ADENDA Nº 03

LICITACIÓN PÚBLICA NACIONAL POR EL PROCEDIMIENTO DE SUBASTA A LA BAJA ELECTRÓNICA N° 19/2018 PARA LA "ADQUISICIÓN DE EQUIPOS DE NETWORKING, MATERIALES DE FIBRA ÓPTICA Y OTDR" ID N° 350.558

Asunción, 13 de noviembre de 2018

PETROPAR comunica a las empresas interesadas en participar de la **LICITACIÓN PÚBLICA NACIONAL POR EL PROCEDIMIENTO DE SUBASTA A LA BAJA ELECTRÓNICA N° 19/2018 PARA LA "ADQUISICIÓN DE EQUIPOS DE NETWORKING, MATERIALES DE FIBRA ÓPTICA Y OTDR" ID N° 350.558,** a fin de dar cumplimiento cabal a los principios generales de las Contrataciones Públicas, **Art. 4º de la Ley 2051/03, las siguientes modificaciones al Pliego de Bases y Condiciones:**

MODIFICACION Nº 01

SE MODIFICAN LAS FECHAS INICIO DE CARGA DE PROPUESTAS, CIERRE DE CARGA DE PROPUESTAS, ETAPA COMPETITIVA, ENTREGA DE OFERTAS Y APERTURA FISICA DE LAS OFERTAS QUEDANDO CONFORME AL SISTEMA DE INFORMACION DE LAS CONTRATACIONES PUBLICAS (SICP).

MODIFICACION Nº 02

EN LA SECCIÓN III "REQUISITOS DE LOS BIENES Y/O SERVICIOS REQUERIDOS", EN EL PUNTO 1 "ESPECIFICACIONES TÉCNICAS", EN EL APARTADO 1.2 "CONSIDERACIONES GENERALES DE PROYECTO PARA TODOS LOS ÍTEMS", SE MODIFICAN LOS NUMEROS 8 Y 9 QUEDANDO DE LA SIGUIENTE MANERA:

8	**Fabricación**	Todos los materiales deben ser de fabricación reciente nuevos y estar en excelentes condiciones al momento de la entrega.	Exigido
9	**Garantías**	Todos los ítems deberán contar con una garantía escrita de 24 (veinticuatro) meses contados a partir del Acta de Recepción definitiva de los bienes.	Exigido

MODIFICACION Nº 03

EN LA SECCIÓN III "REQUISITOS DE LOS BIENES Y/O SERVICIOS REQUERIDOS", EN EL PUNTO 1 "ESPECIFICACIONES TÉCNICAS", SE MODIFICA EL APARTADO 1.3 "DETALLE DE LAS ESPECÍFICACIONES TÉCNICAS", QUEDANDO DE LA SIGUIENTE MANERA:

1.3 Detalle de las Especificaciones Técnicas

ADQUISICION DE EQUIPOS DE NETWORKING.			
ITEM 1 - ROUTER TIPO 1			
N°	**ESPECIFICACION Y/O FUNCIONALIDAD**	**CARACTERÍSTICAS**	**Mínimo Exigido**
1	**Cantidad**	1 (uno)	Exigido
2	**Marca**	**Indicar**	Exigido
3	**Modelo**	**Indicar**	Exigido
4	**Procedencia**	**Indicar**	Exigido
5	**Generalidades**	El equipo deberá estar diseñado para funcionar como router de Borde Enterprise	Exigido
		Deberá ser rackeable.	Exigido
		Deberá soportar memoria Flash al menos de 8 GB.	Exigido
		Deberá soportar al menos 8GB de memoria RAM.	Exigido
		Fuente de Alimentación 110-220V, 50/60Hz.	Exigido
		Temperatura de Funcionamiento 0° C - 40° C	Exigido

Ing. Pedro Gustavo Duarte
Director Int. DTI-PETROPAR

Oficina Central, Asunción, Chile 753 casi Víctor Haedo - Edificio Centro Financiero
Teléfono: (+595 21) 448 503/8 R.A. Fax Secretaría General: (+595 21) 452 306
www.petropar.gov.py

Ing. Silvio David López
Jefe Int. de Unidad Técnica - DTI
PETROPAR

ADENDA Nº 03
LICITACIÓN PÚBLICA NACIONAL POR EL PROCEDIMIENTO DE SUBASTA A LA BAJA ELECTRÓNICA N° 19/2018 PARA LA "ADQUISICIÓN DE EQUIPOS DE NETWORKING, MATERIALES DE FIBRA ÓPTICA Y OTDR" ID N° 350.558

6	**Interfaces**	Deberá contar al menos con 2 interfaces 1Gigabit Ethernet RJ45 y al menos una interfaz 1 Gigabit Ethernet SFP las mismas podrán ser usadas como WAN o LAN.	Exigido
		Deberá soportar indistintos tipos de transceiver, al menos 1000Base-BX, 1000Base-EX, 1000Base-LX/LH, 1000Base-SX, 1000Base-ZX, 1000Base-T	Exigido
7	**Performance**	Deberá soportar un performance al menos hasta 90 Mbps.	Exigido
8	**Funcionalidades y Protocolos**	Deberá soportar al menos los siguientes protocolos:	Exigido
		· IPv4	Exigido
		· IPv6	Exigido
		· OSPF	Exigido
		· BGP	Exigido
		· IS-IS	Exigido
		· IGMPv3	Exigido
		· PIM SM	Exigido
		· IPSec	Exigido
		Deberá soportar ACL.	Exigido
9	**Administración**	Deberá contar con soporte de Interfaz CLI (Telnet, SSHv2 y Puerto Serial).	Exigido
		Debe soportar las siguientes funcionalidades: Syslog, SNMP	Exigido
10	**Certificaciones**	UL60950-1	Exigido
		EN 60950-1	Exigido
		IEC 60950-1	Exigido
		EN55022	Exigido
		EN55024	Exigido
11	**Garantía (escrita)**	Por defectos de fábrica, Soporte de atención de hardware, repuestos y Mano de Obra, traslado de los equipos de la oficina del cliente al proveedor y viceversa a cargo del oferente: 24 meses	Exigido
		Todos los equipos deben contar con certificación de calidad de fabricación ISO 9001:2008 o equivalente.	Exigido
12	**Plazo para remplazo de bienes defectuosos**	Corrección o reparación de cualquier defecto o sustitución del suministro no aceptado a completa satisfacción de la contratante en el plazo de 8 horas como máximo contados a partir del reclamo por escrito efectuado por la contratante.	Exigido
		La contratante podrá disponer de lo suministrado hasta la reposición por parte del Proveedor de la nueva partida que remplace a la no aceptada	Exigido

ITEM 2 - ROUTER TIPO 2			
N°	**ESPECIFICACION Y/O FUNCIONALIDAD**	**CARACTERÍSTICAS**	**Mínimo Exigido**
1	**Cantidad**	2 (dos)	Exigido
2	**Marca**	**Indicar**	Exigido
3	**Modelo**	**Indicar**	Exigido
4	**Procedencia**	**Indicar**	Exigido
5	**Generalidades**	El equipo deberá estar diseñado para funcionar como router de Borde	Exigido
		Deberá soportar memoria Flash al menos de 256 MB.	Exigido
		Deberá soportar al menos 1GB de memoria RAM.	Exigido
		Fuente de Alimentación 110-220V, 50/60Hz.	Exigido
		Temperatura de Funcionamiento 0° C - 40° C	Exigido
6	**Interfaces**	Deberá contar al menos con 1 interfaz SFP y al menos 1 interfaz FE como WAN. Como LAN, deberá contar con al menos 6 interfaces 1GE de los cuales al menos 3 deben ser PoE.	Exigido
7	**Funcionalidades y Protocolos**	Deberá soportar al menos los siguientes protocolos:	Exigido
		· IPv4	Exigido
		· IPv6	Exigido

Ing. Pedro Gustavo Duarte
Director Int. DTI-PETROPAR

Oficina Central, Asunción, Chile 753 casi Víctor Haedo – Edificio Centro Financiero
Teléfono: (+595 21) 448 503/8 R.A. Fax Secretaría General: (+595 21) 452 306
www.petropar.gov.py

Ing. Silvio David López Roice
Jefe Int. de Unidad Técnica - DTI
PETROPAR

ADENDA Nº 03

LICITACIÓN PÚBLICA NACIONAL POR EL PROCEDIMIENTO DE SUBASTA A LA BAJA ELECTRÓNICA N° 19/2018 PARA LA "ADQUISICIÓN DE EQUIPOS DE NETWORKING, MATERIALES DE FIBRA ÓPTICA Y OTDR" ID N° 350.558

		· OSPF	Exigido
		· BGP	Exigido
		· IGMPv3	Exigido
		· IPSec	Exigido
8	**Administración**	Deberá contar con soporte de Interfaz CLI (Telnet, SSHv2 y Puerto Serial).	Exigido
		SNMP v3	Exigido
		Deberá soportar RADIUS	Exigido
9	**Certificaciones**	CISPR22 o similares	Exigido
		EN55022 o similares	Exigido
		EN61000 o similares	Exigido
		ICES-003 o similares	Exigido
		EN50082 o similares	Exigido
		EN55024 o similares	Exigido
10	**Garantía (escrita)**	por defectos de fábrica, Soporte de atención de hardware, repuestos y Mano de Obra, traslado de los equipos de la oficina del cliente al proveedor y viceversa a cargo del oferente: 24 meses.	Exigido
		Todos los equipos deben contar con certificados de calidad de fabricación ISO 9001:2008 o equivalente.	Exigido
11	**Plazo para remplazo de bienes defectuosos**	Corrección o reparación de cualquier defecto o sustitución del suministro no aceptado a completa satisfacción de la contratante en el plazo de 8 horas como máximo contados a partir del reclamo por escrito efectuado por la contratante.	Exigido
		La contratante podrá disponer de lo suministrado hasta la reposición por parte del Proveedor de la nueva partida que remplace a la no aceptada	Exigido

ITEM 3 - SWITCH TIPO 1			
N°	**ESPECIFICACION Y/O FUNCIONALIDAD**	**CARACTERÍSTICAS**	**Mínimo Exigido**
1	**Cantidad**	2 (dos)	Exigido
2	**Marca**	**Indicar**	Exigido
3	**Modelo**	**Indicar**	Exigido
4	**Procedencia**	**Indicar**	Exigido
5	**Características Generales**	Switching capacity no menor a 1.7 Tbps	Exigido
		Forwarding rate menor o >=a 1.0 bpps	Exigido
		Deberá soportar al menos 280,000 MAC Address	Exigido
		El switch deberá proveer 48 puertos 10GBASE-T y 4 puertos QSFP28. Los 48 puertos deben soportar 1GBASE y 10GBASE, los 4 puertos QSFP28 deben soportar 10, 40 y 100Gbps.	Exigido
		Al menos, 48 (cuarenta y ocho) puertos del switch deben manejar de manera simultánea puertos a 1GE y a 10GE de velocidad.	Exigido
		Rendimiento de tráfico line-rate capa 2 y capa 3 sobre todos sus puertos	Exigido
		El equipo no deberá tener más de 1RU.	Exigido
		Jumbo Frames no menor a 9000 bytes	Exigido
6	**Funcionalidades LAN**	Manejo de puertos ruteados	Exigido
		Manejo de subinterfaces en puertos físicos y canales de puertos	Exigido
		Manejo de interfaces virtuales de switcheo	Exigido
		Soporte de 7000 rutas multicast	Exigido
		Manejo de listas de control de acceso	Exigido
		Manejo de listas de control de acceso en capa 2 del tipo macaddress y tipo de protocolo	Exigido

Ing. Pedro Gustavo Duarte
Director Int. DTI-PETROPAR

Oficina Central, Asunción, Chile 753 casi Víctor Haedo - Edificio Centro Financiero
Teléfono: (+595 21) 448 503/8 R.A. Fax Secretaría General: (+595 21) 452 306
www.petropar.gov.py

Ing. Silvio David López Rolón
Jefe Int. de Unidad Técnica - DTI
PETROPAR

		Manejo de listas de control de acceso en capa 3 del tipo IPv4, ICMP, TCP y UDP	Exigido
		Manejo de los protocolos de ruteo RIP v2, OSPFv2 y BGP	Exigido
		Manejo de VRRP o similar	Exigido
		Soporte de jumbo frames en todos los puertos	Exigido
		Soporte de 802.1s	Exigido
		Soporte de 802.1w	Exigido
		Compatibilidad con 802.1D.	Exigido
		Soporte de etiquetado de tramas para identificación de VLANs (802.1Q)	Exigido
		Soporte de 10GE (802.3ae)	Exigido
		Soporte de hasta 4000 VLANs	Exigido
		Soporte de BGP-, OSPF-, RIP	Exigido
		Soporte de LACP (Link Aggregation Control Protocol) IEEE 802.3ad	Exigido
		Manejo de PIMv2 modo sparse, SSM	Exigido
		Manejo de IGMP v1, v2 y v3	Exigido
		Clasificación de tráfico para calidad de servicio en capa 2 (IEEE 802.1p)	Exigido
7	**Administración**	Fuentes de poder y módulos de ventilación redundantes	Exigido
		El equipo debe permitir la circulación del aire a través de él de la parte frontal a la parte trasera	Exigido
		Redundancia de alimentación N+1	Exigido
		Redundancia de ventilación N+1	Exigido
		Puerto dedicado 10/100/1000 para administración fuera de banda	Exigido
		Soporte de SNMP v1, v2 y v3	Exigido
8	**Sistema de Management**		
		Deberá permitir servicios AAA y soportar tanto TACACS+, RADIUS y logeo directo	Exigido
		Deberá incluirse también las actualizaciones (updates y upgrades) a nuevas versiones mientras dure el periodo de garantía (12 meses).	Exigido
9	**Certificado de Calidad**	Certificación de calidad ISO 9001:2008 o equivalente	Exigido
10	**Implementación**	El Oferente deberá realizar todas las tareas de instalación física y configuración del equipamiento ofertado.	Exigido
		El Oferente debe incluir como parte de la oferta, todos los componentes necesarios que permitan la ampliación requerida.	Exigido
11	**Soporte y garantía**	por defectos de fábrica, Soporte de atención de hardware, repuestos y Mano de Obra, traslado de los equipos de la oficina del cliente al proveedor y viceversa a cargo del oferente 24 meses.	Exigido
12	**Plazo para remplazo de bienes defectuosos**	Corrección o reparación de cualquier defecto o sustitución del suministro no aceptado a completa satisfacción de la contratante en el plazo de 8 horas como máximo contados a partir del reclamo por escrito efectuado por la contratante.	Exigido
		La contratante podrá disponer de lo suministrado hasta la reposición por parte del Proveedor de la nueva partida que remplace a la no aceptada	Exigido

ITEM 4 - SWITCH TIPO 2			
Nº	**ESPECIFICACION Y/O FUNCIONALIDAD**	**CARACTERÍSTICAS**	**Mínimo Exigido**
1	**CANTIDAD**	2 (dos)	Exigido
2	**MARCA**	INDICAR	Exigido
3	**MODELO**	INDICAR	Exigido
4	**PROCEDENCIA**	INDICAR	Exigido
5	**INTERFACES**	Puertos SFP: 24	Exigido
		Slots para uplink 10G SFP: 2	Exigido
		El oferente deberá incluir en su oferta la provisión e instalación de 4 módulos SFP+ (10 Gbs) Multimodo, 2 modulos en cada equipo.	Exigido
		El oferente deberá incluir en su oferta la provisión e instalación de módulos SFP de 1/10 Gbs con la siguiente distribucion:	Exigido
		- 10 (diez) módulos SFP 1/10 Gbps Monomodo	

Ing. Pedro Gustavo Duarte
Director Int. DTI-PETROPAR
Oficina Central, Asunción, Chile 753 casi Víctor Haedo - Edificio Centro Financiero
Teléfono: (+595 21) 448 503/8 R.A. Fax Secretaría General: (+595 21) 452 306
www.petropar.gov.py
Ing. Silvio David
Jefe Int. de Unidad Técnica - DTI
PETROPAR

ADENDA Nº 03
LICITACIÓN PÚBLICA NACIONAL POR EL PROCEDIMIENTO DE SUBASTA A LA BAJA ELECTRÓNICA N° 19/2018 PARA LA "ADQUISICIÓN DE EQUIPOS DE NETWORKING, MATERIALES DE FIBRA ÓPTICA Y OTDR" ID N° 350.558

		- 38 (treinta y ocho) SFP 1/10 Gbps Multimodo	
		- Distribuidos equitativamente en cada equipo	
		Puerto local para administración desde consola: 1	Exigido
6	**PERFORMANCE**	Layer 2 Forwarding Rate: Capacidad de procesamiento (Non Blocking, basado sobre paquetes 64-byte), en Mpps: al menos 67	Exigido
		Capacidad de Switch Fabric media (en Gbps): al menos 90	Exigido
		MAC Address Entries: al menos 32000	Exigido
		Memoria RAM en GB: al menos 3	Exigido
		Memoria Flash en GB: al menos 2	Exigido
		MTBF (Horas): al menos 300000	Exigido
		Cantidad de VLAN Ids: al menos 4000	Exigido
		Mecanismo de reclasificación de frames Ethernet en todos los puertos del equipo, con hasta 8 colas de prioridad distintas por cada puerto.	Exigido
		Mecanismo de monitoreo de puertos remotamente	Exigido
7	**LAN STANDARDS**		
		IEEE_802.1d (Spanning Tree Protocol)	Exigido
		IEEE_802.1p (LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization)	Exigido
		IEEE_802.1Q (Virtual LANs - VLAN)	Exigido
		IEEE_802.1x (Port Based Network Access Control)	Exigido
		IEEE_802.1s (Multiple Spanning Tree)	Exigido
		IEEE_802.3 (CSMA/CD o Ethernet)	Exigido
		IEEE_802.3u (100 Mbps (Fast Ethernet)	Exigido
		IEEE_802.3ab (1000 Mbps - Gigabit Ethernet)	Exigido
		IEEE_802.3ad (Link Aggregation)	Exigido
		IEEE_802.3z (Gigabit Ethernet over fiber standards – 1000BaseX)	Exigido
		IEEE_802.1w (Rapid Spanning Tree Protocol - RSTP)	Exigido
		IEEE_802.3x (Flow Control IEEE 802.1p)	Exigido
8	**SEGURIDAD**	Debe poseer la capacidad de limitar e identificar las Mac de las estaciones que accedan a la red	Exigido
		Debe poseer la capacidad de controlar la cantidad de tráfico que ingresa al switch descartando el trafico excedente	Exigido
		Debe poseer la capacidad de deshabilitar un puerto de usuario al ingreso de una trama tipo BPDU	Exigido
		Debe permitir mecanismos para filtrado de tráfico en Mac de origen y destino	Exigido
		Debe permitir detectar y mitigar ataques basados en protocolo DHCP	Exigido
		Debe permitir detectar y mitigar ataques basados en protocolo ARP	Exigido
		Debe poseer la posibilidad de autenticar usuarios para prevenir accesos no autorizados a la red	Exigido
		Debe soportar autenticación de clientes basados en direcciones Mac	Exigido
		Debe permitir utilizar varios métodos de autenticación de usuarios	Exigido
		Debe soportar autenticación web para clientes que no soporta 802.1x	Exigido
		Debe permitir crear filtros basados en IP en interfaces L2	Exigido
		Debe soportar la creación de una VLAN para invitados	Exigido
9	**PROTOCOLOS**	RFC 768 User Datagram Protocol (UDP)	Exigido
		RFC 783 Trivial File Transfer Protocol (TFTP)	Exigido
		RFC 791 Internet Protocol (IP)	Exigido
		RFC 792 Internet Control Message Protocol (ICMP)	Exigido
		RFC 793 Transmission Control Protocol (TCP)	Exigido
		RFC 826 Address Resolution Protocol (ARP)	Exigido
		RFC 854 Telnet	Exigido
		RFC 1157 Simple Network Management Protocol Version 1 (SNMPv1)	Exigido
		RFC 1901 SNMPv2c	Exigido
		RFC 2273-2275 SNMPv3	Exigido
		RIP v2	Exigido
		OSPF	Exigido

Ing. Pedro Gustavo Duarte
Director Int. DTI-PETROPAR

Oficina Central: Asunción, Chile 753 casi Víctor Haedo - Edificio Centro Financiero
Teléfono: (+595 21) 448 503/8 R.A. Fax Secretaría General: (+595 21) 452 306
www.petropar.gov.py

ADENDA Nº 03
LICITACIÓN PÚBLICA NACIONAL POR EL PROCEDIMIENTO DE SUBASTA A LA BAJA ELECTRÓNICA N° 19/2018 PARA LA "ADQUISICIÓN DE EQUIPOS DE NETWORKING, MATERIALES DE FIBRA ÓPTICA Y OTDR" ID N° 350.558

		BGP	Exigido
		PBR	Exigido
		IS-ISv4	Exigido
10	**CERTIFICACIONES**	FCC Part 15 Class A o similares	Exigido
		AS/NZS CISPR22 Class A o similares	Exigido
		CE Markingz o similares	Exigido
		CNS13438 Class A o similares	Exigido
		EN 55024 o similares	Exigido
		EN 55022 o similares	Exigido
		CAN/CSA-C22.2 No. 60950-1 o similares	Exigido
		IEC 60950-1 o similares	Exigido
		UL 60950-1 o similares	Exigido
		ISO 9001:2008 o similares	Exigido
		(ROHS) 5 o similares	Exigido
		(CLEI) o similares	Exigido
11	**ALIMENTACIÓN ELÉCTRICA**	Fuente redundante para 200 a 240 V, 47 a 55 Hz y cables: 2	Exigido
12	**RANGO DE TEMPERATURA EN ACTIVIDAD**	De -5° a 45° C	Exigido
13	**ACCESORIOS**	Todos los accesorios requeridos para entregar el equipo en perfecto estado de operación (Módulos, software, patch cords de fibra para todos los mudulos SFP, power cord, cables para puertos Stacks.). Debera incluir 24 patch cord de fibra 1,5 metros por cada equipo.	Exigido
14	**CONFIGURACIÓN**	Cada equipo ofertado debe incluir módulo stack y cable stack. Se conformará un stack entre 2 equipos.	Exigido
		La Empresa se encargará de la configuración del equipo de comunicación de tal manera que sea funcional con los demás equipos adquiridos.	Exigido
15	**Garantía (escrita)**	por defectos de fábrica, Soporte de atención de hardware, repuestos y Mano de Obra, traslado de los equipos de la oficina del cliente al proveedor y viceversa a cargo del oferente: 24 meses.	Exigido
		Todos los equipos deben contar con certificados de calidad fabricación ISO 9001:2008 o equivalente.	Exigido
16	**Plazo para remplazo de bienes defectuosos**	Corrección o reparación de cualquier defecto o sustitución del suministro no aceptado a completa satisfacción de la contratante en el plazo de 8 horas como máximo contados a partir del reclamo por escrito efectuado por la contratante.	Exigido
		La contratante podrá disponer de lo suministrado hasta la reposición por parte del Proveedor de la nueva partida que remplace a la no aceptada	Exigido

ITEM 5 - SWITCH TIPO 3			
N°	**ESPECIFICACION Y/O FUNCIONALIDAD**	**CARACTERÍSTICAS**	**Mínimo Exigido**
1	**CANTIDAD**	24 (veinticuatro)	Exigido
2	**MARCA**	INDICAR	Exigido
3	**MODELO**	INDICAR	Exigido
4	**PROCEDENCIA**	INDICAR	Exigido
5	**INTERFASES**	Puertos Ethernet 1G PoE+: 24	Exigido
		Slots para uplink 10G SFP: 2	Exigido
		El oferente deberá incluir en su oferta la provisión e instalación de al menos	Exigido
		1 módulo SFP (1/10Gb) multimodo.	Exigido
		1 módulo SFP (1/10Gb) monomodo.	Exigido

Ing. Pedro Gustavo Duarte
Director Int. DTI-PETROPAR
Oficina Central: Asunción, Chile 753 casi Víctor Haedo - Edificio Centro Financiero
Teléfono: (+595 21) 448 503/8 R.A. Fax Secretaría General: (+595 21) 452 306
www.petropar.gov.py
Ing. Silvio David López Roldán
Jefe Int. de Unidad Técnica - DTI
PETROPAR

ADENDA Nº 03

LICITACIÓN PÚBLICA NACIONAL POR EL PROCEDIMIENTO DE SUBASTA A LA BAJA ELECTRÓNICA N° 19/2018 PARA LA "ADQUISICIÓN DE EQUIPOS DE NETWORKING, MATERIALES DE FIBRA ÓPTICA Y OTDR" ID N° 350.558

		Puerto local para administración desde consola: 1	Exigido
6	**PERFORMANCE**	Layer 2 Forwarding Rate: Capacidad de procesamiento (Non Blocking, basado sobre paquetes 64-byte), en Mpps: 48	Exigido
		Capacidad de Switch Fabric media (en Gbps): 85	Exigido
		MAC Address Entries: 16000	Exigido
		Capacidad MTU en bytes: 9000	Exigido
		Memoria RAM en GB: 1	Exigido
		Memoria Flash al menos 128 MB	Exigido
		MTBF (Horas): 300000	Exigido
		Cantidad de VLANs: 1000	Exigido
		Cantidad de VLAN Ids: 4000	Exigido
		Mecanismo de monitoreo y copia de tráfico de puertos remotamente	Exigido
		Mecanismos para establecer políticas y mapas de tráfico basado en las direcciones origen y destino de IP, MACADDRESS y puertos TCP-UDP.	Exigido
7	**LAN STANDARDS**	IEEE 802.1AB (LLDP)	Exigido
		IEEE_802.1d (Spanning Tree Protocol)	Exigido
		IEEE_802.1p (LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization)	Exigido
		IEEE_802.1Q (Virtual LANs - VLAN)	Exigido
		IEEE_802.1x (Port Based Network Access Control)	Exigido
		IEEE_802.3s (Multiple Spanning Tree)	Exigido
		IEEE_802.3u (100 Mbps (Fast Ethernet)	Exigido
		IEEE_802.3ab (1000 Mbps - Gigabit Ethernet)	Exigido
		IEEE_802.3ae (10GE)	Exigido
		IEEE_802.3ad (Link Aggregation)	Exigido
		IEEE 802.3az	Exigido
		IEEE_802.3z (Gigabit Ethernet over fiber standards – 1000BaseX)	Exigido
		IEEE_802.3w (Rapid Spanning Tree Protocol - RSTP)	Exigido
		IEEE_802.3x (Flow Control IEEE 802.1p)	Exigido
8	**SEGURIDAD**	Debe poseer la capacidad de limitar e identificar las Mac de las estaciones que accedan a la red	Exigido
		Debe poseer la capacidad de controlar la cantidad de tráfico que ingresa al switch descartando el trafico excedente	Exigido
		Debe permitir detectar y mitigar ataques basados en protocolo DHCP	Exigido
		Debe permitir detectar y mitigar ataques basados en protocolo ARP	Exigido
		Debe poseer la posibilidad de autenticar usuarios para prevenir accesos no autorizados a la red	Exigido
		Debe soportar autenticación de clientes basados en direcciones Mac	Exigido
		Debe permitir utilizar varios métodos de autenticación de usuarios	Exigido
		Debe soportar autenticación web para clientes que no soporta 802.1x	Exigido
		Debe permitir apagar una VLAN en un puerto cuando ocurra una violación sin apagar el puerto completamente.	Exigido
9	**PROTOCOLOS**	RFC 768 User Datagram Protocol (UDP)	Exigido
		RFC 783 Trivial File Transfer Protocol (TFTP)	Exigido
		RFC 791 Internet Protocol (IP)	Exigido
		RFC 792 Internet Control Message Protocol (ICMP)	Exigido
		RFC 793 Transmission Control Protocol (TCP)	Exigido
		RFC 826 Address Resolution Protocol (ARP)	Exigido
		RFC 854 Telnet	Exigido
		RFC 1112 Internet Group Management Protocol (IGMP)	Exigido
		RFC 3376 IGMP v3	Exigido
		RFC 1157 Simple Network Management Protocol Version 1 (SNMPv1)	Exigido
		RFC 1901 SNMPv2c	Exigido
		RFC 2273-2275 SNMPv3	Exigido

Ing. Pedro Gustavo Duarte
Director Int. DTI-PETROPAR

Oficina Central, Asunción, Chile 753 casi Víctor Haedo - Edificio Centro Financiero
Teléfono: (+595 21) 448 503/8 R.A. Fax Secretaría General: (+595 21) 452 306
www.petropar.gov.py

Ing. Silvio David López Rolón
Jefe Int. de Unidad Técnica - DTI
PETROPAR

ADENDA Nº 03
LICITACIÓN PÚBLICA NACIONAL POR EL PROCEDIMIENTO DE SUBASTA A LA BAJA ELECTRÓNICA N° 19/2018 PARA LA "ADQUISICIÓN DE EQUIPOS DE NETWORKING, MATERIALES DE FIBRA ÓPTICA Y OTDR" ID N° 350.558

		RIP v2	Exigido
		OSPF	Exigido
		BGPv4	Exigido
		PBR	Exigido
		RFC 2474 Differentiated Services (DiffServ) Precedence	Exigido
10	**CERTIFICACIONES**	FCC Part 15 Class A o similares	Exigido
		AS/NZS CISPR22 Class A o similares	Exigido
		EN 55024 o similares	Exigido
		EN 55022 o similares	Exigido
		IEC 60950-1 o similares	Exigido
		UL 60950-1 o similares	Exigido
		ISO 9001:2008 o similares	Exigido
		CE (CE mark) o similares	Exigido
11	**ALIMENTACION ELECTRICA**	Fuente para 200 a 240 V, 50 Hz y cables: 1	Exigido
12	**ACCESORIOS**	Todos los accesorios requeridos para entregar el equipo en perfecto estado de operación Módulos, software, patch cords de 1,5 metros para todos los puertos, power cord	Exigido
13	**CONFIGURACION**		
		El oferente se encargará de la configuración del equipo de comunicación de tal manera que sea funcional con los demás equipos adquiridos.	Exigido
14	**Garantía (escrita)**	por defectos de fábrica, Soporte de atención de hardware, repuestos y Mano de Obra, traslado de los equipos de la oficina del cliente al proveedor y viceversa a cargo del oferente: 24 meses.	Exigido
		Todos los equipos deben contar con certificados de calidad fabricación ISO 9001:2008 o equivalente.	Exigido
15	**Plazo para remplazo de bienes defectuosos**	Corrección o reparación de cualquier defecto o sustitución del suministro no aceptado a completa satisfacción de la contratante en el plazo de 8 horas como máximo contados a partir del reclamo por escrito efectuado por la contratante.	Exigido
		La contratante podrá disponer de lo suministrado hasta la reposición por parte del Proveedor de la nueva partida que remplace a la no aceptada	Exigido

ITEM 6 - NEXT GENERATION FIREWALL TIPO 1			
N°	**ESPECIFICACION Y/O FUNCIONALIDAD**	**CARACTERÍSTICAS**	**Mínimo Exigido**
1	**Cantidad**	**2 (dos)**	Exigido
2	**Marca**	**Indicar**	Exigido
3	**Modelo**	**Indicar**	Exigido
4	**Procedencia**	**Indicar**	Exigido
5	**Generalidades**	La solución ofrecer protección de seguridad de la infraestructura tecnológica, permitiendo lograr la eficiencia máxima en la detección y prevención de ataques, a través de funcionalidades de detección de anomalías en protocolos de red, minimizando los falsos positivos y falsos negativos en la identificación de ataques, con una administración centralizada contra amenazas conocidas o desconocidas y ataques híbridos.	Exigido
		El fabricante debe contar con un grupo de investigación sobre vulnerabilidades y amenazas informáticas, para lo cual deberá presentar la documentación respectiva en el descubrimiento de las mismas.	Exigido
		El proceso de actualización de vulnerabilidades y otros aspectos del mantenimiento (como parches y upgrades) deberá ser mediante el sitio Web del fabricante del producto y de varias formas: por medio del propio producto, bajando del sitio Web un archivo de actualización o bien automáticamente.	Exigido

Ing. Pedro Gustavo Duarte
Director Int. DTI-PETROPAR

Oficina Central, Asunción, Chile 753 casi Víctor Haedo - Edificio Centro Financiero
Teléfono: (+595 21) 448 503/8 R.A. Fax Secretaría General: (+595 21) 452 306
www.petropar.gov.py

Ing. Silvio David López Rolón
Jefe Int. de Unidad Técnica - DTI
PETROPAR

ADENDA Nº 03

LICITACIÓN PÚBLICA NACIONAL POR EL PROCEDIMIENTO DE SUBASTA A LA BAJA ELECTRÓNICA N° 19/2018 PARA LA "ADQUISICIÓN DE EQUIPOS DE NETWORKING, MATERIALES DE FIBRA ÓPTICA Y OTDR" ID N° 350.558

		La solución de administración debe permitir mecanismos de integración en forma de APIs abiertas, para lo cual deberá de presentar la documentación respectiva con cuales tecnologías se cumple con este modo de integración.	Exigido
		Debe proveer la funcionalidad de firewalling stateful para controlar el tráfico entrante y saliente de la red de datos con un performance de al menos 2 Gbps.	Exigido
		Deberá soportar a lo menos 1000 VLANs, a través del estándar 802.1q.	Exigido
		Debe soportar al menos 1.000.000 de conexiones simultáneas	Exigido
		Debe soportar al menos 10.000 conexiones nuevas por segundo	Exigido
		Debe soportar alta disponibilidad, Activo/Activo y Activo/Pasivo.	Exigido
		Debe poseer al menos 10 interfaces 1 GE de cobre, y 4 interfaces 1GE SFP.	Exigido
		Debe asegurar una performance adecuada para manejar 2 Gbps de tráfico con las funcionalidades de firewalling, de IPS y Visibilidad y Control de Aplicaciones, operando al mismo tiempo, sin degradación en el desempeño del equipo.	Exigido
		Debe proveer una interfaz de administración gráfica, así como acceso vía línea de comando.	Exigido
		Debe proveer funcionalidades de inspección de tráfico y tomar acciones preventivas (IPS – Intrusion Prevention System).	Exigido
		Debe soportar los protocolos de enrutamiento dinámicos BGP, EIGRP, OSPF y RIP.	Exigido
		Debe poder funcionar en modalidad ruteada (Layer 3) y transparente (Layer 2).	Exigido
		El equipo debe proveer un método de actualización automática de patrones considerados como peligrosos para la inspección de tráfico (IPS).	Exigido
		El IPS debe incorporar tecnología de reputación, correlación global de amenazas, detección de amenazas por anomalía y firmas.	Exigido
		Debe proveer soporte para bloquear aplicaciones peer-to-peer, como Kazaa, eDonkey y otras.	Exigido
		Debe ser capaz de bloquear aplicaciones que hagan uso indebido del puerto-80 como Skype, MSN y otros sistemas de mensajería instantánea.	Exigido
		Debe ser capaz de inspeccionar, operar y soportar protocolos VoIP como SIP, H323, MGCP, TAPI, y SCCP, incluso en escenarios con NAT.	Exigido
		El equipamiento no debe contener piezas móviles en su sistema de almacenamiento de datos.	Exigido
		Debe soportar tecnologías de priorización, manejo y encolamiento de trafico VoIP para ofrecer calidad de servicio, usando mecanismos del tipo encolamiento prioritario (PQ).	Exigido
		El sistema debe poder integrarse con sistemas externos tales como sistemas de seguridad web y ofrecer servicios de valor agregado como single-sign-on para mejorar la experiencia del usuario. También debe poder entregar información al sistema de seguridad web para permitir la obtención de información de grupo pertinente para la aplicación de políticas respectivas.	Exigido
		Debe soportar un mecanismo para captura y exportación de tráfico y de simulación de tráfico para facilitar detección y resolución de inconvenientes.	Exigido
		Debe proveer un sistema de fácil uso, paso a paso para configuración de VPNs IPSec, del tipo wizard.	Exigido
		El equipo debe soportar algún método para identificar y marcar eventos - como más o menos riesgosos- para llamar la atención del operador cuando así sea requerido, como un "ranking de riesgos" para registros del IPS.	Exigido
		Se deberá incluir reporte de organismo reconocido e independiente (no propio del fabricante) que muestre rendimiento en modalidad de firewall con todas las signaturas habilitadas.	Exigido
6	**VPN**	El equipamiento debe soportar IPSEC VPNs orientado a acceso remoto y conectividad entre múltiples sitios.	Exigido
		Debe ofrecer una performance de VPN de al menos 700 Mbps.	Exigido
		Debe soportar al menos 1200 túneles sitio a sitio IPSec.	Exigido
		La solución debe incluir un mecanismo de control de acceso a la red para los usuarios conectados vía VPN.	Exigido
		Deberá poder autenticar al usuario, chequeando contra una base de datos externa Active Directory.	Exigido
7	**IPS**	Monitorear el tráfico de red para prevenir ataques, port scanning, ataques de denegación de servicio y tráfico malicioso.	Exigido
		Dispositivo debe proporcionar como mínimo un throughput de 2 Gbps para el análisis del tráfico que cruza en el segmento de red.	Exigido

Ing. Pedro Gustavo Duarte
Director Int. DTI-PETROPAR

Ing. Silvio David López Rolón
Jefe Int. de Unidad Técnica - DTI
PETROPAR

Oficina Central, Asunción, Chile 753 casi Víctor Haedo – Edificio Centro Financiero
Teléfono: (+595 21) 448 503/8 R.A. Fax Secretaría General: (+595 21) 452 306
www.petropar.gov.py

ADENDA Nº 03

LICITACIÓN PÚBLICA NACIONAL POR EL PROCEDIMIENTO DE SUBASTA A LA BAJA ELECTRÓNICA N° 19/2018 PARA LA "ADQUISICIÓN DE EQUIPOS DE NETWORKING, MATERIALES DE FIBRA ÓPTICA Y OTDR" ID N° 350.558

			El dispositivo debe ser una solución de software y hardware basado en appliances, el cual tenga la capacidad de realizar su monitoreo y prevención de manera en línea además de ser de un sólo fabricante.	Exigido
			El dispositivo debe permitir la autenticación de usuarios y administradores a través de integración con RADIUS.	Exigido
			El monitoreo del dispositivo debe ser transparente para los usuarios y operar en la capa 2 del modelo de OSI, por lo que las interfaces no requieren de una dirección IP ni una dirección MAC.	Exigido
			El dispositivo debe permitir una inspección inteligente, basándose en el análisis estadístico de flujo de datos en la red, optimizando el proceso para identificar y proteger la red contra ataques.	Exigido
			El dispositivo podrá configurarse en modo transparente; es decir, de detección en línea, pero sin bloquear tráfico. El sistema sólo alerta que eventos serían bloqueados.	Exigido
			El dispositivo debe soportar un motor de detección que inspeccione no solo los detalles de la capa de red, además información residente en cabeceras de los paquetes, a través de una gama amplia de protocolos.	Exigido
			El dispositivo debe permitir la configuración de modo transparente para todo el tráfico o apenas para paquetes especificados por dirección IP, protocolo, VLAN ID incluyendo frames 802.1q.	Exigido
			El dispositivo debe permitir la creación de reglas y filtros de acceso.	Exigido
			El dispositivo debe tener la capacidad de detectar tráfico anómalo o vulnerabilidades en las siguientes aplicaciones Instant Messenger y P2P: AOL Instant Messenger; MSN Messenger; Yahoo! Messenger; ICQ; Gnutella; Kazaa; BitTorrent.	Exigido
			El dispositivo debe ser capaz de inspeccionar el tráfico asociado a distintos segmentos de redes diferentes (en lugar de tener una sola política por interfaz).	Exigido
			El dispositivo debe contar como mínimo con las siguientes técnicas de análisis de trafico: identificación del protocolo a través del puerto utilizado; identificación de protocolos que utilizan puertos aleatorios; identificación de protocolos en forma independiente del puerto utilizado.	Exigido
			El dispositivo debe ser resistente a diversas técnicas de URL obfuscation en ataques basados en HTML.	Exigido
			El dispositivo debe soportar reglas de detección basada en un leguaje abierto permitiendo a los usuarios crear sus propias reglas.	Exigido
			El dispositivo debe soportar los siguientes tipos de respuestas: bloquear, ignorar, guardar en un log, enviar correo electrónico, SNMP, respuestas definidas por el usuario, cambios de configuración a equipos de seguridad o de red de terceros, sugerencia de cambios a la política en base al análisis de impacto de un evento.	Exigido
			El dispositivo debe soportar el modo de implementación Inline, en donde se monitorea y protege los segmentos de datos, con tráfico activo de red pasando por el, lo que permite prevenir los ataques de estos segmentos y bloqueado en tiempo real.	Exigido
			El dispositivo debe soportar el modo de implementación Pasivo, permitiendo el monitoreo a través de los HUBs y / o puertos SPAN de switches, siendo el tráfico de red reflejando en el, lo que le permite monitorear el tráfico de ataques.	Exigido
			El dispositivo debe de soportar la identificación y protección de ataques en protocolos de Voice over IP (VoIP) sobre SIP.	Exigido
			El dispositivo debe tener la capacidad de construir un perfil para la identificación de dispositivos móviles, para lo cual debe incluir la siguiente información: track usuarios, vulnerabilidades, aplicaciones. (Sin necesidad de hardware o software separado).	Exigido
			El dispositivo deberá ser capaz de hacer recomendación de afinación (tuning) de políticas en base a la información aprendida de la red, mostrando un registro de las reglas recomendadas.	Exigido
			El dispositivo debe proveer la detección de anomalías de tráfico y análisis de impacto por evento para evitar ataques de día cero, como una funcionalidad dentro del mismo IPS y sin necesidad del uso de aplicaciones adicionales como sistema de detección de anomalías o scanners.	Exigido
			El dispositivo debe permitir tener la flexibilidad de controlar políticas a nivel de dispositivo, puerto, VLAN y direcciones IP.	Exigido
			El dispositivo deberá ser capaz de agregar a su base de datos de conocimiento los resultados de un análisis a través de NMAP, este deberá ser incluido como parte del mismo módulo de correlación.	Exigido
			El dispositivo debe de proveer monitoreo de segmentos de red en modo promiscuo analizando encabezamiento (header) y el área de datos (payload)	Exigido

Oficina Central, Asunción, Chile 753 casi Víctor Haedo – Edificio Centro Financiero
Teléfono: (+595 21) 448 503/8 R.A. Fax Secretaría General: (+595 21) 452 306
www.petropar.gov.py

Ing. Pedro Gustavo Duarte
Director Int. DTI-PETROPAR

Ing. Silvio David López Roldán
Jefe Int. de Unidad Técnica - DTI
PETROPAR

		de los paquetes que transitan en la red (deep packet inspection), detectando ataques y tráfico no autorizado o sospechoso.	
		El dispositivo deberá identificar vulnerabilidades de los hosts de la red en tiempo real y sin necesidad de correr un análisis de vulnerabilidades.	Exigido
		El dispositivo debe tener la habilidad de decodificar e inspeccionar todos los protocolos apoyados IPv4, y cualquier ataque asociado o mal uso incluso si está encapsulado en IPv6.	Exigido
		El dispositivo debe poder realizar capturas de tráfico para el análisis de evidencia en formato soportado por TCPDUMP y .ENC (estándar para el software de análisis de protocolos). El archivo puede ser usado para hacer playback del ataque. Se aceptarán propuestas que consideren la captura de tráfico para el análisis de evidencia en formato compatible con libpcap (compatible a su vez con TCPDUMP), y opcionalmente en formato ENC.	Exigido
		El dispositivo debe permitir un análisis dinámico y en tiempo real en para crear un mapa de la red monitoreada, incluyendo al menos lo siguiente parámetros: Redes existentes; Host activos; Nuevos Host o servers en la red; Nuevas MAC address en la red; Máquinas virtuales nuevas o existentes; Sistema operativo de cada uno de los host identificados; Servicios activos de cada uno de los host identificados; Aplicaciones activas de cada uno de los host identificados; Vulnerabilidades de cada uno de los host identificados.	Exigido
		Dispositivo deberá poder crear perfiles de tráfico con reglas específicas para monitorear el tráfico entre dos hosts de la red y crear una alarma cuando cierto umbral sea rebasado.	Exigido
		El dispositivo debe ser capaz de recopilar información pasiva de los hosts de la red y sus actividades, tales como: sistema operativo; servicios, puertos abiertos; aplicaciones y vulnerabilidades, permitiendo la correlación de datos, eliminación de falsos positivos y políticas de cumplimiento. (Sin necesidad de hardware o software separado).	Exigido
		El dispositivo debe tener la capacidad de ser administrado a través de conexiones SSH, CLI y HTTPS.	Exigido
		El dispositivo debe ser capaz de identificar todos los hosts que presenten un atributo o condición especifica de incumplimiento de la política.	Exigido
		El dispositivo debe ser capaz de proporcionar mayor visibilidad sobre cómo se consume el ancho de banda, ya sea por dirección o puerto, permitiendo ayudar en la solución de problemas de interrupciones o degradaciones de rendimiento de la red. (Sin necesidad de hardware o software separado).	Exigido
		El dispositivo debe soportar sincronización de horario a través de NTP (Network Time Protocol).	Exigido
		El dispositivo debe proveer la capacidad de realizar un respaldo de la configuración de la plataforma en tiempo real, o por un horario definido.	Exigido
		El dispositivo debe soportar IP Reputation, además debe permitir la creación de listas negras y listas blancas y debe contar con una base de datos propia, pero además debe permitir el poder configurar cualquier base de datos de terceros.	Exigido
		El dispositivo debe contar con al menos las siguientes de objetos de IP Reputation: Bots, CnC, Malware, Attacker, Suspicious.	Exigido
		El dispositivo debe proporcionar la capacidad inteligente para correlacionar los eventos de intrusión priorizándolo por tipo de bandera de impacto, en donde se categorice por: 0 Unknown; 1 Vulnerable; 2 Potentially Vulnerable; 3 Currently Not Vulnerable; 4 Unknown Target.	Exigido
		El dispositivo debe soportar integración a través del directorio activo y/o LDAP para determinar el comportamiento de la red a través de direcciones IP asociadas a los eventos sospechosos.	Exigido
		El dispositivo debe proporcionar una completa visión del comportamiento de la red para detectar nuevas amenazas, incluyendo la capacidad de establecer líneas de base de tráfico a través de técnicas de flujos.	Exigido
		El dispositivo debe contar con al menos las siguientes categorías de reglas: File-Executables; DoS; DoS; Exploit; P2P; Pua-Adware; Scada; Web-IIS; SQL; Indicator-Obfuscation; Sensitive-Data; RPC; Botnet.	Exigido
		El dispositivo debe poder soportar reglas por plataforma tal como: Apple; Cisco; Compaq; HP; IBM; Juniper; Microsoft; Nokia; RedHat; Suse; Sun; Juniper.	Exigido
		El dispositivo debe soportar reglas de contenido con al menos los siguientes parámetros: Message; Reference; Action; Protocol; SID; GID; Direction, Source IP, Destination IP, Source port; Destination port; Rule overhead, Metadata.	Exigido
		El dispositivo debe contar con la capacidad de crear reglas que permitan enviar tráfico directamente a través del dispositivo sin que sea inspeccionado.	Exigido

Ing. Pedro Gustavo Duarte
Director Int. DTI-PETROPAR

Oficina Central, Asunción, Chile 753 casi Víctor Haedo – Edificio Centro Financiero
Teléfono: (+595 21) 448 503/8 R.A. Fax Secretaría General: (+595 21) 452 306
www.petropar.gov.py

Ing. Silvio David López Rolón
Jefe Int. de Unidad Técnica - DTI
PETROPAR

		El dispositivo debe contar con la capacidad de crear un perfil de tráfico, con base al fuljo de datos recolectados durante un periodo especifico.	Exigido
		El dispositivo debe soportar interfaces en modo MDI/MDIX (Medium Dependent Interface).	Exigido
		El dispositivo debe tener de forma nativa recursos de detección y prevención de ataques de DoS y DDoS. Esta capacidad deve permitir el control de comunicaciones por mecanismos "Rate-based" para condiciones de Syn-Flood y control de conecciones simultaneas máximas para direcciones IP, CIDR.	Exigido
		El dispositivo debe soportar la creación de objetos por nombre ya sea por: network, puertos, Vlan, URL, filtros de aplicación y zonas de seguridad.	Exigido
		El dispositivo debe poder controlar las aplicaciones en cualquier puerto.	Exigido
		El dispositivo debe detectar mínimo 1700 aplicaciones y categorizarlas por riesgo y relevancia empresarial.	Exigido
		El dispositivo debe estar basado sobre firmas en vulnerabilidades permitiendo la detección de ataques desconocidos o variaciones de ataques conocidos.	Exigido
		El dispositivo debe controlar la detección de archivos a través de las acciones: Allow, Interfactive Block y Interactive Block with reset.	Exigido
		El dispositivo debe permitir la funcionalidad de gestión SNMP e integrarse a productos de red de terceros para proporcionar indicadores clave de estado operacional a grupos de operaciones de red y de operaciones de seguridad.	Exigido
		El dispositivo debe de proveer la opción de consulta, de un histórico de los eventos sucedidos en los equipos ofertados desde la consola principal, con el fin de realizar análisis forense.	Exigido
		El dispositivo debe proteger contra ataques sobre aplicaciones Web como: shell command injections, Server-site injection, cross-site scripting, directory traversal.	Exigido
		El dispositivo debe ser capaz de identificar todos los hosts que presenten un atributo o condición especifica de incumplimiento de la política.	Exigido
		El dispositivo debe contar con la capacidad de crear un perfil de tráfico, con base al fuljo de datos recolectados durante un periodo especifico.	Exigido
		El dispositivo debe ser capaz de reducir significativamente el esfuerzo del operador y la aceleración de respuesta a las amenazas por dar prioridad a las alertas de forma automática.	Exigido
		El dispositivo debe ser capaz de proporcionar de forma automática los adecuados controles permitiendo la protección el tráfico enviado a través de puertos de comunicación no estándares.	Exigido
		El dispositivo deberá ser capaz de crear perfiles de cumplimiento con alguna normativa de seguridad para emitir una alarma cuando alguno de los servicios no permitidos por una normativa de seguridad sea utilizado en el segmento de red acotado por la normativa de seguridad.	Exigido
		El dispositivo debe ser capaz de esperar pasivamente la recopilación de información sobre los flujos de sesión para todos los hosts, incluyendo el tiempo inicio/fin, puertos, servicios y cantidad de datos.	Exigido
		El dispositivo deberá ser capaz de crear un mapa de flujo de tráfico entre host de la red, para guardar registro de la cantidad de tráfico entre los dispositivos de la red.	Exigido
		El dispositivo deberá ser capaz de detectar anomalías de tráfico en la red, en base a los patrones de tráfico identificados.	Exigido
		El dispositivo deberá permitir una integración automática para realizar un cambio de configuración o enviar información a módulos de terceros como: Scanners de vulnerabilidades; SIEM systems; Firewall; Routers; Switches.	Exigido
		El dispositivo deberá incluir un sistema de integración con directorio activo, del mismo fabricante, que provea las siguientes características:	Exigido
		a. Deberá permitir la integración con el directorio activo de la red para tener un mapeo de usuario e IP utilizada actualmente.	Exigido
		b. Deberá permitir tener la información de contacto de los usuarios que están siendo atacados.	Exigido
		c. Los eventos de seguridad reportados deberán mostrar el usuario que está generando o recibiendo el ataque y generar una alerta o tomar acciones en base al perfil del usuario en cuestión.	Exigido
		d. Deberá de poder generar un mapa de eventos de seguridad generados/recibidos por usuario.	Exigido
		e. Deberá de poder generar un mapa de tráfico generado/recibido por usuario.	Exigido

Ing. Silvio David López Rolón
Jefe Int. de Unidad Técnica - DTI

Ing. Pedro Gustavo Duarte
Director Int. DTI-PETROPAR

Oficina Central, Asunción, Chile 753 casi Víctor Haedo - Edificio Centro Financiero
Teléfono: (+595 21) 448 503/8 R.A. Fax Secretaría General: (+595 21) 452 306
www.petropar.gov.py

ADENDA Nº 03

LICITACIÓN PÚBLICA NACIONAL POR EL PROCEDIMIENTO DE SUBASTA A LA BAJA ELECTRÓNICA Nº 19/2018 PARA LA "ADQUISICIÓN DE EQUIPOS DE NETWORKING, MATERIALES DE FIBRA ÓPTICA Y OTDR" ID Nº 350.558

		f. Deberá ser capaz de mantener un mapa de los usuarios, IP actual, tipo de aplicación usada, y un historial de las IPS que ese usuario ha usado en el tiempo.	Exigido
		El dispositivo deberá de soportar syslog para eventos de filtrado y errores del sistema.	Exigido
		El dispositivo deberá de soportar la capacidad de generar alertas a través de: syslog, correo electrónico y SNMP.	Exigido
		El dispositivo debe soporta creación de ACL (Access Control List – Lista de Control de Acceso), especificando las direcciones IP que se les permite comunicarse con la dirección.	Exigido
		El dispositivo deberá tener una funcionalidad de "packet level" para realizar actividades de análisis forense.	Exigido
		El dispositivo debe tener la capacidad de creación de reglas basadas en: segmento monitoreado (puerto del appliance); dirección IP origen y destino; puertos origen y destino.	Exigido
		El dispositivo deberá soportar el remontaje de paquetes TCP fragmentados.	Exigido
		El dispositivo deberá soportar la búsqueda de firmas por nombre a través de la interfaz gráfica.	Exigido
		El dispositivo deberá soportar la desfragmentación de paquetes IP fragmentados y/o coincidentes.	Exigido
		El dispositivo debe de soportar inspección de tráfico en GRE.	Exigido
		El dispositivo deber contar con cobertura de filtros que protejan las vulnerabilidades de internet Explorer.	Exigido
		El dispositivo debe soportar la creación de reglas rápidas (Fast-path) que permita el envío de trafico directamente a través del dispositivo sin inspección.	Exigido
		El dispositivo debe soportar geolocalización; permitiendo obtener al menos la siguiente información: país, código postal, longitud, latitud, zona horaria.	Exigido
		El dispositivo debe permitir bloquear tráfico por geolocalización; ya sea por país o continente	Exigido
8	**URL Filtering**	Deberá contar con funcionalidad de filtro de URL.	Exigido
		Deberá soportar filtro URL basado en categorías	Exigido
		Deberá incluir al menos 80 categorías.	Exigido
		Deberá contar con una base de URL categorizadas de al menos 250 millones de sitios.	Exigido
		El Filtro de URL, deberá incluir funcionalidad que permita categorizar, así mismo, deberá analizar la reputación y el nivel de riesgos de los sitios visitados.	Exigido
		Deberá permitir inspección SSL, desencriptando tráfico HTTPS.	Exigido
9	**Análisis y Gestión**	La solución deberá incluir una herramienta de análisis y gestión según los siguientes requerimientos:	Exigido
		Administrar, correlacionar y priorizar eventos permitiendo; seguimiento en tiempo real de ataques o usos indebidos, tratamiento de eventos, creación automática de incidentes y excepciones, identificación de falsos positivos y la integración de eventos generados por dispositivos de terceros.	Exigido
		El sistema de administración centralizada debe tener la capacidad de desempeñar el análisis automatizado de impactos al correlacionar eventos IDS & IPS con el estado de la vulnerabilidad, la información del sistema operativo para determinar la posibilidad de éxito contra el objetivo.	Exigido
		El sistema de administración centralizada debe soportar la integración de productos de análisis de vulnerabilidades.	Exigido
		El sistema de administración centralizada debe soportar ajustes dinámicos de severidad en los ataques como resultado de la correlación de eventos.	Exigido
		El sistema de administración centralizada debe soportar la correlación de datos de vulnerabilidades, soporte a la correlación de patrones de ataques (múltiples eventos identificados como un único ataque).	Exigido
		El sistema de administración centralizada debe soportar reportes en formato texto y gráfico, con exportación en los formatos HTML, PDF e CSV.	Exigido
		El sistema de administración centralizada debe soportar la correlación de patrones de ataques (múltiples eventos identificados como un único ataque). Esto se refiere a que el equipo ofertado sea lo suficientemente inteligente para que pueda identificar eventos similares y los pueda relacionar como una sola anomalía, con aplicaciones del mismo fabricante.	Exigido
		El sistema de administración centralizada debe soportar consola remota con interfaz gráfica, consola remota Web en formato gráfico para el uso en modo de consulta, perfiles diferentes de usuarios.	Exigido

Ing. Pedro Gustavo Duarte
Director Int. DTI-PETROPAR

Ing. Silvio David López Roldán
Jefe Int. de Informática - DTI
PETROPAR

ADENDA Nº 03

LICITACIÓN PÚBLICA NACIONAL POR EL PROCEDIMIENTO DE SUBASTA A LA BAJA ELECTRÓNICA N° 19/2018 PARA LA "ADQUISICIÓN DE EQUIPOS DE NETWORKING, MATERIALES DE FIBRA ÓPTICA Y OTDR" ID N° 350.558

		El sistema de administración debe proveer la capacidad de visualizar las versiones de software y hardware de los equipos desde la consola principal y desde cada equipo por separado.	Exigido
		El sistema de administración centralizada debe soportar auditoria de las actividades de los usuarios.	Exigido
		El sistema de administración centralizada debe ser soportar poder ejecutarse en la versión de Vmware ESX/ESXi 3.5, 4.1 o superior.	Exigido
		El sistema de administración centralizada debe soportar actualización remota de los dispositivos tanto a nivel de hardware como de software.	Exigido
		El sistema de administración centralizada deberá permitir reportes detallados sobre lo siguiente: Nuevos host en la red; Vulnerabilidades existentes en la red; Servicios existentes en la red; anomalías de tráfico; Perfiles de tráfico; Sistemas operativos existentes en la red; Vulnerabilidades por cada host; Uso de tráfico por aplicación; Uso de tráfico por usuario; Uso de tráfico por host; Uso de tráfico por servicio; Eventos de seguridad por impacto en la red; Eventos de seguridad por criticidad de la vulnerabilidad.	Exigido
		El sistema de administración centralizada debe generar reportes en forma automática y enviarlos a una cuenta de correo electrónico para agilizar el proceso de análisis.	Exigido
		El sistema de administración centralizada debe contar con información detallada de ayuda para firmas. Cuando aparece una amenaza en la pantalla de la consola, el usuario debe tener la capacidad de visualizar información detallada acerca de la vulnerabilidad hacia la cual está dirigida la amenaza. Ello debe incluir una explicación de la vulnerabilidad, de los sistemas que pueden verse afectados, de información sobre falsos positivos, de información CVE, de explicaciones para parcheo o restauración y de URLs.	Exigido
		Deberá contar con herramientas integradas para tener visibilidad en forma de graficas en tiempo real e historial sobre el estado de salud, como mínimo de: CPU, interfaces, memoria, performance, disco, temperatura.	Exigido
		El sistema de administración centralizada debe tener la posibilidad de realizar análisis de inteligencia con facilidad.; incluyendo análisis basados en el contexto lógico del evento siendo evaluado. Entre los ejemplos se encuentran el retorno de todos los eventos desde el IP fuente elegido, el retorno de todas las vulnerabilidades asociadas con el puerto objetivo elegido, etc. Deben incluirse mecanismos capaces de desempeñar los ejemplos anteriores, y más. El usuario debe poder navegar y analizar, con facilidad, más de un millón de eventos al día.	Exigido
		El sistema de administración centralizada debe contar con soporte para la personalización de la pantalla de la consola. El usuario debe poder personalizar el contenido de la pantalla y los filtros con base en la dirección IP, rango de red, protocolo, tipo de evento, nombre de evento y servicio, para después guardar dicha configuración bajo nombres personalizados para su uso futuro.	Exigido
		El sistema de administración centralizada deberá ser capaz de integrarse con tecnologías de seguridad de terceros (Firewall, IPS Wireless, Switches, Routers etc) para generar acciones yo configuraciones necesarias para remediación de incidentes de seguridad.	Exigido
		El sistema de administración centralizada debe incluir reportes previamente definidos. La consola debe tener la capacidad de producir métricas gráficas y reportes de comparación con base en segmentos de tiempo. La información en los reportes debe estar disponible para un grupo de activos, para todo un sitio o para toda una empresa. Asimismo, el usuario debe poder llegar hasta estos reportes para visualizar los detalles pertinentes.	Exigido
		El sistema de administración centralizada debe proporcionar la capacidad de activar, desactiva y modificar las reglas individuales, por grupos o categoría de normas.	Exigido
		El sistema de administración centralizada debe proporcionar la capacidad de seleccionar informes pre-definidos y la posibilidad completa de personalización y generación de nuevos reportes.	Exigido
		El sistema de administración centralizada debe incluir las capacidades de flujo de trabajo para la gestión del ciclo de vida completo de un evento, desde la notificación inicial a través de cualquier respuesta y resolución de las actividades que sean necesarias.	Exigido
		El sistema de administración centralizada debe ser compatible con múltiples opciones para responder automáticamente a las amenazas detectas ya sea por alertas automatizados y/o remediación del firewall.	Exigido
		El sistema de administración centralizada debe soporta roles múltiples para el usuario dentro de los cuales deben estar: Administrator; Maintenance	Exigido

Ing. Pedro Gustavo Duarte
Director Int. DTI-PETROPAR

Oficina Central, Asunción, Chile 753 casi Víctor Haedo - Edificio Centro Financiero
Teléfono: (+595 21) 448 503/8 R.A. Fax Secretaría General: (+595 21) 452 306
www.petropar.gov.py

Ing. Silvio David López Roión
Jefe Int. de Unidad Técnica - DTI
PETROPAR

		User; Policy & Response Administrator; Intrusio Event Analyst; Real-Time Network Awareness. Estos roles deben dar lugar o prevenir el uso de ciertos privilegios de parte del usuario. Los privilegios deben incluir una gama de funciones administrativas de reporte o visualización.	
		El sistema de administración centralizada debe incluir un mecanismo de integración, en forma de APIs abiertas y / o interfaces estándar, para permitir una respuesta automática a las amenazas de los componentes externos y las aplicaciones de recuperación, tales como routers, firewalls, etc.	Exigido
		El sistema de administración centralizada debe incluir un mecanismo de integración, en forma de APIs abiertas y / o interfaces estándar, para permitir a los eventos y registro de datos sean compartidos con la red externa y las aplicaciones de gestión de seguridad, tales como sistemas de ticketing, SIEM, plataformas de sistemas de gestión y registro de las herramientas de gestión.	Exigido
		El sistema de administración centralizada debe incluir un mecanismo de integración, en forma de APIs abiertas y / o interfaces estándar, para recibir información de fuentes externas, como bases de datos de gestión de configuración, herramientas de administración de vulnerabilidades y sistemas de gestión de parches, de correlación de amenazas y política de TI propósitos de cumplimiento.	Exigido
		El sistema de administración centralizada debe incluir un mecanismo de integración, en forma de APIs abiertas y / o interfaces estándar, para exportar información SNMP para sistemas de gestión de la red.	Exigido
		El sistema de administración centralizada debe deberá ser capaz de agregar a su base de datos de conocimiento los resultados de un análisis de vulnerabilidades realizado por un analizador de vulnerabilidades (escaner) incluido en el mismo módulo de correlación.	Exigido
		El sistema de administración centralizada deberá ser capaz de hacer recomendación de afinación (tuning) de políticas en base a la información aprendida de la red, mostrando un registro de las reglas recomendadas.	Exigido
		El sistema de administración centralizada deberá ser capaz de crear un perfil de tráfico de la red para crear baselines del tráfico existente en la red.	Exigido
		El sistema de administración centralizada deberá poder crear perfiles de tráfico con reglas específicas para monitorear el tráfico entre dos hosts de la red y crear una alarma cuando cierto umbral sea rebasado.	Exigido
		El sistema de administración centralizada deberá ser capaz de detectar anomalías de tráfico en la red, en base a los patrones de tráfico identificados.	Exigido
		El sistema de administración debe soportar la funcionalidad de exportar (Export) e importar (Import) políticas, dashboard, búsquedas, workflows.	Exigido
		El sistema de administración centralizada deberá ser capaz de crear perfiles de cumplimiento con alguna normativa de seguridad, para emitir una alarma cuando algún servicio no permitido por una normativa de seguridad sea utilizado en el segmento de red acotado por la normativa de seguridad.	Exigido
		El sistema de administración centralizada deberá ser capaz de realizar un escaneo de vulnerabilidades a los hosts de la red para validar la existencia de las vulnerabilidades o como una respuesta a un incidente, por ejemplo al detectar un nuevo.	Exigido
		El sistema de administración centralizada deberá permitir la integración con el directorio activo de la red para tener un mapeo de usuario e IP utilizada actualmente.	Exigido
		El sistema de administración centralizada deberá permitir tener la información de contacto de los usuarios que están siendo atacados.	Exigido
		El sistema de administración centralizada deberá a través de los eventos de seguridad detectados mostrar el usuario que está generando o recibiendo el ataque y generar una alerta o tomar acciones en base al perfil del usuario en cuestión.	Exigido
		El sistema de administración centralizada deberá de poder generar un mapa de eventos de seguridad generados/recibidos por usuario.	Exigido
		El sistema de administración centralizada deberá de poder generar un mapa de tráfico generado/recibido por usuario.	Exigido
		El sistema de administración centralizada deberá ser capaz de mantener un mapa de los usuarios, IP actual, tipo de aplicación usada, y un historial de las direcciones IP que ese usuario ha usado en el tiempo.	Exigido
		El sistema de administración centralizada deberá soportar la funcionalidad de calendarizar tareas administrativas tal como: ejecutar respaldos, aplicación de políticas, generación de reportes, ejecutar scaneos, aplicar recomendaciones en la política, importar actualizaciones.	Exigido

Ing. Pedro Gustavo Duarte
Director Int. DTI-PETROPAR

Ing. Silvio David López Rolón
Jefe Int. de Unidad Técnica - DTI
PETROPAR

Oficina Central, Asunción, Chile 753 casi Víctor Haedo - Edificio Centro Financiero
Teléfono: (+595 21) 448 503/8 R.A. Fax Secretaría General: (+595 21) 452 306
www.petropar.gov.py

ADENDA Nº 03

LICITACIÓN PÚBLICA NACIONAL POR EL PROCEDIMIENTO DE SUBASTA A LA BAJA ELECTRÓNICA N° 19/2018 PARA LA "ADQUISICIÓN DE EQUIPOS DE NETWORKING, MATERIALES DE FIBRA ÓPTICA Y OTDR" ID N° 350.558

		El sistema de administración centralizada deberá soportar la funcionalidad para la creación de un ciclo de vida de un incidente, permitiendo el cambio del estado del incidente.	Exigido
		El sistema de administración centralizada deberá permitir la generación a través de un documento en formato pdf la configuración de la política aplicada.	Exigido
10	**Garantía**	por defectos de fábrica, Soporte de atención de hardware, repuestos y Mano de Obra, traslado de los equipos de la oficina del cliente al proveedor y viceversa a cargo del oferente: 24 meses.	Exigido
		Todos los equipos deben contar con certificados de calidad de fabricación ISO 9001:2008 o equivalente.	Exigido
11	**Plazo para remplazo de bienes defectuosos**	Corrección o reparación de cualquier defecto o sustitución del suministro no aceptado a completa satisfacción de la contratante en el plazo de 8 horas como máximo contados a partir del reclamo por escrito efectuado por la contratante.	Exigido
		La contratante podrá disponer de lo suministrado hasta la reposición por parte del Proveedor de la nueva partida que remplace a la no aceptada	Exigido

<u>Observación:</u> LOS DEMAS PUNTOS DEL PLIEGO DE BASES Y CONDICIONES NO CITADOS EN ESTA ADENDA PERMANECEN INVARIABLES.

Abg. Félix Chávez
Director
Dirección Operativa de Contrataciones

Ing. Silvio David López Rolón
Jefe Int. de Unidad Técnica - DTI
PETROPAR

Ing. Pedro Gustavo Duarte
Director Int. DTI-PETROPAR

Oficina Central, Asunción, Chile 753 casi Víctor Haedo - Edificio Centro Financiero
Teléfono: (+595 21) 448 503/8 R.A. Fax Secretaría General: (+595 21) 452 306
www.petropar.gov.py