcha de un dispositivo de seguridad perimetral que permita garantizar la protección de nuestra infraestructura tecnológica y la información institucional.

La implementación de este dispositivo es de suma importancia para mitigar los riesgos asociados a posibles ataques cibernéticos, accesos no autorizados o cualquier otra amenaza que pueda comprometer la confidencialidad, integridad y disponibilidad de nuestros datos y sistemas. Además, considerando el avance continuo de las tecnologías y las exigencias actuales en materia de seguridad informática, este equipo nos permitirá modernizar nuestras capacidades de defensa y cumplimiento de normativas relacionadas con la protección de datos. Dentro del proceso, se considera necesario incluir los siguientes aspectos:

- Adquisición del dispositivo de seguridad perimetral: Selección de un equipo que cumpla con los requerimientos técnicos necesarios para nuestra institución.
- Capacitación del personal: Entrenamiento especializado para el personal encargado de su administración y mantenimiento.
- Configuración inicial: Instalación y parametrización según las necesidades y políticas de seguridad de la institución.

KIKE ÁLVAREZ
• A L C A L D E •



EMPRESA PÚBLICA MUNICIPAL DE TRÁNSITO DE EL GUABO

Creada mediante Ordenanza Municipal, sancionada el 15 de Diciembre del 2023



UNIDAD DE SISTEMAS

- Puesta en marcha: Validación de su operatividad y funcionamiento.

Es importante resaltar que esta inversión contribuirá a fortalecer nuestra infraestructura tecnológica y garantizará la continuidad de nuestras operaciones de manera segura y eficiente.

Con lo expuesto, solicito a usted considere autorizar la "ADQUISICIÓN, CAPACITACIÓN, CONFIGURACIÓN Y PUESTA EN MARCHA DE UN DISPOSITIVO DE SEGURIDAD PERIMETRAL PARA LA EMPRESA PÚBLICA MUNICIPAL DE TRÁNSITO DE EL GUABO", para lo cual adjunto al presente:

1. El Informe de Necesidad, y los
2. Términos de referencia del producto a Adquirir.

Particular que solicito para los fines consiguientes.

Atentamente:


Ing. Johnny Urdin González, Mgs
JEFE LA UNIDAD DE SISTEMAS
EMPRESA PUBLICA MUNICIPAL DE TRANSITO DE EL GUABO



KIKE ALVAREZ
• A L C A L D E •



EMPRESA PÚBLICA MUNICIPAL DE TRÁNSITO DE EL GUABO

Creada mediante Ordenanza Municipal, sancionada el 15 de Diciembre del 2023



ESPECIFICACIONES TÉCNICAS EN HARDWARE PARA LA “ADQUISICIÓN, CAPACITACIÓN, CONFIGURACIÓN Y PUESTA EN MARCHA DE UN DISPOSITIVO DE SEGURIDAD PERIMETRAL PARA LA EMPRESA PÚBLICA MUNICIPAL DE TRÁNSITO DE EL GUABO”

UNIDAD REQUIRIENTE: SISTEMAS

RESPONSABLE DE LA ADQUISICIÓN: ING. JOHNNY URGIN GONZALEZ

CARGO: JEFE DE LA UNIDAD DE SISTEMAS

NOMBRE DEL PROYECTO:

ADQUISICIÓN, CAPACITACIÓN, CONFIGURACIÓN Y PUESTA EN MARCHA DE UN
DISPOSITIVO DE SEGURIDAD PERIMETRAL PARA LA EMPRESA PÚBLICA MUNICIPAL DE
TRÁNSITO DE EL GUABO

1. ANTECEDENTES:

En el sector público ecuatoriano, la implementación de dispositivos de seguridad informática enfrenta desafíos significativos, relacionados tanto con el cumplimiento normativo como con las limitaciones estructurales y operativas. Aunque la normativa vigente establece la obligatoriedad de implementar medidas de ciberseguridad, existen barreras que dificultan su correcta adopción, como la falta de presupuesto, personal capacitado, y la resistencia al cambio por parte de las entidades administrativas.

El marco jurídico ecuatoriano relacionado con la seguridad informática incluye varias disposiciones que buscan garantizar la protección de datos e infraestructura crítica en el sector público:

Ley Orgánica de Protección de Datos Personales (LOPD): Art. 15: Obliga a los responsables de tratamiento a implementar medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales, incluyendo el uso de tecnologías apropiadas para prevenir riesgos de accesos no autorizados, pérdidas o alteraciones.

Art. 33: Establece que el sector público debe garantizar la implementación de sistemas seguros de tratamiento de datos, priorizando tecnologías que aseguren la integridad y confidencialidad de la información.

Ley Orgánica de Telecomunicaciones: Art. 66: Refiere la responsabilidad de los prestadores de servicios de telecomunicaciones, incluidos los sistemas de información, de establecer protocolos de seguridad para prevenir vulnerabilidades en los sistemas que utilizan.



EMPRESA PÚBLICA MUNICIPAL DE TRÁNSITO DE EL GUABO

Creada mediante Ordenanza Municipal, sancionada el 15 de Diciembre del 2023



Normativa Técnica de la Secretaría Nacional de Gestión de Riesgos y Ciberseguridad (ACCESS): Dicta lineamientos para el diseño e implementación de políticas de ciberseguridad en las instituciones públicas, incluyendo el uso de firewalls, antivirus, sistemas de detección de intrusos y otras herramientas tecnológicas.

Ley Orgánica del Sistema Nacional de Contratación Pública (LOSNC): Art. 2 y Art. 6: Obligan a las entidades públicas a garantizar que los servicios y equipos contratados incluyan medidas de seguridad informática, promoviendo estándares de calidad adecuados.

2. OBJETIVOS:

Realizar la adquisición de un dispositivo de seguridad perimetral para la empresa pública municipal de tránsito de El Guabo

3. ALCANCE:

En el presente informe se describen las especificaciones técnicas del equipo firewall propuesto para proporcionar la seguridad informática en la Empresa Pública Municipal de Tránsito de El Guabo, a fin de que se logre minimizar los inconvenientes a nivel de amenazas e incidentes de seguridad informática. El firewall es un dispositivo esencial para proteger las redes informáticas contra accesos no autorizados, monitorear y controlar el tráfico de datos entrante y saliente, y mantener la seguridad general del sistema.

4. DISPOSITIVOS CON LOS QUE CUENTA LA ENTIDAD:

Los dispositivos disponibles para la configuración de la red, con Switches, cableado estructurado bajo la normativa para RJ45, cámaras IP con servicio web disponibilidad 24/7 por 30 días, router de control de tráfico de mínimas prestaciones, No existe un dispositivo firewall.

5. METODOLOGIA DE TRABAJO

El proveedor adjudicado entregara el Hardware para seguridad perimetral requerido, según los requerimientos descritos en el presente informe.

6. PRODUCTOS Y SERVICIOS ESPERADOS

El equipo firewall es un dispositivo, con capacidad para proteger redes internas/externas en entornos corporativos, industriales, etc. Este equipo soporta configuraciones avanzadas, incluyendo filtrado de tráfico, detección de intrusos y análisis en tiempo real.





EMPRESA PÚBLICA MUNICIPAL DE TRÁNSITO DE EL GUABO

Creada mediante Ordenanza Municipal, sancionada el 15 de Diciembre del 2023



7. ESPECIFICACIONES TECNICAS:

Adquisición de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la red empresarial.

La solución debe ser de tipo appliance de propósito específico. No se aceptan equipos de propósito genérico (PC o Servidores) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS X o GNU/Linux.

7.1 CAPACIDAD

- Throughput mínimo de Next Generation Firewall de 2500 Mbps
- Throughput mínimo de Firewall 10000 Mbps
- Throughput mínimo de IPS 3000 Mbps
- Throughput mínimo de VPN IPSec 5000 Mbps
- La plataforma debe soportar mínimo 5 millones de conexiones simultáneas.
- La plataforma debe soportar mínimo 65 000 nuevas sesiones por segundo.
- Mínimo 10 interfaces de red 10/100/1000 en cobre, formato RJ45 para tráfico de datos.
- Mínimo 2 interfaces de red 1G PoE.
- Mínimo 1 ranura de expansión para puertos adicionales.
- La solución debe tener una fuente de alimentación 100-240 VCA, 50-60 Hz con 2.^a fuente de alimentación redundante opcional.
- La plataforma de hardware debe tener capacidad mínima de almacenamiento de 64 GB a través de disco sólido o SSD.
- Los requerimientos deberán ser comprobados con documentación pública del fabricante.

7.2 CARACTERÍSTICAS GENERALES

- Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv3).
- Soportar DNS Dinámico en las interfaces de red del equipo de seguridad.
- Soportar túneles GRE como punto inicio o finalización del túnel.
- Soporte de ruteo a base de políticas (policy based routing), es decir ruteo por origen y destino.
- Soporte de modos de alta disponibilidad, tanto Activo/Activo como Activo/Pasivo.





EMPRESA PÚBLICA MUNICIPAL DE TRÁNSITO DE EL GUABO

Creada mediante Ordenanza Municipal, sancionada el 15 de Diciembre del 2023



- Soporte de despliegue en modo transparente y modo Gateway.
- Debe permitir la detección y bloqueo de ataques de Denegación de Servicio (DoS), definiendo un umbral máximo de conexiones por segundo por tipo de paquete (SYN, ICMP, UDP) o configurando políticas de IPS.

7.3 FUNCIONALIDADES DE FIREWALL

- Reglas configurables basadas en red de origen, red de destino, protocolo, país origen, país destino, puerto de comunicación y acción posible.
- Las acciones posibles deberán incluir como mínimo permitir o denegar tráfico.
- Adicionalmente las reglas deberán ser configurables considerando grupos de usuarios pertenecientes a la base de datos local del equipo, externos via LDAP y/o Radius y externos de forma transparente (integrándose transparentemente con el directorio activo).
- Para las reglas con autenticación realizada de forma no transparente deberá proporcionarse un portal de autenticación.
- Las reglas deberán poder ser configuradas según horarios, incluyendo día, mes y año.
- Deberá soportar reglas de firewall en IPv6.

7.4 IDENTIFICACIÓN DE USUARIOS

- Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de autenticación vía LDAP, Active Directory, eDirectory y base de datos local.
- Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente.
- Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Adicionalmente se podrá añadir un segundo factor de autenticación.





EMPRESA PÚBLICA MUNICIPAL DE TRÁNSITO DE EL GUABO

Creada mediante Ordenanza Municipal, sancionada el 15 de Diciembre del 2023



7.5 TRAFFIC SHAPPING Y QOS

- Con la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube o Netflix por ejemplo), se requiere que la solución tenga la capacidad de controlarlas por políticas de máximo de ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones.
- Soportar la creación de políticas de QoS por: dirección de origen y destino, por usuario y grupo de LDAP/AD, por aplicaciones, por puerto.
- El QoS debe permitir la definición de clases por: ancho de banda garantizado en Kilobytes por segundo, ancho de banda máximo en Kilobytes por segundo, prioridad de tráfico en al menos tres niveles de importancia.

7.6 VPN

- Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPSec o SSL.
- Las VPN client-to-site deben permitir la conexión por medio de agente instalado en el sistema operativo.
- Soportar VPN con algoritmos de cifrado 256-bit AES y 3DES
- Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN.
- Soportar autenticación vía AD/LDAP, TACACS+, SAML, RADIUS y Doble Factor de Autenticación (2FA).
- Debe permitir definir segmentos de red para ser agregadas de forma automática en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN.
- Debe asignar una IP a cada cliente que se conecte a la VPN en formato IPv4 e IPv6, de forma automática mediante un pool de IP.
- El agente de VPN client-to-site debe ser compatible al menos con: Windows 7 SP2, Windows 8.1, Windows 10, MacOS X.

7.7 CONTROL DE APLICACIONES

- La solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.
- La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.





EMPRESA PÚBLICA MUNICIPAL DE TRÁNSITO DE EL GUABO

Creada mediante Ordenanza Municipal, sancionada el 15 de Diciembre del 2023



- La solución debe tener un listado de al menos 3000 aplicaciones ya definidas por el fabricante.
- El listado de aplicaciones debe actualizarse periódicamente.
- Debe permitir en las políticas de control de aplicaciones ser aplicado por segmento de red o por usuario.

7.8 FILTRO DE CONTENIDO WEB

- Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías.
- La solución debe tener un listado de al menos 90 categorías de filtro de navegación web.
- Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida.
- Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables.
- La solución de Filtrado de Contenido debe soportar el forzado de "Safe Search" o "Búsqueda Segura" independientemente de la configuración en el browser del usuario. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales. Esta funcionalidad se soportará al menos para Google, Yahoo! y Bing.
- Será posible definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por usuario y por grupos.
- Se deberá poder hacer cache del contenido estático de las páginas para mejorar la experiencia de navegación del usuario final.
- El sistema debe permitir la inspección de tráfico cifrado en SSL de forma selectiva. Con ello se podrá personalizar la habilitación la inspección de una red, un usuario o excepcionar a una categoría de filtro web.





EMPRESA PÚBLICA MUNICIPAL DE TRÁNSITO DE EL GUABO

Creada mediante Ordenanza Municipal, sancionada el 15 de Diciembre del 2023



7.9 PREVENCIÓN DE AMENAZAS CONOCIDAS - SISTEMA DE PREVENCIÓN DE INTRUSOS (IPS)

- Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus (Antimalware de red), Antibot y Protección de Amenazas Avanzadas integrados en el propio appliance, sin necesidad de integrar otro tipo de consola para administrar este módulo.
- Deberá permitir la protección de este servicio por política de control de acceso.
- La solución debe tener un listado de al menos 7000 firmas de prevención de intrusos.
- Deberá tener la posibilidad de crear firmas IPS personalizadas a través de la interfaz gráfica del producto.
- Las firmas de ataque deberán actualizarse automáticamente sin la necesidad de coordinar ventanas de mantenimiento.
- Permitir la inspección y bloqueo en por lo menos los siguientes protocolos: HTTP, HTTP/2, FTP, SMB, SMTP, IMAP, POP, RDP, Java, ASP.
- Debe soportar granularidad en las políticas de IPS, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio, usuario y grupo de usuarios y la combinación de todos esos ítems.

7.10 ANÁLISIS DE MALWARE DE DÍA CERO

- El dispositivo de seguridad debe ser capaz de enviar archivos transferidos de forma automática para análisis en una plataforma de tipo sandbox, la cual podrá ser en versión nube o appliance on-premise.
- En caso se trate de sandbox cloud, deberá ser una nube propia del Vendedor con certificación de seguridad y privacidad de datos, como mínimo SOC Tipo 1. En caso el postor no cumpla con este requerimiento, podrá de forma alternativa proponer una solución de sandbox on-premise del mismo fabricante.
- Ya sea como versión on-premise o cloud, el sandbox deberá ser capaz de detectar el malware desconocido en un tiempo promedio de 5 minutos.
- En caso se trate de sandbox on-premise, deberá contar por lo menos con 8 máquinas virtuales con un mix de sistemas operativos para analizar el malware de la Entidad.





EMPRESA PÚBLICA MUNICIPAL DE TRÁNSITO DE EL GUABO

Creada mediante Ordenanza Municipal, sancionada el 15 de Diciembre del 2023



- Soportar el análisis de archivos maliciosos en ambiente controlado emulando sistemas operativos Windows.
- Debe soportar la inspección de archivos que viajen por los protocolos HTTP, HTTPS, HTTP/2, FTP, SMTP, POP3, IMAP y SMB.
- Deberá soportar el análisis de archivos ejecutables (EXE) de 32-bit y 64-bit, DLLs, archivos comprimidos (ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, XZ, 7ZIP), archivos office (.doc, .docx, .docm, .rtf, .xls, .xlsx, .xlsm, .ppt, .pptx, .pptm), archivos PDF (.pdf, .xpf) en el ambiente controlado.
- La subida de archivos debe ser de forma automática.

7.11 ADMINISTRACIÓN Y REPORTERÍA LOCAL

- El equipo deberá ofrecer una interfaz de reportes integrada a la interfaz de administración en el mismo dispositivo de forma embebida, sin incurrir en un costo adicional.
- El sistema reportería debe residir en el mismo appliance Firewall, no se permitirá una licencia adicional ni ningún equipo (Virtual, Hardware o Cloud) para lograr esta funcionalidad.
- Debe contar con cientos de informes integrados con opción de personalizar: paneles (tráfico, seguridad y cociente de amenazas del usuario), aplicaciones (riesgo de aplicaciones, aplicaciones bloqueadas, aplicaciones sincronizadas, motores de búsqueda, servidores web, coincidencia de palabras clave web, FTP), red y amenazas (IPS, ATP, inalámbrico, Security Heartbeat, Sandstorm), VPN, correo electrónico, cumplimiento (HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA)
- Monitoreo de actividad actual: estado del sistema, usuarios en vivo, conexiones IPSec, usuarios remotos, conexiones en vivo, clientes inalámbricos, cuarentena y ataques DoS.
- Programación de informes a varios destinatarios por grupo de informes con opciones de frecuencia flexibles.
- Capacidad de exportar informes como HTML, PDF, Excel (XLS).
- Personalización de la retención de registros por categoría
- Visor de registro en vivo con todas las funciones con vista de columna y vista detallada con potentes opciones de búsqueda y filtro, ID de regla con hipervínculo y personalización de la vista de datos





EMPRESA PÚBLICA MUNICIPAL DE TRÁNSITO DE EL GUABO

Creada mediante Ordenanza Municipal, sancionada el 15 de Diciembre del 2023



- Capacidad de visualizar y almacenar desde la misma consola del firewall, los informes y/o reportes por tiempo ilimitado (Limitado únicamente a la capacidad de almacenamiento del Firewall)
- Reporte del nivel de riesgo por usuario, calificando dicho nivel de riesgo en base al comportamiento en Internet del usuario, y al estar ligado a la autenticación, debe poder mostrar el detalle de la información del usuario y su actividad.

7.12 GESTIÓN CENTRALIZADA

- La solución debe permitir la gestión de los equipos Firewall y los informes de estos equipos, desde una sola consola de gestión basada en la nube del proveedor, donde, además, esta consola debe de proporcionar gestión de políticas por grupos de equipos.
- La gestión de políticas de grupo debe permitir que los objetos, la configuración y las políticas se modifiquen una vez y se sincronicen automáticamente con todos los Firewall del grupo.
- La consola debe proporcionar una pista de auditoría histórica completa y un seguimiento del estado de los cambios en las políticas del grupo.
- La consola además debe permitir la gestión de firmware de los equipos, así como el respaldo de los últimos cinco archivos de configuración para cada firewall.
- Las actualizaciones de firmware se deben ofrecen al administrador de la consola de tal manera que con un solo clic se pueda aplicar dicha actualización a cualquier dispositivo manejado dentro de la consola.
- La solución debe permitir implementaciones “Zero-Touch” desde esta consola central, permitiendo exportar la configuración para cargarla en un dispositivo desde una unidad flash, conectando así automáticamente al dispositivo a la consola Central.
- Debe permitir la programación de actualizaciones de firmware
- Debe permitir la generación de Informes de múltiples firewalls.
- Debe además permitir guardar, programar y exportar informes desde esta consola central.
- Esta Consola de gestión debe ser sin ningún costo adicional.



EMPRESA PÚBLICA MUNICIPAL DE TRÁNSITO DE EL GUABO

Creada mediante Ordenanza Municipal, sancionada el 15 de Diciembre del 2023



7.13 GARANTÍA Y SOPORTE

- Garantía de hardware y RMA.
- Soporte de fábrica 24x7 por teléfono y chat y vía correo electrónico en inglés y soporte 8x5 en español.
- Actualizaciones y parches de seguridad GRATIS.
- Actualizaciones y mejoras GRATUITAS de funciones de software

7.14 PROTECCIÓN SERVIDORES WEB

- El Firewall deberá garantizar funcionalidades de WAF (Web Application Firewall). Esta funcionalidad se debe incorporar dentro del mismo appliance, no se permitirá firewall que no soporte esta funcionalidad o bien no se permitirá que requieran de algún appliance adicional (Virtual, Hardware o Cloud) para lograr dichas funcionalidades.
- El appliance debe soportar la funcionalidad de WAF con las siguientes características
 - Modo de despliegue en proxy reverso.
 - Protección básica de ataques de tipo SQL injection, cross-site scripting y directory traversal.
 - Escaneo de virus de archivos entrantes al servidor web.
 - Protección vía hardening de formularios web.
 - Opción de descifrado de tráfico SSL.
 - Firmado de cookies web con firmas digitales.
 - Opción de balanceo de carga integrado que permita distribuir las visitas del portal web en varios servidores.
 - Para el soporte completo a programación basadas microservicios el balanceador debe tener Soporte de enrutamiento basado en la ruta o path-based routing.
 - Soporte del protocolo Outlook anywhere.

8. EXPERIENCIA GENERAL MINIMA DEL OFERENTE:

NUMERO DE PROFESIONALES	LISTA DEL PERSONAL TENICO CLAVE
1	Técnico, Tecnólogo o ingeniero: Tener experiencia en instalación, mantenimiento y puesta en marcha de





EMPRESA PÚBLICA MUNICIPAL DE TRÁNSITO DE EL GUABO

Creada mediante Ordenanza Municipal, sancionada el 15 de Diciembre del 2023



	dispositivos de seguridad perimetral, incluyendo rowters y otros dispositivos de red.
--	---

Adicionalmente deberá incluir personal de apoyo técnico que considere conveniente, el mismo que no requiere ninguna documentación adicional, pero que podrá ser verificado durante la vigencia del contrato.

9. INSTRUMENTOS Y EQUIPOS DISPONIBLES:

No se requiere dispositivos adicionales.

10. PRESUPUESTO REFERENCIAL:

DESCRIPCIÓN	VALOR
CAPACITACION TECNICA ASOCIADA A LA PLATAFORMA ADQUIRIDA / MODALIDAD 8X5 / ALCANCE REMOTO - CTA	250.00
IMPLEMENTACION Y CONFIGURACION DE LA PLATAFORMA ADQUIRIDA / MODALIDAD 8X5 / ALCANCE REMOTO - ICPR	250.00
FIREWALL DE SEGURIDAD PERIMETRAL	2920.00
SOPORTE TECNICO ASOCIADO A LA PLATAFORMA ADQUIRIDA / MODALIDAD 8X5 / ALCANCE REMOTO - SOPT	500.00

11. PLAZO DE EJECUCION:

El plazo de entrega será de máximo diez (10) días calendario, contados a partir de la notificación.

12. FORMAS Y CONDICIONES DE PAGO:

La forma de pago se efectuará una vez entregado el bien, y los documentos previstos para el pago, así mismo la garantía técnica del producto.

13. OBLIGACIONES DEL CONTRATISTA:

El contratista debe proteger y salvar de responsabilidad a la Entidad Contratante y a sus representantes de cualquier reclamo o juicio que surgiera como consecuencia de la contravención o falta de cumplimiento de cualquier norma jurídica por parte del contratista o su personal. En caso de encontrar en los documentos contractuales una discrepancia o





EMPRESA PÚBLICA MUNICIPAL DE TRÁNSITO DE EL GUABO

Creada mediante Ordenanza Municipal, sancionada el 15 de Diciembre del 2023



contradicción con relación a cualquier norma jurídica, el contratista deberá informar de esto a la entidad contratante.

14. OBLIGACIONES DEL CONTRATANTE:

- Dar solución a las peticiones y problemas que se presenten en la ejecución del contrato, en un plazo de 5 días contados a partir de la petición escrita formal por el contratista.
- Cumplir con las obligaciones establecidas en el contrato, y en los documentos de este de forma ágil y oportuna.
- Las demás propias de cada contrato.

Particular que comunico para los fines pertinentes.

Atentamente:



Firmado electrónicamente por:
JOHNNY EDGAR URDIN
GONZALEZ

Ing. Johnny Urdin González, Mgs
Jefe de la Unidad de Sistemas

EMPRESA PÚBLICA MUNICIPAL DE TRANSITO DE EL GUABO EPMT-G





**EMPRESA PUBLICA MUNICIPAL DE TRANSITO
DE EL GUABO
UNIDAD DE SISTEMAS**

INFORME

DETERMINACIÓN DE LA NECESIDAD

Fundamento: Nuevo Reglamento de Contratación Pública, Art. 44

No. UDS-002-EPMT-G-2025

1. ANTECEDENTES

TIPO DE PRODUCTO:	BIEN	X	SERVICIO		OBRA		CONSULTORÍA
IDENTIFICACIÓN DEL OBJETO: No anteponer verbos como “contratar” o “adquirir”, simplemente se deberá determinar el objeto de la contratación. Considerar Art. 48 del nuevo Reglamento.	“ADQUISICIÓN, CAPACITACIÓN, CONFIGURACIÓN Y PUESTA EN MARCHA DE UN DISPOSITIVO DE SEGURIDAD PERIMETRAL PARA LA EMPRESA PÚBLICA MUNICIPAL DE TRÁNSITO DE EL GUABO”						
CÓDIGO CPC: (Clasificador Central de Productos) Revisar Art. 104.1 de la Codificación SERCOP	452400017						
FECHA: (día/mes/año)	08/01/2025						
ÁREA REQUIRENTE:	UNIDAD DE SISTEMAS						
RESPONSABLE DEL ÁREA REQUIRENTE: Determinar cuál es el área requirente de acuerdo con la estructura organizacional de la entidad contratante.	Nombre del titular del área requirente			Cargo del funcionario			
	ING. JOHNNY URDIN GONZÁLEZ			UNIDAD DE SISTEMAS			
RESPONSABLE DEL REQUERIMIENTO: Observar la NCI 200-06 (un técnico afín al objeto de contratación deberá elaborar el presente requerimiento junto con los estudios previos a los que hace referencia el Art. 23 LOSNCP).	Nombre del funcionario responsable del requerimiento			Cargo del funcionario			
	ING. JOHNNY URDIN GONZÁLEZ			JEFE DE LA UNIDAD DE SISTEMAS			
¿QUIÉN GENERO LA NECESIDAD?	SUBDIRECCIÓN DE COMPRAS PÚBLICAS						
REQUERIMIENTO: Utilizar correctamente el lenguaje: Adquisición (para bienes) Contratación (para servicios, consultorías y construcción de obras)	“ADQUISICIÓN, CAPACITACIÓN, CONFIGURACIÓN Y PUESTA EN MARCHA DE UN DISPOSITIVO DE SEGURIDAD PERIMETRAL PARA LA EMPRESA PÚBLICA MUNICIPAL DE TRÁNSITO DE EL GUABO”						
PROYECTO CUP: (Código Único de Proyecto) (Aplica en proyectos de inversión) Conforme Art. 118 del Código Orgánico de Planificación y Finanzas Públicas. (Se deberá adjuntar proyecto en formato SENPLADES).	NO APLICA						

2. DESARROLLO

2.1. FUNDAMENTOS DE LA CONTRATACIÓN:

Se deberá redactar los antecedentes de la entidad contratante indicando las normas jurídicas que regulan su actividad institucional, así como un breve resumen de la necesidad imperante de adquirir o contratar el objeto de contratación.

La Empresa Pública Municipal de Tránsito de El Guabo se administra observando las Normas legales vigentes; es así que atendiendo a las actualizaciones del Reglamento General a La Ley Orgánica del Sistema Nacional de Contratación Pública en su Art. 33.- Expediente de contratación y conocedores de los Art. 232,233,234 del Código Integral Penal se torna indispensable proveerse de infraestructura tecnológica complementaria que permita mantener servidores de respaldo, plataformas dedicadas al almacenamiento de información digital, la implementación de software que permita la gestión más eficiente de los archivos digitales, la implementación de nuevos mecanismos para la gestión de acceso de usuarios y la gestión de copias de respaldo.

Robustecer la infraestructura existente permitirá a la Empresa mejorar la administración de los usuarios internos y su organización en torno a la información digital que genera cada uno de ellos; a la vez se la asegura contra fugas o

pérdidas.
2.2. SITUACIÓN ACTUAL / JUSTIFICACIÓN DE COMPRA: Se deberá indicar con precisión las razones por las cuales la entidad contratante debe invertir con recursos públicos la adquisición de un determinado bien, o la contratación de una construcción de obra, prestación de servicios o consultorías. .- En el caso de bienes se deberá justificar la inexistencia del bien en bodega. .- En el caso de arrendamiento de bienes se deberá justificar el beneficio institucional frente a la alternativa de adquisición. .- Considerar Arts. 36 y 42 del nuevo Reglamento General de la LOSNCP.
Esta Empresa actualmente no se cuenta con un dispositivo de seguridad perimetral. Con la finalidad de asegurar los servicios, procesos y aprovechar al máximo las características de hardware de servidores que se ha pensado contratar es necesario virtualizarlos y para lograr este cometido la Empresa necesita contratar servicios que efectúen el acondicionamiento y las configuraciones precisas en los servidores que actualmente posee la institución; de tal forma que la infraestructura se vuelva escalable es decir que las próximas adquisiciones de hardware se integren con lo instalado, y además brindarle la seguridad y confiabilidad en lo mayormente posible.
2.3. ANÁLISIS BENEFICIO/EFICIENCIA/EFFECTIVIDAD Considerar la NCI 408-07 Evaluación financiera y el Nuevo Reglamento de Contratación Pública, Art. 44
BENEFICIO El equipo firewall ofrece una solución robusta y confiable para la protección de redes contra amenazas externas e internas. Con características avanzadas como filtrado, detección de intrusos, VPN, etc., este dispositivo es adecuado para dar seguridad a las diferentes áreas informáticas de la Empresa Pública Municipal de Tránsito de El Guabo. Además, cumple con los requisitos de rendimiento y escalabilidad para soportar las operaciones a medida que crecen las necesidades de seguridad; El equipo de seguridad Firewall, provee los siguientes beneficios: 1. Protección de los sistemas administrativos: Los sistemas que manejan información crítica, como multas, registros vehiculares y permisos, estarán protegidos contra accesos no autorizados o ataques cibernéticos. 2. Control del tráfico interno y externo: Permite regular y monitorear el flujo de datos entre la red interna de la institución y el exterior, asegurando que solo el tráfico autorizado sea permitido. 3. Prevención de ataques cibernéticos: Bloquea intentos de intrusión, ataques de malware y denegación de servicio (DDoS), que pueden comprometer la disponibilidad de los servicios públicos. 4. Cumplimiento normativo: Ayuda a cumplir con normativas de protección de datos y estándares de ciberseguridad aplicables a entidades públicas. 5. Continuidad de los servicios: Evita interrupciones de los sistemas que soportan las operaciones críticas de la institución.
EFFECTIVIDAD:
Capacidad de Protección • Prevención de Amenazas: Debe detectar y bloquear amenazas avanzadas, como ransomware, phishing y spyware. • Filtrado de Contenido: Restringe el acceso a sitios web maliciosos o no relacionados con las operaciones de la institución. • Inspección de Tráfico en Tiempo Real: Analiza los datos entrantes y salientes para identificar patrones sospechosos.
Rendimiento • Capacidad de Conexiones Concurrentes: Asegura que el firewall pueda gestionar múltiples usuarios simultáneamente sin afectar el desempeño de la red. • Ancho de Banda Soportado: Debe manejar el tráfico de datos esperado por la institución, considerando crecimiento futuro.
Escalabilidad y Flexibilidad • Adaptación al Crecimiento: Capacidad de ampliarse o integrarse con nuevos sistemas y aplicaciones. • Soporte para Redes VPN: Permite conexiones seguras para empleados remotos o enlaces interinstitucionales.
Gestión y Monitoreo • Alertas y Registros: Proporciona reportes detallados y alertas en tiempo real sobre incidentes de seguridad. • Facilidad de Administración: Debe ser manejable por el personal técnico del departamento de sistemas.
Relación Costo-Beneficio El firewall debe ofrecer un equilibrio entre su costo y las funcionalidades que aporta, asegurando que la inversión sea adecuada a las necesidades y presupuesto de la institución.

2.4. DETALLE DEL REQUERIMIENTO:

Detallar con precisión los ítems del objeto de contratación (no se necesita dar especificaciones técnicas)

Ítem	Detalle del producto	CPC	Unidad	Cantidad	V. Unit.	V. total
1	CAPACITACION TECNICA ASOCIADA A LA PLATAFORMA ADQUIRIDA / MODALIDAD 8X5 / ALCANCE REMOTO - CTA	452400017	H.	5	50.00	250.00
2	IMPLEMENTACION Y CONFIGURACION DE LA PLATAFORMA ADQUIRIDA / MODALIDAD 8X5 / ALCANCE REMOTO - ICPR	452400017	H.	5	50.00	250.00
3	FIREWALL DE SEGURIDAD PERIMETRAL	452400017	U.	1	2920.00	2920.00
4	SOPORTE TECNICO ASOCIADO A LA PLATAFORMA ADQUIRIDA / MODALIDAD 8X5 / ALCANCE REMOTO - SOPT	452400017	H.	10	50	500.00

2.5. PLAZO DE EJECUCIÓN:

(Recuerde que la unidad de medida del tiempo será en días calendario o plazo)

Considerar las reglas de inicios de plazos contractuales contempladas en el Art. 288 del nuevo Reglamento General de la LOSNCP y Arts. 112 y Art. 530 de la Codificación de las resoluciones del SERCOP.

PLAZO:	10 días calendario
CONTADO A PARTIR DE:	De la notificación de la Orden de Compra
JUSTIFICACIÓN:	Es un tiempo prudente para que el proveedor planifique la visita para ejecutar la instalación y puesta en marcha del equipo.

CALENDARIO DE ENTREGAS: aplica exclusivamente si el objeto de contratación es divisible, por consiguiente, se establecerán los cronogramas de entrega de los bienes:

2.6. ENTREGAS:

. - Determinar si el objeto de contratación es divisible y susceptible de recepciones parciales.

. - Considerar Art. 316 y siguientes del nuevo Reglamento General de la LOSNCP.

Total:	Una sola entrega
Parcial 1:	No aplica
Parcial 2:	No aplica
...	En caso de haber más entregas parciales o diferentes condiciones de las entregas parciales conforme lo ítems se deberá adjuntar como documento aparte el numeral 7 del presente formulario.

2.7. FORMA Y CONDICIONES DE PAGO:

En caso de otorgar un anticipo el contratista debe tener una cuenta en un banco público, de conformidad con el segundo inciso del Art. 76 del Código Orgánica de Planificación y Finanzas Públicas y el último inciso del Art. 299 de la Constitución de la República del Ecuador.

Considerar el Art. 265 del nuevo Reglamento General de la LOSNCP (anticipo máximo el 50%).

CONTRA ENTREGA:	X	PAGO POR PLANILLA:		OTRA:		ANTICIPO:		PORCENTAJE:	
JUSTIFICACIÓN DE LA CONDICIÓN DE PAGO:	El ciento por ciento (100%) del valor total, contra entrega de lo adquirido por la Empresa Pública Municipal de Tránsito de El Guabo								

2.8. LOCALIDAD EN DONDE SE EJECUTARÁ LA CONTRATACIÓN DEL BIEN O SERVICIO

PROVINCIA:	EL ORO
CANTÓN	EL GUABO
LUGAR	EMPRESA PÚBLICA MUNICIPAL DE TRÁNSITO DE EL GUABO

12.- DIRECCIÓN DE ENTREGA DE OFERTAS

NO APLICA

2.9. GARANTÍAS:

. - Revisar los Arts. 74, 75 y 76 de la Ley Orgánica del Sistema Nacional de Contratación Pública -LOSNCP-

. - Considerar los Arts. 260 al 265 del nuevo Reglamento General de la LOSNCP.

a) Anticipo		b) Técnica	X	c) Fiel cumplimiento	
--------------------	--	-------------------	----------	-----------------------------	--

Observaciones sobre las garantías:	La garantía cubrirá sobre los trabajos de instalación y problemas de hardware.		
Forma de Garantía: Revisar Art. 73 de la LOSNCP	Tendrá vigencia de tres años desde la firma del acta entrega recepción de los servicios		
Garantía de asesoramiento (Aplica exclusivamente para la contratación de consultoría de estudios previos en obras). Considerar: NCI 408-34 y Arts. 284 al 295 de la codificación de las resoluciones.	NO APLICA		
2.10. TIPO DE ADJUDICACIÓN: Aplica en procedimientos de ferias inclusivas, licitación, cotización e ínfima cuantía.			
a) Total		X	b) Parcial
2.11. FORMA Y CONDICIONES DE PAGO: Revisar los Arts. 82 y 83 de la LOSNCP y Art. 267 al 284 del nuevo Reglamento General de la LOSNCP.			
Aplica: SI		NO	X Contra Entrega
Fórmula:		NO APLICA	
2.12. MULTAS: Considerar el Art. 71 de la LOSNCP y Arts. 292 y 293 del Nuevo Reglamento General de la LOSNCP.			
a) Retraso injustificado porcentaje diario:		1 x 1000	
b) justificación:		Es un porcentaje prudente de acuerdo nivel de gravedad del incumplimiento.	
Otras causas: (Determine todas las causas que puedan ocasionar daño a la Administración Pública por cualquier clase de incumplimiento por parte del contratista y que ameriten la aplicación de una multa; se deberá tipificar la conducta y la multa correspondiente en cada caso)		No aplica	
		No aplica	
2.13. REQUISITOS MÍNIMOS: (metodología cumple / no cumple) (De ser necesario pueden ir como anexo)			
No.	Tipo de requisito Mínimo		Detalle/Observación
1	Experiencia General: Considerar Art. 65 de la Codificación de las Resoluciones del SERCOP. Considerar: Resoluciones 077-2017 y 078-2017		Si aplica
	Justificación:		Para asegurar la calidad de servicios que va a contratar la Empresa en la prestación de servicios de mantenimiento de equipos informáticos y electrónicos. Experiencia adquirida en los últimos 5 años previos a la publicación del presente procedimiento
	¿Cómo debe ser justificada? (Detallar los documentos con los cuales debe acreditar la experiencia)		El oferente deberá presentar UNO o VARIOS certificados o actas de entrega recepción definitiva, que la sumatoria de dichos instrumentos alcancen mínimo el 10% del presupuesto referencial
	Justificación:		Experiencia adquirida en los últimos (años): 5 años previos a la publicación del procedimiento
	¿Cómo debe ser justificada? (Detallar los documentos con los cuales debe acreditar la experiencia)		El oferente deberá presentar UNO o VARIOS certificados o actas de entrega recepción definitiva por entidades públicas o privadas, que la sumatoria de dichos instrumentos alcancen mínimo el 5% del presupuesto referencial
3	Personal técnico Mínimo:		Nivel de Estudios: Tercer Nivel en Sistemas, Electrónica, o carreras afines a tecnología de la información Capacitación: capacitado en las marcas a realizarse los mantenimientos

	¿Cómo debe ser justificada? (Detallar los documentos con los cuales debe acreditar la experiencia)	CERTIFICADO DE REGISTRO DE TÍTULO emitido SENECHT Certificado emitido por el fabricante de al menos dos de las macas de los equipos a ser intervenidos que acredita al técnico estar capacitado.
4	Experiencia del personal técnico:	Técnico, Tecnólogo o ingeniero: Tener experiencia en instalación, mantenimiento y puesta en marcha de dispositivos de seguridad perimetral, incluyendo routers y otros dispositivos de red.
	¿Cómo debe ser justificada? (Detallar los documentos con los cuales debe acreditar la experiencia)	Certificado de trabajo que avalen la experiencia mínima de 3 años durante los últimos 5 años
4	Herramientas de trabajo:	No aplica
5	Equipo o maquinaria mínimos:	No aplica
6	Documentos habilitantes de la oferta:	No aplica
7	Servicio pos venta:	No aplica
8	Verificación de estado tributario, SRI	Si aplica
9	Verificación del Estado del oferente en el Registro Único de Proveedores, RUP;	No aplica
10	Especificaciones técnicas	Si aplica

2.14. PARÁMETROS DE CALIFICACIÓN POR PUNTAJE NO APLICA

(Aplica exclusivamente cuando la evaluación de la oferta es por puntaje)

No.	Tipo de parámetro:	Detalle
1	Oferta económica:	No aplica
2	Plazo propuesto:	No aplica
3	Experiencia General adicional:	No aplica
4	Experiencia Específica adicional:	No aplica
5	Especificaciones técnicas	No aplica
6	Porcentaje de Valor Agregado Ecuatoriano Mínimo (VAE)	No aplica

3. CONCLUSIONES:

La implementación de un firewall eficiente es crítica para la Empresa Pública Municipal de Tránsito de El Guabo, considerando el manejo de datos sensibles y el cumplimiento de las normativas de seguridad. Un firewall con capacidades avanzadas, como la detección de intrusiones (IDS/IPS), inspección profunda de paquetes (DPI) y soporte para VPN, garantizará la protección contra amenazas y la continuidad operativa de los servicios públicos.

4. FIRMAS DE RESPONSABILIDAD DEL REQUERIMIENTO:

 Firmado electrónicamente por: JOHNNY EDGAR URDIN GONZALEZ		
Elaborado por:	Ing. Johnny Urdin González	
Cargo:	JEFE DE LA UNIDAD DE SISTEMAS	
CODIGO SOCE:	0FU2K8UTJ2	