“ADQUISICIÓN DE EQUIPOS DE RED PARA CASA MATRIZ Y SUCURSAL VILLA MORRA”

ESPECIFICACIONES TÉCNICAS

A. ANTECEDENTE

Las presentes especificaciones técnicas tienen por objeto establecer los detalles de los requerimientos técnicos (hardware y software) e informaciones mínimas referentes a la “**ADQUISICIÓN DE EQUIPOS DE RED PARA CASA MATRIZ Y SUCURSAL VILLA MORRA”**. Esta contratación incluye:

Equipos tecnológicos, Firewalls, Switches, Access Points y Cableado de Red de Datos

Instalación eléctrica, instalación de Cableado tales como Estructurado de Red y puesta en funcionamiento de los equipos con responsabilidad global del Oferente Adjudicado.

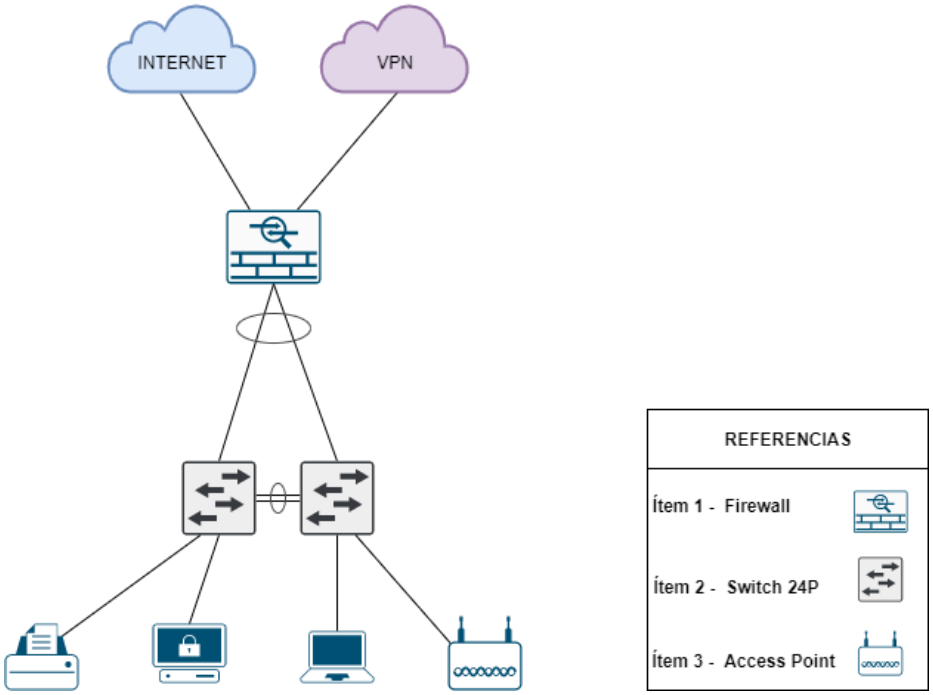
Asistencia técnica preventiva y correctiva con provisión de repuestos, por 36 meses.

B. OBJETO DEL SERVICIO

Objetivo General de la entidad: "*Promover el desarrollo económico y social del país a través de servicios bancarios y financieros, priorizando los proyectos de fomento estratégicos e inclusivos".*

Para cumplir con este objetivo la institución está abocada a la adquisición de nueva arquitectura de altos estándares de seguridad que garanticen la confidencialidad, integridad y disponibilidad de los procesos del BNF. Los Oferentes deberán ser capaces de suministrar, instalar, configurar, mantener y dar soporte a toda la arquitectura ofrecida y que permita satisfacer los requerimientos del BNF detallados en la EETT

La arquitectura, topología, distribución y conexionado de los bienes de cada sucursal del BNF requerida, objeto de la presente licitación se muestran a continuación.



C. ALCANCE

- ✓ Sucursal Villa Morra: Este proyecto contempla la renovación tecnológica del local del BNF en donde funcionan la Oficina de Villa Morra, a fin de garantizar la óptima instalación de los equipamientos de red.
- ✓ Firewall SDWAN: Corresponde a un equipo de borde, el cual se encargará de la terminación de las VPNs y la agregación de los enlaces de proveedores. Debe contar con las licencias de SDWAN según especificaciones técnicas
- ✓ Switch: se encargará de interconectar los dispositivos finales a la red del BNF.
- ✓ Access Point: brindará conectividad WiFi para los usuarios de las sucursales, será gestionado por el firewall solicitado por este llamado por lo cual permitirá una gestión de politicas de seguridad centralizada para la red cableada e inalámbrica.
- ✓ El Oferente deberá entregar una descripción técnica detallada y explícita de los equipos ofertados y explicará en detalle cómo se alcanza el cumplimiento de lo requerido en este Pliego. Esto será considerado de carácter SUSTANCIAL. Para ello el Oferente deberá presentar una Planilla de Datos Técnicos.

Marco General
El proyecto de reingeniería de la infraestructura tecnológica, ha sido desarrollado por la GTIC del BNF y comprende la restructuración total del sistema de comunicación de las distintas Sucursales descripto en el proyecto de alcance.

En este marco manifestamos que el BNF actualmente cuenta con **dependencias tecnológicas** en cuanto a plataforma de seguridad y networking existentes, por las cuales la convocante ya ha realizado una inversión importante años anteriores adquiriendo equipos de altas prestaciones en la dos plataforma mencionada, y que también se ha invertido constantemente en la capacitación técnica para la gestión, administración, monitoreo y solución inmediata de problemas en Técnicos Propio del BNF, que justifica considerablemente dejar como Dependencia Tecnológica los mismos. En la capa de red de Borde actualmente existen equipos de seguridad del fabricante FORTINET, por lo tanto, es necesaria la completa integración a nivel de L2 a L7, SD-WAN y todas las funcionalidades de los nuevos equipos requeridos en el Ítem 1 con esta tecnología ya instalada y en producción en el BNF.

D. SECCIÓN SUMINISTROS O SERVICIOS REQUERIDOS

1. SOFTWARE-DEFINED WAN.

En la actualidad, con el gran crecimiento del uso de las redes móviles, las aplicaciones en la nube y los incrementos de los anchos de banda; las organizaciones se encuentran en un proceso de transformación digital.
Dicho proceso afecta a las redes WAN en aspectos como:

- El crecimiento de tráfico hacia la WAN.
- Falta de visibilidad y control de aplicaciones que corren en la red.
- El aseguramiento de los usuarios ante amenazas.
- El control del ancho de banda de los usuarios o las aplicaciones que usan.
- El mantenimiento de los niveles de servicio.
- Etc.

Esto provoca que la arquitectura WAN tradicional se quede obsoleta y se genere la necesidad de un nuevo modelo más ágil, menos costoso, con altos niveles de servicio, agnóstico al tipo de enlace y/o proveedor de servicio. Entonces, bajo las premisas anteriores, es necesario optar por un nuevo modelo de comunicaciones, el cual permita dar respuesta a las demandas de las organizaciones.

Para lograrlo, el BNF desea implementar una solución que tenga la capacidad de implementar y administrar tanto los mecanismos de distribución de tráfico a través de diferentes enlaces, como la seguridad de los usuarios, manteniendo los niveles de servicio óptimos para el desempeño del uso de las aplicaciones de los usuarios y la red wan en general.

Esta solución debe ser compatible con la solución existente y debe garantizar el acceso seguro y eficiente a los servicios brindados por el Banco Nacional de Fomento.

Para la conectividad WAN, los equipos ofertados deberán ser compatible con el equipo de seguridad actualmente existente en el BNF Fortigate 1200D. La misma se encargará de funcionar como concentrador de VPN para los enlaces con las sucursales, permitiendo armar al fabric SDWAN para el BNF, con esto se busca tener mayor visibilidad, gestión y políticas unificadas de la red de Borde, por lo tanto, es necesaria la completa integración.

Todos los equipos deberán contar con features de performance y seguridad que permitan garantizar la calidad de los servicios brindados. De manera a garantizar la correcta integración de las soluciones ofertadas, el oferente deberá contar con personal técnico calificado para la configuración y el soporte de todos los componentes involucrados.

ÍTEM 1 - FIREWALL SD WAN – TIPO 1

FIREWALL TIPO 1				
Ítems	**Especificación y/o Funcionalidad**	**Características**	**Mínimo Exigido**	**El equipo ofertado cumple con las especificaciones requeridas (sí / no)**
Fabricante			Exigido	
Modelo:			Exigido	
Número de Parte			Exigido	
Cantidad:		**4**	Exigido	
#	**Características técnicas**	**Especificaciones técnicas mínimas solicitadas**	**Carácter**	**Ofrecido**
1	Capacidades	Throughput de por lo menos 10 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6	Exigido	
2		Soporte a por lo menos 650.000 conexiones simultaneas	Exigido	
3		Soporte a por lo menos 30.000 nuevas conexiones por segundo	Exigido	
4		Throughput de al menos 6 Gbps de VPN IPSec	Exigido	
5		Debe contar con la capacidad de levantar 150 túneles de VPN IPSec site-to-site simultáneos	Exigido	
6		Debe contar con la capacidad de levantar 300 túneles de clientes VPN IPSec simultáneos	Exigido	
7		Throughput de al menos 850 Mbps de VPN SSL	Exigido	
8		Soportar al menos 180 clientes de VPN SSL simultáneos	Exigido	
9		Soportar al menos 1.3 Gbps de throughput de IPS	Exigido	
10		Soportar al menos 620 Mbps de throughput de Inspección SSL	Exigido	
11		Soportar al menos 1.7 Gbps de throughput de Application Control	Exigido	
12		Soportar al menos 920 Mbps de throughput de NGFW	Exigido	

13		Soportar al menos 650 Mbps de throughput de Threat Protection	Exigido	
14		Contar con al menos 5 interfaces 1Gbps RJ45 y 2 interfaces SFP	Exigido	
15		Incluir la capacidad de contar con 10 sistemas virtuales lógicos (Contextos) por appliance	Exigido	
16	Características Generales	La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo.;	Exigido	
17		Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;	Exigido	
18		Las funcionalidades de protección de red que conforman la plataforma de seguridad, puede ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;	Exigido	
19		La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;	Exigido	
20		Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación;	Exigido	
21		La gestión del equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;	Exigido	
22		Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;	Exigido	
23		Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;	Exigido	
24		Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;	Exigido	

25		Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);	Exigido	
26		Los dispositivos de protección de red deben soportar DHCP Relay;	Exigido	
27		Los dispositivos de protección de red deben soportar DHCP Server;	Exigido	
28		Los dispositivos de protección de red deben soportar sFlow;	Exigido	
29		Los dispositivos de protección de red deben soportar Jumbo Frames;	Exigido	
30		Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;	Exigido	
31		Debe ser compatible con NAT dinámica (varios-a-1);	Exigido	
32		Debe ser compatible con NAT dinámica (muchos-a-muchos);	Exigido	
33		Debe soportar NAT estática (1-a-1);	Exigido	
34		Debe admitir NAT estática (muchos-a-muchos);	Exigido	
35		Debe ser compatible con NAT estático bidireccional 1-a-1;	Exigido	
36		Debe ser compatible con la traducción de puertos (PAT);	Exigido	
37		Debe ser compatible con NAT Origen;	Exigido	
38		Debe ser compatible con NAT de destino;	Exigido	
39		Debe soportar NAT de origen y NAT de destino de forma simultánea;	Exigido	
40		Debe soportar NAT de origen y NAT de destino en la misma política	Exigido	
41		Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;	Exigido	
42		Debe ser compatible con NAT64 y NAT46;	Exigido	
43		Debe implementar el protocolo ECMP;	Exigido	
44		Debe soportar SD-WAN de forna nativa	Exigido	
45		Debe soportar el balanceo de enlace hash por IP de origen;	Exigido	

46		Debe soportar el balanceo de enlace por hash de IP de origen y destino;	Exigido	
47		Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces;	Exigido	
48		Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;	Exigido	
49		Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red;	Exigido	
50		Enviar logs a sistemas de gestión externos simultáneamente;	Exigido	
51		Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;	Exigido	
52		Debe soporta protección contra la suplantación de identidad (anti-spoofing);	Exigido	
53		Implementar la optimización del tráfico entre dos dispositivos;	Exigido	
54		Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);	Exigido	
55		Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);	Exigido	
56		Soportar OSPF graceful restart;	Exigido	
57		Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;	Exigido	
58		Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;	Exigido	
59		Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;	Exigido	
60		Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;	Exigido	

61		Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;	Exigido	
62		Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;	Exigido	
63		Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;	Exigido	
64		La configuración de alta disponibilidad debe sincronizar: Sesiones;	Exigido	
65		La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;	Exigido	
66		La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;	Exigido	
67		La configuración de alta disponibilidad debe sincronizar: Tablas FIB;	Exigido	
68		En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;	Exigido	
69		Debe soportar la creación de sistemas virtuales en el mismo equipo;	Exigido	
70		Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos;	Exigido	
71		Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales;	Exigido	
72		La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web	Exigido	

		(HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso;		
73		Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos);	Exigido	
74		Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;	Exigido	
75		El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red;	Exigido	
76		Debe existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi;	Exigido	
77		La consola de administración debe soportar como minimo, ingles, Español y Portugues.	Exigido	
78		La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad	Exigido	
79		La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.	Exigido	
80	Control por Politica de Firewall	Debe soportar controles de zona de seguridad;	Exigido	
81		Debe contar con políticas de control por puerto y protocolo;	Exigido	
82		Contar con políticas por aplicación, grupos estáticos de	Exigido	

		aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones;		
83		Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;	Exigido	
84		Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;	Exigido	
85		Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;	Exigido	
86		Debe soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.	Exigido	
87		Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);	Exigido	
88		Debe soportar integración de nubes publicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes	Exigido	
89		Debe soportar el protocolo estándar de la industria VXLAN;	Exigido	
90		La solución debe permitir la implementación de SD-WAN	Exigido	
91		En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por politicas, IPSEC VPN;	Exigido	
92		la solución debe soportar la integración nativa con solución de sandboxing, protección de correo electronico, cache y Web application firewall.	Exigido	

93	Control de Aplicación	Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;	Exigido	
94		Detección de miles de aplicaciones en 16 categorias, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico;	Exigido	
95		Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;	Exigido	
96		Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor;	Exigido	
97		Para trafico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante;	Exigido	
98		Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;	Exigido	
99		Actualización de la base de firmas de la aplicación de forma automática;	Exigido	
100		Limitar el ancho de banda utilizado por las aplicaciones,	Exigido	

		basado en IP, por politica de usuarios y grupos;		
101		Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;	Exigido	
102		Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante;	Exigido	
103		El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;	Exigido	
104		Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;	Exigido	
105		Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;	Exigido	
106		Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;	Exigido	
107		Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;	Exigido	
108		Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc);	Exigido	
109		Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;	Exigido	
110		Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas,	Exigido	

		tales como: Categoría de Aplicación;		
111		Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente	Exigido	
112	Prevención de Amenazas	Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;	Exigido	
113		Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);	Exigido	
114		Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;	Exigido	
115		Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;	Exigido	
116		Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos;	Exigido	
117		Deber permitir el bloqueo de vulnerabilidades y exploits conocidos	Exigido	
118		Debe incluir la protección contra ataques de denegación de servicio;	Exigido	
119		Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;	Exigido	
120		Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;	Exigido	
121		Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;	Exigido	

122		Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;	Exigido	
123		Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);	Exigido	
124		Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc;	Exigido	
125		Detectar y bloquear los escaneos de puertos de origen;	Exigido	
126		Bloquear ataques realizados por gusanos (worms) conocidos;	Exigido	
127		Contar con firmas específicas para la mitigación de ataques DoS y DDoS;	Exigido	
128		Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);	Exigido	
129		Debe poder crear firmas personalizadas en la interfaz gráfica del producto;	Exigido	
130		Identificar y bloquear la comunicación con redes de bots;	Exigido	
131		Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo;	Exigido	
132		Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;	Exigido	
133		Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos;	Exigido	
134		Los eventos deben identificar el país que origino la amenaza;	Exigido	
135		Debe incluir protección contra virus en contenido HTML y	Exigido	

		Javascript, software espía (spyware) y gusanos (worms);		
136		Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;	Exigido	
137		Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad;	Exigido	
138		En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles;	Exigido	
139		Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube);	Exigido	
140	Filtrado de URL	Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora);	Exigido	
141		Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito;	Exigido	
142		Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;	Exigido	

143		Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL;	Exigido	
144		Tener por lo menos 75 categorías de URL;	Exigido	
145		Debe tener la funcionalidad de exclusión de URLs por categoría;	Exigido	
146		Permitir página de bloqueo personalizada;	Exigido	
147		Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio);	Exigido	
148		Además del Explicit Web Proxy, soportar proxy web transparente;	Exigido	
149	Identificación de Usuarios	Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;	Exigido	
150		Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basados en usuarios y grupos de usuarios;	Exigido	
151		Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc;	Exigido	
152		Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las	Exigido	

		políticas de granularidad / control basados en usuarios y grupos de usuarios;		
153		Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la políticas/control basados en usuarios y grupos de usuarios;	Exigido	
154		Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo);	Exigido	
155		Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios;	Exigido	
156		Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;	Exigido	
157		Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;	Exigido	
158		Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;	Exigido	
159	QoS	Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming;	Exigido	

160		Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;	Exigido	
161		Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;	Exigido	
162		Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;	Exigido	
163		Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;	Exigido	
164		Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;	Exigido	
165		En QoS debe permitir la definición de tráfico con ancho de banda garantizado;	Exigido	
166		En QoS debe permitir la definición de tráfico con máximo ancho de banda;	Exigido	
167		En QoS debe permitir la definición de colas de prioridad;	Exigido	
168		Soportar marcación de paquetes DiffServ, incluso por aplicación;	Exigido	
169		Soportar la modificación de los valores de DSCP para Diffserv;	Exigido	
170		Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);	Exigido	
171		Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;	Exigido	
172	Filtro de Datos	Permite la creación de filtros para archivos y datos predefinidos;	Exigido	
173		Los archivos deben ser identificados por tamaño y tipo;	Exigido	
174		Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones;	Exigido	
175		Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;	Exigido	
176		Soportar la identificación de archivos cifrados y la aplicación	Exigido	

		de políticas sobre el contenido de este tipo de archivos;		
177		Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares;	Exigido	
178	Geo Localización	Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;	Exigido	
179		Debe permitir la visualización de los países de origen y destino en los registros de acceso;	Exigido	
180		Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;	Exigido	
181	VPN	Soporte VPN de sitio-a-sitio y cliente-a-sitio;	Exigido	
182		Soportar VPN IPSec;	Exigido	
183		Soportar VPN SSL;	Exigido	
184		La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512	Exigido	
185		La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;	Exigido	
186		La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);	Exigido	
187		La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);	Exigido	
188		Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;	Exigido	
189		Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;	Exigido	
190		Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo	Exigido	

		que facilita el proceso throubleshooting;		
191		Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy;	Exigido	
192		Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL;	Exigido	
193		Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;	Exigido	
194		Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;	Exigido	
195		Deberá mantener una conexión segura con el portal durante la sesión;	Exigido	
196		El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.	Exigido	
197	Garantía	La oferta deberá incluir soporte técnico por parte del oferente en modalidad onsite 24x7x4, por un periodo mínimo de 36 meses	Exigido	
198		La oferta deberá incluir una garantía de 3 (tres) años como mínimo, esta garantía deberá ser provista directamente por el fabricante de la solución ofertada y la misma deberá incluir reposición de partes. No serán aceptadas garantías de partner local por más que estas incluyan reposición de partes. Se solicita carta del fabricante de la solución ofertada dirigida a la convocante donde referencie el presente llamado y manifieste la duración, tipo y modalidad de garantía y reposición de parte ofertado por el oferente.	Exigido	
199		La oferta deberá incluir suscripción a todo el	Exigido	

		licenciamiento necesario por un periodo mínimo de 3 (Tres) años.		
200		El oferente deberá presentar una carta del fabricante dirigida a la convocante en donde se haga mención del presente llamado, autorizando al oferente a presentar oferta, brindar servicio técnico y el reemplazo de partes por garantía del bien ofertado.	Exigido	
201		Todos estos puntos son requerimientos mínimos y no sé aceptarán ofertas que no cumplan con las mismas. Esto a los efectos de garantizar la calidad y compatibilidad de los dispositivos solicitados; así como los servicios de post-venta (servicio técnico con mano de obra certificada por el fabricante; piezas originales; laboratorios autorizados por el fabricante).	Exigido	

ÍTEM 2 - FIREWALL SDWAN – TIPO 2

FIREWALL TIPO 2				
Ítems	**Especificación y/o Funcionalidad**	**Características**	**Mínimo Exigido**	**El equipo ofertado cumple con las especificaciones requeridas (sí / no)**
Fabricante			Exigido	
Modelo:			Exigido	
Número de Parte			Exigido	
Cantidad:		**3**	Exigido	
#	**Características técnicas**	**Especificaciones técnicas mínimas solicitadas**	**Carácter**	**Ofrecido**
1	Capacidades	Throughput de por lo menos 5 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6	Exigido	
2		Soporte a por lo menos 600.000 conexiones simultaneas	Exigido	
3		Soporte a por lo menos 30.000 nuevas conexiones por segundo	Exigido	
4		Throughput de al menos 4 Gbps de VPN IPSec	Exigido	
5		Debe contar con la capacidad de levantar 200 túneles de VPN IPSec site-to-site simultáneos	Exigido	
6		Debe contar con la capacidad de levantar 200 túneles de clientes VPN IPSec simultáneos	Exigido	
7		Throughput de al menos 450 Mbps de VPN SSL	Exigido	
8		Soportar al menos 180 clientes de VPN SSL simultáneos	Exigido	
9		Soportar al menos 1 Gbps de throughput de IPS	Exigido	
10		Soportar al menos 300 Mbps de throughput de Inspección SSL	Exigido	
11		Soportar al menos 900 Mbps de throughput de Application Control	Exigido	
12		Soportar al menos 800 Mbps de throughput de NGFW	Exigido	
13		Soportar al menos 600 Mbps de throughput de Threat Protection	Exigido	
14		Contar con al menos 5 interfaces 1Gbps RJ45	Exigido	

15		Incluir la capacidad de contar con 10 sistemas virtuales lógicos (Contextos) por appliance	Exigido	
16	Características Generales	La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo.;	Exigido	
17		Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;	Exigido	
18		Las funcionalidades de protección de red que conforman la plataforma de seguridad, puede ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;	Exigido	
19		La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;	Exigido	
20		Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación;	Exigido	
21		La gestión del equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;	Exigido	
22		Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;	Exigido	
23		Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;	Exigido	
24		Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;	Exigido	
25		Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);	Exigido	

26		Los dispositivos de protección de red deben soportar DHCP Relay;	Exigido	
27		Los dispositivos de protección de red deben soportar DHCP Server;	Exigido	
28		Los dispositivos de protección de red deben soportar sFlow;	Exigido	
29		Los dispositivos de protección de red deben soportar Jumbo Frames;	Exigido	
30		Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;	Exigido	
31		Debe ser compatible con NAT dinámica (varios-a-1);	Exigido	
32		Debe ser compatible con NAT dinámica (muchos-a-muchos);	Exigido	
33		Debe soportar NAT estática (1-a-1);	Exigido	
34		Debe admitir NAT estática (muchos-a-muchos);	Exigido	
35		Debe ser compatible con NAT estático bidireccional 1-a-1;	Exigido	
36		Debe ser compatible con la traducción de puertos (PAT);	Exigido	
37		Debe ser compatible con NAT Origen;	Exigido	
38		Debe ser compatible con NAT de destino;	Exigido	
39		Debe soportar NAT de origen y NAT de destino de forma simultánea;	Exigido	
40		Debe soportar NAT de origen y NAT de destino en la misma política	Exigido	
41		Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;	Exigido	
42		Debe ser compatible con NAT64 y NAT46;	Exigido	
43		Debe implementar el protocolo ECMP;	Exigido	
44		Debe soportar SD-WAN de forna nativa	Exigido	
45		Debe soportar el balanceo de enlace hash por IP de origen;	Exigido	
46		Debe soportar el balanceo de enlace por hash de IP de origen y destino;	Exigido	

47		Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces;	Exigido	
48		Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;	Exigido	
49		Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red;	Exigido	
50		Enviar logs a sistemas de gestión externos simultáneamente;	Exigido	
51		Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;	Exigido	
52		Debe soporta protección contra la suplantación de identidad (anti-spoofing);	Exigido	
53		Implementar la optimización del tráfico entre dos dispositivos;	Exigido	
54		Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);	Exigido	
55		Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);	Exigido	
56		Soportar OSPF graceful restart;	Exigido	
57		Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;	Exigido	
58		Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;	Exigido	
59		Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;	Exigido	
60		Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;	Exigido	
61		Soportar la configuración de alta disponibilidad activo / pasivo y	Exigido	

		activo / activo: En modo transparente;		
62		Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;	Exigido	
63		Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;	Exigido	
64		La configuración de alta disponibilidad debe sincronizar: Sesiones;	Exigido	
65		La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;	Exigido	
66		La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;	Exigido	
67		La configuración de alta disponibilidad debe sincronizar: Tablas FIB;	Exigido	
68		En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;	Exigido	
69		Debe soportar la creación de sistemas virtuales en el mismo equipo;	Exigido	
70		Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos;	Exigido	
71		Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales;	Exigido	
72		La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de	Exigido	

		configuración de sistemas virtuales (contextos) por ambos tipos de acceso;		
73		Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos);	Exigido	
74		Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;	Exigido	
75		El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red;	Exigido	
76		Debe existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi;	Exigido	
77		La consola de administración debe soportar como minimo, ingles, Español y Portugues.	Exigido	
78		La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad	Exigido	
79		La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.	Exigido	
80	Control por Politica de Firewall	Debe soportar controles de zona de seguridad;	Exigido	
81		Debe contar con políticas de control por puerto y protocolo;	Exigido	

82		Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones;	Exigido	
83		Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;	Exigido	
84		Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;	Exigido	
85		Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;	Exigido	
86		Debe soportar automatización de situaciones como deteción de equipos comprometidos, estado del sistema, cambios de onfiguración, eventos especificos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.	Exigido	
87		Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);	Exigido	
88		Debe soportar integración de nubes publicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes	Exigido	
89		Debe soportar el protocolo estándar de la industria VXLAN;	Exigido	
90		La solución debe permitir la implementación de SD-WAN	Exigido	
91		En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por politicas, IPSEC VPN;	Exigido	
92		la solución debe soportar la integración nativa con solución de sandboxing, protección de correo electronico, cache y Web application firewall.	Exigido	

93	Control de Aplicación	Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;	Exigido	
94		Detección de miles de aplicaciones en 16 categorias, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico;	Exigido	
95		Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;	Exigido	
96		Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor;	Exigido	
97		Para trafico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante;	Exigido	
98		Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;	Exigido	
99		Actualización de la base de firmas de la aplicación de forma automática;	Exigido	
100		Limitar el ancho de banda utilizado por las aplicaciones,	Exigido	

		basado en IP, por politica de usuarios y grupos;		
101		Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;	Exigido	
102		Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante;	Exigido	
103		El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;	Exigido	
104		Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;	Exigido	
105		Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;	Exigido	
106		Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;	Exigido	
107		Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;	Exigido	
108		Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc);	Exigido	
109		Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;	Exigido	
110		Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas,	Exigido	

		tales como: Categoría de Aplicación;		
111		Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente	Exigido	
112	Prevención de Amenazas	Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;	Exigido	
113		Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);	Exigido	
114		Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;	Exigido	
115		Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;	Exigido	
116		Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos;	Exigido	
117		Deber permitir el bloqueo de vulnerabilidades y exploits conocidos	Exigido	
118		Debe incluir la protección contra ataques de denegación de servicio;	Exigido	
119		Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;	Exigido	
120		Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;	Exigido	
121		Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;	Exigido	

122		Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;	Exigido	
123		Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);	Exigido	
124		Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc;	Exigido	
125		Detectar y bloquear los escaneos de puertos de origen;	Exigido	
126		Bloquear ataques realizados por gusanos (worms) conocidos;	Exigido	
127		Contar con firmas específicas para la mitigación de ataques DoS y DDoS;	Exigido	
128		Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);	Exigido	
129		Debe poder crear firmas personalizadas en la interfaz gráfica del producto;	Exigido	
130		Identificar y bloquear la comunicación con redes de bots;	Exigido	
131		Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo;	Exigido	
132		Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;	Exigido	
133		Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos;	Exigido	
134		Los eventos deben identificar el país que origino la amenaza;	Exigido	
135		Debe incluir protección contra virus en contenido HTML y	Exigido	

		Javascript, software espía (spyware) y gusanos (worms);		
136		Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;	Exigido	
137		Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad;	Exigido	
138		En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles;	Exigido	
139		Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube);	Exigido	
140	Filtrado de URL	Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora);	Exigido	
141		Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito;	Exigido	
142		Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;	Exigido	

143		Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL;	Exigido	
144		Tener por lo menos 75 categorías de URL;	Exigido	
145		Debe tener la funcionalidad de exclusión de URLs por categoría;	Exigido	
146		Permitir página de bloqueo personalizada;	Exigido	
147		Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio);	Exigido	
148		Además del Explicit Web Proxy, soportar proxy web transparente;	Exigido	
149	Identificación de Usuarios	Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;	Exigido	
150		Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basados en usuarios y grupos de usuarios;	Exigido	
151		Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc;	Exigido	
152		Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las	Exigido	

		políticas de granularidad / control basados en usuarios y grupos de usuarios;		
153		Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la políticas/control basados en usuarios y grupos de usuarios;	Exigido	
154		Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo);	Exigido	
155		Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios;	Exigido	
156		Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;	Exigido	
157		Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;	Exigido	
158		Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;	Exigido	
159	QoS	Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming;	Exigido	

160		Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;	Exigido	
161		Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;	Exigido	
162		Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;	Exigido	
163		Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;	Exigido	
164		Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;	Exigido	
165		En QoS debe permitir la definición de tráfico con ancho de banda garantizado;	Exigido	
166		En QoS debe permitir la definición de tráfico con máximo ancho de banda;	Exigido	
167		En QoS debe permitir la definición de colas de prioridad;	Exigido	
168		Soportar marcación de paquetes DiffServ, incluso por aplicación;	Exigido	
169		Soportar la modificación de los valores de DSCP para Diffserv;	Exigido	
170		Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);	Exigido	
171		Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;	Exigido	
172	Filtro de Datos	Permite la creación de filtros para archivos y datos predefinidos;	Exigido	
173		Los archivos deben ser identificados por tamaño y tipo;	Exigido	
174		Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones;	Exigido	
175		Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;	Exigido	
176		Soportar la identificación de archivos cifrados y la aplicación	Exigido	

		de políticas sobre el contenido de este tipo de archivos;		
177		Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares;	Exigido	
178	Geo Localización	Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;	Exigido	
179		Debe permitir la visualización de los países de origen y destino en los registros de acceso;	Exigido	
180		Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;	Exigido	
181	VPN	Soporte VPN de sitio-a-sitio y cliente-a-sitio;	Exigido	
182		Soportar VPN IPSec;	Exigido	
183		Soportar VPN SSL;	Exigido	
184		La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512	Exigido	
185		La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;	Exigido	
186		La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);	Exigido	
187		La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);	Exigido	
188		Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;	Exigido	
189		Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;	Exigido	
190		Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo	Exigido	

		que facilita el proceso throubleshooting;		
191		Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy;	Exigido	
192		Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL;	Exigido	
193		Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;	Exigido	
194		Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;	Exigido	
195		Deberá mantener una conexión segura con el portal durante la sesión;	Exigido	
196		El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.	Exigido	
197	Garantía	La oferta deberá incluir soporte técnico por parte del oferente en modalidad onsite 24x7x4, por un periodo mínimo de 36 meses	Exigido	
198		La oferta deberá incluir una garantía de 3 (tres) años como mínimo, esta garantía deberá ser provista directamente por el fabricante de la solución ofertada y la misma deberá incluir reposición de partes. No serán aceptadas garantías de partner local por más que estas incluyan reposición de partes. Se solicita carta del fabricante de la solución ofertada dirigida a la convocante donde referencie el presente llamado y manifieste la duración, tipo y modalidad de garantía y reposición de parte ofertado por el oferente.	Exigido	
199		La oferta deberá incluir suscripción a todo el	Exigido	

		licenciamiento necesario por un periodo mínimo de 3 (Tres) años.		
200		El oferente deberá presentar una carta del fabricante dirigida a la convocante en donde se haga mención del presente llamado, autorizando al oferente a presentar oferta, brindar servicio técnico y el reemplazo de partes por garantía del bien ofertado.	Exigido	
201		Todos estos puntos son requerimientos mínimos y no sé aceptarán ofertas que no cumplan con las mismas. Esto a los efectos de garantizar la calidad y compatibilidad de los dispositivos solicitados; así como los servicios de post-venta (servicio técnico con mano de obra certificada por el fabricante; piezas originales; laboratorios autorizados por el fabricante).	Exigido	

ÍTEM 3 – SWITCH 24 DE PUERTOS POE

SWITCH DE 24 PUERTOS			
Ítems	**Especificación y/o Funcionalidad**	**Características**	**Mínimo Exigido**
1	**Cantidad**	**7**	Exigido
2	**Marca**	Indicar	Exigido
3	**Modelo**	Indicar	Exigido
4	**Procedencia**	Indicar	Exigido
5	**Tipo de switch**	Utiización como switch de acceso	Exigido
6	**Interfaces**	Debe contar con 24 puertos ethernet 10/100/1000 Base-T energizados en su totalidad con características POE	Exigido
7		Debe contar con al menos 4 puertos uplink con capacidad de 1 Gigabit ethernet	Exigido
8		De manera a garantizar la total compatibilidad de la solución, los módulos a ser proveídos deberán ser del mismo fabricante del equipo	Exigido
9	**Stacking o apilamiento**	Vinculación de equipos por puertos de uso exclusivo para Stack excluyendo las interfaces de RED	Exigido
10		Como mínimo 8 (Ocho) equipos agrupados para administrar con un único acceso administrativo	Exigido
11		Capacidad mínima de 74 Gbps ancho de banda del Stack utilizando los puertos específicos de stacking	Exigido
12		Deberá incluir los accesorios necesarios para el Stacking	Exigido
13		Configuración desde una única dirección IP y para su administración actuarán como un único equipo	Exigido
14	**Características del equipo**	Deben tener un tamaño de 1U y ser rackeables en infraestructuras de 19”	Exigido
15		Deberá poseer como mínimo 1024 MB de memoria DRAM.	Exigido
16		Deberá poseer una memoria Flash reescribible de al menos 2024 MB	Exigido
17		Fuente de poder interna con rango de operación entre 100-240VAC/50-60Hz con cable de alimentación con toma tipo americano.	Exigido
18		Deberá contar mínimamente con capacidad PoE de 370W	

19		Deberá soportar un rango de temperatura de operación como mínimo entre 0° y 45° C y un rango de Humedad no condensada de 10 a 90 %.	Exigido
20		Deberá tener un tiempo promedio entre fallas (MTBF) de al menos 380000 horas	Exigido
21		Debe contar con ranura para adicionar fuente redundante	Exigido
22		Debe soportar funciones layer 2	Exigido
23		Debe soportar funciones layer 3	Exigido
24	**Sistema operativo**	Debe ser apto para funcionar con tecnologías de (SDN) Software Defined Network	Exigido
25		Debe soportar una programabilidad basada en modelos	Exigido
26		Debe soportar telemetría de streamming	Exigido
27		Debe soportar scripting en Python	Exigido
28		Debe soportar la corrección de bugs	Exigido
29	**Rendimiento**	Capacidad de switcheo de al menos 54 Gbps	Exigido
30		Capacidad de forwarding mínima de 40 mpps	Exigido
31		Deberá soportar al menos 16000 MAC Address	Exigido
32		Deberá soportar al menos 900 rutas multicast	Exigido
33		Deberá soporta una cantidad mínima 2500 entradas de ruteo IPV4	Exigido
34		El equipo debe soportar Jumbo Frames de 9198 bytes como mínimo.	Exigido
35	**Protocolos y Funcionalidades**	Deberá soportar los siguientes protocolos de ruteo IP unicast: RIPv1, RiIPv2, OSPF, RIPng	Exigido
36		Deberá soportar los siguientes protocolos de ruteo IP multicast: PIM, PIM-SM, SSM	Exigido
37		Deberá soportar los siguientes protocolos de ruteo IP versión 6: OSPFv3, EIGRP (RFC 7868) o similar	Exigido
38		IEEE 802.1 ae	Exigido
39		IEEE 802.3 at	Exigido
40		IEEE 802.3 af	Exigido
41		IEEE 802.1x Identify-Based Networking Services (IBNS)	Exigido
42		IEEE 802.1s Per-Vlan group Spanning Tree Protocol	Exigido
43		IEEE 802.1d Spanning Tree Protocol	Exigido
44		IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)	Exigido
45		IEEE 802.3ad Link Aggregation Control Protocol (LACP)	Exigido
46		IEEE 802.3x Flow Control	Exigido
47		IEEE 802.1q VLAN Tagging	Exigido
48		IEEE 802.1p Class Of Service (Cos)	Exigido
49		IEEE 802.3 10BASE-T	Exigido

50		IEEE 802.3u 100BASE-T	Exigido
51		IEEE 802.3ab 1000BASE-T	Exigido
52		IEEE 802.3z 1000BASE-X	Exigido
53		RFC 768 (UDP)	Exigido
54		RFC 783 O RFC 1350 Trivial File Transfer Protocol (TFTP)	Exigido
55		RFC 791 Internet Protocol (IP)	Exigido
56		RFC 792 Internet Control Message Protocol (ICMP)	Exigido
57		RFC 793 Transmission Control Protocol (TCP)	Exigido
58		RFC 826 Adress Resolution Protocol (ARP)	Exigido
59		RFC 854 Telnet	Exigido
60		RFC 951 Bootstrap Protocool (BOOTP)	Exigido
61		RFC 3376 IGMP v3	Exigido
62		RFC 1157 Simple Network Management Protocol Version 1 (SNMP v1)	Exigido
63		RFC 1901 SNMPv2c	Exigido
64		RFC 3410 SNMP v3	Exigido
65		RFC 2474 Differentiated Services (DiffServ)	Exigido
66		Soporte de seguridad del puerto mediante filtrado por dirección MAC, limitación de direcciones MAC por puerto	Exigido
67		Soporte de tráfico mirroring por puerto o por VLAN	Exigido
68		Deberá poseer al menos 8 colas salientes por puerto	Exigido
69		Deberá soportar IGMP snooping	Exigido
70		Deberá permitir el control de tormentas de broadcast, multicast y unicast en cada puerto	Exigido
71		Deberá soportar sincronización horaria por medio de Network Timing Protocol (NTP) según RFC 1305.	Exigido
72	**Administración**	Deberá de contar con la posibilidad de administración mediante GUI Nativa de fácil utilización	Exigido
73		Soporte de gestión centralizada mediante software (SDN) Software defined network	Exigido
74		Deberá tener soporte de AAA utilizando Radius como mínimo	Exigido
75		Debe contar con la posibilidad de generar diferentes perfiles de usuarios de administración con diferentes grados de autorización para el acceso y ejecución de las distintas tareas de gestión de la red	Exigido
76		Soporte de autenticación de usuarios de acuerdo al estándar IEEE 802.1x	Exigido
77		Servicio de configuración por medio de puerto de consola.	Exigido

78		Servicio de configuración por medio de consola remota Telnet según RFC 854 sobre transporte TCP/IP según RFC 793	Exigido
79		Soporte de gestión remota segura por SNMPv3	Exigido
80		Soporte de gestión remota segura por SSHv2	Exigido
81		Capacidad de Remote Monitoring versión 2 (RMON II).	Exigido
82	**Certificaciones**	Deberá cumplir al menos con las siguientes normas de Compatibilidad Electromagnética (EMC) y (EMI): BSMI clase A, ICES-003 Clase A, CISPR 32 Clase A, CISPR 35, AS/NZS 3548 Clase A	Exigido
83		Deberá cumplir con al menos las normas de seguridad UL 60950-1 y/o CAN/CSA-C22 No 60950-1 y/o, IEC 60950-1 y/o TUV/GS (EN60950-1) y poseer marca de la CE (CE mark)	Exigido
84		Reduction of Hazardous Substances (ROHS) 5	Exigido
85	**Asistencia en el sitio**	Nivel de soporte Del tipo 8x5 por un periodo de 36 meses	Exigido
86		El proveedor deberá prestar el servicio, reparación, provisión de insumos, mano de obra y todo otro elemento que garantice el correcto funcionamiento de los bienes ofertados mientras dure el contrato y a partir de la puesta en marcha hasta el término del periodo de garantía.	Exigido
87		El proveedor deberá dar asistencia técnica en el sitio declarado por el BNF, una vez reportado el problema, y si la solución al mismo así lo requiere. Esta asistencia comprende la solución de incidencias de funcionamiento lógico, parametrización o configuración del equipo proveído en este llamado, así como de cualquiera de los módulos del mismo que se encuentren bajo la cobertura del soporte	Exigido
88	**Contacto**	El proveedor deberá facilitar números telefónicos de urgencia, direcciones de correo, y una página Web para proceder a la comunicación del problema.	Exigido
89	**Asistencia remota**	El proveedor deberá poner a disposición del ministerio de BNF una línea directa a soporte técnico (Help Desk) que cubrirá la asistencia telefónica para los diagnósticos y la resolución de problemas relacionados con el funcionamiento del equipo y de todos los módulos que lo componen y que se encuentren bajo la cobertura del soporte. Esta asistencia comprende la solución de incidencias de funcionamiento lógico, parametrización o configuración del equipo, así como de cualquiera de los módulos del mismo que se encuentren bajo la cobertura	Exigido

		del soporte. Esta asistencia deberá ser prestada de manera inmediata.	
90		El proveedor deberá prestar el servicio de atención telefónica del tipo 8x5 a los reclamos, esto quiere decir 5 días a la semana, 8 horas por día.	Exigido
91	**Garantía**	Soporte de atención de hardware, repuestos y Mano de Obra, traslado de los equipos de la oficina del cliente al proveedor y viceversa a cargo del oferente: 36 meses.	
		Atención de fallas con acceso directo al centro de asistencia técnica del fabricante del producto modalidad 8x5xNBD los 365 días del año.	
		Reemplazo avanzado de partes (hardware) en caso de fallas, gestionado por el fabricante en un tiempo de "NBD" basado en almacenes de repuestos a nivel nacional.	
		Todo Potencial Oferente deberá presentar una autorización del Fabricante. En caso de ser Distribuidor autorizado, deberá presentar la autorización expedida por el Representante para el Paraguay de la marca ofertada y esta autorización deberá estar acompañada del Documento que acredite la representación invocada y lo habilite a nombrar distribuidor.	

ÍTEM 4 – ACCESS POINT

ACCESS POINT				
Ítems	**Especificación y/o Funcionalidad**	**Características**	**Mínimo Exigido**	**El equipo ofertado cumple con las especificaciones requeridas (sí / no)**
Fabricante			Exigido	
Modelo:			Exigido	
Número de Parte			Exigido	
Cantidad:		**10**	Exigido	
#	**Características técnicas**	**Especificaciones técnicas mínimas solicitadas**	**Carácter**	**Ofrecido**
1	Uso del equipo	Uso interno	Exigido	
2	Antenas	Antenas internas	5	
3		Número de RADIOS	3	
4		Ganancia de la antena	- 4 dBi para 2.4 GHz - 5 dBi para 5 GHz	
5	Capacidad RADIO 1	Frecuencia	2.4 GHz	
6		Velocidad máxima	hasta 1100 Mbps	
7		Potencia máxima de transmisión	hasta 255 mW	
8		Capacidad de clientes conectados	mínimo 500	
9		Modulación	BPSK, QPSK, QAM64, QAM256 y QAM1024	
10		Soporta MIMO	Exigido	
11		Canal	4x4 20/40 MHz	
12	Capacidad RADIO 2	Frecuencia	5 GHz	
13		Velocidad máxima	hasta 2400 Mbps	
14		Potencia máxima de transmisión	hasta 200 mW	
15		Capacidad de clientes conectados	mínimo 500	
16		Modulación	BPSK, QPSK, QAM64, QAM256 y QAM1024	
17		Soporta MIMO	Exigido	

18		Canal	- 4x4 20/40/80MHz - 2x2 160MHz	
19	Capacidad RADIO 3	Frecuencia	2.4 GHz / 5 GHz	
20		Soporta MIMO	Exigido	
21	Interfases	Puerto 100/1000 Base-T RJ45	2	
22		Puerto serial RS-232 RJ45	1	
23		USB tipo A	1	
24		Botón de reset	Exigido	
25		Indicador LED modo OFF	Exigido	
26	Alimentación	Tipo de alimentación POE	Exigido	
27		Inyector POE	Exigido	
28		Hit-less PoE Failover	Exigido	
29		Consumo máximo	25 Watts	
30	SSIDs	Hasta un máximo de 16	Exigido	
31		Tipos soportados	-Local Bridge -Mesh -Tunnel	
32	Funcionalidades Generales	Debe permitir el acceso de los dispositivos a la red a través de la wireless y que posea todas sus configuraciones centralizadas en controlador inalámbrico;	Exigido	
33		Debe soportar el modo de operación centralizado, o sea, su operación depende del controlador inalámbrico que es responsable de gestionar las políticas de seguridad, calidad de servicio (QoS) y monitoreo de la radiofrecuencia;	Exigido	
34		Debe identificar automáticamente el controlador inalámbrico al que se conectará;	Exigido	
35		Debe permitir administrarse remotamente a través de links WAN;	Exigido	
36		Debe poseer capacidad dual-band con radios 2.4GHz y 5GHz operando simultáneamente, además de permitir configuraciones independientes para cada radio;	Exigido	
37		El tráfico de los dispositivos conectados a la red inalámbrica debe realizarse de forma centralizada a través del túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes deben	Exigido	

		ser encapsulados hasta el controlador inalámbrico;		
38		Cuando sea encapsulado, el tráfico debe ser encriptado a través de DTLS o IPSEC;	Exigido	
39		Debe permitir el tráfico de los dispositivos conectados a la red inalámbrica de forma distribuida (local switching), o sea, el tráfico debe ser conmutado localmente en la interfaz LAN del punto de acceso y no necesitará ser encapsulado hasta el controlador inalámbrico;	Exigido	
40		Cuando el tráfico sea distribuido y la autenticación con PSK, en caso de fallo en la comunicación entre los puntos de acceso y el controlador inalámbrico, los usuarios asociados deben permanecer asociados a los puntos de acceso y al mismo SSID. Debe permitirse la conexión de nuevos usuarios a la red inalámbrica;	Exigido	
41		En conjunto con el controlador inalámbrico, debe optimizar el rendimiento y la cobertura inalámbrica (RF), realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados;	Exigido	
42		Deberá soportar la funcionalidad de ajuste automático de potencia para extender la cobertura en caso de falla del punto de acceso vecino gerenciado por la misma controladora;	Exigido	
43		Debe soportar mecanismos para la detección y mitigación de puntos de acceso no autorizados, también conocidos como Rogue APs;	Exigido	
44		En conjunto con el controlador inalámbrico, debe implementar mecanismos de protección para identificar ataques a la infraestructura inalámbrica (wIDS / wIPS);	Exigido	
45		En conjunto con el controlador inalámbrico, debe permitir la creación de múltiples dominios de movilidad (SSID) con	Exigido	

		configuraciones distintas de seguridad y red;		
46		El punto de Acceso deberá soportar (MLD) - Maximum Likelihood Demodulation;	Exigido	
47	Estándares y cumplimientos	802.11a, 802.11b, 802.11g, 802.11n, 802.1ac, 802.1ax	Exigido	
48		Wi-Fi Alliance Certified	Exigido	
49		RoHS	Exigido	
50		FCC	Exigido	
51		CE	Exigido	
52		Tiempo medio entre fallos (MTBF)	10 años o más	
53	Autenticación Usuarios / Dispositivos	WPA	Exigido	
54		WPA2	Exigido	
55		WPA3	Exigido	
56		Preshared key	Exigido	
57		Web Captive Portal	Exigido	
58		Filtrado de MAC	Exigido	
59	Capacidad de monitoreo de wireless	Modo de radio de escaneo no autorizado	Exigido	
60		Soporte de WIPS y WIDS	Exigido	
61		Packet Sniffer	Exigido	
62		Analizador de espectro	Exigido	
63	Dimenciones y montaje	Montaje en techo, sendero y pared	Exigido	
64		Kit para montaje en techo, sendero y pared	Exigido	
65		Peso máximo	1 Kg.	
66	Garantía del Fabricante	Garantía del fabricante que esté disponible 24 horas, 7 días a la semana, con reposición de parte dañada en 4 horas. El contrato debe contemplar acceso a la Web del fabricante para apertura de casos de soporte, acceso de descarga de software para mantenimiento y cambio de equipo en caso de fallas (RMA). Se deberá poder acceder a este servicio directo con el Fabricante, sin intervención del proveedor.	36 meses	
67	Autorización del Fabricante	Presentar documentación emitida por el fabricante donde avale al oferente ser Partner Certificado.	Exigido	
68	Antigüedad de la empresa	Acreditar una antigüedad no menor de 3 años en el mercado del Paraguay en actividades relativas al	Exigido	

		ramo de Telecomunicaciones o networking.		
69	Experiencia	El oferente deberá comprobar experiencia en proyectos de implementación de puntos de acceso en el sector público y/o privado paraguayo, de al menos 3 proyectos en los últimos 3 años.	Exigido	
70	Implementación	Se debe incluir los servicios de Instalación e Implementacion por personal certificado, del equipamiento ofertado.	Exigido	
71	Compatibilidad	El equipo ofertado debe ser compatible con la infraestructura y topología de red del BNF y permitir la integración y administración del mismo a través del firewall solicitado en el presente llamado.	Exigido	
72	Instalación y Mano de obra	Sera responsabilidad del Proveedor la provisión total de los componentes accesorios y materiales necesarios sea cableado de red y/o Inyector PoE, patch cord, y cualquier otro componente requerido para la instalación y puesta en funcionamiento total del equipo. Además de efectuar las instalaciones bajo los estándares de calidad del fabricante de lo ofertado y de acuerdo con buenas prácticas aplicables, debiendo presentar el proyecto de instalación a ser aprobado por la Dirección de Informática, quien tiene la última decisión. También en caso de que sea requerido el retiro y ordenado de cableado del área para el cual los equipos están destinados, esto correrá totalmente a cargo del Proveedor, sin costo extra para el BNF. Se deberá incluir los trabajos necesarios para la integración con la plataforma IP existente de los equipos requeridos, cuando aplique para el Ítem ofertado.	Exigido	

		Todo requerimiento, incluido software, que sea necesario para la instalación y puesta en funcionamiento en un 100% a satisfacción de la Dirección de Informática, corre a cuenta del proveedor.		

*	Descripción del Servicio	Cantidad	Unidad de Medida del Servicio	Lugar de entrega de los bienes	Fecha(s) final(es) de entrega de los bienes
1	**FIREWALL SD WAN – TIPO 1**	4	Unidad	Casa Matriz del Banco Nacional de Fomento, Gerencia de Área de Tecnología informática.	90 (noventa) días corridos posterior a la firma del contrato.
2	**FIREWALL SDWAN – TIPO 2**	3	Unidad	Casa Matriz del Banco Nacional de Fomento, Gerencia de Área de Tecnología informática.	90 (noventa) días corridos posterior a la firma del contrato.
3	**SWITCH 24 DE PUERTOS POE**	7	Unidad	Casa Matriz del Banco Nacional de Fomento, Gerencia de Área de Tecnología informática.	90 (noventa) días corridos posterior a la firma del contrato.
4	**ACCESS POINT**	10	Unidad	Casa Matriz del Banco Nacional de Fomento, Gerencia de Área de Tecnología informática.	90 (noventa) días corridos posterior a la firma del contrato.