ANEXO DEL CONTRATO No. LS/RTV/35952/007/2011 B, DE LA LICITACIÓN SIMPLIFICADA RELATIVA A LA ADQUISICIÓN DE REFACCIONES, HERRAMIENTAS Y EQUIPO DE INFORMATICA PARA RADIOTELEVISIÓN DE VERACRUZ.

Partida	*Descripción y características*	*Unidad de medida*	*Cantidad*	*P.U.*	*IMPORTE*
6	**Switches de Acceso de 48 puertos POE** **Características Generales** • El equipo deberá de contar con 48 puertos 10/100/1000Base Tx autosensados, POE, cuatro de estos puertos deberán soportar tecnología SFP. • El equipo deberá de contar con soporte a desempeño a velocidad de cable, es decir, el 100% de los puertos operando a máxima velocidad sin bloqueo ni sobresuscripción. • El equipo deberá de contar con un protocolo de anillo metropolitano. • Deberá de contar con un desempeño mínimo de 96 Gbps y 72 Mpps. • El equipo proveer al menos 480 Watts de potencia para POE, a dividirse en todos los puertos y asignarse de acuerdo al estándar 802.3af • Deberá soportar redundancia en fuente de poder. **Funcionalidades:** • Soporte mínimo a 16,000 direcciones de MAC. • Soporte a agregación dinámica de enlaces vía 802.3ad • Monitoreo de puertos basado en listas de control de acceso. • Limitación del ancho de banda basado en listas de control de acceso. • Limitación de ancho de banda de trafico de broadcast , multicast y unicast desconocidos. • Monitoreo digital óptico o “Digital Optical Monitoring”. • Soporte a CDP “Cisco Discovery Protocol”. • Auto-configuración de dispositivos de VoIP. • Configuración de múltiples servidores de syslog. • Sincronizar de la fecha y la hora mediante un servidor de SNTP o “Simple Network Time Protocol”. • Soporte a VCT o “Virtual Cable Testing” utilizando TDR “Time Domain Reflectometry” para diagnostico de fallas en el cableado estructurado así como de RFC “Remote Fault Notification “ para puertos de Gigabit Ethernet. • Ajuste de IPG “Interpacket Gap” • Soporte a paquetes tipo “Jumbo Frames” con un mínimo de tamaño de 10240 bytes .	Pieza	1	$ 68,168.75	$ 68,168.75

	• Soporte a LLDP y LLDP-MED • Deberá de soportar la retransmisión de paquetes de DHCP de diferentes VLANS. • Deberá de contar con soporte a ECMP “Equal Cost Multi Path”. • Deberá de soportar la configuración simultánea de mínimo de 1,000 rutas de ipV4 y de 255 interfaces virtuales de capa 3. • Administración • Listas de control de acceso para controlar el acceso administrativo. • Port flap dampening. • Monitoreo Remoto (RMON) • sFlow via RFC 3167 con soporte a la extracción de los nombre de usuarios de EAP . • Acceso a la línea de comandos vía Telnet y puerto Serial. • Interface de administración vía GUI a través de HTTPS/SSL. • Soporte a SNMPv1 , SNMPv2 y SNMPv3. **Administración vía IPv6** El equipo deberá de soportar la administración del mismo mediante el protocolo de Ipv6 con las siguientes características: • Dirección de Ipv6 tipo Link-Local • Listas de control de acceso de Ipv6 • Herramientas de diagnostico de Ipv6 como “traceroute” y “ping” • Resolución de nombres o “DNS” vía Ipv6 • Administración vía HTTP/HTTPS vía Ipv6 • Syslog vía IPv6 • SCP y SSH vía IPv6 • SNMPv1/v2/v3 vía IPv6 • SNTP • TACACS/TACACS+ • Telnet • TFTP **Seguridad** • Soporte a 802.1x con asignación dinámica de ACL , Filtros de MAC y VLAN • Listas de control de acceso para filtrado de tráfico en tránsito. • Filtro de restricción de trafico basado en direcciones de MAC.				

	• Soporte de encripción tipo AES para SSHv2. • Autentificación , Autorización y Contabilización (AAA) • Protección contra ataques de negación de Servicios. • DHCP Snooping • Listas de control de acceso dinámicas con autentificación de múltiples dispositivos por puerto. • Inspección dinámica de ARP • IP Source Guard • Filtrado de Capa 2 a través de dirección fuente y destino de MAC. • Capacidad de deshabilitar el aprendizaje de direcciones de MAC. • Seguridad basada en direcciones de MAC • Copia segura mediante SCP • Servidor de SSH v2 **Spanning Tree** Deberá de contar con el soporte a las siguientes características de Spanning Tree: • 802.1d Spanning Tree • 802.1s Multiple Spanning Tree • 802.1w Rapid Spanning Tree (RSTP) • Soporte a la configuración concurrente de hasta 254 instancias de STP. • Compatibilidad con PVST/PVST+ • Compatibilidad con PVRST+ • Además deberá de contar con funciones para asegurar el árbol de STP. **VLANS** Deberá de contar con las siguientes características : • Configuración de mínimo 4,000 VLANS • 802.1q • Vlans de modo dual. • GVRP • Vlans basadas en puerto • Vlans basadas en protocolo (IPX, AppleTalk , IPv4 e IPv6) • Vlans basadas en subnets • Grupos de Vlans • Vlans privadas • Vlans tipo Q in Q con encapsulación vía el tipo de Ethernet 8100 • Monitoreo basado en Vlans • Vlans basadas en direcciones de MAC.				

	Calidad de Servicio (QoS) Deberá de soportar los siguientes algoritmos de Calidad de Servicio: • Strict Priority • Weighted Round Robin (WRR) • Combinación de SP y WRR • 8 colas de prioridad. • DiffServ • Limitación del ancho de banda basado en listas de acceso y QoS • Mapeo de prioridades mediante Listas de control de acceso. • Mapeo de DSCP con valores del 1 al 8. **Multicast** Deberá de contar con el soporte de los siguientes protocolos de Multicast: • IGMP v1/v2 Snooping • IGMP v3 Snooping • IGMP v1/v2/v3 Snooping por VLAN • IGMP v2/v3 Fast Leave (con rastreo de grupos) • Filtrado de IGMP • MLD v1/v2 Snooping • MLD fast leave para v1 • Rastreo de MLD y fast leave para v2 • Configuracion estatica de MLD y de grupos de IGMP con soporte para proxy. • PIM-SM v2 Snooping **Ruteo (Capa 3)** Capacidad de contar con los siguientes protocolos de ruteo. • Ruteo de subredes directamente conectadas • Rutas estáticas • Anuncios de RIP v1/v2 • Capacidad de Así mismo, el equipo podrá ser actualizado para ejecutar ruteo dinámico basado en (no se debe incluir la licencia para estos protocolos): • OSPFv1,v2 • RIP V1 , V2				

	Compatibilidad Para garantizar la compatibilidad de los equipos, el equipo deberá de contar con el soporte a los siguientes protocolos: IEEE • 802.1ab Station and Media Access Control Connectivity Discovery • 802.1d Ethernet Bridging • 802.1 MAC Bridges • 802.1p Mapping to Priority Queue • 802.1p/q VLAN Tagging • 802.1q Generic VLAN Registration Protocol (GVRP) • 802.1s Multiple Spanning tree • 802.1w Rapid Spanning Tree • 802.1x Port-based Network Access Control • 802.3 10Base-T • 802.3ab 1000Base-T • 802.3ad Link Aggregation • 802.3u 100Base-TX • 802.3z 1000Base-SX , 1000Base-LX • 802.3x Flow Control El proveedor deberá presentar: Carta en original por parte del fabricante donde se obligue solidariamente con el proveedor a avalar las características técnicas que no se encuentren respaldadas en los folletos (deberán ser impresas, en hojas membretadas y suscritas por el representante legal del fabricante). Carta en original por parte del fabricante especifique que es distribuidor certificado. Carta en original por parte del fabricante que asegure que el integrador cuenta con personal certificado. Deberá garantizar mediante carta compromiso, llevar a cabo la instalación, configuración, implementación y puesta en marcha de los equipos. Cumpliendo con las siguientes actividades y configuraciones: 1. Verificación del sitio designado para la instalación física de la unidad. 2. Desempacado de equipo y verificación de correcto funcionamiento. 3. Verificación del punto eléctrico de conexión. 4. Verificación de conectividad IP en el puerto designado proveniente de la red				

	interna. 5. Instalación física de la unidad. 6. Definición de políticas de seguridad. 7. Definición de roles de usuarios o equipos. 8. ASIGNACIÓN DE politicas de seguridad y rol al puerto correspondiente del Switch. 9. Generación de VLANs de acuerdo a los roles de usuario. 10. Definición de roles de servicio. 11. Definición de umbrales de calidad de servicio. 12. Asignación de umbrales. 13. Habilitación del switch para la plataforma de monitoreo.				
7	**Switches de Acceso de 24 puertos POE.** **Características Generales** • El equipo deberá de contar con 24 puertos 10/100/1000Base Tx autosensados, POE, cuatro de estos puertos deberán soportar tecnología SFP. • El equipo deberá de contar con soporte a desempeño a velocidad de cable, es decir, el 100% de los puertos operando a máxima velocidad sin bloqueo ni sobresuscripción. • El equipo deberá de contar con un protocolo de anillo metropolitano. • Deberá de contar con un desempeño mínimo de 48 Gbps y 36 Mpps. • El equipo deberá proveer PoE Clase 3 (15.4W) en los 24 puertos de manera simultánea, de acuerdo al estándar 802.3af. • Deberá soportar redundancia en fuente de poder. **Funcionalidades:** • Soporte mínimo a 16,000 direcciones de MAC. • Soporte a agregación dinámica de enlaces vía 802.3ad • Monitoreo de puertos basado en listas de control de acceso. • Limitación del ancho de banda basado en listas de control de acceso. • Limitación de ancho de banda de trafico de broadcast , multicast y unicast desconocidos. • Monitoreo digital óptico o “Digital Optical Monitoring”. • Soporte a CDP “Cisco Discovery Protocol”. • Auto-configuración de dispositivos de VoIP. • Configuración de múltiples servidores de syslog.	EQUIPO	2	56, 678.96	113,357.92

	• Sincronizar de la fecha y la hora mediante un servidor de SNTP o “Simple Network Time Protocol”. • Soporte a VCT o “Virtual Cable Testing” utilizando TDR “Time Domain Reflectometry” para diagnostico de fallas en el cableado estructurado así como de RFC “Remote Fault Notification “ para puertos de Gigabit Ethernet. • Ajuste de IPG “Interpacket Gap” • Soporte a paquetes tipo “Jumbo Frames” con un mínimo de tamaño de 10240 bytes . • Soporte a LLDP y LLDP-MED • Deberá de soportar la retransmisión de paquetes de DHCP de diferentes VLANS. • Deberá de contar con soporte a ECMP “Equal Cost Multi Path”. • Deberá de soportar la configuración simultánea de mínimo de 1,000 rutas de ipV4 y de 255 interfaces virtuales de capa 3. **Administración** • Listas de control de acceso para controlar el acceso administrativo. • Port flap dampening. • Monitoreo Remoto (RMON) • sFlow via RFC 3167 con soporte a la extracción de los nombre de usuarios de EAP . • Acceso a la línea de comandos vía Telnet y puerto Serial. • Interface de administración vía GUI a través de HTTPS/SSL. • Soporte a SNMPv1 , SNMPv2 y SNMPv3. **Administración vía IPv6** El equipo deberá de soportar la administración del mismo mediante el protocolo de Ipv6 con las siguientes características: • Dirección de Ipv6 tipo Link-Local • Listas de control de acceso de Ipv6 • Herramientas de diagnostico de Ipv6 como “traceroute” y “ping” • Resolución de nombres o “DNS” vía Ipv6 • Administración vía HTTP/HTTPS vía Ipv6 • Syslog vía IPv6 • SCP y SSH vía IPv6 • SNMPv1/v2/v3 vía IPv6 • SNTP • TACACS/TACACS+				

	• Telnet • TFTP **Seguridad** • Soporte a 802.1x con asignación dinámica de ACL , Filtros de MAC y VLAN • Listas de control de acceso para filtrado de tráfico en tránsito. • Filtro de restricción de trafico basado en direcciones de MAC. • Soporte de encripción tipo AES para SSHv2. • Autentificación , Autorización y Contabilización (AAA) • Protección contra ataques de negación de Servicios. • DHCP Snooping • Listas de control de acceso dinámicas con autentificación de múltiples dispositivos por puerto. • Inspección dinámica de ARP • IP Source Guard • Filtrado de Capa 2 a través de dirección fuente y destino de MAC. • Capacidad de deshabilitar el aprendizaje de direcciones de MAC. • Seguridad basada en direcciones de MAC • Copia segura mediante SCP • Servidor de SSH v2 **Spanning Tree** Deberá de contar con el soporte a las siguientes características de Spanning Tree: • 802.1d Spanning Tree • 802.1s Multiple Spanning Tree • 802.1w Rapid Spanning Tree (RSTP) • Soporte a la configuración concurrente de hasta 254 instancias de STP. • Compatibilidad con PVST/PVST+ • Compatibilidad con PVRST+ • Además deberá de contar con funciones para asegurar el árbol de STP. **VLANS** Deberá de contar con las siguientes características : • Configuración de mínimo 4,000 VLANS • 802.1q • Vlans de modo dual. • GVRP • Vlans basadas en puerto				

	• Vlans basadas en protocolo (IPX, AppleTalk , IPv4 e IPv6) • Vlans basadas en subnets • Grupos de Vlans • Vlans privadas • Vlans tipo Q in Q con encapsulación vía el tipo de Ethernet 8100 • Monitoreo basado en Vlans • Vlans basadas en direcciones de MAC. **Calidad de Servicio (QoS)** Deberá de soportar los siguientes algoritmos de Calidad de Servicio: • Strict Priority • Weighted Round Robin (WRR) • Combinación de SP y WRR • 8 colas de prioridad. • DiffServ • Limitación del ancho de banda basado en listas de acceso y QoS • Mapeo de prioridades mediante Listas de control de acceso. • Mapeo de DSCP con valores del 1 al 8. **Multicast** Deberá de contar con el soporte de los siguientes protocolos de Multicast: • IGMP v1/v2 Snooping • IGMP v3 Snooping • IGMP v1/v2/v3 Snooping por VLAN • IGMP v2/v3 Fast Leave (con rastreo de grupos) • Filtrado de IGMP • MLD v1/v2 Snooping • MLD fast leave para v1 • Rastreo de MLD y fast leave para v2 • Configuracion estatica de MLD y de grupos de IGMP con soporte para proxy. • PIM-SM v2 Snooping **Ruteo (Capa 3)** Capacidad de contar con los siguientes protocolos de ruteo. • Ruteo de subredes directamente conectadas • Rutas estáticas • Anuncios de RIP v1/v2 • Capacidad de				

	Así mismo, el equipo podrá ser actualizado para ejecutar ruteo dinámico basado en (no se debe incluir la licencia para estos protocolos): • OSPFv1,v2 • RIP V1 , V2 **Compatibilidad** Para garantizar la compatibilidad de los equipos, el equipo deberá de contar con el soporte a los siguientes protocolos: IEEE • 802.1ab Station and Media Access Control Connectivity Discovery • 802.1d Ethernet Bridging • 802.1 MAC Bridges • 802.1p Mapping to Priority Queue • 802.1p/q VLAN Tagging • 802.1q Generic VLAN Registration Protocol (GVRP) • 802.1s Multiple Spanning tree • 802.1w Rapid Spanning Tree • 802.1x Port-based Network Access Control • 802.3 10Base-T • 802.3ab 1000Base-T • 802.3ad Link Aggregation • 802.3u 100Base-TX • 802.3z 1000Base-SX , 1000Base-LX • 802.3x Flow Control **El proveedor deberá presentar:** Carta en original por parte del fabricante donde se obligue solidariamente con el proveedor a avalar las características técnicas que no se encuentren respaldadas en los folletos (deberán ser impresas, en hojas membretadas y suscritas por el representante legal del fabricante). Carta en original por parte del fabricante especifique que es distribuidor certificado. Carta en original por parte del fabricante que asegure que el integrador cuenta con personal certificado. Deberá garantizar mediante carta compromiso, llevar a cabo la instalación, configuración, implementación y puesta en marcha de los equipos. Cumpliendo con las siguientes actividades y configuraciones: 1. Verificación del sitio designado para la instalación física de la unidad. 2. Desempacado de equipo y verificación de correcto funcionamiento. 3. Verificación del punto eléctrico de conexión.				

	4. Verificación de conectividad IP en el puerto designado proveniente de la red interna. 5. Instalación física de la unidad. 6. Definición de políticas de seguridad. 7. Definición de roles de usuarios o equipos. 8. Asignación de politicas de seguridad y rol al puerto correspondiente del Switch. 9. Generación de VLANs de acuerdo a los roles de usuario. 10. Definición de roles de servicio. 11. Definición de umbrales de calidad de servicio. 12. Asignación de umbrales. 13. Habilitación del switch para la plataforma de monitoreo.				
8	**Solución integral de unificación de amenazas administradas y conectividad de voz y datos** Sistema de Seguridad informática que sea del tipo Administración Unificada de Amenazas (UTM por sus siglas en inglés), donde se deberán ofrecer **ya incluidas y listas para ser utilizadas,** las funcionalidades que abajo se detallan, pudiendo ser todas ellas en una sola caja o en cajas diferentes, el dispositivo debe ser una appliance de propósito específico basado en tecnología ASIC y que sea capaz de brindar una solución de "Complete Content Protection". Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux. Capacidad de incrementar el rendimiento de VPN a través de soluciones en hardware dentro del mismo dispositivo **(mediante el uso de un ASIC).** Capacidad de re-ensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware **(mediante el uso de un ASIC).** El equipo deberá poder ser configurado en modo Gateway o en modo transparente en la red en modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP, sistema operativo pre-endurecido específico para seguridad que sea compatible con el appliance. Por seguridad y facilidad de administración y operación, no se aceptan soluciones sobre sistemas operativos genéricos tales como GNU/Linux, FreeBSD, SUN Solaris, HP-UX de HP, AIX de IBM o Microsoft Windows **Firewall.** Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs. Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando	EQUIPO	1	91,959.40	91,959.40

	en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall. Las reglas del firewall deberán tomar en cuenta dirección IP fuente (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando. Las acciones de las reglas deberán contener al menos el aceptar o rechazar la comunicación. Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino. Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo. Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año). Capacidad de hacer traslación de direcciones estático, uno a uno, NAT. Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT. Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario). Se debe considerar al menos el tener una interface/puerto DMZ y 2 puertos para enlaces WAN. Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (*Relay*) de solicitudes DHCP. Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs. Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas. Soporte a políticas de ruteo (policy routing). El soporte a políticas de ruteo deberá permitir que ante la presencia de dos enlaces a Internet, se pueda decidir cuál de tráfico sale por un enlace y qué tráfico sale por otro enlace. Soporte a ruteo dinámico RIP V1, V2, OSPF y BGP. Soporte a ruteo de multicast. Deberá realizar VPN IPSec con soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site) Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES. Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits Posibilidad de crear VPN's entre Gateway y clientes con IPSec. Esto es, VPNs IPSec site-to-site y VPNs IPSec client-to-site. a VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN) en modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para				

	ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall. Capacidad de realizar SSL VPNs, soporte a certificados PKI X.509 para construcción de VPNs SSL, soporte a asignación de aplicaciones permitidas por grupo de usuarios. Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet. Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL. Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning). La VPN SSL integrada deberá soportar a través de algún plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS. Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL. Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente. **Traffic Shapping / QoS** Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall. Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo. Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo. Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia. **Autenticación y Certificación Digital.** Capacidad de integrarse con Servidores de Autenticación RADIUS. Capacidad nativa de integrarse con directorios LDAP. Capacidad incluida, al integrarse con Microsoft Windows Active Directory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto “Single-Sign-On”. Capacidad de autenticar usuarios para cualquier aplicación que se ejecute bajo los protocolos TCP/UDP/ICMP. Debe de mostrar solicitud de autenticación (Prompt) al menos para Web (HTTP), FTP y Telnet. Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site). Soporte a inclusión en autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol) y mediante archivos. Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP. Antivirus en tiempo real, 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 categorización del contenido. La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP deberá estar completamente integrada a la administración del dispositivo appliance, que permita la aplicación de esta protección por política de control de acceso. Por desempeño y eficiencia, el antivirus deberá funcionar bajo el esquema "Wild list" (Virus en activo solamente) en el cual los virus conocidos que están activos en el Internet son los que se detectan y se detienen. El appliance deberá de manera opcional poder inspeccionar por todos los virus conocidos (Zoo List). El Antivirus integrado deberá tener la capacidad de poner en cuarentena archivos encontrados infectados que estén circulando a través de los protocolos HTTP, FTP, IMAP, POP3, SMTP. El Antivirus deberá incluir capacidades de detección y detención de tráfico spyware, adware y otros tipos de malware/grayware que pudieran circular por la red. El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging) para al menos MSN Messenger. El antivirus deberá ser capaz de filtrar archivos por extensión El antivirus deberá ser capaz de filtrar archivos por tipo de archivo (ejecutables por ejemplo) sin importar la extensión que tenga el archivo Capacidad de actualización automática de firmas Antivirus mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas). **AntiSpam.** La capacidad AntiSpam incluida deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje. La capacidad AntiSpam incluida deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address) La capacidad AntiSpam deberá poder consultar una base de datos donde se revise por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y checksum del mensaje, como mecanismos para detección de SPAM En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje. **Filtraje de URLs (URL Filtering).**				

	Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 39 millones de sitios web en la base de datos. Filtrado de contenido basado en categorías en tiempo real, 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 categorización del contenido. Configurable directamente desde la interfaz de administración del dispositivo appliance. Con capacidad para permitir esta protección por política de control de acceso. Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables. Capacidad de filtrado de scripts en páginas web (JAVA/Active X). **Protección contra intrusos (IPS).** Capacidad de detección de más de 1400 ataques. Capacidad de actualización automática de firmas IPS mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas) El Detector y preventor de intrusos deberá de estar orientado para la protección de redes. El detector y preventor de intrusos 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 detector y preventor de intrusos 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. Esta deberá permitir la protección de este servicio por política de control de acceso. El detector y preventor de intrusos deberá soportar captar ataques por Anomalía (Anomaly detection) además de firmas (signature based / misuse detection). Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo. Tecnología de detección tipo Stateful basada en Firmas (signatures). Actualización automática de firmas para el detector de intrusos El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios. Mecanismos de detección de ataques: Reconocimiento de patrones, Análisis de protocolos, Detección de anomalías Detección de ataques de RPC (Remote procedure call) Protección contra ataques				

	de Windows o NetBios Protección contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail o POP (Post Office Protocol) Protección contra ataques DNS (Domain Name System) Protección contra ataques a FTP, SSH , Telnet y rlogin Protección contra ataques de ICMP (Internet Control Message Protocol).Métodos de notificación: Alarmas mostradas en la consola de administración del appliance. Alertas vía correo electrónico. **Filtraje de tráfico VoIP, *Peer-to-Peer* y Mensajería instantánea.** Soporte a aplicaciones multimedia tales como (incluyendo) : SCCP (Skinny), H.323, SIP, Real Time Streaming Protocol (RTSP). El dispositivo deberá técnicas de detección de P2P y programas de archivos compartidos (peer-to-peer), soportando al menos Yahoo! Messenger, MSN Messenger, ICQ y AOL Messenger para Messenger, y BitTorrent, eDonkey, GNUTella, KaZaa, Skype y WinNY para Peer-to-peer. En el caso de los programas para compartir archivos (peer-to-peer) deberá poder limitar el ancho de banda utilizado por ellos, de manera individual. **Alta Disponibilidad.** Posibilidad en Firewall Soporte a Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle. Alta Disponibilidad en modo Activo-Pasivo Alta Disponibilidad en modo Activo-Activo Posibilidad de definir al menos dos interfaces para sincronía El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red. **Características de Gerencia.** Interfase gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfase debe soportar SSL sobre HTTP (HTTPS) La interfase gráfica de usuario (GUÏ) vía Web deberá poder estar en español y en inglés, configurable por el usuario. Interfase basada en línea de comando (CLI) para administración de la solución. Puerto serial dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto. Comunicación cifrada y autenticada con username y password, tanto como para la interfase gráfica de usuario como la consola de administración de línea de comandos (SSH o telnet) El administrador del sistema podrá tener las opciones incluídas de autenticarse vía password y vía certificados digitales. Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar. El equipo ofrecerá la flexibilidad para especificar que Los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet,http o HTTPS. El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier				

	equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningun software adicional. Soporte de SNMP versión 2 Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall. Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red. **Virtualización.** El dispositivo deberá poder virtualizar los servicios de seguridad mediante “Virtual Systems”, “Virtual Firewalls” o “Virtual Domains” La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS y Antivirus Se debe incluir la licencia para al menos 8 (ocho) instancias virtuales dentro de la solución a proveer. Cada instancia virtual debe poder tener un administrador independiente La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales. Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red. La solución debería contar con al menos las siguientes certificaciones y cumplir con los siguientes estándares Certificación ICSA para el Firewall. Certificación ICSA IPSEC. (VPN IPSec) Certificación ICSA para SSL-TLS (VPN SSL) Certificación ICSA para el Detector de Intrusos (IPS) Certificación ICSA para el Antivirus Certificación NSS como UTM Certificación Common Criteria como EAL4+ soporte documentado de los siguientes RFCs: RFC 0768, RFC 0791, RFC 0792, RFC 0793, RFC 0822, RFC 1035, RFC 1112, RFC 1119, RFC 1123, RFC 1191, RFC 1323, RFC 1340, RFC 1349, RFC 1519, RFC 1577, RFC 1700, RFC 1812, RFC 1918, RFC 2131, RFC 2181, RFC 2225, RFC 2236, RFC 2373, RFC 2460, RFC 2461, RFC 2462, RFC 2474, RFC 2822, RFC 3232, RFC 3456, RFC 3513, RFC 4291, RFC 1866, RFC 1867, RFC 1945, RFC 2068, RFC 2616, RFC 2817, RFC 2854, RFC 1321, RFC 1631, RFC 1829, RFC 2104, RFC 2401, RFC 2403, RFC 2404, RFC 2405, RFC 2406, RFC 2407, RFC 2408, RFC 2409, RFC 2410, RFC 2411, RFC 2412, RFC 2459, RFC 2631, RFC 2637, RFC 2661, RFC 3706. Soporte documentado a los siguientes estándares de criptografía: PKCS #7 (RFC 2315), PKCS #10 (RFC 2986), PKCS #12. El equipo debe por lo menos ofrecer las siguientes características de desempeño y conectividad rendimiento de antivirus 95Mbps, ips 500Mbps, que soporte 500,000 sesiones concurrentes, 15000 nuevas sesiones por segundo firewall 5Gbps por segundo, el túnel de VPN deberá ofrecer 2.5Gbps, con capacidad de crear 100,000 políticas, deberá ser compatible con RoHS libre de DMF.				

	4 Interfaces 10/100/1000, 8 10/100 Switch Interfaces, 1 puerto FSM Storage Bay y 3 USB. El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, cajas de correo, conexiones, equipos que pasan a través de la vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS y URL Filtering debe proveerse por al menos 1 año **El proveedor de la solución deberá incluir:** Carta en original por parte del fabricante donde se avala como Distribuidor Autorizado específica para esta licitación. Carta por parte del fabricante en original que avale que el proveedor cuenta con personal técnico capacitado para la instalación del proyecto. Carta directa del fabricante en original firmada por el representante legal que respalde que la garantía de los equipos puede ser tramitada directamente por el proponente. El proveedor deberá realizar la instalación, configuración, implementación y puesta a punto en sitio por personal capacitado, cubriendo los siguientes puntos: • Pruebas de Conexión a Internet desde el Firewall. • Generación de políticas para el uso del internet(hasta 6 niveles de uso de Internet). • Configuración de las políticas por Usuario, Segmento de Red, o IP única. • Pruebas de los Niveles o Políticas implementadas. • Configuración de VPN punto a punto con sitio central (Xalapa). • Optimización de VPN. • Pruebas de Trafico sobre VPN (Voz y Datos). El proveedor brindará un curso de capacitación con una duración de 8 horas al personal técnico del organismo. El contenido del curso deberá incluir como mínimo la configuración, puesta en marcha y administración de las funcionalidades de los equipos propuestos, así como la solución a problemas que pudiera presentar los equipos propuestos.				
		SUBTOTAL			**$ 273,486.07**
		IVA			**43, 757.77**
		TOTAL			**$ 317,243.84**