ANEXO TÉCNICO

1. JUSTIFICACIÓN.

Los equipos de seguridad del Perímetro "Firewall", son equipos de propósito específico destinado a proteger una red interna contra ataques cibernéticos provenientes del exterior; los Firewalls son instalados en la frontera con internet controlando los accesos de entrada y salida para que solo sean permitidos los autorizados mediante una política de seguridad.

La Alcaldía Miguel Hidalgo necesita proteger la red interna de los posibles ataques que se pudieran originar desde Internet, de igual manera, es necesario controlar el tráfico interno para proteger a los usuarios cuando navegan en internet mediante reglas de acceso, políticas de seguridad y publicación de servicios.

Debido a los constantes cambios tecnológicos en los cuales nos hemos visto involucrados, la rápida migración de aplicaciones a la nube, el uso de herramientas de colaboración y el aumento en la demanda de recursos de las diferentes áreas de la Alcaldía, se vuelve indispensable adquirir un nuevo Firewall que sea más robusto, con tecnología de última generación para cubrir las necesidades actuales y permita un paulatino crecimiento sin la necesidad de cambiar el Firewall por al menos 3 años, para garantizar la disponibilidad Integridad y confiabilidad de la información.

Por lo antes mencionado existe la urgente necesidad de renovar la licencia del Firewall que actualmente nos brinda el servicio de seguridad (Fortigate 900D-BDL), el cual, estará próximo a tener un año en operación, así como licencia. La Alcaldía requiere tener un equipo actualizado que permita soportar la carga de tráfico generada por las aplicaciones y nuevos servicios desplegados para asegurar el correcto funcionamiento y operación de la red, así mismo, de acuerdo a los requerimientos mínimos estipulados por la Agencia Digital de Innovación Publica (ADIP).

1.1 DIAGNÓSTICO.

La seguridad ha sido el principal problema a tratar cuando se conectan los usuarios al Internet, ya que han incrementado la demanda de servicios, como lo son Consultas web, correo electrónico, aplicaciones de colaboración, servicios en la nube, publicación de servicios para la ciudadanía, entre otros. En la Alcaldía Miguel Hidalgo se ha incrementado todo lo concerniente a la seguridad de los sistemas, debido a que se exponen los datos privados, así como la infraestructura de red a cualquier tipo de ataque proveniente de Hackers o sitios malintencionados por eso mismo la licencia debe estar actualizada para tener un buen funcionamiento.

1.2 OBJETIVO.

Contar con la actualización de la licencia del Firewall modelo Fortigate 900D-BDL, el cual requiere ser actualizado para brindar los servicios de seguridad y conectividad que demanda la alcaldía, los usuarios y al mismo tiempo mantener las políticas de seguridad y control para prevenir el acceso no-autorizado a los recursos propios de la red.
Esto nos ayudara a mantener la estructura actual de operación, es indispensable que el Firewall este en óptimas condiciones.

1.3 BENEFICIOS.

Contar con una licencia, permitirá mantener la estructura de seguridad y red actual, se podrá desplegar de mejor manera el servicio de Red Inalámbrica y homologarlo hacia las Oficinas de la Alcaldía con tan solo la integración de nuevos Access Point. Se podrá replicar el uso agente de VPN hacia todos los usuarios de las diferentes áreas de la Alcaldía para brindar accesos a los recursos privados en caso de una emergencia sanitaria que impida regresar a las oficinas, se obtendrá un mejor rendimiento en el servicio de Internet al integrarlo con la nueva infraestructura de Switches con soporte para 10GB con lo cual, el acceso a las aplicaciones críticas y las páginas WEB tendrán una mejor respuesta de cara hacia la ciudadanía.

La implementación de todos esos beneficios permite garantizar la disponibilidad, integridad, confidencialidad y el adecuado uso de la información desde cualquier lugar, evitando exponerla a las amenazas del exterior e interior.

2. ÁREA SOLICITANTE Y SUPERVISIÓN DEL SERVICIO.

Subdirección de Tecnologías de la información, supervisado por la Jefatura de Unidad Departamental de Análisis de la Infraestructura.

3. SUSTENTO LEGAL DEL REQUERIMIENTO.

De conformidad al Capítulo II, De las Atribuciones Generales de los Titulares de las Direcciones General de las Alcaldías, artículo 75 que enuncia que: "A los titulares de la Direcciones Generales de las alcaldías, corresponde las siguientes atribuciones:" fracción "IV. Planear, programar, organizar, controlar, evaluar y supervisar el desempeño de las labores encomendadas a las Unidades Administrativas y Unidades Administrativas de Apoyo Técnico-Operativo que le estén adscritas.

Así como, en la publicación de la Gaceta Oficial de la Ciudad de México del Registro de Estructura Orgánica OPA-MIH-1/010119 Alcaldía Miguel Hidalgo, publicada el 01 de febrero de 2019, que enuncia a la Dirección General de Administración y en su estructura esta la Dirección de Modernización Administrativa y dentro de esta la Subdirección de Tecnologías de la Información, que, de conformidad al Manual Administrativo aplicable y vigente, tienen las siguientes funciones respecto a este tema:

Dirección de Modernización: Dirigir el análisis de los procesos de trabajo dentro de la estructura de la Alcaldía para identificar áreas susceptibles de mejora y promover proyectos de innovación, así como la adopción de mejores prácticas; y Velar que la Alcaldía disponga de tecnologías de la información actuales para el mejor desempeño de las funciones.

4. DESCRIPCIÓN Y ESPECIFICACIÓN DEL SERVICIO.

Se deberá reemplazar la licencia del firewall de Seguridad con el que cuenta la Alcaldía Miguel Hidalgo desde 2022 (Equipo con licencia de uso del Firewall de Seguridad Perimetral Fortigate 900D-BDL) para 1200 equipos con posibilidad de crecimiento. La nueva solución deberá estar basada en un servicio usando un dispositivo de hardware, totalmente administrable de forma local, así mismo el proveedor deberá de realizar las actualizaciones de firmware a una versión estables esto con la finalidad de mantener el equipo actualizado y prevenir posibles vulnerabilidades, en caso de que se presente alguna falla, intermitencia en algunas de las políticas o servicios que se brindan a la Alcaldía Miguel Hidalgo el proveedor deberá de realizar el downgrade del firmware garantizando el correcto funcionamiento, dichas actividades se deberán realizar en un horario en el cual no se vean afectadas las actividades de los usuario.

5. CONDICIONES GENERALES.

El prestador del servicio estará obligado a proporcionar los servicios de instalación de la licencia, para mantener los módulos correspondientes.

- IPS Service.
- AV.
- Botnet IP/ Dominio.
- Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak.
- Web Filtering Service.
- Antispam Service.
- Security Rating Service.
- Controladora Wireless.
- Virtual Private Network.
- Security mobile Detection IoT.
- Seguridad Industrial.

6. PENAS CONVENCIONALES.

Como pena convencional a cargo del **"El prestador de servicios"** por incumplimiento del contrato, deficiencia o mala calidad de los servicios y/o de los materiales utilizados y por el atraso en la prestación de los servicios serán los siguientes:

SUPUESTO	PORCENTAJE DE LA PENA	BASE PARA LA APLICACIÓN

Que no esté instalado el servicio dentro de los plazos señalados e las presentes bases.	1%	Sobre el monto antes del IVA que resulte de la suma de los conceptos y cantidades requeridos para el servicio.
Que los conceptos y cantidades solicitadas para cada evento no estén instalados en el horario indicado por el área solicitante.	1%	Sobre el monto antes del IVA que resulte de la suma de los conceptos y cantidades requeridos para el servicio.

7. VIGENCIA DE LA PRESTACIÓN DEL SERVICIO.

A partir de la vigencia del contrato al 31 de diciembre de 2026.

8. PARTIDA PRESUPUESTAL.

Los recursos destinados a cubrir el gasto del servicio son ingresos en participaciones federales asignados a las funciones y actividades de la Dirección de Modernización Administrativa, partida específica **3271 "Arrendamiento de activos intangibles".**

9. FACTURACIÓN.

"El prestador de servicios" deberá cumplir con el procedimiento que se estipula en el "Instructivo para pago a prestadores de servicios de la Alcaldía Miguel Hidalgo" que se le entrega para dicho propósito.

Las presentes especificaciones técnicas deberán forman parte integrante del Contrato de prestación de servicios que se suscriba con la persona física o moral que sea adjudicada.

10. ALCANCE.

La solución deberá proveer con los siguientes puntos:

10.1 Funcionalidades y Características del Sistema:

10.1.1 Características del dispositivo:

- El dispositivo debe ser un equipo 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 reensamblado 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.
- El sistema operativo debe incluir un servidor de DNS que permita resolver de forma local ciertas consultas de acuerdo a la configuración del administrador.
- El equipo de seguridad debe soportar el uso del protocolo ICAP con el fin de poder delegar tareas a equipos terceros con el fin de liberar procesamiento del mismo.
- El equipo deberá contar con Interfaces de alta velocidad para permitir la flexibilidad de implementación (10GE, 25GE y 40GE).
- El equipo debe tener rendimiento superior del cortafuegos para IPv4/IPv6, SCTP y multidifusión tráfico con latencia ultrabaja de hasta dos microsegundos.
- El equipo debe tener VPN, CAPWAP y aceleración de túnel IP.

- El equipo deberá contar con modulo de Prevención de intrusiones basada en anomalías, descarga de suma de comprobación y desfragmentación de paquetes.
- Rendimiento mejorado de IPS con la capacidad única de coincidencia de firmas en SPU.
- Capacidades de inspección de SSL basadas en las últimas novedades de la industria.
- El equipo deberá Detectar contenido malicioso en velocidades multigigabit.
- El equipo deberá ser de una plataforma verdaderamente consolidada con un solo sistema operativo y panel de vidrio para toda la superficie de ataque digital.
- El equipo deberá contar con protección líder en la industria.
- El Equipo deberá ser recomendado por NSS Labs, VB100, AV Comparatives y seguridad y rendimiento validados por ICSA.
- El equipo deberá aprovechar las últimas tecnologías, como las basadas en el engaño de seguridad.
- El equipo deberá Controlar miles de aplicaciones, bloquear los últimos exploits y filtrar el tráfico web en función de millones de clasificaciones de URL en tiempo real.
- El equipo deberá tener compatibilidad con TLS 1.3.
- El equipo deberá prevenir, detectar y mitigar automáticamente ataques avanzados en cuestión de minutos con una seguridad integrada impulsada por IA y protección avanzada contra amenazas.
- El equipo deberá utilizar aceleración de hardware SPU para aumentar la seguridad de la red rendimiento.
- El equipo deberá permitir visibilidad completa de usuarios, dispositivos y aplicaciones en toda la superficie de ataque y la aplicación de políticas de seguridad consistentes, independientemente de la ubicación de los equipos.
- El equipo deberá proteger contra vulnerabilidades explotables de la red con efectividad de seguridad IPS validada por la industria, baja latencia y optimización rendimiento de la red.
- El equipo deberá bloquear automáticamente las amenazas en el tráfico descifrado usando el rendimiento de inspección SSL más alto de la industria, incluido el último estándar TLS 1.3 con cifrado obligatorio.
- El equipo deberá bloquear proactivamente ataques sofisticados recientemente descubiertos en tiempo real (Ataques de día Zero).
- El equipo deberá estar preparado con capacidades de SD-WAN y con la capacidad de detectar, contener y aislar amenazas con segmentación automática.
- El equipo deberá estar preparado para SDN (Redes impulsadas por la seguridad) que protejan, aceleren y unifiquen la red y la experiencia del usuario.
- El equipo deberá estar preparado para ZTNA (Acceso a la red de Zero Confianza) que identifique y proteja a los usuarios y dispositivos en tiempo real, dentro y fuera de la red.
- El equipo deberá estar preparado para DCS (Seguridad de nube dinámica) que proteja y controle la infraestructura de nube y sus aplicaciones.
- El equipo deberá estar preparado para AI-DSO (Operaciones de seguridad impulsadas por Inteligencia Artificial) que prevengan, detecten, aíslen y respondan a las ciberamenazas.
- El equipo deberá estar preparado para brindar seguridad Móvil para 4G, 5G e IoT, que incluya al menos: NAT44, NAT444, NAT64/DNS64, NAT46 para 4G Gi/sGi y para conectividad y seguridad 5G N6.

10.1.2 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 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.
- Será posible definir políticas de firewall que sean independientes del puerto de origen y puerto de destino.
- Las reglas del firewall deberán tomar en cuenta dirección IP origen (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.

- 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).
- Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos.
- Debe poder definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP).
- 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).
- La solución deberá tener la capacidad de balancear carga entre servidores. Esto es realizar una traslación de una única dirección a múltiples direcciones de forma tal que se distribuya el tráfico entre ellas.
- En la solución de balanceo de carga entre servidores, debe soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID.
- En la solución de balanceo de carga de entre servidores deben soportarse mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible.
- El equipo deberá permitir la creación de políticas de tipo Firewall con capacidad de seleccionar campos como dirección, identificador de usuarios o identificador de dispositivos para el caso de dispositivos móviles como smartphones y tabletas.
- El equipo deberá permitir la creación de políticas de tipo VPN con capacidad de seleccionar campos como IPSEC o SSL según sea el tipo de VPN.
- La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP.
- La solución de seguridad deberá permitir la creación de servicios de Firewall para implementar dentro de las políticas de seguridad y categorizarlos de manera personalizada.
- La solución será capaz de integrar los servicios dentro de las categorías de Firewall predefinidas o personalizadas y ordenarlos alfabéticamente.
- El dispositivo de seguridad podrá determinar accesos y denegación a diferentes tipos de tráfico predefinidos dentro de una lista local de políticas.
- La solución será capaz de habilitar o deshabilitar el paso de tráfico a través de procesadores de propósito especifico, si el dispositivo cuenta con estos procesadores integrados dentro del mismo.
- La solución podrá crear e implementar políticas de tipo Multicast y determinar el sentido de la política, así como también la habilitación del NAT dentro de cada interface del dispositivo.
- El dispositivo de seguridad será capaz de crear e integrar políticas contra ataques DoS las cuales se deben poder aplicar por interfaces.
- El dispositivo de generar logs de cada una de las políticas aplicadas para evitar los ataques de DoS.
- La solución de seguridad permitirá configurar el mapeo de protocolos a puertos de manera global o especifica.
- La solución capaz de configurar el bloqueo de archivos o correos electrónicos por tamaño, o por certificados SSL inválidos.
- El dispositivo integrara la inspección de tráfico tipo SSL y SSH bajo perfiles predefinidos o personalizados.
- El dispositivo será capaz de ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico.
- Tendrá la capacidad de hacer escaneo a profundidad de trafico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis.
- La solución permitirá bloquear o monitorear toda la actividad de tipo Exec, Port-Forward, SSH-Shell, y X-11 SSH.

10.1.3 Conectividad y Sistema de ruteo:

- 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, BGP y IS-IS.
- Soporte a ruteo dinámico RIPng, OSPFv3.
- La configuración de BGP debe soportar Autonomous System Path (AS-PATH) de 4 bytes.
- Soporte de ECMP (Equal Cost Multi-Path).
- Soporte de ECMP con peso. En este modo el tráfico será distribuido entre múltiples rutas, pero no en forma equitativa, sino en base a los pesos y preferencias definidas por el administrador.
- Soporte de ECMP basado en comportamiento. En este modo, el tráfico será enviado de acuerdo a la definición de una ruta hasta que se alcance un umbral de tráfico. En este punto se comenzará a utilizar en paralelo una ruta alternativa.
- Soporte a ruteo de multicast.
- La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow.
- La solución podrá habilitar políticas de ruteo en IPv6.
- La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6.
- La solución deberá soportar la creación de políticas de tipo Firewall y VPN y subtipo por dirección IP, tipos de dispositivo y por usuario, con IPv6.
- La solución será capaz de habilitar funcionalidades de UTM (Antivirus, Filtrado Web, Control de Aplicaciones, IPS,Filtrado de correo, DLP, ICAP y VoIP) dentro de las políticas creadas con direccionamiento IPv6.
- El dispositivo debe integrar la autenticación por usuario o dispositivo en IPv6.
- El dispositivo deberá soportar la inspección de tráfico IPv6 en modo proxy explicito.
- Deberá ser capaz de integrar políticas con proxy explicito en IPv6.
- La solución podrá restringir direcciones IPv6 en modo proxy explicito.
- Deberá hacer NAT de la red en IPv6.
- La solución será capaz de comunicar direccionamiento IPv6 a servicios con IPv4 a través de NAT.
- Como dispositivo de seguridad deberá soportar la inspección de tráfico IPv6 basada en flujo.
- La solución deberá ser capaz de habilitar políticas de seguridad con funcionalidades IPS, Filtrado Web, Control de Aplicaciones, Antivirus y DLP, para la inspección de tráfico en IPv6 basado en flujos.
- La solución contara con una base de administración de información interna generada por sesiones sobre IPv6.
- Deberá ser capaz de habilitar la funcionalidad de Traffic Shaper por IP dentro de las políticas creadas en IPv6.
- El dispositivo podrá tener la capacidad de transmitir DHCP en IPv6.
- La solución tendrá la funcionalidad de habilitar DHCP en IPv6 por interface.
- La solución deberá contar con soporte para sincronizar por sesiones TCP en IPv6 entre dispositivos para intercambio de configuración en Alta Disponibilidad.
- El dispositivo podrá ser configurado mediante DHCP en IPv6 para comunicarse con un servidor TFTP donde se encontrará el archivo de configuración.
- El dispositivo podrá hacer la función como servidor DHCP IPv6.
- La solución será capaz de configurar la autenticación por usuario por interface en IPv6.

10.1.4 VPN IPSec/L2TP/PPTP:

- Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).
- Soporte para IKEv2 y IKE Configuration Method.

- Debe soportar la configuración de túneles PPTP.
- Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES.
- Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits.
- Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14.
- Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.
- Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site.
- La 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.
- Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de túneles nativos de Windows y MacOS X.

10.1.5 VPN SSL:

- Capacidad de realizar SSL VPNs.
- Soporte a certificados PKI X.509 para construcción de VPNs SSL.
- Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN.
- Soporte de renovación de contraseñas para LDAP y RADIUS.
- 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 algun 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.
- Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios.
- Los portales personalizados deberán soportar al menos la definición de:
  - Widgets a mostrar.
  - Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC.
  - Esquema de colores.
  - Soporte para Escritorio Virtual.
  - Política de verificación de la estación de trabajo.
- La VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, entendiéndose como un entorno de trabajo seguro que previene contra ciertos ataques además de evitar la divulgación de información.
- Para la configuración de cluster, en caso de caída de uno de los dispositivos, la VPN SSL que estuviera establecida, debe restablecerse en el otro dispositivo sin solicitar autentificación nuevamente.

10.1.6 Traffic Shapping / QoS:

- Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall.
- Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión.
- Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general.

- 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.

10.1.7 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 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".
- 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.
- Debe ser posible definir puertos alternativos de autenticación para los protocolos http, FTP y Telnet.
- Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).
- La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios.
- Deben poder definirse usuarios y grupos en un repositorio local del dispositivo.
- Para los administradores locales debe poder definirse la política de contraseñas que especificará como mínimo:
  - Longitud mínima permitida.
  - Restricciones de tipo de caracteres: numéricos, alfanuméricos, etc.
  - Expiración de contraseña.
- Debe poder limitarse la posibilidad de que dos usuarios o administradores tengan sesiones simultáneas desde distintas direcciones IP.

10.1.8 Antivirus:

- 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.
- El Antivirus deberá poder configurarse en modo Proxy como en modo de Flujo. En el primer caso, los archivos serán totalmente reconstruídos por el motor antes de hacer la inspección. En el segundo caso, la inspección de antivirus se hará por cada paquete de forma independiente.
- 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.
- El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6.
- 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.
- El antivirus deberá soportar múltiples bases de datos de virus de forma tal de que el administrador defina cuál es conveniente utilizar para su implementación evaluando desempeño y seguridad.
- El appliance deberá de manera opcional poder inspeccionar por todos los virus conocidos.
- 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 integrado tendrá la capacidad de poner en cuarentena a los clientes cuando se haya detectado que los mismos envían archivos infectados con virus.
- El Antivirus deberá incluír 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).

10.1.9 AntiSpam:

- La capacidad antispam incluída 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 incluída 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.

10.1.10 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 54 millones de sitios web en la base de datos.
- Debe poder categorizar contenido Web requerido mediante IPv6.
- 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.
- La solución debe permitir realizar el filtrado de contenido, tanto realizando reconstrucción de toda la sesión (modo proxy) como realizando inspección paquete a paquete sin realizar reconstrucción de la comunicación (modo flujo).
- 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. Estos mensajes de remplazo deberán poder aplicarse para conexiones http y https, tanto en modo proxy como en modo flujo.
- Los mensajes de remplazo deben poder ser personalizados por categoría de filtrado de contenido.
- Capacidad de filtrado de scripts en páginas web (JAVA/Active X).
- La solución de Filtraje de Contenido debe soportar el forzamiento de “Safe Search” o “Búsqueda Segura” independientemente de la configuración en el browser del usuario. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales. Esta funcionalidad se soportará al menos para Google, Yahoo! y Bing.
- Será posible definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos.
- Será posible exceptuar la inspección de HTTPS por categoría.
- Debe contar con la capacidad de implementar el filtro de Educacion de Youtube por Perfil de Filtro de Contenido para tráfico HTTP, garantizando de manera centralizada, que todas las sesiones aceptadas por una política de seguridad con este perfil, van a poder acceder solamente a contenido de tipo Educativo en Youtbube, bloqueando cualquier tipo de contenido no Educativo.
- El sistema de filtrado de URLs debe tener al menos 3 métodos de inspección:
  - Modo de Flujo: La página es inspeccionada paquete a paquete sin reconstruir la página completa.

- Modo Proxy: La página es reconstruida completamente para ser analizada a profundidad.
- Modo DNS: La inspección se basa únicamente en la categorización del dominio consultado.

- Se debe incluir la funcionalidad de reputación basada en filtrado de URLs.
- La funcionalidad de reputación busca que, al acceder a páginas de contenido no deseado (tales como Malware, pornografía, consumo de ancho de banda excesivo, etc) se asigne un puntaje a cada usuario o IP cada vez visita una página de esta índole. De acuerdo a esto se extrae los usuarios que infringen las políticas de filtrado con más frecuencia con el fin de detectar zombies dentro de la red.
- El sistema de filtrado de URLs debe incluir la capacidad de definir cuotas de navegación basadas en volumen de tráfico consumido.
- Se debe incorporar la funcionalidad de filtrado educativo de Youtube (Youtube Education Filter).
- En dicho sistema cada organismo obtiene un ID de Youtube para habilitar el contenido educativo del mismo. Se deberá insertar dicho código en la configuración de filtrado de URLs del equipo para poder habilitar únicamente el contenido educativo de Youtube.
- Acceso web seguro contra riesgos internos y externos, incluso para tráfico encriptado de alto rendimiento.
- Experiencia de usuario mejorada con web dinámica y almacenamiento en caché de video.
- Se deberá bloquear y controlar el acceso web basado en usuarios o grupos de usuarios a través de URL y dominios.
- Se deberá evitar la pérdida de datos y descubrir la actividad del usuario para conocer y aplicaciones en la nube desconocidas.
- Se deberá bloquear solicitudes de DNS contra dominios maliciosos.
- Deberá tener protección avanzada multicapa contra malware de día cero y amenazas enviadas a través de la web.

10.1.11 Protección contra intrusos (IPS):

- El Detector y preventor de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror.
- Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores.
- Capacidad de detección de más de 4000 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 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 variaciones de protocolo y además por firmas de ataques conocidos (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.
- Actualización automática de firmas para el detector de intrusos.
- El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios.
- Métodos de notificación:
  - Alarmas mostradas en la consola de administración del appliance.
  - Alertas vía correo electrónico.
  - Debe tener la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado.

- La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma “indefinida”, hasta que un administrador tome una acción al respecto.
- Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque, así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP.

- Se debe incluir protección contra amenazas avanzadas y persistentes (Advanced Persistent Threats). Dentro de estos controles se debe incluir:
  - Protección contra botnets: Se deben bloquear intentos de conexión a servidores de Botnets, para ello se debe contar con una lista de los servidores de Botnet más utilizado. Dicha lista debe actualizarse de forma periódica por el fabricante.
  - Sandboxing: La funcionalidad de Sandbox hace que el archivo sea ejecutado en un ambiente seguro para analizar su comportamiento y, a base del mismo, tomar una accion sobre el mismo.
- Se deberá Implementar parches virtuales a nivel de red para proteger contra vulnerabilidades explotables de la red y optimizar el tiempo de protección de la red.

10.1.12 Prevención de Fuga de Información (DLP):

- La solución debe ofrecer la posibilidad de definir reglas que permitan analizar los distintos archivos que circulan a través de la red en búsqueda de información confidencial.
- La funcionalidad debe soportar el análisis de archivos del tipo: MS-Word, PDF, Texto, Archivos comprimidos.
- Debe soportarse el escaneo de archivos en al menos los siguientes protocolos: HTTP, POP3, SMTP, IMAP, NNTP y FTP.
- Ante la detección de una posible fuga de información deben poder aplicarse el menos las siguientes acciones: Bloquear el tráfico del usuario, Bloquear el tráfico de la dirección IP de origen, registrar el evento.
- En caso del bloqueo de usuarios, la solución debe permitir definir por cuánto tiempo se hará el bloqueo o en su defecto bloquear por tiempo indefinido hasta que el administrador tome una acción.
- La solución debe soportar la capacidad de guardar una copia del archivo identificado como posible fuga de información. Esta copia podría ser archivada localmente o en otro dispositivo.
- La solución debe permitir la búsqueda de patrones en archivos mediante la definición de expresiones regulares.
- Se debe proveer la funcionalidad de filtrado de fuga de información. Dentro de las técnicas de detección se debe considerar como mínimo las siguientes:
  - Filtrado por tipo de archivo.
  - Filtrado por nombre de archivo.
  - Filtrado por expresiones regulares: Se detectarán los archivos según las expresiones regulares que se encuentren dentro de los mismos.
  - Fingerprinting: Se tomará una muestra del archivo que se considere como confidencial. Según esto se bloquearán archivos que sean iguales a esta muestra.
  - Watermarking: Se insertará un "sello de agua" dentro del archivo considerado como confidencial. De acuerdo a esto se analizarán los archivos en busca de este sello de agua, este se detectará incluso si el archivo sufrió cambios.

10.1.13 Control de Aplicaciones:

- Lo 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.
- La solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante.
- El listado de aplicaciones debe actualizarse periódicamente.
- Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.

- Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.
- Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping.
- Preferentemente deben soportar mayor granularidad en las acciones.

10.1.14 Inspección de Contenido SSL:

- La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado mediante TLS al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S.
- La inspección deberá realizarse mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle).
- La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.
- Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado.
- El equipo debe ser capaz de analizar contenido cifrado (SSL o SSH) para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Prevención de Fuga de Información, Antivirus e IPS.

10.1.15 Controlador Inalámbrico (Wireless Controller):

- El dispositivo debe tener la capacidad de funcionar como Controlador de Wireless.
- En modo de Controlador de Wireless tendrá la capacidad de configurar múltiples puntos de acceso (Access Points: APs) reales de forma tal de que se comporten como uno solo. Cómo mínimo deberá controlar los SSID, roaming entre APs, configuraciones de cifrado, configuraciones de autenticación.
- Debe soportar la funcionalidad de detección y mitigación de puntos de acceso (APs). Rogue Access Point Detection.
- El controlador de Wireless tendrá la capacidad de configurar la asignación de direcciones IP mediante DHCP a las estaciones de trabajo conectadas a los APs.
- Deberá tener la capacidad de monitorear las estaciones de trabajo, clientes wireless, conectadas a alguno de los APs.
- La solución debe contar con la funcionalidad de WIDS (Wireless IDS), la capacidad de monitorear el tráfico wireless para detectar y reportar posibles intentos de intrusión.
- Debe contar con un sistema de aprovisionamiento de usuarios invitados para red wifi, que permita la creación sencilla de accesos para invitados, por medio de un portal independiente.
- El equipo debe tener capacidad de que estos usuarios invitados con acceso inalámbrico, tengan la opción de colocar o no contraseña, con tiempo limitado y configurable para la expiración de la cuenta.
- El controlador inalámbrico debe estar en la capacidad de balancear la carga entre los puntos de acceso (Access Points) soportando por lo menos los siguientes métodos de balanceo: Access Point Hand-off, Frequency Hand-off.
- Debe contar con la capacidad de realizar Bridge SSID, permitiendo que una red inalámbrica y un segmento cableado LAN pertenezcan a la misma rubred.
- El dispositivo deberá ser capaz de administrar los dispositivos wireless AP de la misma plataforma, tanto en consola CLI como a través de una interfaz gráfica (GUI).
- El dispositivo debe tener la capacidad de controlar varios puntos de acceso de la misma plataforma de forma remota.
- El dispositivo debe poder cifrar la información que se envía hacia los puntos de acceso de la misma plataforma, sobre los cuales se esté teniendo control y gestión.
- El dispositivo debe permitir la administración y manejo tanto de redes cableadas como inalámbricos dentro del mismo segmento de red.
- El equipo debe tener la capacidad de reconocer y monitorear diferentes tipos de dispositivos de comunicación móvil como Smartphones Android, Blackberry y Iphone; diferentes tipos de consolas de juego como Xbox, PlaySation, Nintendo, PSP; diferentes tipos de tabletas con SO Androide o tabletas Ipad.
- El equipo debe tener la capacidad de controlar el acceso a la red de los diferentes dispositivos antes mencionados a través de ACLs por MAC.

- El equipo deberá permitir el crear diferentes niveles de acceso a la red en función del tipo de dispositivo que se conecte, siendo estos: Smartphones, Tabletas, Laptoos, PCs (tanto en Windows como en Linux).
- El equipo debe permitir la separación de redes al menos entre usuarios internos e invitados, permitiendo la colocación de reglas en función de los dispositivos móviles conectados.

10.1.16 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.
- La solución debe contar con un ALG (Application Layer Gateway) de SIP.
- Debe poder hacerse inspección de encabezados de SIP.
- Deben poder limitarse la cantidad de requerimientos SIP que se hacen por segundo. Esto debe poder definirse por cada método SIP.
- La solución debe soportar SIP HNT (Hosted NAT Transversal).
- La solución deberá integrar la inspección de tráfico basado en flujo utilizando un motor de IPS dentro del mismo dispositivo para escaneo de paquetes.
- Deberá ser capaz de hacer inspección tráfico SSH en modo proxy explicito.
- La solución de seguridad podrá hacer inspección de tráfico HTTP, HTTPS y FTP sobre HTTP en modalidad proxy explicito con las funcionalidades de IPS, Antivirus, Filtrado Web, Control de Aplicaciones y DLP, todo en un mismo dispositivo.
- El dispositivo tendrá la opción para configurar sus interfaces integradas en modo Sniffer con funcionalidades de Filtrado Web, Control de Aplicaciones, Antivirus e IPS.

10.1.17 Optimización WAN y Web Caching:

- La solución deberá permitir la creación de perfiles para la aplicación de Optimización WAN e indicar bajo que protocolos se ejecutará.
- Deberá ser capaz de activar en modo transparente dentro de los perfiles de Optimización WAN y seleccionar un determinado grupo de usuarios para autenticación de acceso.
- El dispositivo deberá soportar la desfragmentación dinámica de paquetes para detectar fragmentos persistentes de distintos archivos o datos adjuntos dentro del tráfico bajo protocolos desconocidos.
- La solución debe ser capaz de generar y aplicar perfiles de Optimización WAN para los usuarios.
- El dispositivo de seguridad podrá integrar contenido de inspección dentro de sus políticas de seguridad con Optimización WAN.
- La solución integrara dentro de cada interface la capacidad de hacer túneles de Optimización WAN.
- Deberá ser capaz de configurar Optimización WAN en modo Activo/Pasivo.
- Solución capaz de aplicar web cache a tráfico HTTP y HTTPS dentro de las políticas de seguridad incluyendo también Optimización WAN y web proxy cache.
- Dispositivo capaz de habilitar el almacenamiento en caché web tanto en el lado del cliente y del lado de la solución.
- La solución podrá recibir el tráfico HTTPS en nombre del cliente, abrirá y extraerá el contenido del tráfico cifrado para inspeccionar y almacenar en cache para el envío al usuario final.
- El dispositivo tendrá la opción de integrar un certificado SSL determinado para la el cifrado de tráfico.
- La solución capaz de configurar el cache de trafico HTTP y HTTPS bajo distintos puertos a los predeterminados (80 y 443).
- La solución debe ser capaz de habilitar opciones para depurar la funcionalidad de Web Cache a determinadas URL.

10.1.18 Alta Disponibilidad:

- El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6.
- 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.
- Será posible definir interfaces de gestión independientes para cada miembro en un clúster.

10.1.19 Características de Administración:

- Interface 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 interface debe soportar SSL sobre HTTP (HTTPS).
- La interface gráfica de usuario (GUI) vía Web deberá poder estar en español y en inglés, configurable por el usuario.
- Interface 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 usuario y contraseña, tanto como para la interface gráfica de usuario como la consola de administración de línea de comandos (SSH o telnet).
- El administrador del sistema podrá tener las opciones incluidas de autenticarse vía usuario/contraseña 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 ningún software adicional.
- Soporte de SNMP versión 2.
- Soporte de SNMP versión 3.
- Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos.
- Soporte para almacenamiento de eventos en un repositorio que pueda consultarse luego con SQL.
- 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.
- Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión.
- Permitir que el administrador de la plataforma pueda definir qué funcionalidades están disponibles o deshabilitadas para ser mostradas en la interfaz gráfica.
- Contar con facilidades de administración a través de la interfaz gráfica como listas de edición a través de click derecho.
- Contar con facilidades de administración a través de la interfaz gráfica como ayudantes de configuración (setup wizard).
- Contar con la posibilidad de agregar una barra superior (Top Bar) cuando los usuarios estén navegando con información como el ID de usuario, cuota de navegación utilizada, y aplicaciones que vayan en contra de las políticas de la empresa.
- Contar con herramientas graficas para visualizar fácilmente las sesiones en el equipo, que permitan adicionarse por el administrador en la página inicial de la solución (dashboard), incluyendo por lo menos por defecto Top de sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación.

10.1.20 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.
- Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual.
- Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual.
- Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual.
- Debe ser posible definir enlaces de comunicación entre los sistemas virtuales sin que el tráfico deba salir de la solución por medio de enlaces o conexiones virtuales, y estas conexiones deben poder realizarse incluso entre instancias virtuales en modo NAT y en modo Transparente.

10.1.21 Análisis de Seguridad y Almacenamiento de Logs en la Nube:

- La solución de seguridad debe contar con una solución en la nube que permita centralización de reportes, análisis de tráfico, administración de configuraciones, y almacenamiento de logs sin la necesidad de software o hardware adicional para esta función.
- Contar con funcionalidad de Análisis de archivos sospechosos en la nube en caso que no se cuente con suficiente información en la solución de seguridad para calificar el tráfico como legitimo o ilegitimo, por medio de técnicas de Caja de Arena o Sandboxing.
- Almacenamiento de Logs hasta 1 Giga por equipo incluido con capacidad de crecimiento en caso de requerirse.
- Debe permitir administración centralizada de todos los equipos de la solución de seguridad perimetral desde una misma interfaz.
- Permitir Monitoreo y alertas en tiempo real.
- Debe contar con Reportes predefinidos y la opción de personalización, así como contar con herramientas de análisis.
- Debe permitir visualizar de manera sencilla que todos los equipos de seguridad perimetral gestionados cuenten con la misma versión de firmware o sistema operativo para garantizar la homogeneidad en la red.

10.1.22 Actualizaciones de plataforma:

- La solución contara con el servicio de actualización de firmas para dispositivos sobre BYOD.
- El dispositivo tendrá la opción de conectarse a los servidores NTP de los Laboratorios de Investigación y Actualización propietarios del mismo fabricante para actualización del horario de sistema local.
- Sera capaz de hacer consultas a los servidores DNS de los Laboratorios de Investigación y Actualización del mismo fabricante para resolución y categorización de sitios web dentro de los perfiles para Filtrado Web.
- Tendrá la capacidad de hacer consultas a los servidores DNS de los Laboratorios de investigación y Actualización mismos del fabricante sobre reputación de direcciones IP.

11. ENTREGABLES.

Al término de la aplicación de la actualización de la licencia del equipo, el proveedor deberá proporcionar:

11.1 Copia impresa de la licencia aplicada por un año.

11.2 Respaldo de la configuración antes y después de aplicar la actualización de la licencia, debidamente firmada por personal de la Dirección de Modernización Administrativa.

11.3 Puesta en punto del servicio de filtrado de contenido.

12. NIVELES DE SERVICIOS.

El tiempo de respuesta se deberá de brindará de acuerdo a la siguiente tabla.

PRIORIDAD	TIEMPO DE RESPUESTA MÁXIMA	
	Asistencia Remota	Asistencia en Sitio
Baja	8 horas	24 horas
Media	4 horas	12 horas
Alta	2 horas	8 horas
Critica	Inmediato	4 horas

Los reportes se pueden hacer mediante un correo electrónico que proporcione el proveedor ganador y un número telefónico.

13. GARANTÍAS

- El tiempo de garantía será por un año a la firma del contrato.
- Soporte presencial en un máximo de 2 horas por incidente.
- Soporte vía telefónica las 24hrs x 7 días.
- Atención remota o en sitio de usuarios.
- Registro, seguimiento y solución a incidentes reportados
- Apoyo y orientación en la operación de equipo de comunicación.

14. REQUERIMIENTOS DEL LICITANTE.

La licencia del equipo Firewall deberá ser reemplazada por una vigente con su última versión existente en el mercado.

14.1 Carta firmada por el representante legal del fabricante en el que manifieste que el licitante es certificado, que cuenta con la capacitación y experiencia necesaria para implementar la solución integral de seguridad del sistema de Firewall y que cuenta con al menos un ingeniero certificado para soportar e implementar la citada solución con experiencia de al menos 2 años en el manejo del producto, y quienes serán los que proporcionen el servicio.

14.2 Carta de la licitante firmada por su representante legal en la que se compromete a proporcionar y mantener actualizado el software y hardware del firewall y sus complementos con los niveles de servicio requeridos (El proveedor atenderá los problemas o fallas que se presenten en el equipo 7x24 durante la duración del contrato, dentro de las instalaciones de la Alcaldía).

14.3 El servicio deberá de contemplar la instalación y/o reinstalación del software en los equipos que la Alcaldía designe, así como un soporte técnico por personal especializado.

14.4 Migración de las, políticas y configuraciones en ventanas de tiempo definidas por el área de redes.

14.5 6 visitas de servicio presenciales al año, estas pueden ser programadas o utilizadas en caso de contingencia. Dichas visitas según programadas por personal de la Dirección de Informática.

14.6 El licitante deberá garantizar el servicio de instalación de la licencia, así como también del equipo que sea necesario reemplazar, sin costo extra para la Alcaldía y por la duración del contrato.

ANEXO TÉCNICO

1. JUSTIFICACIÓN.

Las necesidades de los ciudadanos de la Alcaldía Miguel Hidalgo obligan a la integración de las TIC en la Administración Pública con el objetivo de promover la transparencia, la eficiencia y la participación ciudadana.

Las herramientas tecnológicas como las plataformas digitales como lo son los sitios web son capaces de proporcionar servicios públicos a ciudadanos, así mismo, ofrecen nuevas oportunidades para un acceso ciudadano más directo y conveniente, además de información oficial.

Los avances tecnológicos, actualizaciones, la conectividad y el consumo digital de los ciudadanos usuarios de estos servicios han rebasado la capacidad operativa del actual sitio, convirtiéndolo en una plataforma obsoleta, no funcional, que imposibilita al gobierno dar los servicios públicos digitales, lo que deriva en la construcción de un nuevo sitio que atienda los ciudadanos de manera eficiente, con información actualizada y permita a los ciudadanos utilizarla desde cualquier dispositivo con acceso a internet.

Las herramientas digitales deben mantener un proceso de mejora continua que nos llevará a actualizar constantemente nuestros estándares de diseño y comunicación, con el fin de que las nuevas versiones sean cada vez mejores, lamentablemente el es calaje de este sitio se encuentra en su tope máximo en el que solo es posible trabajar con reparaciones provisionales que no permiten un servicio eficaz para la ciudadanía.

La innovación en el gobierno impulsa la eficacia y eficiencia, también transforma los procesos para proveer información, trámites y una plataforma de participación ciudadana de una manera eficaz y transparente, para lo que es necesario la renovación constante de las herramientas tecnológicas.

Esta es una modernización de fondo en la manera de comunicarnos y brindar servicios a los ciudadanos, que utiliza las ventajas de los medios digitales para escuchar, promover tu participación y colaboración en el diseño de mejores servicios y políticas públicas.

Para que este cambio gubernamental se aplique y pueda convertirse en una realidad, el sitio web debe ser sustituido por uno que cumpla y atienda las necesidades técnicas de para su utilización.

1.1 DIAGNOSTICO.

La consultoría especializada web que estuvo funcionando en la administración del 2018 al 2021 no consideraban los ejes clave que contribuyen a garantizar un servicio de calidad: accesibilidad, encontrabilidad, interactividad, operabilidad y usabilidad. Cabe señalar que sus códigos fuentes ya no se pueden actualizar y en consecuencia ya no podemos darle soporte.

Los resultados del diagnóstico se marcarán de acuerdo a su funcionalidad o respuesta en escala de eficiente, algo eficiente, poco eficiente e ineficiente.

1.2 OBJETIVO.

La Alcaldía requiere de un análisis estratégico desde la estructura del contenido y elementos gráficos, hasta la usabilidad e interacción con el usuario.

El análisis requerido incluirá el proceso de trabajo y características de las estrategias que llevaremos a cabo para el desarrollo del proyecto.

En dicha consultoría se establecerán las acciones, actividades con la tecnología adecuadas para la programación.

1.3 BENEFICIOS.

Con este proyecto, la Alcaldía se verá beneficiada al identificar de manera puntual aquellas áreas de oportunidad, duplicidad de funciones y/o ausencia de acciones que limiten el cumplimiento normativo y la eficiencia administrativa.

2. ÁREA SOLICITANTE Y SUPERVISIÓN DEL SERVICIO.

Dirección de Modernización Administrativa, el cual beneficiara a todas las áreas de esta Alcaldía.
El responsable del proyecto será:
Mtro. Rafael Calderón Jiménez
Dirección de Modernización Administrativa
Teléfono: 5276-7700 ext. 2045 y 2303.
Correo electrónico: rafaelcalderon@miguelhidalgo.gob.mx

3. SUSTENTO LEGAL DEL REQUIRIMIENTO.

De conformidad al Capítulo II, De las Atribuciones Generales de los Titulares de las Direcciones General de las Alcaldías, artículo 75 que enuncia que: "A los titulares de la Direcciones Generales de las alcaldías, corresponde las siguientes atribuciones:" fracción "IV. Planear, programar, organizar, controlar, evaluar y supervisar el desempeño de las labores encomendadas a las Unidades Administrativas y Unidades Administrativas de Apoyo Técnico-Operativo que le estén adscritas.
Así como, en la publicación de la Gaceta Oficial de la Ciudad de México del Registro de Estructura Orgánica OPA-MIH-1/010119 Alcaldía Miguel Hidalgo, publicada el 01 de febrero de 2019, que enuncia a la Dirección General de Administración y en su estructura esta la Dirección de Modernización Administrativa y dentro de esta la Subdirección de Tecnologías de la Información, que, de conformidad al Manual Administrativo aplicable y vigente, tienen las siguientes funciones respecto a este tema:
Dirección de Modernización: Dirigir el análisis de los procesos de trabajo dentro de la estructura de la Alcaldía para identificar áreas susceptibles de mejora y promover proyectos de innovación, así como la adopción de mejores prácticas; y Velar que la Alcaldía disponga de tecnologías de la información actuales para el mejor desempeño de las funciones.

4. DESCRIPCIÓN Y ESPECIFICACIONES TÉCNICAS DEL SERVICIO.

PARTIDA	DESCRIPCIÓN	UNIDAD DE MEDIDA
Única	Consultoría especializada web	Servicio

Se requiere la contratación del "Servicio de Consultoría y Desarrollo Web" para conseguir que la alcaldía Miguel Hidalgo pueda crecer en su presencia en internet, aumentar la interacción con la ciudadanía y mejorar la difusión de información a base de dictar una nueva línea de contenidos, cambios en la imagen institucional, detectar qué mejoras se pueden aplicar para que el rendimiento de la página sea mayor y la experiencia de navegación para el ciudadano sea más satisfactoria.

SERVICIOS:

1.1 Consultoría especializad en desarrollo.

a) Diagnóstico del sitio actual y áreas de oportunidad:

- ✓ Generar el reporte de ranking del sitio.
- ✓ Pruebas de velocidad, carga y navegación.
- ✓ Análisis de la información y funcionalidad clave.
- ✓ Auditoria de rendimiento SEO.
- ✓ Determinar si su sitio web tiene enlaces rotos de forma sistemática.
- ✓ Determinar la eficiencia en los principales motores de búsqueda (Google, Yahoo, Bing) entre otros.

- ✓ Determinar cómo los Googlebot están accediendo a su página web.
- ✓ Realizar un diagnóstico externo de errores y falencias que pueden afectar el posicionamiento de su web.
- ✓ Diagnóstico de imágenes.
- ✓ Texto reconocido por los buscadores.
- ✓ Determinar posibles errores de servidor.
- ✓ Pruebas de navegación con diferentes dispositivos.
- ✓ Estructura y usabilidad de su sitio web.

b) Diseño estratégico para 3 nuevos micrositios de la alcaldía:
- ✓ Crear el mapa de navegación.
- ✓ Desarrollo de contenidos
- ✓ Meta descripciones SEO
- ✓ Levantamiento de imágenes
- ✓ Diseño gráfico

5. PENAS CONVENCIONALES.

Como pena convencional a cargo del "El prestador de servicios" por incumplimiento del contrato, deficiencia o mala calidad de los servicios y/o de los materiales utilizados y por el atraso en la prestación de los servicios serán los siguientes:

SUPUESTO	PORCENTAJE DE LA PENA	BASE PARA LA APLICACIÓN
Que no esté instalado el servicio dentro de los plazos señalados de las presentes bases.	1%	Sobre el monto antes del IVA que resulte de la suma de los conceptos y cantidades requeridos para el servicio.
Que los conceptos y cantidades solicitadas para cada evento no estén instalados en el horario indicado por el área solicitante.	1%	Sobre el monto antes del IVA que resulte de la suma de los conceptos y cantidades requeridos para el servicio.

6. VIGENCIA DE LA PRESTACIÓN DEL SERVICIO.

A partir de la vigencia del contrato al 31 de diciembre de 2026.

7. PARTIDA PRESUPUESTAL.

Los recursos destinados a cubrir el gasto del servicio son ingresos en participaciones federales asignados a las funciones y actividades de la Dirección de Modernización Administrativa, partida específica **3331 "Servicios de consultoría administrativa, procesos, técnica y en tecnologías de la información".**

8. FACTURACIÓN.

"El prestador de servicios" deberá cumplir con el procedimiento que se estipula en el "Instructivo para pago a prestadores de servicios de la Alcaldía Miguel Hidalgo" que se le entrega para dicho propósito.

Las presentes especificaciones técnicas deberán forman parte integrante del Contrato de prestación de servicios que se suscriba con la persona física o moral que sea adjudicada.

9. ALCANCE.

a) Compilación de Información.
b) Análisis de la Información.

c) Presentación del Diagnóstico.
d) Propuesta de recomendaciones aplicables a los resultados del diagnóstico.

10. ENTREGABLES.

- Informe de Evaluación de la Situación Actual: Un informe detallado que identifique las fortalezas, debilidades y oportunidades de mejora del sitio web en términos de arquitectura de información, usabilidad, experiencia del usuario, accesibilidad, rendimiento y seguridad.
- Plan de Incorporación de Nuevas Funcionalidades y Micrositios: Un plan estratégico que defina las nuevas funcionalidades a implementar en el sitio web para mejorar la interacción con los ciudadanos, así como el desarrollo de micrositios para contenido focalizado y campañas específicas.
- Guía de Contenido Actualizado y Relevante: Una guía que establezca los lineamientos y procedimientos para supervisar y actualizar regularmente el contenido del sitio web, asegurando que sea relevante y de alta calidad.
- Informe de Mantenimiento Técnico y Seguridad: Un informe que describa la revisión de la estabilidad técnica y seguridad del sitio web, incluyendo las medidas implementadas para actualizar el software, realizar copias de seguridad y proteger la integridad de la información y la privacidad de los usuarios.
- Informe de Monitoreo de Resultados: Un informe que muestre las métricas y análisis para medir el rendimiento del sitio web y evaluar la efectividad de las mejoras implementadas después de la actualización y cambios.
- Estrategia de Promoción y Participación Ciudadana: Un plan estratégico que contemple las actividades para promover el sitio web entre la comunidad y fomentar la participación ciudadana a través de campañas de difusión, redes sociales y colaboración con organizaciones locales.

11. GARANTÍAS.

- El tiempo de garantía será por un año a la firma del contrato.
- Asistencia técnica vía telefónica las 24hrs x 7 días.
- Atención remota o en sitio de usuarios.
- Apoyo y orientación en la operación de equipo de comunicación y sistemas.
- Se considera la contratación de un prestador de servicios que opere de la mano con el equipo de la dirección de Modernización Administrativa.