ADENDA N° 3

LICITACIÓN POR CONCURSO DE OFERTAS (LCO) Nº 02/2018 – "ADQUISICIÓN DE EQUIPOS, INSUMOS, SOFTWARE INFORMÁTICOS Y MUEBLES"
ID N° 349.034

Asunción, 02 de julio 2018

Señores
OFERENTES
Presente

La Unidad Operativa de Contrataciones de la Secretaría Nacional de Turismo, procede a modificar precios de los ítems: **N° 9 y 10 del Lote N° 4**; **N° 1 del Lote N° 5; N° 2 del** Lote N° 6. Se han agregado los **lotes N° 7 y 8** en la planilla de precios en el **Sistema de Información de las Contrataciones Públicas- SICP.** Asimismo, se procede a realizar enmiendas en el Pliego de Bases y Condiciones quedando redactado de la siguiente manera:

SECCIÓN III. SUMINISTROS REQUERIDOS

1. Especificaciones Técnicas

ADQUISICIÓN DE INSUMOS, SOFTWARE Y EQUIPOS INFORMÁTICOS

Lote N° 1 - Notebooks de gama alta

ÍTEM Nº	Descripción del Equipo	Detalles técnicos	Exigido
1	Notebooks de gama alta	Ver Plantillas en el SICP. Este ítem cuenta con atributos estándar en la plantilla del Sistema de Información de Contrataciones Públicas (SICP), las especificaciones técnicas del mismo se encuentran en dicho sistema, esto en cumplimiento a lo dispuesto en la Res. DNCP N° 1991/2017.-	Exigido

Lote N° 2 - Notebooks de gama media

ÍTEM Nº	Descripción del Equipo	Detalles técnicos	Exigido
1	Notebooks de gama media	Ver Plantillas en el SICP. Este ítem cuenta con atributos estándar en la plantilla del Sistema de Información de Contrataciones Públicas (SICP), las especificaciones técnicas del mismo se encuentran en dicho sistema, esto en cumplimiento a lo dispuesto en la Res. DNCP N° 1991/2017.-	Exigido

Lote N° 3 - Equipos

Misión: Somos un órgano orientador, promotor, facilitador y regulador del desarrollo del turismo en Paraguay, en beneficio de visitantes y ciudadanía en general.
Tembipota: Ore niko temimoĩmby romohesakã, romoherakuã, rombohape ha rogueroguatáva umi mba'e ikatúva ojehechauka Paraguáipe, ovisitáva ha mayma tetãygua rayhupápe.

ÍTEM Nº	Descripción del Equipo	Detalles técnicos		Exigido
1	UPS de 1000 VA	Potencia nominal	1000 VA	1000 V
		voltaje	230 V	230 V
		Frecuencia	50/60 Hz	Exigido 50/60 H
		topología	Línea interactiva	Línea i
		Configuración	Torre	Torre
2	Router WIFI - VPN	Estándares y Protocolos	IEEE 802.11b/g/n, 802.3, 802.3u, 802.3ab	Exigido
		TCP/IP, DHCP, ICMP, NAT, PPPoE, SNTP, HTTP, DNS, IPSec, PPTP, L2TP		Exigido
		Interfaz	1 puerto WAN Gigabit	Exigido
		3 puertos LAN Gigabit		Exigido
		1 puerto WAN/LAN Gigabit		Exigido
		Medios de Red	10BASE-T: cable UTP categoría 3, 4, 5 (Máx 100m)	Exigido
		100BASE-TX: cable UTP categoría 5, 5E (Máx 100m)		Exigido
		1000BASE-T: cable UTP categoría 5, 5E (Máx 100m)		Exigido
		Cantidad de Ventiladores	Sin ventilador	Exigido
		Botones	Power On/Off, Wi-Fi On/Off, Reset	Exigido
		Fuente de Alimentación	Fuente de alimentación externa (salida: 12VDC/1.0A)	Exigido
		Antenas	2 antenas desmontables de 5dBi	Exigido
		Flash	8MB	Exigido
		DRAM	64MB (DDRII)	Exigido
		LED	PWR, SYS, WLAN, WAN, WAN/LAN, LAN	Exigido
		Dimensiones	8.2 x 5.0 x 1.0 in.(209 x 126 x 26 mm)	Exigido
		RENDIMIENTO		Exigido
		Sesiones Concurrentes	10000	Exigido
		Rendimiento NAT	160Mbps	Exigido
		Rendimiento VPN IPsec	38Mbps	Exigido
		CARACTERÍSTICAS INALÁMBRICAS		Exigido
		Frecuencia	2.4-2.4835 GHz	Exigido
		Potencia de Transmisión	<20dBm (EIRP)	Exigido
		Funciones Inalámbricas	Radio wireless on/off, bridge WDS, WMM, Estadísticas	Exigido

Palma 468 haimete 14 de Mayo, Paraguay - Pumbyry: (595 21) 441-530 -
infosenatur@senatur.gov.py - www.paraguay.travel

			inalámbricas	
		Seguridad Inalámbrica	WEP, WPA/WPA2, WPA-PSK/WPA2-PSK	Exigido
		Red de Invitados	Sí	Exigido
		Multi-SSID	Hasta 8 SSIDs	Exigido
		FUNCIONES BÁSICAS		Exigido
		Tipo de conexión WAN	IP dinámica, IP estática, PPPoE, PPTP, L2TP, Acceso dual, BigPond	Exigido
		DHCP	Servidor/Cliente DHCP	Exigido
		Reserva DHCP		Exigido
		Clonado MAC	Modifica la dirección MAC WAN/LAN	Exigido
		Configuración del Switch	Port Mirror	Exigido
		Control de velocidad		Exigido
		Configuración de puertos		Exigido
		VLAN por puerto		Exigido
		IPTV	IGMP Proxy	Exigido
		IGMP Snooping		Exigido
		FUNCIONES AVANZADAS		Exigido
		Balanceo de Carga	Balance de carga inteligente	Exigido
		Políticas de Routing		Exigido
		Vinculación de protocolos		Exigido
		Backup de enlaces (Timing, Failover)		Exigido
		Detección online		Exigido
		NAT	NAT One-to-One	Exigido
		NAT Multi-redes		Exigido
		Virtual Server		Exigido
		Port Triggering		Exigido
		UPnP		Exigido
		FTP/H.323/SIP/IPSec/PPTP ALG		Exigido
		Routing	Enrutamiento estático	Exigido
		Enrutamiento dinámico (RIP v1/v2)		Exigido
		Modo Sistema	NAT, Sin NAT, Enrutamiento clásico	Exigido
		Control de Tráfico	Control de ancho de banda basadi en IP/puerto	Exigido
		Garantía & Limitación de ancho de banda		Exigido
		Políticas de programación temporal		Exigido
		Límite de sesiones basado en IP		Exigido

		VPN		Exigido
		VPN IPsec	30 túneles VPN IPSec	Exigido
		VPN IPSec LAN-to-LAN y Client-to-LAN		Exigido
		Modos de negociación Main, Aggressive		Exigido
		Algoritmos de encriptación DES, 3DES, AES128, AES192, AES256		Exigido
		Algoritmos de autenticación MD5, SHA1		Exigido
		Modos de gestión de claves Manual, IKE		Exigido
		NAT Traversal (NAT-T) IPSec		Exigido
		Dead Peer Detection (DPD)		Exigido
		Perfect Forward Secrecy (PFS)		Exigido
		VPN PPTP	8 túneles VPN PPTP	Exigido
		VPN PPTP Servidor/Cliente		Exigido
		PPTP con encriptación MPPE		Exigido
		VPN L2TP	8 túneles VPN L2TP	Exigido
		VPN L2TP Servidor/Cliente		Exigido
		L2TP sobre IPSec		Exigido
		VPN Pass-through	IPSec (ESP), PPTP, L2TP	Exigido
		SEGURIDAD		Exigido
		Control de Aplicación	IM, P2P, Web IM, Web SNS, Web Media Protocol/Proxy Blocking	Exigido
		Defensa contra Ataques	Defensa para TCP/UDP/ICMP Flood	Exigido
		Bloqueo de TCP Scan (Stealth FIN/Xmas/Null)		Exigido
		Bloqueo de Ping desde WAN		Exigido
		Filtrado	Filtro de MAC	Exigido
		Filtro de URL/Keywords		Exigido
		Filtro de contenido web (Java, ActiveX, Cookies)		Exigido
		Inspección ARP	Envío de paquetes GARP	Exigido
		Escaneo ARP por WAN/LAN		Exigido
		Asociación IP-MAC		Exigido
		GESTIÓN		Exigido
		Servicio	Servidor PPPoE	Exigido
		E-Bulletin		Exigido
		DNS Dinámico (Dyndns, No-IP, Peanuthull, Comexe)		Exigido
		Mantenimiento	Interfz de gestión basado en web	Exigido
		Gestión remota		Exigido
		Exporta & Importa configuración		Exigido

		Sincronización NTP		Exigido
		Soporte de Syslog		Exigido
3	**Router WIFI**	Interfaz	4 puertos 10/100 / 1000Mbps LAN, 1 10/100 / 1000Mbps puerto WAN	Exigido
		1 puerto USB 3.0 + 1 puerto USB 2.0		Exigido
		Botón	Botón WPS, botón de reinicio, inalámbrico de encendido / apagado, el LED de encendido / apagado, encendido / apagado Botón	Exigido
		Antena	4 antenas desmontables	Exigido
		Fuente de alimentación externa	12V / 5ª	Exigido
		Estándares inalámbricos: IEEE 802.11ac / n / a 5 GHz IEEE 802.11b / g / n de 2,4 GHz		Exigido
		Frecuencia: 2,4 GHz y 5 GHz		Exigido
		Tasa de señal	2167Mbps en 5 GHz, 2,4 GHz 1000 Mbps en	Exigido
		Funciones inalámbricas	Activar / Desactivar radio inalámbrica, WMM,	Exigido
		Seguridad inalámbrica	64/128-bit WEP, WPA / WPA2, WPA-PSK / WPA-PSK2	Exigido
		Poder de transmisión: FCC: <30 dBm		Exigido
		Calidad de servicio: WMM, Control de Ancho de Banda		Exigido
		Tipo de WAN	IP dinámica / estática IP / PPPoE /	Exigido
		PPTP (Acceso dual) / L2TP (Acceso dual) / Bigpond administración		Exigido
		Control de Acceso, Gestión Local, gestión remota		Exigido
		DHCP	Servidor, cliente, lista de clientes DHCP, Reserva Dirección, Port Forwarding, Servidor Virtual, la activación de puertos, UPnP, DMZ, DNS Dinámico DynDns, NO-IP Transferencia VPN PPTP, L2TP, IPSec VPN	Exigido

		Control de acceso: Control Parental, Control de Gestión Local,		Exigido
		Lista de ordenadores, acceso Programación, Gestión de Reglas protocolos		Exigido
		Es compatible con IPv4 e IPv6		Exigido
		Compartiendo USB: Soporte de Samba (almacenamiento) / Servidor FTP / Media Server /		Exigido
		Servidor de impresión		Exigido
		VPN IPSec: Soporta hasta 10 túneles VPN IPSec, servidor VPN PPTP, OpenVPN		Exigido
		Requisitos del sistema	Microsoft Windows 98, NT, 2000, XP, Vista ™ o Windows 7, 8, 8.1, 10, MAC OS, NetWare, UNIX o Linux	Exigido
		Internet Explorer 11, Firefox 12.0, Chrome 20.0, Safari 4.0, u otro navegador compatible con Java.		Exigido
4	**Disco Duro Externo**	Capacidad	2TB	Exigido
		Velocidad	7200 RPM	Exigido
5	**Fuente de energía**	Potencia	250W	Exigido
		Tipo	ATX	Exigido
6	**Teclado USB**	Idioma	Español	Exigido
7	**Mouse USB**	Optico con 3 botones		Exigido
8	**Mouse pad**	Mouse pad de goma		Exigido
9	**Memoria de 4GB**	Tipo DDR4 2133 MGz		Exigido
10	**Memoria de 4GB**	Tipo DDR3 1333 MGz		Exigido
11	**Memoria de 4GB para notebook**	Tipo DDR3 1333 MGz		Exigido
12	**Switch de 16 puertos administrables**	Tarjetas y puertos instalados	16 Puertos Ethernet 100/1000 Base-TX	Exigido
			4 Puertos GBE SFP	Exigido
			1 Puerto Local para administración desde consola ADMI	Exigido
		Velocidad	Capacidad de Procesamiento (Non Blocking), 10 Mbps	Exigido

		Normas Técnicas	Compatible con los estándares IEEE_802.3, IEEE_802.3u, IEEE_802.3x, IEEE_802.1p, IEEE_802.1Q, IEEE_802.1d, IEEE_802.3ad, IEEE_802.1x	Exigido
		Protocolos	Soporte a los siguientes protocolos y aplicaciones IP, ICMP, TCP, UDP, ART, SNMPV3, TFTP, BOOTP, TELNET, SGH, ICMP, HTTP, Dift Serv	Exigido
		Alimentación Eléctrica	Fuente para 200 a 240 V, 47 a 55 Hz, cables	Exigido
		Rango de Temperatura en Actividad	De 0º a 40º C	Exigido
		Accesorios	Todos los accesorios requeridos para entregar el equipo en perfecto estado de operación (software, patch cords, power cord, etc.)	Exigido
		Pach Core Adicional total 3	(LC – SC), con las siguientes características: seben ser multimodos, dúplex, 1,5 metros para interconexión en Rack de piso del Switch a un DIO	Exigido
		Configuración	La empresa se encargará de la configuración del equipo de comunicación de tal manera que sea funcional con los demás equipos instalados en la red local. El técnico deberá estar calificado y/o certificado para el caso	Exigido

		Instalación	Instalación del equipo de comunicación en el Rack a ser indicado por el personal del Dpto. de Informática	Exigido
		Garantía	El proveedor deberá entregar el equipo e insumos nuevos y con garantía de 2 años, con mantenimiento, suministro de partes, traslado del equipo de la oficina del cliente al proveedor y viceversa a cargo del proveedor	Exigido
13	**Switch de 24 puertos administrables**	Tarjetas y puertos instalados	24 Puertos Ethernet 100/1000 Base-TX	Exigido
			4 Puertos GBE SFP	Exigido
			1 Puerto Local para administración desde consola ADMI	Exigido
		Velocidad	Capacidad de Procesamiento (Non Blocking), 10 Mbps	Exigido
		Normas Técnicas	Compatible con los estándares IEEE_802.3, IEEE_802.3u, IEEE_802.3x, IEEE_802.1p, IEEE_802.1Q, IEEE_802.1d, IEEE_802.3ad, IEEE_802.1x	Exigido
		Protocolos	Soporte a los siguientes protocolos y aplicaciones IP, ICMP, TCP, UDP, ART, SNMPV3, TFTP, BOOTP, TELNET, SGH, ICMP, HTTP, Dift Serv	Exigido
		Alimentación Eléctrica	Fuente para 200 a 240 V, 47 a 55 Hz, cables	Exigido
		Rango de Temperatura en Actividad	De 0º a 40º C	Exigido

		Accesorios	Todos los accesorios requeridos para entregar el equipo en perfecto estado de operación (software, patch cords, power cord, etc.)	Exigido
		Pach Core Adicional total 3	(LC – SC), con las siguientes características: seben ser multimodos, dúplex, 1,5 metros para interconexión en Rack de piso del Switch a un DIO	Exigido
		Configuración	La empresa se encargará de la configuración del equipo de comunicación de tal manera que sea funcional con los demás equipos instalados en la red local. El técnico deberá estar calificado y/o certificado para el caso	Exigido
		Instalación	Instalación del equipo de comunicación en el Rack a ser indicado por el personal del Dpto. de Informática	Exigido
		Garantía	El proveedor deberá entregar el equipo e insumos nuevos y con garantía de 2 años, con mantenimiento, suministro de partes, traslado del equipo de la oficina del cliente al proveedor y viceversa a cargo del proveedor	Exigido
14	**Switch de 48 puertos administrables**	Tarjetas y puertos instalados	48 Puertos Ethernet 100/1000 Base-TX	Exigido
			4 Puertos GBE SFP	Exigido
			1 Puerto Local para administración	Exigido

			desde consola ADMI	
		Velocidad	Capacidad de Procesamiento (Non Blocking), 10 Mbps	Exigido
		Normas Técnicas	Compatible con los estándares IEEE_802.3, IEEE_802.3u, IEEE_802.3x, IEEE_802.1p, IEEE_802.1Q, IEEE_802.1d, IEEE_802.3ad, IEEE_802.1x	Exigido
		Protocolos	Soporte a los siguientes protocolos y aplicaciones IP, ICMP, TCP, UDP, ART, SNMPV3, TFTP, BOOTP, TELNET, SGH, ICMP, HTTP, Dift Serv	Exigido
		Alimentación Eléctrica	Fuente para 200 a 240 V, 47 a 55 Hz, cables	Exigido
		Rango de Temperatura en Actividad	De 0º a 40º C	Exigido
		Accesorios	Todos los accesorios requeridos para entregar el equipo en perfecto estado de operación (software, patch cords, power cord, etc.)	Exigido
		Pach Core Adicional total 3	(LC – SC), con las siguientes características: seben ser multimodos, dúplex, 1,5 metros para interconexión en Rack de piso del Switch a un DIO	Exigido
		Configuración	La empresa se encargará de la configuración del equipo de comunicación de tal manera que sea funcional con los demás equipos instalados en la red local. El técnico deberá estar calificado y/o	Exigido

			certificado para el caso	
		Instalación	Instalación del equipo de comunicación en el Rack a ser indicado por el personal del Dpto. de Informática	Exigido
		Garantía	El proveedor deberá entregar el equipo e insumos nuevos y con garantía de 2 años, con mantenimiento, suministro de partes, traslado del equipo de la oficina del cliente al proveedor y viceversa a cargo del proveedor	Exigido
15	**Switch de 8 puertos administrables**	Tarjetas y puertos instalados	8 Puertos Ethernet 100/1000 Base-TX	Exigido
			4 Puertos GBE SFP	Exigido
			1 Puerto Local para administración desde consola ADMI	Exigido
		Velocidad	Capacidad de Procesamiento (Non Blocking), 10 Mbps	Exigido
		Normas Técnicas	Compatible con los estándares IEEE_802.3, IEEE_802.3u, IEEE_802.3x, IEEE_802.1p, IEEE_802.1Q, IEEE_802.1d, IEEE_802.3ad, IEEE_802.1x	Exigido
		Protocolos	Soporte a los siguientes protocolos y aplicaciones IP, ICMP, TCP, UDP, ART, SNMPV3, TFTP, BOOTP, TELNET, SGH, ICMP, HTTP, Dift Serv	Exigido

		Alimentación Eléctrica	Fuente para 200 a 240 V, 47 a 55 Hz, cables	Exigido
		Rango de Temperatura en Actividad	De 0º a 40º C	Exigido
		Accesorios	Todos los accesorios requeridos para entregar el equipo en perfecto estado de operación (software, patch cords, power cord, etc.)	Exigido
		Pach Core Adicional total 3	(LC – SC), con las siguientes características: seben ser multimodos, dúplex, 1,5 metros para interconexión en Rack de piso del Switch a un DIO	Exigido
		Configuración	La empresa se encargará de la configuración del equipo de comunicación de tal manera que sea funcional con los demás equipos instalados en la red local. El técnico deberá estar calificado y/o certificado para el caso	Exigido
		Instalación	Instalación del equipo de comunicación en el Rack a ser indicado por el personal del Dpto. de Informática	Exigido
		Garantía	El proveedor deberá entregar el equipo e insumos nuevos y con garantía de 2 años, con mantenimiento, suministro de partes, traslado del equipo de la oficina del cliente al proveedor y viceversa a cargo del proveedor	Exigido
16	**Disco Duro para PC de 1 TB**	Capacidad de 1 TB, Velocidad de 7200 RPM		Exigido

		Tipo de conexión	SATA	Exigido
17	**Disco Duro para notebook de 1 TB**	Capacidad de 1 TB, Velocidad de 7200 RPM		Exigido
		Tipo de conexión	SATA	Exigido
18	Lector grabador de CD/DVD para PC	Grabador de CD - DVD		Exigido
		Velocidad de escritura (Máx.): 16x DVD/40x CD		Exigido
		Velocidad de re-escritura (Máx.): 8x DVD/24x CD		Exigido
		Búfer: 4MB		Exigido
		Dispositivo Soportado: Doble capa - BD-ROM/DVD-RAM/±R/±RW		Exigido
		Interfaz: Serial ATA		Exigido
19	**Lector grabador de CD/DVD externo USB**	TIPOS DE TRANSFERENCIA: ESCRIBA		Exigido
		DVD-R	2x CLV, 4x PCAV, 8x CAV	Exigido
		DVD-R (DL)	2x CLV, 4x PCAV, 6x PCAV	Exigido
		M-DISC	4x	Exigido
		DVD-RAM	2x, 3x ZCLV, 5x PCAV (Ver.2.2) (12x Medios: No compatible)	Exigido
		DVD + R (DL)	2.4x CLV, 4x PCAV, 6x PCAV	Exigido
		DVD + R	2.4x CLV, 4x PCAV, 8x CAV	Exigido
		DVD + RW	2.4x, 3.3x CLV, 4x ZCLV, 8x ZCLV (8x disco de velocidad: 3.3x CLV, 8x ZCLV)	Exigido
		CD-R	10x CLV, 16x PCAV, 24x CAV	Exigido
		CD-RW	4x, 10xCLV, 16x ZCLV, 24x ZCLV (Alta velocidad: 10xCLV, Ultra velocidad: 24x ZCLV, Ultra velocidad más: 24x ZCLV)	Exigido
		DVD-RW	2x CLV, 4x, 6x ZCLV	Exigido
		TASAS DE TRANSFERENCIA: LEER		Exigido

		M-DISC	8x	Exigido
		DVD-Video (disco compatible con CSS)	4x máximo (capa única / doble)	Exigido
		CD-DA (DAE)	Máx. 24x	Exigido
		DVD-RAM (Ver.2.2)	6x	Exigido
		DVD-R / RW / ROM	8x / 8x / 8x máx.	Exigido
		DVD-R DL	8x máx.	Exigido
		DVD + R DL	8x máx.	Exigido
		DVD + R / + RW	8x / 8x máx.	Exigido
		TIEMPO DE ACCESO		Exigido
		DVD ROM	167 ms typ	Exigido
		CD ROM	139 ms typ	Exigido
		DVD-RAM (Ver.2.2)	203 ms typ	Exigido
		TASA SOSTENIDA		Exigido
		DVD ROM	11.08Mbytes / s (8x) máx.	Exigido
		CD ROM	3,600 kB / s (24x) máx.	Exigido
		TAMAÑO DEL BÚFER		Exigido
		TAMAÑO DEL BÚFER	0.75MB Función de prevención de subejecución incrustada	Exigido
		INTERFAZ DE HOST		Exigido
		Externo (Host)	USB 2.0 (480 Mbits / s)	Exigido
20	**Procesador para PC**	Cantidad de núcleos: 2		Exigido
		Cantidad de subprocesos: 4		Exigido
		Frecuencia básica del procesador: 3.20 GHz		Exigido
		Caché: 3 MB SmartCache		Exigido
		Velocidad del bus: 8 GT/s DMI3		Exigido
		Tamaño de memoria máximo: 64 GB		Exigido
		Tipos de memoria: DDR4-1866/2133, DDR3L-1333/1600		Exigido
		Cantidad máxima de canales de memoria: 2		Exigido
		Máximo de ancho de banda de memoria: 34,1 GB/s		Exigido
		Memoria máxima de video de gráficos: 64 GB		Exigido
		Salida de gráficos: eDP/DP/HDMI/DVI		Exigido
		Compatibilidad con 4K		Exigido
		Revisión de PCI Express: 3.0		Exigido
		Configuraciones de PCI Express : Up to 1x16, 2x8, 1x8+2x4		Exigido
		Cantidad máxima de líneas PCI Express: 16		Exigido
		Conjunto de instrucciones: 64-bit		Exigido
21	**Placa Madre**	Memoria hasta 64 GB 2133MHz DDR4		Exigido

		1x PCI-E 3.0 x16		Exigido
		2x PCI-E 3.0 x4 (en la ranura x8)		Exigido
		LAN GbE doble w		Exigido
		2x DP, 1 DVI-I, pantallas independientes 3x a través de gráficos, puerto VGA para BMC		Exigido
		4x SATA3 (6 Gbps); RAID 0, 1, 5, 10		Exigido
		E / S: 1x SATA DOM, 2x COM, TPM 1.2 cabecera, ALC 888S HD Audio		Exigido
		Soporta entrada de alimentación de 12V DC		Exigido
22	**Gaveta para disco SATA de 2,5" y 3,5"**	Tipo: Estación de acoplamiento		Exigido
		de entrada: 100-240V, 50 / 60Hz, 1.0A.		Exigido
		Salida: 12.0V-2000mA; 5.0V-3500mA.		Exigido
		Interfaz de salida: Mini USB 5 - pin; 2 puertos USB 2.0, 5 ranuras para tarjetas del lector, el puerto SATA-e; 3.5 "puerto IDE, SATA 1/2 puertos.		Exigido
		RANURA CF: 1 CF / CF2 / Extreme CF / CF Extreme3 / Ultra2 CF / HS CF / MD.		Exigido
		MS ranura: MS / MS Duo / MS PRO / MS PRO DUO / MS MagicGate / MS MagicGate PRO / MS DUO MagicGate / MS PRO DUO MagicGate / MS PRO / Extreme Extreme3MS PRO / Ultra2 MS PRO / HS MS MagicGate PRO / HS MS PRO DUO MagicGate / MS ROM / MS Select.		Exigido
		Ranura SD: SD / mini SD / SD Extreme / extremo 3 SD / Ultra 2 SD / MMC 1 / MMC 2 / MMC 4.0 / RS MMC / HS RS MMC / Micro SD (T-Flash).		Exigido
		RANURA X-memoria:. X-Memory		Exigido
		F-SLOT: TF memoria		Exigido
23	**Aspiradora/soplador a manual**	Potencia	600W	Exigido
		Velocidad Máx.	16000rpm	Exigido
		Longitud del Cable	2.5m	Exigido
		Incluye	Bolsa colectora de Polvo.	Exigido
24	**Caja de cable UPT cat 5e**	Caja de 300 mts.		Exigido
25	**Tarjeta de RED LAN PCI**	Estándares y protocolos	IEEE 802.3, 802.3u, 802.3x	Exigido
		CSMA / CD, TCP / IP, PCI Revisión 2.1 / 2.2		Exigido
		Interfaz		Exigido
		Puerto RJ45 de PCI de 100 / 1000 Mbps de 32 bits		Exigido
		Tasas de transferencia de datos	100/1000Mbps para modo Half-Duplex	Exigido
				Exigido
		Indicador LED	Link / Act	Exigido

		Control de flujo	Control de flujo IEEE 802.3x (Full-Duplex)	Exigido
26	**Adaptador de RED WIFI USB**	Interfaz	USB 2.0	Exigido
		Dimensiones	93.5 x 26 x 11mm (3.7 x 1.0 x 0.4 in.)	Exigido
		Tipo de Antena	Omnidirectional desmontable (RP-SMA)	Exigido
		Ganancia de Antena	3dBi	Exigido
				Exigido
27	**Pinza de red**	Crimpa terminales de redes telefónicas y de computadoras RJ11 , RJ12 y RJ45		Exigido
		Corta y pela cables eléctricos.		Exigido
		Cuerpo producido en chapas de acero.		Exigido
		Láminas en acero inoxidable.		Exigido
		Pintura electrostática.		Exigido
		Mangos con revestimiento especial.		Exigido
28	**Cautin soldador**	Potencia	70W	Exigido
		Tensión	220V	Exigido
		Debe ir acompañado de un rollo de estaño tipo 60/40 de 50 mts. O más		Exigido
29	**Pasta térmica**	Pasta térmica disipadora de calor para CPU		Exigido
30	**Cable de vídeo HDMI**	Cable HDMI Flat 1.4		Exigido
		De 3 metros como mínimo		
		Entrada y salida HDMI		Exigido
		Conector 19 pin		Exigido
		Cable reforzado		Exigido
		Transferencia de alta velocidad		Exigido
31	**Supresor de pico**	Doble lado		Exigido
		10 tomas		Exigido
		110/220 Volts		Exigido

32	**Conversor de HDMI a VGA**	Soporta resolución Full HD 1080p Salida 3.5 mm para conectar bocinas o un amplificador de audio	Exigido Exigido
33	**Auricular con micrófono**	SENSIBILIDAD: 104 dB POTENCIA: 30 mW IMPEDANCIA: 32 ohmios FRECUENCIA: 50- 10.000 Hz LONGITUD DEL CABLE: 1.2 Metros CONECTOR: 3,5 mm estéreo	Exigido Exigido Exigido Exigido Exigido Exigido
34	**Fuente de energía**	Potencia 650W Tipo ATX	Exigido
35	**Pen Drive 128 GB**	USB 3.0	Exigido
36	**Cable USB**	3 Metros como mínimo	Exigido
37	**Web Cam**	STREAMING FULL HD 1080P	Exigido
38	**Lector de tarjetas 5 en 1**	Multi lector USB de tarjetas	Exigido
39	**Bolsón para herramientas**	Multiples bolsilos internos y externos 53 cms como mínimo	Exigido Exigido
40	**Proyector Multimedia**	**Método de Proyección:** Montaje frontal techo / sobre mesa **Método de visualización:** Matriz activa TFT de polisilicona **Número de Pixeles:** 786,432 x 3LCD **Relación de Aspecto:** 4:3 Nativa, soporte a 16:9 y 16:10 **Resolución Nativa:** 1024 x 768 (XGA) **Tipo de Lámpara:** 245 W UHE **Vida Útil de la Lámpara:** 2500 (Normal) / 4000 (Modo Eco) **Relación de Proyección:** 1.38 – 2.24 **Corrección de Trapecio:** Vertical ±30 grados; Horizontal: ±30 grados **Relación de Contraste:** Hasta 3000:1 **Procesamiento del Color:** 10 bits **Reproducción del Color:** Hasta 1.07 billones de colores	Exigido Exigido Exigido Exigido Exigido Exigido Exigido Exigido Exigido Exigido Exigido Exigido

		Lente de Proyección:	Exigido
		Tipo: Zoom y enfoque manual	Exigido
		Número - F: 1.51 - 1.99	Exigido
		Longitud Focal: 18.2 – 29.2 mm	Exigido
		Relación de Zoom: 1.0 - 1.6 óptica	Exigido
		Control y Monitoreo Remoto: RJ-45 x 1	Exigido
		Conexiones: HDMI, VGA, AV	Exigido
		Accesorio: Bolsón para traslado del proyector	Exigido

Lote N°4 - Muebles para CIRDTUR

ÍTEMS N°	MUEBLES	ESPECIFICACIONES TÉCNICAS
1	**Módulo Fijo Simple**	1 módulo de metal estantería deslizante mecánico, fijo simple 2.20 metros de alto x 2.40 metros de ancho, de frente x 0.40 de fondo. Con 5 niveles de bandeja regulables de altura.
2	**Módulo Móvil**	1 módulo móvil de metal estantería deslizante mecánico doble de 2.20 metros de alto por 2.40 metros de ancho de frente x 0.80 metros de fondo, con 5 niveles de bandeja regulable de altura.
3	**Módulo Móvil**	1 modulo móvil de metal estantería deslizante mecánico, tapa de 2.20metros de alto x 2.40 metros de frente x 0.40 de fondo con 5 niveles de bandeja regulable de altura.
4	**Mobiliario para el área de lectura (Mesa)**	1 mesa de trabajo: de madera aglomerado tipo melamina de 0,90 x 1.60, altura 0.80 cm, dos patas en forma de T, tapa en placa melamina de 25 mm de espesor. Tapa en color nogal, patas metálicas en color negro. Se sugiere estructura tubular de metal color negro, de 25 x 2 mm. Soldada a perfil L 30 x 30 x 2 mm. apernada a cubierta**.**
5	**Mobiliario para el área de lectura (Sillas)**	6 sillas 4 patas, caño redondo de acero 7/8 pulgadas pintado en negro, en pintura epoxi Horneado. Sin posa brazos, tapizado símil cuero, color negro, espuma inyectada (estándar)

6	**Mostrador para la recepción**	1 mostrador para la recepción en, madera aglomerado tipo melamina, color nogal, 1.00 m por 0.40 cm por 0.90 cm de altura, con cajonera.
7	**Silla para el personal**	1 Silla giratoria estándar acolchada color negro símil cuero con tratamiento anti-corrosivo y anti-ferrugoso por fosfatización y acabamiento en pintura epoxica en color negro de alta resistencia a abrasivos e impactos, con 5 ruedas de doble giro, cuerpo 100% en nylon 6.6 de diámetro de la rueda con 50 mm y banda de rodaje con doble inyección, con acabamiento en poliuretano. . Eje central en acero SAE 1020.
8	**Escritorio**	1 Escritorio de madera aglomerado tipo melanina: Largo= 1.20 mts. Alto= 0.73 mts. Ancho= 0.60 mts. Con 3 cajones y pantalla cubre piernas, color nogal. Cajonera normal en Melanina de 25 mm, resistente a abrasivos, bordes rectos encabezados con tapacantos en polietileno con superficie visible y espesor de 2 mm de color negro, con cerradura.
9	**Vitrinas**	1 Vitrina de vidrio de 8 mm, madera /metal, 07.0 de ancho, 1,00 de largo, 0.90 de altura, bandejas de vidrio de 8 mm, con medidas de seguridad. Para la guarda de materiales selectos.
10	**Ficheros**	1 fichero, móvil y modulable, de metal, dotados de porta etiquetas, 4 gavetas, altura: 1,36cms. Largo: 0,47cms. Profundidad: 0,48cms, terminación esmalte sintético mate, color claro, con cerradura central**.**

Lote N° 5 - Computadoras de escritorio de gama alta para CIRDTUR

Ítem	Descripción del Equipo	Detalles técnicos	Exigido
1	**Computadoras de escritorio de gama media**	**Ver Plantillas en el SICP. Este ítem cuenta con atributos estándar en la plantilla del Sistema de Información de Contrataciones Públicas (SICP), las especificaciones técnicas del mismo se encuentran en dicho sistema, esto en cumplimiento a lo dispuesto en la Res. DNCP N° 1991/2017.-**	

Lote N° 6 - Equipos Informáticos para CIRDTUR

ÍTEM N° 1 - SERVIDOR		
Característica	**Detalle mínimo exigido**	
FACTOR DE FORMA	Rackeable de 2U máximo	
PROCESADOR	Número de procesadores instalados	Uno, con capacidad de poder agregar un segundo procesador de iguales características a futuro.
	Cantidad de núcleos	Ocho núcleos como mínimo
	Velocidad de reloj	2.1 GHz como mínimo
	Memoria Caché L3	20 MB como mínimo
ARQUITECTURA	Compatibilidad 64Bits	
MEMORIA	Capacidad instalada	128 GB como mínimo
	Cantidad de slots	24 slots como mínimo
	Tipo	RDIMM DDR4 2400 MHz como mínimo
	Tipos de Protección soportados	ECC, Memory Mirroring y Memory Sparing como mínimo
DISCO DURO	Capacidad solicitada	02 (dos) unidades de 300 GB, SAS de al menos 10.000 rpm, 12 Gbps o superior
		06 (seis) unidades de 600 GB, SAS de al menos 10.000 rpm, 12 Gbps o superior
	Tecnología y Capacidad de Ampliación	Hot Swap SAS o SATA de 2.5 pulgadas, con capacidad de albergar hasta 8 discos internos inicialmente, expandible al menos hasta 16 discos.
		Capacidad de soportar discos de estado sólido (SSD)
	Controlador	Controlador RAID con caché tipo flash de 2GB y con soporte de los niveles RAID 0, 1, 5, 6, 10, 50 y 60.
RANURAS DE EXPANSIÓN	3 Slots PCI-Express 3.0, con posibilidad de ampliar hasta 9 slots PCIe 3.0 como mínimo.	
MEDIO ÓPTICO	Capacidad de poder agregar a futuro una unidad DVD de manera interna.	
INTERFACES DE PERIFÉRICOS	Puertos USB: cuatro unidades (por lo menos dos de ellos de tecnología 3.0)	
	Gráfico DB-15: una unidad posterior y con capacidad de adicionar una delantera a futuro.	
	Serial: una unidad como mínimo	
	Soporte para agregar a futuro un adaptador de tarjetas SD y con capacidad de realizar espejado entre dichas tarjetas.	
GRÁFICOS	Puerto grafico de 16MB integrado con resolucion maxima de 1600x1200 a 75 Hz con 16 M colores.	
FUENTE DE ALIMENTACIÓN	Fuente de poder que no supere los 550 watts y sea cambiable en caliente, en configuración redundante. Certificación 80 PLUS Platinum o similar como mínimo	
COMUNICACIONES	Cuatro puertos Gigabit Ethernet RJ-45 integrados.	

Palma 468 haimete 14 de Mayo, Paraguay - Pumbyry: (595 21) 441-530 -
infosenatur@senatur.gov.py - www.paraguay.travel

ÍTEM N° 1 - SERVIDOR	
Característica	**Detalle mínimo exigido**
SISTEMA OPERATIVOS SOPORTADOS	Microsoft® Windows Server 2012 o superior
	Red Hat® Enterprise Linux® 6.7 x64 o superior
	SUSE Linux Enterprise Server 11 x64 SP4 o superior
	VMware® vSphere (ESXi) 5.5 U3 o superior
	Oracle VM 3.3 o superior
	Citrix XenServer 6.5 o superior
	Ubuntu 16.04 LTS o superior
SISTEMA OPERATIVO A SER INSTALADO	Window Server 2016
GARANTÍA ESCRITA	3 (tres años) On Site. El servicio de garantía deberá ser realizado por técnicos certificados del CAS (Centro Autorizado de Servicios) avalado por el Fabricante.
CARACTERÍSTICAS RAS	Diagnóstico de fallas de hardware en el equipo mediante LEDs frontales e internos.
	El equipo debe contar con análisis predictivo de fallas que cubra los siguientes componentes del sistema: procesador, VRM, memoria, discos, fuente de poder y ventiladores.

ÍTEM N° 2- SCANNER	
CARÁCTERÍSTICAS MÍNIMAS	El equipo ofertado debe ser de uso exclusivo para digitalización de documentos de gran capacidad y velocidad.
	No se admiten equipos multifuncionales. Se requiere que el equipo presente funcionalidades exclusivas para la digitalización de documentos.
TIPO DE ESCANER	Escáner plano o variante, con bandeja de alimentación automática
RESOLUCION DE CAPTURA	Soportado para A3, A4, A5, A6, B4, B5, B6, Carta, Legal, Ejecutivo (Horizontal y Vertical)
PROFUNDIDAD DE COLOR	entrada: 48 Bits Color / 16 Bits Monocromo, salida: 24 Bits Color / 8 Bits Monocromo o similares características
VISOR DE TRABAJO DE DIGITALIZACION	Requerido
VELOCIDAD DE DIGITALIZACION	Monocromo: 100 imagen/min. - Color: 100 imagen/min. medido con tamaño: A4 , resolución: 200 / 300 ppp, Monocromo: 100 páginas/minuto - Color: 100 páginas/minuto medido con tamaño: A4 , resolución: 200 / 300 ppp o características mínimas similares
FIABILIDAD DE CARGA DE TRABAJO DIARIA	Superior a 20.000 páginas diarias

Palma 468 haimete 14 de Mayo, Paraguay - Pumbyry: (595 21) 441-530 -
infosenatur@senatur.gov.py - www.paraguay.travel

FUENTE DE ALIMENTACIÓN DE DOCUMENTOS	500 páginas o superior
ESCANEADO DOBLE	Requerido
FUNCIONES BÁSICAS REQUERIDAS	Saltar páginas vacías, Ajustes de escaneado predefinidos, División automática del área, Corrección automática de posición inclinada, Reconocimiento automático multi-documento, Reconocimiento automático de blanco-negro/color, Salida de imagen dual (solo para Windows), Rotación automática, Mejora del texto, Mejora de márgenes, Máscara de enfoque, Destramado, Corrección de encuadernación, Creación automática de carpetas, Reconocimiento de códigos de barras, Compatible con zona OCR-A y B, Separación de tareas manual / automática. Se aceptan características similares.
FORMATOS DE SALIDA	JPEG, TIFF, TIFF múltiple, PDF, PDF / lote, PDF con opción de búsqueda, PDF seguro
FUNCION DE COMPRESION	No excluyente
FUNCIONALIDAD INTEGRADA	FTP, Carpetas de Red, Correo Electrónico requeridos
CONECTIVIDAD	• USB 2.0 o superior requerido • Interfaz de Red 100/1000 requerido
VOLTAJE	CA 100 V – 240 V
COMPATIBILIDAD	• Windows 7 x64 • Windows 8 x64 • Windows 10 x64 • Windows Server 2008 o superior x64 • Linux x64
ACCESORIOS	• Equipo, Cable de alimentación, Instrucciones de instalación, Software (CD), Cable USB, Certificado de garantía • Bandeja de documentos • Software de manipulación de documentos propio del fabricante
GARANTIA	Escrita por el fabricante, con representación en el país y soporte técnico.

ÍTEM N°3 - Switch de 16 puertos administrables	
Caracteristicas Generales	
Capas	Switch de capa 2 minimo
Interfaces en el chasís	Debe incluir mínimo: 4 1G/10G RJ45 Ports 12 1G/10G SFP+ Ports

	1 RJ45 Serial Console Port
Interfaces SFP +	Incluir al menos: 12 Modulos SFP+
Rendimiento	Al menos: Tasa de envio de al menos 238,10 Mpps. Capacidad de conmutación: 320Gbps. El equipo debe ser no-bloqueante a 160 Gbps
	Administración y Monitoreo
Consola	Al menos un (1) interfaz serial RJ45. los equipos deben ser administrados desde una unica consola

Acceso y configuración	Al menos vía: - Línea serial de comandos (CLI) para recuperación de emergencia. Configuración completa vía: - HTTP - HTTPs - SSL
Protocolos	Al menos: SNMP
Mirroring	Captura de tráfico de entrada y salida con el fin de ser analizado, enviándolo a un puerto local o remoto
	Requerimientos L2
MAC addresstable	16k direcciones MAC
VLANs Tramas	Al menos: - 802.1Q Maximo 255 VLANs simultáneas Soporte de tramas de hasta 8 kbytes.
Protocolos y Estándares	Al menos: IEEE 802.1Q. IEEE 802.1w.
	IEEE 802.1x Radius VLAN
Link Aggregation	Al menos: LACP
Supresión de tormentas	Limitación de tráfico de tormentas broadcast, multicast y unicast

	Hardware y Energía
Montaje	Debe traer todos los accesorios para montaje y operación en rack estándar, 1U maximo
Alimentación eléctrica	Soporte: - 100 VAC a 240 VAC - 50 Hz a 60 Hz.

Palma 468 haimete 14 de Mayo, Paraguay - Pumbyry: (595 21) 441-530 -
infosenatur@senatur.gov.py - www.paraguay.travel

Certificaciones	CE, FCC, IC
	Garantía y Servicio
Garantía de fábrica	Al menos 1 año de Garantía emitido por el fabricante
INSTALACION, CONFIGURACION Y GARANTÍA	El oferente deberá entregar, instalar y configurar el equipo de acuerdo a las necesidades de la institución
	El oferente se compromete a efectuar la implementación de
	la solución llave en mano encargándose de la interoperabilidad de esta solución con los equipos existentes en el cliente.

Lote N° 7 - Licencias para SENATUR

	ÍTEM 1 – Cal de Windows
CAL de Windows	WinSvrCAL 2016 OLP NL Gov UsrCAL
	ÍTEM 2 - CAL de Exchange
CAL de Exchange	ExchgStdCAL 2016 OLP NL Gov UsrCAL

ÍTEM 3- SOFTWARE ANTIVIRUS PARA COMPUTADORA	
Capacidad Requerida	**Exigido**
Consola de administración centralizada	SI
Protección web	SI
Reputación de descargas	SI
Control web / bloqueo de URL basado en categorías	SI
Control de periféricos (p. ej. USB)	SI
Restricción de aplicaciones	SI
Firewall	SI
Escaneado de archivos anti-malware	SI
Protección activa	SI
Análisis de comportamiento previo a la ejecución (HIPS)	SI
Bloqueo de aplicaciones no deseadas	SI
Análisis de comportamiento en tiempo de ejecución (HIPS)	SI
Eliminación de malware automatizada	SI

ÍTEM 4- SISTEMA DE SEGURIDAD PERIMETRAL FIREWALL DE PRÓXIMA GENERACIÓN NGFW
Calidad del Fabricante:
El fabricante del Firewall de Próxima Generación NGFW debe estar posicionado como líder del ultimo cuadrante Gartner en soluciones UTM (Junio de 2017)
Debe estar posicionado en el Cuadrante Superior al 90% de NSS Labs de 2017 para Firewalls de Próxima Generación (Next Generation Firewall). Este cuadrante evalúa las soluciones más favorables en su TCO en cuanto a relación entre

Palma 468 haimete 14 de Mayo, Paraguay - Pumbyry: (595 21) 441-530 -
infosenatur@senatur.gov.py - www.paraguay.travel

precio y eficiencia
Características del dispositivo:
El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo.
El dispositivo debe ser un equipo de propósito específico.
El dispositivo debe estar catalogado como un appliance de seguridad.
Debe proveer visibilidad y trazabilidad por usuario y/o aplicación.
El equipo debe analizar contenido cifrado (SSL) para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Antivirus e IPS.
Debe estar licenciado para operar en alta disponibilidad activo-pasivo y activo-activo.
Debe soportar alta disponibilidad activo-activo en modo transparente.
Capacidades de Detección y Prevención de Intrusos (IPS):
Protección de servidores por vulnerabilidades conocidas
El IPS deberá estar integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos.
La interfaz de administración del IPS deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio.
Debe actualizar de manera automática las firmas para el sistema de detección de intrusos.
Capacidades de Control de aplicaciones:
Visibilidad y Control del tráfico de la red por aplicaciones (Ejemplo: Permitir Facebook pero no sus juegos, Permitir Youtube pero no HD o subida de videos, Permitir Gmail pero no el chat o subir/bajar archivos, etc).
Controlar el ancho de banda por usuario y/o por aplicación.
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.
El listado de aplicaciones debe actualizarse periódicamente.
Capacidades de Prevención de Malware Avanzado:
Antivirus/Antimalware de red con cobertura para dispositivos fuera del control de la empresa (Tablets, Smartphones).
Debe ser capaz de analizar, establecer control de acceso y detener ataques y virus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.
El Antivirus deberá incluir capacidades de detección y bloqueo de tráfico spyware, adware y otros tipos de malware/grayware que pudieran circular por la red.
Debe permitir identificar y bloquear conexiones hacia servidores de Centro de Control de Botnets.
Debe permitir identificar o bloquear la descarga de archivos por extensión, tipo y nombre de archivo.
El dispositivo deberá de contar con protección contra ataques persistentes (ATP) integrada en el equipo.
Capacidades de Sandboxing en la Nube
El appliance de seguridad ofertado debe poder habilitar el servicio de Sandboxing en la nube para análisis y detonación de malware potencial
Capacidades de Filtrado de Navegación Web:
Prevención de infección por páginas de riesgo alto.
Bloqueo de páginas por URL con al menos 92 categorías
Filtrado de contenido basado en al menos 92 categorías en tiempo real. Facilidad para incorporar control de sitios a los

cuales naveguen los usuarios, mediante categorías.
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.
La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado (SSL).
Capacidades de Single Sign On:
Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto "Single-Sign-On"
El sistema propuesto deberá contar con la funcionalidad de autenticar usuarios de forma transparente con métodos como: Un portal cautivo vía web; a través del uso de un agente instalado en el dispositivo final; obteniendo la información del directorio activo.
Las tareas de sincronización con el servicio de directorio a utilizar pueden ser integradas en la misma solución o utilizando un dispositivo dedicado para tal fin.
Funcionalidad WAF Integrada
La solución de Firewall debe proveer funcionalidad de Web Application Firewall (WAF) incluida, sin necesidad de adquirir o destinar otro appliance/máquina virtual para proveer esta funcionalidad
Sincronización entre la red Perimetral y la red LAN
Funcionalidad de sincronización entre la red perimetral y los endpoints a nivel de red local para brindar una respuesta ante incidentes en segundos. El dispositivo deberá de contar una integración nativa con los clientes de EndPoint Protection para integrar el estado de salud de los clientes como un elemento más en las reglas de firewall, habilitando con esto la facilidad de poder delimitar el acceso a recursos sensibles como servidores o DMZ´s e Internet si el cliente llega a ser comprometido por algún malware y solo permitiendo el acceso una vez que el cliente vuelva a su estado no comprometido.
Funcionalidad de Protección de Correo entrante SMTP y MTA
Funcionalidad de Antivirus y Antispam del correo entrante via SMTP
Licenciamiento y actualizaciones:
El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo.
Reportes
La solución ofertada debe proveer reportes automáticos y personalizables tanto a nivel de estadísticas, indicadores, trafico, consumo, usuarios riesgosos, cumplimiento regulatorio, entre otros integrados en el mismo Firewall sin requerir ninguna plataforma o maquina adicional
La solución deberá poder ofrecer una plataforma adicional opcional de reportes ejecutivos adicionales a la solución de Firewall ofertada y debe ser del mismo fabricante que el firewall
Gestión Centralizada de Dispositivos:
La solución deberá poder integrarse con un appliance de gestión centralizado de firewalls, el cual deberá ser del mismo fabricante del sistema de Seguridad Perimetral.
Valores de desempeño y conectividad, como mínimo:
• Interfaces de red 1 GE: 8 incluidas con capacidad máxima de 16 interfaces 1 GE con módulos de expansión
• Internal Storage: Un (1) Disco de estado sólido SSD 180 GB
• Memoria RAM: 12 GB DDR4 ECC
• Throughput de Firewall: 33 Gbps

• Throughput de IPS (HTTP): 8.5 Gbps
• Throughput Control de Aplicaciones + IPS + Web Filter: 5.5 Gbps
• Throughput de NGFW: 5.5 Gbps
• Throughput de VPN IPSec: 3.2 Gbps
• Sesiones Concurrentes (TCP): 17.5 Millones
• Throughput Threat Protection: 6 Gbps
• Nuevas conexiones por segundo: 200.000
• 3 Años de garantía y soporte del fabricante. Con servicio telefónico 24x7 y con respuesta al día siguiente laborable de un técnico en las instalaciones, como mínimo.

1. Deberá ofrecer una configuración de zonas de seguridad tales como de LAN/DMZ/WAN asignadas a una o varias Interfaces.
2. Deberá de contar con soporte para tecnologías de monitoreo SNMP y Netflow, sin que esto incurra en una licencia adicional.
3. El dispositivo de ofrecer la Funcionalidad de trabajo en Modo Ruteo (Gateway), Modo Transparente (Bridge), Modo Hibrido (Gateway – Bridge), Modo Proxy y Modo Escucha (Mirror/TAP).
4. Debe ofrecer el manejo centralizado en caso de múltiples equipos en un equipo de la misma firma que permita una óptima y eficiente administración.
5. Firewall Basado en Tecnología de siguiente generación NGFW el cual se deberá de conectarse en alta disponibilidad (HA)
6. El dispositivo debe cumplir con la capacidad para Identificación por Usuario.
7. Deberá ofrecer una protección basada en la identidad del usuario en tiempo real. Esto es integrarse con LDAP, RADIUS, TACACS, de forma simultánea o por separado. Y contar con recursos propios de identificación de usuarios vía Web con captive portal, via un cliente a instalarse en los desktops, tablets y celulares (Android, IOS) y autenticación transparente de usuarios en dominio (Single sign on).
8. Deberá contar con la funcionalidad de aplicar Políticas de Bloqueo basadas en las IP's o Grupos de IP's de diferentes Países o Grupos de Países.
9. Deberá soportar una inspección de antivirus, anti spam, phising, pharming, sistema de prevención de intrusos, sistema de detección de fuga de información sensible (DLP) y filtrado de contenido, soporte a bloqueo de Applets de Java, Cookies y Active X.
10. Deberá ofrecer Prevención de Ataques DoS y DDoS, filtrado de MAC e IP-MAC Spoofing.
11. Deberá tener la capacidad de escanear de virus los protocolos HTTP, HTTPS, FTP, SMTP, POP3, IMAP y además de filtrar los mismos en Túneles de VPN de tal forma que la información que se transmite por este túnel sea libre de malware.
12. Deberá contar con un Área de Cuarentena para los archivos sospechosos de ser malware.
13. Deberá tener la capacidad de aplicar Escaneos y entregas dependiendo el tamaño del archivo, y también bloquearlos dependiendo el tipo de archivo.
14. Deberá ofrecer la opción de agregar una frase a los correos (Disclaimer Signature)
15. Deberá contar con un escaneo de los mensajes de correo en los encabezados, tamaño, recipiente, destino y además de poder marcar cada correo una etiqueta en el Asunto, además de revisar los encabezados de tipo MIME y además de filtrarlo por una Lista Negra Publica (RBL) y Propietaria.

16. Deberá ofrecer una configuración en el módulo de SPAM de Lista Negra y Lista Blanca personalizada.
17. Deberá tener la capacidad de re-direccionar los correos a un Servidor dedicado de Correo, además de usar una tecnología de basada en patrones. Recurrent Pattern Detection (RPD).
18. Deberá ofrecer una Protección de Zero Hour Virus Outbreak.
19. Deberá ofrecer la funcionalidad de Anti-Spam de Entrada / Salida.
20. Deberá ofrecer el cifrado de correo removiendo el cuerpo de correo y adjuntos agregando esto en un PDF protegido por contraseña, misma la que podrá ser asignada por el remitente, el equipo perimetral o el mismo recipiente via un pre-registro del mismo.
21. Deberá soportar Cifrado TLS para los protocolos SMTP, IMAP y POP
22. Deberá incluir motor DLP con escaneo automático de correos y adjuntos para restringir él envió de información sensible.
23. Deberá de incluir listas pre-configuradas de información sensible como tarjetas de crédito o regulaciones internacionales como PII, PCI, HIPAA por nombrar algunos.
24. Deberá incluir Archivado de Correo Integrado en el Equipo
25. Deberá de brindar la funcionalidad de administración de ancho de banda y administración de múltiples links con el método de Weighted Round Robin (WRR), además de soportar un failover en caso de que uno de los enlaces no esté disponible.
26. Descubrimiento de Aplicaciones y Usuarios para la asignación de prioridades.
27. Deberá soportar la funcionalidad de Parent Proxy via FQDN y HTTP Proxy.
28. Deberá ofrecer los Servicios de DDNS y Cliente PPPoE.
29. Debe contar con módulo de reporteo integrado que permita conocer de modo gráfico y detallado las operaciones, sin depender de algún equipo adicional.
30. Deberá incluir la funcionalidad integrada de VPN en SSL (Secure Socket Layer) en el mismo dispositivo.
    - Soporte a Protocolos TCP&UDP sobre el Túnel.
    - Autenticación puede ser vía: Directorio Activo, LDAP, RADIUS, TACACS+, Local.
    - Autenticación Multinivel para el cliente a través de Certificados, Usuario y Contraseña.
    - Asignación de Políticas por usuario y/o grupo
    - Acceso a Red de forma: Total o Parcial.
    - Acceso al cliente basado en Web a través de un Portal.
    - Cliente ligero para acceso a través del Túnel.
    - Acceso granular a los recursos de la Red.
    - Controles y Administración de: Sesión timeout, Dead Peer Detección, Personalización del Portal de acceso.
    - Acceso basado en aplicaciones TCP, entre las cuales debe de incluir: HTTP, HTTPS, RDP, TELNET, SSH, FTP, IBM Server Terminal, FTPS, SFTP, SMB y VNC

31. Deberá soportar los diferentes estándares para túneles de VPN:
    - Encripción - 3DES, DES, AES, Twofish, Blowfish, Serpent
    - Hash Algorithms - MD5, SHA-1
    - Authentication - Preshared key, Digital certificates
    - IPSec NAT Traversal
    - Soporte a Dead peer detection y PFS
    - Diffie Hellman Grupos - 1,2,5,14,15,16
    - Soporte a entidades de una Autoridad Certificadora.
    - Soporte a PPTP, L2TP.

- Soporte a Exportar configuraciones de Conexiones de tipo Cliente IPSec

  Soporte a las diferentes Plataformas:

  WinXP 32/64- bit, Windows Server 2008/2012, Windows Vista,7, 8/8.1 y 10 ya sea a 32/64-bits
- Soporte de Túneles a usuarios finales por Nombre Dominio
- Conexión Redundante de VPN
- Failover de enlaces MPLS a través de VPN IPSec
- Soporte de Overlapping
- Soporte de VPN Hub & Spoke

32. Deberá de contar también con un dispositivo para establecer VPNs de forma automática hacia el sitio central, este dispositivo no deberá de contar con alguna interface de configuración local, sino que toda la configuración de este dispositivo será realizada de forma centralizada en el equipo central, dicho dispositivos deberá de soportar
    - Administración Centralizada de estos dispositivos desde el NGFW principal
    - Sin configuración necesario en el dispositivo, toda configuración se tomará automáticamente por medio de un cloud de aprovisionamiento
    - Túnel encriptado y seguro utilizando Certificados X.509 y encriptación AES256
    - Estos tuneles de VPN se deberán de reflejar como una interface más de red en el NGFW central de tal forma que toda la asignación de permisos incluso DHCP y DNS deber de ser de forma centralizada
    - Soporte a configuración de VLANs
    - Compresión del tráfico enviado por el túnel de VPN.
    - Desautorización remota de estos dispositivos después de un periodo de tiempo de inactividad configurable

33. El dispositivo deberá ofrecer Alta disponibilidad y redundancia:
    - Activo-Activo
    - Activo-Pasivo con sincronización.
    - Failover
    - Alertas en el equipo de cambios de estatus.

34. Deberá ofrecer la siguiente funcionalidad en el mismo Dispositivo. Web Application Firewall (WAF**)**
    - Detección Intuitiva de amenazas y ataques para el Portal WEB (www).
    - Protección contra Robo de Identidades de Sesión, Cross-site Scripting, Inyecciones de SQL, Envenenamiento de Cookies.
    - Re direccionamiento de páginas web en base a los encabezados HTTP
    - Soporte a protocolo Outlook anyware
    - Autenticación reversa en base a formas web o autenticación básica web
    - Motor para endurecimiento de formas web
    - Escaneo dual de Antivirus
    - Exclusiones/Bloqueos en base a IP o rangos de IP´s
    - Soporte al protocolo HTTP0.9/1.0/1.1
    - Servicio de Registro y reportes extenso.
    - Soporte a la detección de ataques Top 10 declarado por OWASP.

35. Deberá soportar los siguientes Protocolos de Ruteo Dinámicos tales como RIP v1 y v2, OSPF, BGP, Multicast

Forwarding, ruteo muticast (PIM-SM), soporte a H323 NAT Transversal.

36. Deberá de soportar los estándares 8021q y 802.3ad
37. Deberá ofrecer un servicio de Políticas de Ruteo
38. Deberá brindar la funcionalidad de Aplicar políticas por usuario, donde se le asigne de forma granular lo siguiente (Criterio de Control de Acceso):
    - Ancho de banda asignado
    - Filtrado de Aplicaciones Web
    - Filtrado de Contenido vía HTTP y HTTPS
    - Prevención de Intrusos
    - Anti-Spam
    - Zona Destino
    - Dirección Física (MAC Address)
    - IP Fuente
    - IP Destino
    - Servicio Calendarizado

39. Deberá contener al menos de 5,400+ firmas en el Sistema de Prevención de Intrusos y podrá ser personalizable.
40. Soporte a inspección de ataques bajo protocolo SCADA.
41. Deberá ofrecer un filtrado para Prevención de intrusos el cual deberá de poder detectar y bloquear de forma enunciativa más no limitativa el siguiente tipo de tráfico:
    - Protocol Anomaly Detection Block
    - Actividad de tipo “Phone home”
    - Keylogger
    - Mapa Geográfico de tráfico (origen y destino de paquetes)
    - Capacidad de Generación de reportes limitada (visibilidad de tráfico, pero no de su origen) vía los privilegios de administrador y totalmente abierta (visibilidad de Trafico con sus orígenes) mediante las credenciales de un usuario adicional. Esto con el fin de preserver de inicio un nivel de confidencialidad para el usuario.

42. Deberá ofrecer un filtrado de contenido Web con una base de datos la cual debe de tener más de 90 categorías y deberá soportar la generación categorías personalizadas, soportando en el filtrado HTTP y HTTPS.
43. Deberá ofrecer una categorización por clasificación de URL’s según el Nivel de Riesgo, Características de las Aplicaciones o el Modo de Conexión.
44. Se debe incluir la característica el cual ofrezca un control de Capa 8 en el acceso a YouTube a una categoría específica de material de videos exclusivo para Escuelas.
45. Deberá soportar mensajes personalizados por categoría y asignación de un horario por categoría para el uso de la misma.
46. Deberá de mantener un registro de todo lo copiado (upload) a Internet vía HTTP para evitar el robo de información, el cual en el registro debe aparecer el Usuario, IP Fuente, Directorio de donde se copió, IP Destino.

47. Deberá contar con Filtrado Aplicaciones el cual pueda controlar el acceso aplicaciones web las cuales no necesariamente utilicen protocolos de navegación normal (HTTP, HTTPS), brindando con esto la facilidad de controlar a nivel granular la actividad de los usuarios hacia internet como por ejemplo el poder permitir el acceso a Redes Sociales delimitando que no tengan acceso a ciertas aplicaciones como por ejemplo Videoconferencias,

mensajería Instantánea o Juegos dentro de la misma red social.

48. Dicho Filtrado Aplicaciones deberá de ser dividido en al menos 20 Categorías como, por ejemplo:
    - Industrial Control System (ICS, SCADA)
    - P2P
    - Proxy and Tunnel
    - Social Networking
    - Streaming Media
    - VoIP

49. Deberá poder integrarse con un Directorio Activo, Controlador de Dominio, LDAP, Radius, TACACS+ o la generación de una base de datos interna para la autenticación de los usuarios, soportando la función de Single Sign On (SSO) para Microsoft Active Directory, Novell eDirectory, Radius, NTLM y VPN´s
50. Debe ser compatible para el uso y soporte de Autenticación de clientes Delgados con MS Windows 2003 y servicio de Terminal.

51. El equipo deberá ofrecer como característica el Servicio de correlacionador de eventos en el mismo dispositivo de forma embebida, sin incurrir en un costo adicional. Este Servicio deberá contar con:
    - Más de 1200+ reportes.
    - Reportes Historicos
    - Busqueda de Reportes
    - Reportes Personalizados
    - Reportes Incluidos de: Seguridad, Spam, Virus, Trafico, Bloqueos
    - Más de 45 Reportes que cumplen con alguna norma o estándar de Seguridad.
    - Todos los reportes exportables a archivos de tipo PDF y Excel.
    - 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.

52. Deberá Contar con analizador de tráfico en tiempo real.
    - Registros en Tiempo real
    - Notificación de estos reportes Vía email, de Virus y ataques
    - Prevención de Intrusos
    - Violaciones de Políticas
    - Filtrado Web por uso de categorías
    - Palabras buscadas en un search engine o buscador
    - Información transferida (Por Host, Grupo y Direcciones IP)
    - Incidencias de Virus por usuario y por dirección IP

53. Deberá ofrecer la opción de configuración vía Web y además una ayuda por pasos en el mismo equipo, una administración por roles administrativos y de múltiples administradores, además de ofrecer un nivel de acceso a usuarios.
54. Deberá contar con un Sistema de Administración vía HTTP, Serial, Telnet, SNMP (v1, v2c), HTTPS, con la capacidad de generar roles de acceso.

55. El sistema operativo deberá ofrecer la capacidad de encriptar el contenido mostrado en los todos los registros que genera el mismo equipo para evitar que sean obtenidos o leídos por una persona no autorizada, además de prevenir que una sola persona tengo el control de la administración de esta información.
56. El equipo debe incluir firmas de Antivirus, IPS y Filtrado de Contenido y Aplicaciones Web para 3 años, sin límite de usuarios.
57. Deberá incluir Soporte, Servicio y Mantenimiento para el equipo 5x8, reemplazo de equipo en caso de falla de Hardware sin costo, actualizaciones de Sistemas Operativos, por 3 años a partir de la fecha de adquisición.

ÍTEM 5 – SISTEMA DE SEGURIDAD PERIMETRAL FIREWALL DE PRÓXIMA GENERACIÓN NGFW
Calidad del Fabricante:
El fabricante del Firewall de Próxima Generación NGFW debe estar posicionado como líder del ultimo cuadrante Gartner en soluciones UTM (Junio de 2017)
Debe estar posicionado en el Cuadrante Superior al 90% de NSS Labs de 2017 para Firewalls de Próxima Generación (Next Generation Firewall). Este cuadrante evalúa las soluciones más favorables en su TCO en cuanto a relación entre precio y eficiencia
Características del dispositivo:
El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo.
El dispositivo debe ser un equipo de propósito específico.
El dispositivo debe estar catalogado como un appliance de seguridad.
Debe proveer visibilidad y trazabilidad por usuario y/o aplicación.
El equipo debe analizar contenido cifrado (SSL) para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Antivirus e IPS.
Capacidades de Detección y Prevención de Intrusos (IPS):
Protección de servidores por vulnerabilidades conocidas
El IPS deberá estar integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos.
La interfaz de administración del IPS deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio.
Debe actualizar de manera automática las firmas para el sistema de detección de intrusos.
Capacidades de Control de aplicaciones:
Visibilidad y Control del tráfico de la red por aplicaciones (Ejemplo: Permitir Facebook pero no sus juegos, Permitir Youtube pero no HD o subida de videos, Permitir Gmail pero no el chat o subir/bajar archivos, etc).
Controlar el ancho de banda por usuario y/o por aplicación.
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.
El listado de aplicaciones debe actualizarse periódicamente.
Capacidades de Prevención de Malware Avanzado:
Antivirus/Antimalware de red con cobertura para dispositivos fuera del control de la empresa (Tablets, Smartphones).
Debe ser capaz de analizar, establecer control de acceso y detener ataques y virus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.

El Antivirus deberá incluir capacidades de detección y bloqueo de tráfico spyware, adware y otros tipos de malware/grayware que pudieran circular por la red.
Debe permitir identificar y bloquear conexiones hacia servidores de Centro de Control de Botnets.
Debe permitir identificar o bloquear la descarga de archivos por extensión, tipo y nombre de archivo.
El dispositivo deberá de contar con protección contra ataques persistentes (ATP) integrada en el equipo.
Capacidades de Sandboxing en la Nube
El appliance de seguridad ofertado debe poder habilitar el servicio de Sandboxing en la nube para análisis y detonación de malware potencial
Capacidades de Filtrado de Navegación Web: Prevención de infección por páginas de riesgo alto.
Bloqueo de páginas por URL con al menos 92 categorías
Filtrado de contenido basado en al menos 92 categorías en tiempo real. Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías.
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.
La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado (SSL).
Capacidades de Single Sign On:
Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto "Single-Sign-On"
El sistema propuesto deberá contar con la funcionalidad de autenticar usuarios de forma transparente con métodos como: Un portal cautivo vía web; a través del uso de un agente instalado en el dispositivo final; obteniendo la información del directorio activo.
Las tareas de sincronización con el servicio de directorio a utilizar pueden ser integradas en la misma solución o utilizando un dispositivo dedicado para tal fin.
Funcionalidad WAF Integrada
La solución de Firewall debe proveer funcionalidad de Web Application Firewall (WAF) incluida, sin necesidad de adquirir o destinar otro appliance/máquina virtual para proveer esta funcionalidad
Sincronización entre la red Perimetral y la red LAN
Funcionalidad de sincronización entre la red perimetral y los endpoints a nivel de red local para brindar una respuesta ante incidentes en segundos.
El dispositivo deberá de contar una integración nativa con los clientes de EndPoint Protection para integrar el estado de salud de los clientes como un elemento más en las reglas de firewall, habilitando con esto la facilidad de poder delimitar el acceso a recursos sensibles como servidores o DMZ´s e Internet si el cliente llega a ser comprometido por algún malware y solo permitiendo el acceso una vez que el cliente vuelva a su estado no comprometido.
Funcionalidad de Protección de Correo entrante SMTP y MTA
Funcionalidad de Antivirus y Antispam del correo entrante via SMTP
Licenciamiento y actualizaciones:
El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo.
Reportes
La solución ofertada debe proveer reportes automáticos y personalizables tanto a nivel de estadísticas, indicadores, trafico, consumo, usuarios riesgosos, cumplimiento regulatorio, entre otros integrados en el mismo Firewall sin requerir

ninguna plataforma o maquina adicional
La solución deberá poder ofrecer una plataforma adicional opcional de reportes ejecutivos adicionales a la solución de Firewall ofertada y debe ser del mismo fabricante que el firewall
Gestión Centralizada de Dispositivos:
La solución deberá poder integrarse con un appliance de gestión centralizado de firewalls, el cual deberá ser del mismo fabricante del sistema de Seguridad Perimetral.
Valores de desempeño y conectividad, como mínimo:
• Interfaces de red 1 GE: 4 incluidas
Internal Storage: Un (1) Disco eMMC 8 GB
Memoria RAM: 2 GB DDR4 ECC
• Throughput de Firewall: 3 Gbps
• Throughput de IPS (HTTP): 580 Mbps
• Throughput Control de Aplicaciones + IPS + Web Filter: 310 Mbps
• Throughput de NGFW: 310 Mbps
• Throughput de VPN IPSec: 225 Mbps
• Sesiones Concurrentes (TCP): 3.2 Millones
• Throughput Threat Protection: 360 Mbps
• Nuevas conexiones por segundo: 15.000
• **Especificaciones inalámbricas**
• Cantidad minima de antenas 2 (DOS)
Capacidad MIMO 2 x 2:2
• Interfaces Wireless 802.11a/b/g/n/ac (2.4 GHz / 5 GHz)
• 3 Años de garantía y soporte del fabricante. Con servicio telefónico 24x7 y con respuesta al día siguiente laborable de un técnico en las instalaciones, como mínimo.

1. Deberá ofrecer una configuración de zonas de seguridad tales como de LAN/DMZ/WAN asignadas a una o varias Interfaces.
2. Deberá de contar con soporte para tecnologías de monitoreo SNMP y Netflow, sin que esto incurra en una licencia adicional.
3. El dispositivo de ofrecer la Funcionalidad de trabajo en Modo Ruteo (Gateway), Modo Transparente (Bridge), Modo Hibrido (Gateway – Bridge), Modo Proxy y Modo Escucha (Mirror/TAP).
4. Debe ofrecer el manejo centralizado en caso de múltiples equipos en un equipo de la misma firma que permita una óptima y eficiente administración.
5. Firewall Basado en Tecnología de siguiente generación NGFW el cual se deberá de conectarse en alta disponibilidad (HA)
6. El dispositivo debe cumplir con la capacidad para Identificación por Usuario.
7. Deberá ofrecer una protección basada en la identidad del usuario en tiempo real. Esto es integrarse con LDAP, RADIUS, TACACS, de forma simultánea o por separado. Y contar con recursos propios de identificación de usuarios vía Web con captive portal, via un cliente a instalarse en los desktops, tablets y celulares (Android, IOS) y autenticación transparente de usuarios en dominio (Single sign on).

8. Deberá contar con la funcionalidad de aplicar Políticas de Bloqueo basadas en las IP's o Grupos de IP's de diferentes Países o Grupos de Países.
9. Deberá soportar una inspección de antivirus, anti spam, phising, pharming, sistema de prevención de intrusos, sistema de detección de fuga de información sensible (DLP) y filtrado de contenido, soporte a bloqueo de Applets de Java, Cookies y Active X.
10. Deberá ofrecer Prevención de Ataques DoS y DDoS, filtrado de MAC e IP-MAC Spoofing.
11. Deberá tener la capacidad de escanear de virus los protocolos HTTP, HTTPS, FTP, SMTP, POP3, IMAP y además de filtrar los mismos en Túneles de VPN de tal forma que la información que se transmite por este túnel sea libre de malware.
12. Deberá contar con un Área de Cuarentena para los archivos sospechosos de ser malware.
13. Deberá tener la capacidad de aplicar Escaneos y entregas dependiendo el tamaño del archivo, y también bloquearlos dependiendo el tipo de archivo.
14. Deberá ofrecer la opción de agregar una frase a los correos (Disclaimer Signature)
15. Deberá contar con un escaneo de los mensajes de correo en los encabezados, tamaño, recipiente, destino y además de poder marcar cada correo una etiqueta en el Asunto, además de revisar los encabezados de tipo MIME y además de filtrarlo por una Lista Negra Publica (RBL) y Propietaria.
16. Deberá ofrecer una configuración en el módulo de SPAM de Lista Negra y Lista Blanca personalizada.
17. Deberá tener la capacidad de re-direccionar los correos a un Servidor dedicado de Correo, además de usar una tecnología de basada en patrones. Recurrent Pattern Detection (RPD).
18. Deberá ofrecer una Protección de Zero Hour Virus Outbreak.
19. Deberá ofrecer la funcionalidad de Anti-Spam de Entrada / Salida.
20. Deberá ofrecer el cifrado de correo removiendo el cuerpo de correo y adjuntos agregando esto en un PDF protegido por contraseña, misma la que podrá ser asignada por el remitente, el equipo perimetral o el mismo recipiente vía un pre-registro del mismo.
21. Deberá soportar Cifrado TLS para los protocolos SMTP, IMAP y POP
22. Deberá incluir motor DLP con escaneo automático de correos y adjuntos para restringir él envió de información sensible.
23. Deberá de incluir listas pre-configuradas de información sensible como tarjetas de crédito o regulaciones internacionales como PII, PCI, HIPAA por nombrar algunos.
24. Deberá incluir Archivado de Correo Integrado en el Equipo
25. Deberá de brindar la funcionalidad de administración de ancho de banda y administración de múltiples links con el método de Weighted Round Robin (WRR), además de soportar un failover en caso de que uno de los enlaces no esté disponible.
26. Descubrimiento de Aplicaciones y Usuarios para la asignación de prioridades.
27. Deberá soportar la funcionalidad de Parent Proxy via FQDN y HTTP Proxy.
28. Deberá ofrecer los Servicios de DDNS y Cliente PPPoE.
29. Debe contar con módulo de reporteo integrado que permita conocer de modo gráfico y detallado las operaciones, sin depender de algún equipo adicional.
30. Deberá incluir la funcionalidad integrada de VPN en SSL (Secure Socket Layer) en el mismo dispositivo.

- Soporte a Protocolos TCP&UDP sobre el Túnel.
- Autenticación puede ser vía: Directorio Activo, LDAP, RADIUS, TACACS+, Local.
- Autenticación Multinivel para el cliente a través de Certificados, Usuario y Contraseña.
- Asignación de Políticas por usuario y/o grupo
- Acceso a Red de forma: Total o Parcial.

- Acceso al cliente basado en Web a través de un Portal.
- Cliente ligero para acceso a través del Túnel.
- Acceso granular a los recursos de la Red.
- Controles y Administración de: Sesión timeout, Dead Peer Detección, Personalización del Portal de acceso.
- Acceso basado en aplicaciones TCP, entre las cuales debe de incluir: HTTP, HTTPS, RDP, TELNET, SSH, FTP, IBM Server Terminal, FTPS, SFTP, SMB y VNC

31. Deberá soportar los diferentes estándares para túneles de VPN:

- Encripción - 3DES, DES, AES, Twofish, Blowfish, Serpent
- Hash Algorithms - MD5, SHA-1
- Authentication - Preshared key, Digital certificates
- IPSec NAT Traversal
- Soporte a Dead peer detection y PFS
- Diffie Hellman Grupos - 1,2,5,14,15,16
- Soporte a entidades de una Autoridad Certificadora.
- Soporte a PPTP, L2TP.
- Soporte a Exportar configuraciones de Conexiones de tipo Cliente IPSec

  Soporte a las diferentes Plataformas:

  WinXP 32/64- bit, Windows Server 2008/2012, Windows Vista,7, 8/8.1 y 10 ya sea a 32/64-bits
- Soporte de Túneles a usuarios finales por Nombre Dominio
- Conexión Redundante de VPN
- Failover de enlaces MPLS a través de VPN IPSec
- Soporte de Overlapping
- Soporte de VPN Hub & Spoke

32. Deberá de contar también con un dispositivo para establecer VPNs de forma automática hacia el sitio central, este dispositivo no deberá de contar con alguna interface de configuración local, sino que toda la configuración de este dispositivo será realizada de forma centralizada en el equipo central, dicho dispositivos deberá de soportar

- Administración Centralizada de estos dispositivos desde el NGFW principal
- Sin configuración necesario en el dispositivo, toda configuración se tomará automáticamente por medio de un cloud de aprovisionamiento
- Túnel encriptado y seguro utilizando Certificados X.509 y encriptación AES256
- Estos tuneles de VPN se deberán de reflejar como una interface más de red en el NGFW central de tal forma que toda la asignación de permisos incluso DHCP y DNS deber de ser de forma centralizada
- Soporte a configuración de VLANs
- Compresión del tráfico enviado por el túnel de VPN.
- Desautorización remota de estos dispositivos después de un periodo de tiempo de inactividad configurable

33. Deberá ofrecer la siguiente funcionalidad en el mismo Dispositivo. Web Application Firewall (WAF**)**

- Detección Intuitiva de amenazas y ataques para el Portal WEB (www).
- Protección contra Robo de Identidades de Sesión, Cross-site Scripting, Inyecciones de SQL, Envenenamiento

de Cookies.

- Re direccionamiento de páginas web en base a los encabezados HTTP
- Soporte a protocolo Outlook anyware
- Autenticación reversa en base a formas web o autenticación básica web
- Motor para endurecimiento de formas web
- Escaneo dual de Antivirus
- Exclusiones/Bloqueos en base a IP o rangos de IP´s
- Soporte al protocolo HTTP0.9/1.0/1.1
- Servicio de Registro y reportes extenso.
- Soporte a la detección de ataques Top 10 declarado por OWASP.

34. Deberá soportar los siguientes Protocolos de Ruteo Dinámicos tales como RIP v1 y v2, OSPF, BGP, Multicast Forwarding, ruteo muticast (PIM-SM), soporte a H323 NAT Transversal.
35. Deberá de soportar los estándares 8021q y 802.3ad
36. Deberá ofrecer un servicio de Políticas de Ruteo
37. Deberá brindar la funcionalidad de Aplicar políticas por usuario, donde se le asigne de forma granular lo siguiente (Criterio de Control de Acceso):
    - Ancho de banda asignado
    - Filtrado de Aplicaciones Web
    - Filtrado de Contenido vía HTTP y HTTPS
    - Prevención de Intrusos
    - Anti-Spam
    - Zona Destino
    - Direccion Fisica (MAC Address)
    - IP Fuente
    - IP Destino
    - Servicio Calendarizado

38. Deberá contener al menos de 5,400+ firmas en el Sistema de Prevención de Intrusos y podrá ser personalizable.
39. Soporte a inspección de ataques bajo protocolo SCADA.
40. Deberá ofrecer un filtrado para Prevención de intrusos el cual deberá de poder detectar y bloquear de forma enunciativa más no limitativa el siguiente tipo de tráfico:
    - Protocol Anomaly Detection Block
    - Actividad de tipo “Phone home”
    - Keylogger
    - Mapa Geografico de tráfico (origen y destino de paquetes)
    - Capacidad de Generacion de reportes limitada (visibilidad de tráfico, pero no de su origen) via los privilegios de administrador y totalmente abierta (visibilidad de Trafico con sus origenes) mediante las credenciales de un usuario adicional. Esto con el fin de preserver de inicio un nivel de confidencialidad para el usuario.

41. Deberá ofrecer un filtrado de contenido Web con una base de datos la cual debe de tener más de 90

categorías y deberá soportar la generación categorías personalizadas, soportando en el filtrado HTTP y HTTPS.

42. Deberá ofrecer una categorización por clasificación de URL's según el Nivel de Riesgo, Características de las Aplicaciones o el Modo de Conexión.
43. Se debe incluir la característica el cual ofrezca un control de Capa 8 en el acceso a YouTube a una categoría específica de material de videos exclusivo para Escuelas.
44. Deberá soportar mensajes personalizados por categoría y asignación de un horario por categoría para el uso de la misma.
45. Deberá de mantener un registro de todo lo copiado (upload) a Internet vía HTTP para evitar el robo de información, el cual en el registro debe aparecer el Usuario, IP Fuente, Directorio de donde se copió, IP Destino.
46. Deberá contar con Filtrado Aplicaciones el cual pueda controlar el acceso aplicaciones web las cuales no necesariamente utilicen protocolos de navegación normal (HTTP, HTTPS), brindando con esto la facilidad de controlar a nivel granular la actividad de los usuarios hacia internet como por ejemplo el poder permitir el acceso a Redes Sociales delimitando que no tengan acceso a ciertas aplicaciones como por ejemplo Videoconferencias, mensajería Instantánea o Juegos dentro de la misma red social.
47. Dicho Filtrado Aplicaciones deberá de ser dividido en al menos 20 Categorías como, por ejemplo:
    - Industrial Control System (ICS, SCADA)
    - P2P
    - Proxy and Tunnel
    - Social Networking
    - Streaming Media
    - VoIP

48. Deberá poder integrarse con un Directorio Activo, Controlador de Dominio, LDAP, Radius, TACACS+ o la generación de una base de datos interna para la autenticación de los usuarios, soportando la función de Single Sign On (SSO) para Microsoft Active Directory, Novell eDirectory, Radius, NTLM y VPN´s
49. Debe ser compatible para el uso y soporte de Autenticación de clientes Delgados con MS Windows 2003 y servicio de Terminal.

50. El equipo deberá ofrecer como característica el Servicio de correlacionador de eventos en el mismo dispositivo de forma embebida, sin incurrir en un costo adicional. Este Servicio deberá contar con:
    - Más de 1200+ reportes.
    - Reportes Historicos
    - Busqueda de Reportes
    - Reportes Personalizados
    - Reportes Incluidos de: Seguridad, Spam, Virus, Trafico, Bloqueos
    - Más de 45 Reportes que cumplen con alguna norma o estándar de Seguridad.
    - Todos los reportes exportables a archivos de tipo PDF y Excel.
    - 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.

51. Deberá Contar con analizador de tráfico en tiempo real.

- Registros en Tiempo real
- Notificación de estos reportes Vía email, de Virus y ataques
- Prevención de Intrusos
- Violaciones de Políticas
- Filtrado Web por uso de categorías
- Palabras buscadas en un search engine o buscador
- Información transferida (Por Host, Grupo y Direcciones IP)
- Incidencias de Virus por usuario y por dirección IP

52. Deberá ofrecer la opción de configuración vía Web y además una ayuda por pasos en el mismo equipo, una administración por roles administrativos y de múltiples administradores, además de ofrecer un nivel de acceso a usuarios.
53. Deberá contar con un Sistema de Administración vía HTTP, Serial, Telnet, SNMP (v1, v2c), HTTPS, con la capacidad de generar roles de acceso.
54. El sistema operativo deberá ofrecer la capacidad de encriptar el contenido mostrado en los todos los registros que genera el mismo equipo para evitar que sean obtenidos o leídos por una persona no autorizada, además de prevenir que una sola persona tengo el control de la administración de esta información.
55. El equipo debe incluir firmas de Antivirus, IPS y Filtrado de Contenido y Aplicaciones Web para 3 años, sin límite de usuarios.
56. Deberá incluir Soporte, Servicio y Mantenimiento para el equipo 5x8, reemplazo de equipo en caso de falla de Hardware sin costo, actualizaciones de Sistemas Operativos, por 3 años a partir de la fecha de adquisición.

	ÍTEM 6 – Licencia para Adobe Creative Cloud
	Adobe Creative Cloud mínimo en la version 2018
	ÍTEM 7 - Corel Draw
	Corel Draw X8

Lote N° 8 - Licencias para CIRDTUR

	ÍTEM 1 – Cal de Windows
CAL de Windows	WinSvrCAL 2016 OLP NL Gov UsrCAL
	ÍTEM 2 - CAL de Exchange
CAL de Exchange	ExchgStdCAL 2016 OLP NL Gov UsrCAL

ÍTEM 3- SOFTWARE ANTIVIRUS PARA COMPUTADORA	
Capacidad Requerida	**Exigido**
Consola de administración centralizada	SI
Protección web	SI
Reputación de descargas	SI
Control web / bloqueo de URL basado en categorías	SI

Control de periféricos (p. ej. USB)	SI
Restricción de aplicaciones	SI
Firewall	SI
Escaneado de archivos anti-malware	SI
Protección activa	SI
Análisis de comportamiento previo a la ejecución (HIPS)	SI
Bloqueo de aplicaciones no deseadas	SI
Análisis de comportamiento en tiempo de ejecución (HIPS)	SI
Eliminación de malware automatizada	SI

	ÍTEM 4 - Licencias Software para backup
Licencia Software de Backup	ESSENTIAL 24 MONTHS RENEWAL FOR BACKUP EXEC V-RAY ED WIN 1 CPU ONPREMISE STANDARD PERPETUAL LICENSE GOV

ÍTEM 5 - Windows Server Datacenter	
Característica	
Windows Server DataCenter	WinSvrDCCore 2016 OLP 16Lic NL Gov CoreLic Qlfd

2. Plan de Entregas

Lote N°	Plazo	Lugar de entrega de los Bienes
1-2-3-5-6-7-8	Dentro de los 7 días corridos contados a partir de la recepción de la orden de compra.	**SECRETARÍA NACIONAL DE TURISMO** de lunes a viernes de 07:00 AM a 15:00 PM
4	Dentro de los 10 días corridos contados a partir de la recepción de la orden de compra.	**SECRETARÍA NACIONAL DE TURISMO** de lunes a viernes de 07:00 AM a 15:00 PM

Todos los demás puntos no mencionados en la presente adenda quedan invariables y con plena vigencia.

Atentamente.

PRESIDENCIA DE LA REPÚBLICA DEL PARAGUAY SECRETARÍA NACIONAL DE TURISMO ASUNCIÓN

LIC. MYRIAN PAREDES
Directora
Dirección de Adquisiciones (UOC)
SENATUR