Anexo – Especificaciones Técnicas

**Renglón Nº 1 (cantidad: 1)**

**Firewall (cortafuegos) con funciones de ruteo y servicios de seguridad.**

**Especificaciones técnicas a cumplir:**
Equipo totalmente nuevo, sin uso, en su empaque original. (no se aceptaran equipos "refurbished" o reacondicionados).

**Especificaciones de Hardware:**
• Al menos 4 Puertos integrados de 10GbE SFP+
• Al menos 4 Puertos integrados de 1GbE (SFP) .
• Al menos 12 Puerto integrados RJ-45 de 1GbE.
• 1 Puerto de administración OOB (Out of Band) de 1 GbE.
• 1 Puerto dedicado para alta disponibilidad (HA) de 1GbE (SFP).
• Al menos 2 Slots PIM (Physical Interface Module).
• 1 Puerto de acceso a Consola (RJ-45 + miniUSB).
• Al menos 1 Puerto USB 2.0 (tipo A).
• Memoria del sistema (RAM) 16 GB (mínimo)
• Almacenamiento inicial de arranque (mSATA) 16 GB (mínimo).
• Almacenamiento secundario (SSD) 120 GB (mínimo).
• Kit para rack 19", 1 U.
• Fuente de alimentación redundante 1 + 1.
• Fuente de alimentación AC interna 220V.
    - Clasificación FCC Clase A.
    - Que Cumpla RoHS RoHS 2.

**Protocolos que debe soportar:**
• Soporte para IPv6 en forma nativa.
• Rutas estáticas.
• RIP (Routing Information Protocol ) v1 / v2.
• OSPF (Open Shortest Path First ) v2 y v3.
• BGP (Border Gateway Protocol) v4.
• Multicast: Protocolo de administración de grupos de Internet (IGMP) v1 / v2.
• Protocol Independent Multicast (PIM).
• Protocolo Simple de Administración de Red o **SNMP** (Simple Network Management Protocol).
• Modo escaso (SM) / modo denso (DM) / multicast específico de la fuente (SSM).
• Protocolo de descripción de sesión (SDP).
• Protocolo de ruteo multicast o multidifucion (DVMRP).
• MSDP (Multicast Source Discovery Protocol).
• Protocolo de configuración de host dinámico (DHCP) cliente / servidor / relay.
• Reenvío de ruta inversa (RPF).
• Encapsulación: VLAN, Protocolo punto a punto sobre Ethernet (PPPoE).
• Protocolo de redundancia de Gateway tal como Hot-Standby Routing Protocol (HSRP) o Virtual Router Redundancy Protocol (VRRP) para IPv4 e IPv6.
• Enrutamiento basado en directivas, enrutamiento basado en origen.
• Caminos múltiples (ECMP).
• MPLS (Multiprotocol Label Switching).
• RSVP (Resource Reservation Protocol).
• LDP (Label Distribution Protocol).
• L2 / L2 MPLS (Multiprotocol Label Switching) VPN, pseudowires.
• Ingeniería de tráfico MPLS y redirección rápida MPLS.

**Funcionalidades de Firewall que debe permitir:**
• Filtrado de paquetes con estado (Stateful) y sin estado (Stateless).
• Filtrado de paquetes stateful con inspecion (SPI) y control de aplicaciones (AIC).
• Definición de reglas basadas en zonas.
• Definición de reglas basadas en ACLs (Access Control List).
• Protección contra DDoS ( Denegación de servicio).
• Protección contra anomalías de protocolo y tráfico.
• Control de acceso unificado (UAC).

• Soportar al menos 8000 reglas.
• SNAT (Source Network Address Translation) , SNAT con PAT (Port Address Translation).
• SNAT estático.
• DNAT (Destination Network Address Translation) con PAT.
• NAT persistente, NAT64.
• Traducción de direcciones IPv6.
• Características NAT (Network address translation): debe incluir la posibilidad de crear NATs dinámicos (N-1 o Hide) y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete y en una sola regla.
• Posibilidad de negar los parámetros de Origen o Destino, es decir que para una regla dada, permite todas las conexiones de origen / destino excepto la especificada en la regla.
• Implementar reglas aplicadas a intervalos de tiempo específicos ( por ejemplo: de lunes a viernes de 8 a 20 hs).

**Funcionalidades de Calidad de Servicio (QoS) que debe soportar:**
• Soporte para 802.1p, DiffServ (DSCP), EXP
• Clasificación basada en VLAN, DLCI (Data Link Connection Identifier), interfas, puertos, paquetes o filtros multi-campos.
• Marcado, recorte y encolamiento de tráfico.
• Clasificación y programación.
• Detección temprana aleatoria (WRED).
• Ancho de banda garantizado y máximo.
• Capacidad para definir políticas de tráfico de entrada.
• Capacidad para definir Canales virtuales.

**Funciones de IPS (Intrusion Prevention System) que debe cumplir:**
• Brindar la posibilidad de realizar identificación de equipos por IP o por MAC.
• Brindar la posibilidad de realizar Filtrado de URLs (Uniform Resource Locator - Localizador Uniforme de Recursos).
• Brindar la posibilidad de realizar Control de Aplicaciones sin la necesidad de introducir una solución adicional y deberá cumplir los siguientes requerimientos:
- Detección
- Control
- Clasificación
- Relevancia
- Bloqueo

• Reconocer más de 3.000 aplicaciones clasificadas por riesgo, y esta base de reconocimiento deberá actualizarse periódicamente.
• Brindar la detección avanzada de amenazas con análisis contextual.
• Brindar la detección avanzada de amenazas con geolocalización .
• Brindar la posiblidad de automatizar tareas, reconfiguradas por el usuario administrador, para que se puedan ejecutar tareas de mantenimiento sin afectar el funcionamiento de las demás capacidades del equipo.
• Deberá mitigar las siguientes amenazas:
- Troyanos
- Gusanos
- Ataques del tipo "Backdoor"
- Escaneo de puertos.
- Spyware.
- Ataques a la infraestructura VolP.
- Ataques a la infraestructura IPv6.
- Ataques del tipo "Buffer Overflow"
- Ataques de Denegación de Servicios Distribuido.
- Ataques del tipo "P2P" (“Pear to Pear” o “Punto a Punto”)
- Anomalías de Aplicación.
- Anomalías de Protocolo.
- Encabezados no validos.
- Fragmentación IP y Segmentación TCP .
- Detección y Mitigación de Amenazas de Múltiples Factores.

- Amenazas de Día Cero (Zero Day) (OPCIONAL).

• La base de firmas deberá actualizarse de manera regular, pudiendo actualizar la base de reglas de manera automática, sí el usuario administrador así lo permite.
• Deberá poder monitorear tráfico en tiempo real sin provocar irrupción del servicio.
• El usuario administrador tendrá la facilidad de configurar el motor de detección y mitigación de ataques de manera individual.
• El usuario administrador tendrá la facilidad de configurar políticas del motor de detección y mitigación de ataques de manera individual.
• Brindar la habilidad de permitir, bloquear o limitar el acceso (basado en tiempo o en ancho de banda).

**Funciones de VPN que debe soportar:**
• Al menos 2000 túneles VPN .
• Túneles: (GRE), IP-IP, Ipsec.
• VPN punto a punto IPsec, VPN automática, VPN de grupo.
• Algoritmos de cifrado IPsec: Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES-256).
• Algoritmos de autenticación IPsec: MD5, SHA-1, SHA-128, SHA-256.
• Infraestructura de claves públicas y privada (PKI) precompartida (X.509).
• Soporte PFS.
• IPv4 e IPv6 IPsec VPN.
• ID de proxy múltiple para VPN punto a punto.
• Intercambio de claves de Internet (IKEv1, IKEv2), NAT-T.
• Enrutador virtual y de calidad de servicio (QoS).
• Detección de puntos muertos (DPD).

**Funciones Alta Disponibilidad ( HA) que debe cumplir:**
• Protocolo VRRP (Virtual Router Redundancy Protocol).
• Estado de alta disponibilidad.
- Clúster “dual BOX”.
- Modos de HA: Activo / pasivo - Activo / activo -
- Sincronización de la configuración.
- Sincronización de sesión de cortafuegos (Firewall).
- Detección de dispositivo / enlace.

• Monitoreo IP con conmutación por error de ruta e interfaz.

**Funciones de Administración, Automatización, Registro e Informes que debe cumplir:**
• Soportar métodos de autenticación, por usuario, por cliente y por sesión.
• Ser capaz de autenticar sesiones de cualquier servicio .
• Permitir el acceso a consola a través de SSH (v2), Telnet, HTTPs.
• Tener todos los conjuntos de reglas, objetos, usuarios locales de todo el funcionamiento del Firewall, almacenados en la consola única de administración.
• Tener la posibilidad de generar un punto de restauración desde la consola de administración que permita volver a una configuración anterior de todas las funcionalidades involucradas en el firewall.
• Descarga inteligente de imágenes.
• Acceso a interfaz por consola y/o web.
• Programación por scripts.
• Soporte de scripts en lenguaje Python.
• Informes de uso y uso de ancho de banda.
• Auto instalación.
• Herramientas de depuración y solución de problemas.
• Almacenar todos los logs y registros del sistema, en la consola de administración para su análisis.
• Realizar logs remoto.
• Realizar backup de las configuraciones.
• Proporcionar una consola gráfica que permita:
- visualizar los logs almacenados.
- filtrar la visualización de los logs/eventos mediante diferentes características, (por ejemplo: direccion IP origen, dirección IP destino, puerto, MAC, regla aplicada,etc).
- proporcionar información estadística de los eventos que se estén visualizando en la misma.
- proporcionar información de tráfico en tiempo real de las interfaces del firewall.
- monitorear uso de CPU, memoria, espacio libre en disco, estado de la licencia de software.

- generar múltiples búsquedas de logs/eventos simultáneamente.
- generar alertas, que notifiquen via log, email o SNMP (Simple Network Management Protocol) , en caso que alguna variable tenga un uso exceso de recurso, (Por ejemplo uso de cpu> 90% ; ancho de banda utilizado por una interface superior a 100 MB)

- Debe permitir la visualización de los eventos en tiempo real generados por todos los servicios de seguridad.
- Debe permitir la generación de reportes periódicos, diarios, semanales, mensuales de los diferentes eventos producidos por los diferentes eventos. Por ejemplo top de ataques de IPS, top origen eventos de IPS, etc.
- Debe permitir enviar los reportes por la herramienta en forma automática.
- Permitir monitoreo del rendimiento en tiempo real (RPM), monitoreo por IP.
- Permitir monitoreo por flujo (Flow).

**Capacidades mínimas de rendimiento que debe soportar:**
- Ancho de banda de Enrutamiento / cortafuegos (tamaño de paquete 64 B) : 1.7 Mpps
- Ancho de banda de Enrutamiento / cortafuegos (tamaño de paquete IMIX) : 5 Gbps
- Ancho de banda de Enrutamiento / firewall (1.518 tamaño de paquete B): 9 Gbps
- Ancho de banda con IPsec VPN (tamaño de paquete IMIX) : 1 Gbps
- Ancho de banda con IPsec VPN (tamaño de paquete 1.400 B): 2 Gbps
- Ancho de banda en Visibilidad y control de aplicaciones: 4 Gbps.
- Ancho de banda de IPS : 3 Gbps.
- Tamaño de la tabla de ruteo (RIB / FIB) IPv4: 2 millones.
- Tamaño de la tabla de ruteo (RIB / FIB) IPv6: 1 millón.
- Sesiones simultáneas (IPv4 o IPv6) al menos 2.000.000.
- Políticas de seguridad, al menos 16.000.
- Conexiones por segundo: 50.000.
- Reglas NAT : 8.000.
- Tamaño de tabla de control de acceso a medios (MAC): 64.000.
- Túneles VPN IPsec : 2.000.
- Túneles GRE 2.000.
- Zonas de máxima seguridad: 512.
- Enrutador virtual, al menos 512.
- VLAN al menos 1000.
- Sesiones de AppID: 512.000.
- Sesiones de IPS: 512.000.
- Sesiones de filtrado de URL : 512.000.

**Software y licencia necesario para que cumpla con las funciones descriptas anteriormente:**
- El equipo debe suministrarse con el software necesario para cubrir el 100% de las funcionalidades descriptas anteriormente.
- El equipo debe tener la posibilidad de actualizar su software en forma regular y/o de descargar nuevas versiones de software provisto por el fabricante.
- Todas las características de ruteo, protocolos, IPS (Intrusion Prevention System) , firewall, QoS (Calidad de Servicio), VPN, HA (Alta Disponibilidad), Administracion, Registro e Informes mencionadas anteriormente, deberán funcionar en forma conjunta, con los valores mínimos de rendimiento indicados.

La licencia de uso del software, deberá tener validez mínima de 1 año.

La fecha de activación de la licencia deberá comenzar 10 dias posteriores a la

recepción del equipo.

La licencia por uso del software deberá ser renovable, por períodos no menores a 1 (un) año de validez.

El equipo ofertado debe contar con una garantía mínima de funcionamiento de 1 (un) año, contado a partir de la puesta en funcionamiento, sobre todo el hardware y software instalado.

El equipo deberá contar con soporte técnico disponibe para consultas telefónicas y/o por correo electrónico.

El equipo debe suministrarse con la documentación necesaria para su configuración y funcionamiento.

## DEBE INCLUIR:

**3 (Tres) Módulos SFP 1G totalmente compatible con el firewall**
**Características:**
Para fibra óptica monomodo, 1310 – 1550 nanómetros. 10 km.
1 Ggps ethernet
Tipo de conector: LC

**3 (Tres) Modulos SFP+ 10G totalmente compatible con el firewall**
Características:
Para fibra óptica multimodo 62,5/125 micrones
10 Gbps ethernet para 30 metros aproximadamente.
Tipo de conector conector: LC

**5 (Cinco) Modulo SFP 1 GB totalmente compatible con el gateway**
Características:
Para fibra óptica multimodo 62,5/125 micrones
1 Gbps ethernet para 30 metros aproximadamente.
Tipo de conector conector: LC

**5 (Cinco) Patch cord de fibra óptica.**
Largo: 3 mts.
Tipo de conector conector: LC-PC dúplex en ambas puntas.
Tipo de fibra óptica: monomodo

**5 (Cinco) Patch cord de fibra óptica.**
Largo: 3 mts.
Tipo de conector conector: LC-PC dúplex en ambas puntas.
Tipo de fibra óptica: multimodo

**Renglón Nº 2 (cantidad: 1)**

**Firewall (cortafuegos) con funciones de ruteo**

**Especificaciones técnicas a cumplir:**
Equipo totalmente nuevo, sin uso, en su empaque original. (no se aceptaran equipos “refurbished” o reacondicionados).

**Especificaciones de Hardware:**
• Al menos 4 Puertos integrados de 10GbE SFP+
• Al menos 4 Puertos integrados de 1GbE (SFP) .
• Al menos 12 Puerto integrados RJ-45 de 1GbE.
• 1 Puerto de administración OOB (Out of Band) de 1 GbE.
• 1 Puerto dedicado para alta disponibilidad (HA) de 1GbE (SFP).
• Al menos 2 Slots PIM (Physical Interface Module).
• 1 Puerto de acceso a Consola (RJ-45 + miniUSB).
• Al menos 1 Puerto USB 2.0 (tipo A).
• Memoria del sistema (RAM) 16 GB (mínimo)
• Almacenamiento inicial de arranque (mSATA) 16 GB (mínimo).
• Almacenamiento secundario (SSD) 120 GB (mínimo).
• Kit para rack 19”, 1 U.
• Fuente de alimentación redundante 1 + 1.
• Fuente de alimentación AC interna 220V.
    - Clasificación FCC Clase A.
    - Que Cumpla RoHS RoHS 2.

# Anexo – Especificaciones Técnicas

**Protocolos que debe soportar:**
• Soporte para IPv6 en forma nativa.
• Rutas estáticas.
• RIP (Routing Information Protocol ) v1 / v2.
• OSPF (Open Shortest Path First ) v2 y v3.
• BGP (Border Gateway Protocol) v4.
• Multicast: Protocolo de administración de grupos de Internet (IGMP) v1 / v2.
• Protocol Independent Multicast (PIM).
• Protocolo Simple de Administración de Red o **SNMP** (Simple Network Management Protocol).
• Modo escaso (SM) / modo denso (DM) / multicast específico de la fuente (SSM).
• Protocolo de descripción de sesión (SDP).
• Protocolo de ruteo multicast o multidifucion (DVMRP).
• MSDP (Multicast Source Discovery Protocol).
• Protocolo de configuración de host dinámico (DHCP) cliente / servidor / relay.
• Reenvío de ruta inversa (RPF).
• Encapsulación: VLAN, Protocolo punto a punto sobre Ethernet (PPPoE).
• Protocolo de redundancia de Gateway tal como Hot-Standby Routing Protocol (HSRP) o Virtual Router Redundancy Protocol (VRRP) para IPv4 e IPv6.
• Enrutamiento basado en directivas, enrutamiento basado en origen.
• Caminos múltiples (ECMP).
• MPLS (Multiprotocol Label Switching).
• RSVP (Resource Reservation Protocol).
• LDP (Label Distribution Protocol).
• L2 / L2 MPLS (Multiprotocol Label Switching) VPN, pseudowires.
• Ingeniería de tráfico MPLS y redirección rápida MPLS.

**Funcionalidades de Firewall que debe permitir:**
• Filtrado de paquetes con estado (Stateful) y sin estado (Stateless).
• Filtrado de paquetes stateful con inspecion (SPI) y control de aplicaciones (AIC).
• Definición de reglas basadas en zonas.
• Definición de reglas basadas en ACLs (Access Control List).
• Protección contra DDoS ( Denegación de servicio).
• Protección contra anomalías de protocolo y tráfico.
• Control de acceso unificado (UAC).
• Soportar al menos 8000 reglas.
• SNAT (Source Network Address Translation) , SNAT con PAT (Port Address Translation).
• SNAT estático.
• DNAT (Destination Network Address Translation) con PAT.
• NAT persistente, NAT64.
• Traducción de direcciones IPv6.
• Características NAT (Network address translation): debe incluir la posibilidad de crear NATs dinámicos (N-1 o Hide) y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete y en una sola regla.
• Posibilidad de negar los parámetros de Origen o Destino, es decir que para una regla dada, permite todas las conexiones de origen / destino excepto la especificada en la regla.
• Implementar reglas aplicadas a intervalos de tiempo específicos ( por ejemplo: de lunes a viernes de 8 a 20 hs).

**Funcionalidades de Calidad de Servicio (QoS) que debe soportar:**
• Soporte para 802.1p, DiffServ (DSCP), EXP
• Clasificación basada en VLAN, DLCI (Data Link Connection Identifier), interfas, puertos, paquetes o filtros multi-campos.
• Marcado, recorte y encolamiento de tráfico.
• Clasificación y programación.
• Detección temprana aleatoria (WRED).
• Ancho de banda garantizado y máximo.
• Capacidad para definir políticas de tráfico de entrada.
• Capacidad para definir Canales virtuales.

**Funciones de VPN que debe soportar:**

• Al menos 2000 túneles VPN .
• Túneles: (GRE), IP-IP, Ipsec.
• VPN punto a punto IPsec, VPN automática, VPN de grupo.
• Algoritmos de cifrado IPsec: Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES-256).
• Algoritmos de autenticación IPsec: MD5, SHA-1, SHA-128, SHA-256.
• Infraestructura de claves públicas y privada (PKI) precompartida (X.509).
• Soporte PFS.
• IPv4 e IPv6 IPsec VPN.
• ID de proxy múltiple para VPN punto a punto.
• Intercambio de claves de Internet (IKEv1, IKEv2), NAT-T.
• Enrutador virtual y de calidad de servicio (QoS).
• Detección de puntos muertos (DPD).

**Funciones Alta Disponibilidad ( HA) que debe cumplir:**
• Protocolo VRRP (Virtual Router Redundancy Protocol).
• Estado de alta disponibilidad.
    • Clúster “dual BOX”.
    • Modos de HA: Activo / pasivo - Activo / activo -
    • Sincronización de la configuración.
    • Sincronización de sesión de cortafuegos (Firewall).
    • Detección de dispositivo / enlace.
• Monitoreo IP con conmutación por error de ruta e interfaz.

**Funciones de Administración, Automatización, Registro e Informes que debe cumplir:**
• Soportar métodos de autenticación, por usuario, por cliente y por sesión.
• Ser capaz de autenticar sesiones de cualquier servicio .
• Permitir el acceso a consola a través de SSH (v2), Telnet, HTTPs.
• Tener todos los conjuntos de reglas, objetos, usuarios locales de todo el funcionamiento del Firewall, almacenados en la consola única de administración.
• Tener la posibilidad de generar un punto de restauración desde la consola de administración que permita volver a una configuración anterior de todas las funcionalidades involucradas en el firewall.
• Descarga inteligente de imágenes.
• Acceso a interfaz por consola y/o web.
• Programación por scripts.
• Soporte de scripts en lenguaje Python.
• Informes de uso y uso de ancho de banda.
• Auto instalación.
• Herramientas de depuración y solución de problemas.
• Almacenar todos los logs y registros del sistema, en la consola de administración para su análisis.
• Realizar logs remoto.
• Realizar backup de las configuraciones.
• Proporcionar una consola gráfica que permita:
    • visualizar los logs almacenados.
    • filtrar la visualización de los logs/eventos mediante diferentes características, (por ejemplo: direccion IP origen, dirección IP destino, puerto, MAC, regla aplicada,etc).
    • proporcionar información estadística de los eventos que se estén visualizando en la misma.
    • proporcionar información de tráfico en tiempo real de las interfaces del firewall.
    • monitorear uso de CPU, memoria, espacio libre en disco, estado de la licencia de software.
    • generar múltiples búsquedas de logs/eventos simultáneamente.
    • generar alertas, que notifiquen via log, email o SNMP (Simple Network Management Protocol) , en caso que alguna variable tenga un uso exceso de recurso, (Por ejemplo uso de cpu> 90% ; ancho de banda utilizado por una interface superior a 100 MB)

• Debe permitir la visualización de los eventos en tiempo real generados por todos los servicios de seguridad.
• Debe permitir la generación de reportes periódicos, diarios, semanales, mensuales de los diferentes eventos producidos por los diferentes eventos. Por ejemplo top de ataques de IPS, top origen eventos de IPS, etc.

• Debe permitir enviar los reportes por la herramienta en forma automática.
• Permitir monitoreo del rendimiento en tiempo real (RPM), monitoreo por IP.
• Permitir monitoreo por flujo (Flow).

**Capacidades mínimas de rendimiento que debe soportar:**
• Ancho de banda de Enrutamiento / cortafuegos (tamaño de paquete 64 B) : 1.7 Mpps
• Ancho de banda de Enrutamiento / cortafuegos (tamaño de paquete IMIX) : 5 Gbps
• Ancho de banda de Enrutamiento / firewall (1.518 tamaño de paquete B): 9 Gbps
• Ancho de banda con IPsec VPN (tamaño de paquete IMIX) : 1 Gbps
• Ancho de banda con IPsec VPN (tamaño de paquete 1.400 B): 2 Gbps
• Ancho de banda en Visibilidad y control de aplicaciones: 4 Gbps.
• Ancho de banda de IPS : 3 Gbps.
• Tamaño de la tabla de ruteo (RIB / FIB) IPv4: 2 millones.
• Tamaño de la tabla de ruteo (RIB / FIB) IPv6: 1 millón.
• Sesiones simultáneas (IPv4 o IPv6) al menos 2.000.000.
• Políticas de seguridad, al menos 16.000.
• Conexiones por segundo: 50.000.
• Reglas NAT : 8.000.
• Tamaño de tabla de control de acceso a medios (MAC): 64.000.
• Túneles VPN IPsec : 2.000.
• Túneles GRE 2.000.
• Zonas de máxima seguridad: 512.
• Enrutador virtual, al menos 512.
• VLAN al menos 1000.
• Sesiones de AppID: 512.000.
• Sesiones de IPS: 512.000.
• Sesiones de filtrado de URL : 512.000.

**Software y licencia necesario para que cumpla con las funciones descriptas anteriormente:**
• El equipo debe suministrarse con el software necesario para cubrir el 100% de las funcionalidades descriptas anteriormente.
• El equipo debe tener la posibilidad de actualizar su software en forma regular y/o de descargar nuevas versiones de software provisto por el fabricante.
• Todas las características de ruteo, protocolos, IPS (Intrusion Prevention System) , firewall, QoS (Calidad de Servicio), VPN, HA (Alta Disponibilidad), Administracion, Registro e Informes mencionadas anteriormente, deberán funcionar en forma conjunta, con los valores mínimos de rendimiento indicados.

La licencia de uso del software, deberá tener validez mínima de 1 año.

La fecha de activación de la licencia deberá comenzar 10 dias posteriores a la

recepción del equipo.

La licencia por uso del software deberá ser renovable, por períodos no menores a 1 (un) año de validez.

El equipo ofertado debe contar con una garantía mínima de funcionamiento de 1 (un) año, contado a partir de la puesta en funcionamiento, sobre todo el hardware y software instalado.

El equipo deberá contar con soporte técnico disponibe para consultas telefónicas y/o por correo electrónico.

El equipo debe suministrarse con la documentación necesaria para su configuración y funcionamiento.

## DEBE INCLUIR:

- **3 (Tres) Módulos SFP 1G totalmente compatible con el firewall**
  Características:
  Para fibra óptica monomodo, 1310 – 1550 nanómetros. 10 km.
  1 Ggps ethernet
  Tipo de conector: LC

- **3 (Tres) Modulos SFP+ 10G totalmente compatible con el firewall**
  Características:

Para fibra óptica multimodo 62,5/125 micrones
10 Gbps ethernet para 30 metros aproximadamente.
Tipo de conector conector: LC

- **5 (Cinco)  Modulo SFP 1 GB totalmente compatible con el gateway**
  Características:
  Para fibra óptica multimodo 62,5/125 micrones
  1 Gbps ethernet para 30 metros aproximadamente.
  Tipo de conector conector: LC

- **5 (Cinco) Patch cord de fibra óptica.**
  Largo: 3 mts.
  Tipo de conector conector: LC-PC dúplex en ambas puntas.
  Tipo de fibra óptica: monomodo

- **5 (Cinco) Patch cord de fibra óptica.**
  Largo: 3 mts.
  Tipo de conector conector: LC-PC dúplex en ambas puntas.
  Tipo de fibra óptica: multimodo