ADENDA Nº 14

Señores

……..

Presente:

Tenemos el agrado de dirigirnos a ustedes, con relación a la Licitación Pública Nacional BNF LPN SBE N° 20/2018, para la "Adquisición de Equipos Informáticos para el BNF", a través del Sistema de Subasta a la baja electrónica. – **ID Nº 344.279.-**

Al respecto, cumplimos en informar la modificación de las fechas, Tope de Respuesta, Inicio de Carga, Cierre, Etapa Competitiva, Entrega y Apertura Física de las ofertas quedando conforme a lo establecido en el Sistema de Información de Contrataciones Públicas (SICP).

Igualmente informamos que el Pliego de Bases y Condiciones que rige la citada licitación queda modificado según lo detallado a continuación:

- **Se suprime los Ítems N° 2, 3 y 5, y todo lo relacionado a los mencionados Ítems dentro del Pliego de Bases y Condiciones y en el SICP. Quedando los Lotes del presente llamado de la siguiente manera:**

Lote 1: Next Generation Firewall (NGFW) para la seguridad de la información perimetral.
Lote 2: Renovación de infraestructura de Seguridad Para el Centro de Datos.
Lote 3: COMPUTADORAS TIPO 1 – Mini AVANZADA
Lote 4: NOTEBOOK TIPO 1 - AVANZADA

- **Sección II – Criterios de Evaluación y Requisitos de Calificación – 2. Requisitos para Calificación Posterior – (b) Experiencia y Capacidad Técnica.**

1.Fotocopia/s simple/s de referencias satisfactorias de clientes del sector financiero, formalizadas por notas que contengan la debida identificación del emisor, como mínimo 3 (tres), de haber provisto los equipamientos y servicios objetos del presente llamado entre los años 2015 al 2018, expedidas por Instituciones Públicas y/o Privadas con quienes mantiene y/o mantuvo relaciones comerciales.
2. Fotocopia/s simple/s de contrato/s ejecutado/s, y/o facturas, y/o recepciones finales de prestación de servicios de soporte técnico informático a Instituciones Públicas y/o Privadas, en el periodo comprendido entre los años (2015 a 2018), cuyos montos sumados representen un monto igual o superior al 30% del monto total ofertado en la presente licitación. Podrán presentarse la cantidad de fotocopia/s de contrato/s ejecutado/s, y/o factura/s, y/o recepciones finales que fueren necesarias para acreditar el monto solicitado, siempre y cuando dichas prestaciones hayan sido realizadas dentro del periodo mencionado. Serán aceptados Fotocopias de contratos ejecutados y/o facturas de recepciones finales donde se demuestre provisión del Lote al cual se presenta.
3. Para el Lote Nº 1, el oferente deberá contar con un mínimo de 3 (tres) años de experiencia con la marca ofertada en la provisión de Next Generation Firewall (NGFW) para la seguridad de la información perimetral en entidades financieras. (2015, 2016,2017) Mínimo 1(uno) por año. Para lo cual el oferente deberá presentar cartas de satisfacción del cliente, así como también contratos y/o facturas que avalen la solución entregada.
4. Para el Lote Nº 2, el oferente deberá contar con un mínimo de 3 (tres) años de experiencia en la marca fortinet en entidades financieras. (2015, 2016,2017). Mínimo 1 (uno) por año. Para lo cual el oferente deberá presentar cartas de satisfacción del cliente, así como también contratos y/o facturas que avalen la solución entregada.
5. Para los Lotes Nº 1 y Nº 2 el oferente deberá presentar con su oferta las siguientes cartas de autorización dirigida a la convocante en donde haga referencia al presente llamado:
- Carta del Fabricante de la marca ofertada.
- Carta del Distribuidor local de la marca Ofertada.
6. Para los Lotes Nº1 y Nº2: Se deberá presentar respaldo por escrito del fabricante vía carta de autorización a la empresa oferente autorizándola a presentar oferta (según formulario 4), servicio

técnico y el cambio de partes por garantía desde la remisión oficial del equipo.

7. Para el Lote N°3 y N°4: Se deberá presentar Licencia de Windows 10 PRO de 64 bits en español última versión, pre instalado y configurado con todas las actualizaciones y activaciones necesarias con posibilidad de Downgrade.

8. Para el Lote N° 3 el oferente deberá presentar con su oferta los siguientes documentos:
   - Certificación de calidad ISO 9001:2008 o similar para todo el equipo en conjunto.
   - Carta de distribución del Representante
   - Carta de Autorización del Fabricante
   - Catálogos especificaciones originales del equipo Ofertado

9. Para el Lote N° 4 el oferente deberá presentar con su oferta los siguientes documentos:
   - Certificación de calidad ISO 9001:2008 o similar.
   - Carta de distribución del Representante
   - Carta de Autorización del Fabricante
   - Catálogos especificaciones originales del equipo Ofertado

<u>Observación:</u> No serán aceptados Certificaciones que cubran solo ensamblados

Criterios de Calificación		
Para oferentes individuales (Físicas o Jurídicas)		
1	El profesional técnico solicitado deberá formar parte del staff permanente de la empresa oferente para el Lote 1 y 2, debiendo presentarse en este caso certificado del IPS o el contrato de trabajo celebrado entre el oferente y el profesional, que deberá abarcar la vigencia del contrato a ser celebrado entre la convocante y el adjudicado.	
2	Par el Lote N°2: 1 (Un) Profesional Fortinet NSE4.	
3	Para el Lote N°2: 1 (Un) Profesional Fortinet NSE5.	
4	Para el Lote N°1: 1 (Un) Profesional Técnico Certificado en la Solución de NGFW	
5	Todo el personal técnico solicitado en los Lotes 1 y 2 deberán ser empleados de la empresa oferente con una antigüedad mínima de doce meses, para demostrar este requerimiento será aceptada la documentación que acredite la inclusión del profesional técnico al IPS o el contrato de trabajo celebrado entre la empresa oferente y el profesional técnico. El personal técnico deberá recidir en la República del Paraguay durante la vigencia del contrato del presente llamado, además deberá contar con documentación paraguaya.	
6	Para el Lote 1 se deberá contar con al menos 2 profesionales con certificación oficial y vigente del fabricante del equipamiento (la certificación presentada deberá ser verificable vía web y estar vigente al momento de la presentación de oferta) por la criticidad del equipamiento requerido esta certificación deberá ser del máximo nivel que dispone el fabricante ofertado.	
Para oferentes en Consorcio.		
1	Líder de Consorcio	El líder del consorcio deberá cumplir con todas las certificaciones técnicas requeridas.

• **<u>Sección III – Requisitos de los Bienes y/o Servicios Requeridos – 1. Especificaciones Técnicas.</u>**

Consideraciones Generales.
El presente llamado tiene como finalidad el fortalecimiento de la plataforma de networking del Banco Nacional de Fomento – BNF, en adelante la convocante.

Objetivo:
Mejorar la seguridad, el desempeño y gestión de la red, con el afán de soportar y asegurar el tráfico de las aplicaciones actuales y futuras de la institución.

Especificaciones Técnicas
El alcance de estas especificaciones tiene como propósito ilustrar a los oferentes interesados en participar los criterios que deberán ser respetados para la presentación de la oferta, tanto para la provisión de los bienes, así como la realización de los servicios requeridos por la convocante.
Todos los bienes y servicios deberán ser ofertados considerando siempre lo solicitado en estas especificaciones técnicas ya que las mismas derivan del análisis realizado a los requerimientos actuales y las previsiones de crecimiento que la convocante determinó.

Alcance de los trabajos.

El oferente que resultara adjudicado deberá realizar el despliegue total de lo solicitado en el presente llamado, incluyendo la activación de la suscripción adquirida, el upgrade de la plataforma y todas las configuraciones que la convocante considere necesarias para el correcto funcionamiento y la segurización de la infraestructura de networkig de la convocante, aunque los mismos no se encuentren descritos en el presente pliego de bases y condiciones.

Diseño esquemático Lote 1 Next Generation Firewall (NGFW) para la seguridad perimetral.

Lote 1: Next Generation Firewall (NGFW) para la seguridad perimetral.

Para este llamado se requiere la provisión de un sistema en Alta disponibilidad el cual será el encargado de dar protección a la infraestructura interna del Banco de los ataques provenientes desde el exterior, cada miembro del sistema deberá ser conectado a los proveedores de servicio de telecomunicaciones (Internet, VPN, RMSP, etc.) a través de interfaces de 1 Gbps y deberán contar con la capacidad suficiente para otorgar un rendimiento optimo para anchos de banda de hasta 300 Mbps para cada servicio.

Los firewalls del perímetro deberán estar conectados a los switches de la capa colapsada de Core/Distribución a través de interfaces de 10 Gbps, permitiendo el upgrade a 40 Gbps cuando la convocante lo considere necesario.

Lote 2: Solución de Seguridad Para el Centro de Datos.

Aquí se solicita la renovación de los servicios de suscripción y reposición de partes de los 2 (Dos) equipos de la marca Fortinet modelo FG-1000C que actualmente se encuentran como Firewall de perímetro.

El oferente deberá considerar en su oferta los servicios profesionales de técnicos certificados por el fabricante para realizar las configuraciones necesarias para reubicar estos dispositivos a la capa de seguridad del centro de datos (Firewall de Datacenter)

Lote 1

Lote 1: Next Generation Firewall (NGFW) para la seguridad de la información perimetral				
Marca:				**El bien ofertado cumple con los requerimientos**
Modelo:				
Número de parte:				
Cantidad:		**2 (Dos) Unidades**		
	Características técnicas	**Especificaciones técnicas mínimas solicitadas**	**Carácter**	**Ofrecido**
1	**Generalidades**	Adquisición de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la información perimetral que incluye filtro de paquetes, control de aplicaciones, administración de ancho de banda (QoS), VPN IPSec y SSL, IPS, prevención contra amenazas de virus, spyware y malware "Zero Day", además de controles de transmisión de datos y acceso a internet componiendo una plataforma de seguridad integrada y robusta. El sistema ofertado para el Lote 1 deberá ser capaz de soportar todo el tráfico WAN y LAN por lo que debe poder crecer en el mismo hardware hasta las siguientes capacidades como mínimo: 55 Gbps Firewall Throughput 13 Gbps IPS Throughput 12 Gbps NGFW Throughput 200,000 nuevas conexiones por segundo 3 a 25 Millones conexiones concurrentes (El equipo deberá contar con una capacidad inicial no menor a 3 millones de conexiones y soportar un crecimiento a 25 millones de conexiones en el mismo sistema) **Los puertos solicitados son mínimamente: 8 puertos 1GB instalados, 2 puertos 10GB instalados y capacidad de soportar puertos de 40GB en el mismo chasis**	Exigido	
2		Por plataforma de seguridad se entiende al sistema ofertado, de un fabricante específico reconocido en el mercado, no se aceptan soluciones open source, o sin el respaldo de un fabricante con presencia mundial.	Exigido	
3		Las características deberán ser confirmadas mediante documentación oficial de acceso público (guías de administración, manuales y/o guías técnicas). No se aceptarán documentos generados expresamente para este proceso (ad-hoc).	Exigido	
4		La solución ofertada deberá ser de un fabricante diferente al equipamiento solicitado en el lote 2.	Exigido	
5	**Formato**	La solución deberá ser rackeable en racks estándar de 19", con los que ya cuenta la Convocante.	Exigido	

6		Los procesadores de los equipos componentes de la solución deben ser de la última generación disponible según la web del fabricante del mismo.	Exigido	
7	**Redundancia y Alta Disponibilidad**	Deberá soportar Alta Disponibilidad sin pérdida de conexiones en caso del fallo de uno los nodos, soporte de Modo Activo-Activo, Activo-Pasivo.	Exigido	
8		La redundancia requerida deberá contemplar todos los componentes de la solución solicitada (Firewall, IPS, AntiSpam, Filtrado Web, Control de Aplicaciones). **- Solamente se requiere protección a los correos entrantes.** **- El servidor de correo electrónico se encuentra dentro de la Red** **- Si contamos con IP pública para el servicio.** **- Contamos con el servicio de MTA de Microsoft** **- El MTA permite Mail Relay**	Exigido	
9		El sistema ofertado deberá contar con fuentes de alimentación redundante, remplazables en caliente.	Exigido	
10	**Interfaces**	1 Gbps RJ45 >= 8	Exigido	
11		10 Gbps >= 2 (Se deberán suministrar los módulos SFP para su conexión.	Exigido	
12		Interfaz de Administración 1 Gbps >= 1	Exigido	
13		El equipamiento ofertado deberá soportar al menos 2 Interfaces de 40 Gbps.	Exigido	
14		Deberá contar con soporte para: 1000BASE-T, 1000BASE-X, 1000BASE-SX, 1000BASE-LX.	Exigido	
15	**Almacenamiento**	La solución deberá prever la capacidad de Almacenamiento de al menos 2 (dos) unidades >= 600 GB.	Exigido	
16	**Administración de la Solución**	Deberá permitir su gestión a travez de un entorno CLI	Exigido	
17		Deberá permitir su gestión a travez de un entorno GUI	Exigido	
18		Deberá soportar conexiones remotas a la interfaz CLI via protocolo SSH.	Exigido	
19		La solución debe permitir la configuración de perfiles de administración, los cuales permitirán la limitación de funciones que pueden ser gerenciados.	Exigido	
20		Debe soportar snmp v2 y v3, syslog remoto	Exigido	
21		La solución deberá soportar un agendado de backup de sus configuraciones.	Exigido	
22	**Funcionalidades Requeridas**	Deberá soportar al menos 4000 VLAN Tags 802.1q	Exigido	
23		Link Aggregation 802.3ad	Exigido	
24		Enrutamiento basado en políticas	Exigido	
25		Re-envio basado en políticas	Exigido	
26		Ruteo multicast (PIM-SM)	Exigido	

27		Deberá contar con soporte para la creación de objetos de red que puedan ser utilizados como dirección IP de interfaces L3	Exigido	
28		Deberá soportar sub-interfaces ethernet lógicas	Exigido	
29		NAT dinamico (Muchos a 1)	Exigido	
30		NAT dinámico (Muchos a Muchos)	Exigido	
31		NAT estático (1 a 1)	Exigido	
32		NAT estático (Muchos a Muchos)	Exigido	
33		NAT estático bidireccional 1 a Muchos	Exigido	
34		Traducción de puerto (PAT)	Exigido	
35		NAT de origen	Exigido	
36		NAT de destino	Exigido	
37		Deberá contar con soporte para la creación de objetos de red que puedan ser utilizados como dirección IP de interfaces L3	Exigido	
38	**Funcionalidades Requeridas**	Deberá permitir el envio de log para sistemas de monitoreo externos vía protocolo TCP y SSL. Permitiendo la configuración de certificados en caso de necesidad para la autenticación del sistema externo de Logs	Exigido	
39		Deberá contar con un sistema anti-spoofing;	Exigido	
40		Deberá soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2, OSPFv3)	Exigido	
41		Deberá soportar como mínimo las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Reglas de seguridad contra DoS (Denial of Service), Desencripción SSL y SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, Activo/Activo, Activo/Pasivo, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones	Exigido	
42		La solución ofertada de seguridad deberá tener la capacidad de operar de forma simultanea mediante el uso de sus interfaces físicas en los siguientes modos: Modo sniffer (monitoreo y análisis del tráfico de red), Capa 2 (l2) y Capa 3 (L3)	Exigido	
43		Modo Sniffer, para inspección vía puerto espejo del tráfico de datos de la red	Exigido	
44	**Modo de Operación de Interfaces**	Modo Capa – 2 (L2), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación	Exigido	
45		Modo Capa – 3 (L3), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación operando como default Gateway de las redes protegidas	Exigido	
46		Modo mixto de trabajo Sniffer, L2 e L3 en diferentes interfaces de red	Exigido	

47		Soporte a configuración de alta disponibilidad Activo/Pasivo e Activo/Activo.	Exigido	
48		En modo transparente	Exigido	
49		En Capa 3.	Exigido	
50	**Política de Firewall**	Deberá soportar controles por zonas de seguridad	Exigido	
51		Deberá permitir controles de políticas por puerto y protocolo.	Exigido	
52		Deberá permitir el Control de políticas por aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en características y comportamiento de las aplicaciones) y categorías de aplicaciones	Exigido	
53		Deberá permitir el control de políticas por usuarios, grupos de usuarios, IPs, redes y zonas de seguridad	Exigido	
54		Deberá permitir el control de políticas por código de País.	Exigido	
55		Deberá realizar control, inspección y desencriptación de SSL por política para tráficode entrada (Inbound) y salida (Outbound)	Exigido	
56		Deberá soportar offload de certificado en inspección de conexiones SSL de entrada (Inbound)	Exigido	
57		Deberá desencriptar tráfico Inbound y Outbound en conexiones negociadas con TLS 1.2	Exigido	
58		Control de inspección y desencriptación de SSH por política	Exigido	
59		Deberá desencriptar tráfico que use certificados ECC (como ECDSA)	Exigido	
60		Control de inspección y desencriptación de SSH por política	Exigido	
61		La plataforma de seguridad deberá implementar copia del tráfico desencriptado (SSL y TLS) para soluciones externas de análisis (Forense de red, DLP, Análisis de Amenazas, entre otras)	Exigido	
62		Bloqueo de los siguientes tipos de archivos: bat, cab, dll, exe, pif, y reg como mínimo	Exigido	
63		Traffic shaping QoS basado en políticas (Prioridad, Garantía y Máximo)	Exigido	
64		QoS basado en políticas para marcación de paquetes (diffserv marking), inclusive por aplicaciones	Exigido	
65		Soporte a objetos y Reglas IPV6.	Exigido	
66		Soporte a objetos y Reglas multicast.	Exigido	
67		Deberá soportar los atributos de agendamiento de las políticas con el objetivo de habilitar y deshabilitar políticas en horarios predefinidos automáticamente.	Exigido	
68		El sistema ofertado deberá poseer la capacidad de reconocer aplicaciones,		

	Control de Aplicaciones	independientemente del puerto y protocolo, debiendo tener las siguientes funcionalidades como mínimo:		
69		Ser posible la liberación y bloqueo solamente de aplicaciones sin la necesidad de liberación/bloqueo de puertos y protocolos	Exigido	
70		Reconocer por lo menos 2.000 aplicaciones diferentes, incluyendo, mas no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, compartición de archivos, e-mail;	Exigido	
71		Reconocer por lo 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, etc;	Exigido	
72		Inspeccionar el payload del paquete de datos con el objetivo de detectar a través de expresiones regulares firmas de aplicaciones conocidas por los fabricantes independiente del puerto y protocolo. El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no.	Exigido	
73		Aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis comportamental del tráfico observado, incluyendo, mas no limitando a Encrypted Bittorrent y aplicaciones VOIP que utilizan criptografía propietaria;	Exigido	
74		Identificar el uso de tácticas evasivas, o sea, deberá tener la capacidad de visualizar y controlar las aplicaciones y los ataques que utilizan tácticas evasivas vía comunicaciones criptografiadas, tales como Skype y ataques mediante el puerto 443.	Exigido	
75		Desencriptografar paquetes con el fin de posibilitar la lectura del payload para verificación de firmas de aplicaciones conocidas por el fabricante, para tráfico criptografiado (SSL y SSH);	Exigido	

76		Realizar decodificación de protocolos con el objetivo de detectar aplicaciones encapsuladas dentro del protocolo y validar si el tráfico corresponde con la especificación del protocolo, incluyendo, mas no limitando a Yahoo! Instant Messenger usando HTTP. La decodificación de protocolo también debe identificar funcionalidades específicas dentro de una aplicación, incluyendo, mas no limitando a la compartición de archivos dentro de Webex. También debe detectar el archivo y otros contenidos que deben ser inspeccionados de acuerdo a las Reglas de seguridad implementadas;	Exigido	
77	**Control de Aplicaciones**	Identificar el uso de tácticas evasivas vía comunicaciones criptografiadas;	Exigido	
78		Actualizar la base de firmas de aplicaciones automáticamente	Exigido	
79		Incluir la capacidad de creación de políticas basadas en el control por aplicación, por categoría de aplicación, subcategoría de aplicación, tecnología y factor de riesgo	Exigido	
80		La tecnología de identificación de aplicaciones deberá estar habilitada por default (motor de inspección base) sin necesidad de habilitar funcionalidades adicionales	Exigido	
81		Reconocer aplicaciones en IPv6	Exigido	
82		Limitar el ancho de banda (download/upload) usado por aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos del LDAP/AD	Exigido	
83		Poseer la capacidad de identificar al usuario de red con integración al Microsoft Active Directory.	Exigido	
84		Ser posible adicionar control de aplicaciones en todas las Reglas de seguridad del dispositivo, o sea, no limitándose solamente a la posibilidad de habilitar control de aplicaciones en algunas Reglas	Exigido	
85		Soportar múltiples métodos de identificación y clasificación de las aplicaciones, por lo menos chequeo de firmas, decodificación de protocolos y análisis heurístico	Exigido	
86		Soportar el control sobre aplicaciones desconocidas y no solamente sobre aplicaciones conocidas, para mantener la seguridad de la red eficiente	Exigido	
87		Permitir nativamente la creación de firmas personalizadas para reconocimiento de aplicaciones propietarias en la propia interface gráfica de la solución, sin la necesidad de acción por parte del fabricante, manteniendo la confidencialidad de las aplicaciones del propietario.	Exigido	

88	**Control de Aplicaciones**	Permitir el uso de expresiones regulares, contexto (sesiones o transacciones) para la creación de firmas personalizadas, usando la posición en el payload de los paquetes TCP y UDP y usando decoders de por lo menos los siguientes protocolos: HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP y File body	Exigido	
89		Permitir la solicitud de inclusión de aplicaciones en la base de firmas de aplicaciones	Exigido	
90		Alertar al usuario cuando una aplicación fuera bloqueada	Exigido	
91		Posibilitar que el control de puertos sea aplicado para todas las aplicaciones	Exigido	
92		Posibilitar la diferenciación de tráficos Peer2Peer (Bittorrent, emule, neonet, etc.) proveyendo granularidad de control/políticas para los mismos	Exigido	
93		Posibilitar la diferenciación de tráficos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) proveyendo granularidad de control/políticas para los mismos	Exigido	
94		Posibilitar la diferenciación y control de partes de las aplicaciones como por ejemplo permitir skype chat y bloquear la transferencia de archivos.	Exigido	
95		Posibilitar a diferenciación de aplicaciones Proxies (ghostsurf, freegate, etc.) proveyendo granularidad de control/políticas para los mismos	Exigido	
96	**Prevención de Amenazas**	Para la seguridad del ambien contra ataques, el sistema deberá poseer módulo de IPS, Antivirus y Anti-Spyware.	Exigido	
97		Deberá incluir firmas de prevención de intrusos (IPS) y bloqueo de archivos maliciosos (Antivirus y Anti-Spyware)	Exigido	
98		Las funcionalidades de IPS, Antivirus y Anti-Spyware deberán operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante.	Exigido	
99		Deberá sincronizar las firmas de IPS, Antivirus, Anti-Spyware cuando esté implementado en alta disponibilidad Activo/Activo e Activo/pasivo	Exigido	

100		Cuando se utilicen las funciones de IPS, Antivirus y Anti-spyware, el equipamiento deberá entregar el mismo performance (no degradar) entre tener 1 única firma de IPS habilitada o tener todas las firmas de IPS, Anti-Vírus y Antispyware habilitadas simultáneamente	Exigido	
101		Las firmas deberán poder ser activadas o desactivadas, o incluso habilitadas apenas en modo de monitoreo	Exigido	
102		Exenciones por IP de origen o de destino deberán ser posibles en las Reglas, de forma general y firma a firma	Exigido	
103		Deberá 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 esos ítem	Exigido	
104		Deberá permitir el bloqueo de vulnerabilidades	Exigido	
105		Deberá permitir el bloqueo de exploits conocidos	Exigido	
106		Deberá incluir seguridad contra ataques de negación de servicios	Exigido	
107	**Prevención de Amenazas**	Deberá poseer los siguientes mecanismos de inspección de IPS: Análisis de parones de estado de conexiones Análisis de decodificación de protocolo Análisis para detección de anomalías de protocolo Análisis Heurística IP Defragmentation Re ensamblado de paquetes de TCP Bloqueo de paquetes malformados Ser inmune y capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc. Detectar y bloquear el origen de portscans Bloquear ataques efectuados por worms conocidos, permitiendo al administrador adicionar nuevos patrones	Exigido	
108		Soportar los siguientes mecanimos de inspección contra amenazas de red: análisis de patrones de estado de conexiones, análisis de decodificación de protocolo, análisis para detección de anomalías de protocolo, análisis heurístico, IP Defragmentation, re ensamblado de paquetes de TCP y bloqueo de paquetes malformados, y aún: Posea firmas específicas para la mitigación de ataques DoS Posea firmas para bloqueo de ataques de buffer overflow Posea firmas para bloqueo de ataques de buffer overflow;	Exigido	

109		Deberá posibilitar la creación de firmas personalizadas por la interfaz gráfica del producto	Exigido	
110		Permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3	Exigido	
111		Soportar bloqueo de archivos por tipo	Exigido	
112		Identificar y bloquear comunicaciones como botnets	Exigido	
113		Deberá soportar varias técnicas de prevención, incluyendo Drop y TCP-RST (Cliente, Servidor y Ambos)	Exigido	
114	**Filtrado URL**	Permitir especificar la política por tempo, horario o determinado período (día, mes, año, día de la semana y hora)	Exigido	
115		Deberá ser posible crear políticas por usuario, grupo de usuario, ips, redes y zonas de seguridad	Exigido	
116		Deberá incluir la capacidad de creación de políticas basadas en la visibilidad y contra de quien está utilizando cual URLs a través de la integración con servicios de directorio, autenticación vía LDAP, Active Directory, E-Directory y base de datos local	Exigido	
117		Deberá permitir poder publicar los logs de URL con la información de los usuarios conforme a lo descrito en la integración con servicios de directorio	Exigido	
118		Deberá soportar la capacidad de crear políticas basadas en control por URL y categoría URL	Exigido	
119		Deberá bloquear el acceso a sitios de búsqueda (Google, Bing y Yahoo!) en el caso de que la opción de Safe Search este deshabilitada. Debe en ese caso exhibir una página de bloqueo dando instrucciones al usuario de como habilitar dicha función	Exigido	
120		Deberá soportar una caché local de URL en el appliance virtual, evitando el delay de comunicación/validación de las URLs	Exigido	
121		Deberá poseer al menos 60 categorías de URLs	Exigido	
122		Deberá soportar la creación de categorías URL custom	Exigido	
123		Deberá soportar la exclusión de URLs del bloqueo por categoría	Exigido	
124		Deberá permitir la personalización de la página de bloqueo	Exigido	
125		Deberá soportar la inclusión a los logs las informaciones de las actividades de los usuarios	Exigido	

126		La solución deberá evitar la fuga de credenciales internas (usuarios y passwords) desde o hacia diferentes categorías de sitios (ejemplo: phising, malware, otros, etc.) pudiendo seleccionar el administrador a que categorías de páginas se le permite a los usuarios pasar credenciales internas y cual no. Incluso se debe poder gestionar el uso indebido de los mismos dentro de la red del cliente.	Exigido	
127	**Filtrado URL**	Deberá poder actualizar de forma automática en 5 minutos o menos las categorías de malware y phising.	Exigido	
128		Debe poseer la capacidad de filtrar páginas web (Url Filtering).	Exigido	
129		Debe poder aplicar restricción de ancho de banda ya sean para cierto tipo de tráfico, streaming de audio o video, p2p.	Exigido	
130		Los mensajes entregados al usuario por parte del URL FILTER (en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables, Facilidad de incorporar sitios a los cuales naveguen los usuarios, y establecer mediante categorías el acceso de los mismos.	Exigido	
131		Deberá incluir a capacidad de creación de políticas basadas en la visibilidad y control de quien está utilizando cuales aplicaciones a través de la integración como servicios de directorio, autenticación vía ldap, Active Directory, E-directory y base de datos local.	Exigido	
132		Deberá poseer integración con Microsoft Active Directory para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios.	Exigido	
133	**Identificación de Usuarios**	Deberá poseer integración con RADIUS para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios.	Exigido	
134		Deberá poseer integración con TACACS+	Exigido	
135		Deberá posea integración con LDAP para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en Usuarios y Grupos de usuarios.	Exigido	

136		Como la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube, ustream, etc) y tener un alto consumo de ancho de banda, se requiere que la solución, a la ves de poder permitir o negar ese tipo de aplicaciones, deberá tener la capacidad de controlarlas por políticas de máximo de ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones, tanto de audio como de vídeo streaming.	Exigido	
137	**QoS**	Soportar la creación de políticas de QoS por: Dirección de origen. Dirección de destino. Por usuario y grupo de LDAP/AD. Por aplicaciones, incluyendo, mas no limitando a Skype, Bittorrent, YouTube y Azureus. Por puerto.	Exigido	
138		El QoS deberá permitir la definición de clases por: Ancho de Banda garantizado Ancho de Banda Máximo Cola de prioridad. Soportar priorización Real Time de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype. Soportar marcación de paquetes Diffserv, inclusive por aplicaciones; Disponer de estadísticas Real Time para clases de QoS. Deberá permitir el monitoreo del uso que las aplicaciones hacen por bytes, sesiones y por usuario.	Exigido	
139		Permitir la creación de filtros para archivos y datos predefinidos	Exigido	
140		Los archivos deberán ser identificados por extensión y firmas	Exigido	
141		Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivos (MS Office, PDF, etc.) identificados sobre aplicaciones (P2P, InstantMessaging, SMB, etc.)	Exigido	
142	**Filtro de Datos**	Soportar la identificación de archivos compactados y las aplicaciones de políticas sobre el contenido de esos tipos de archivos	Exigido	
143		Permitir identificar y opcionalmente prevenir la transferencia de informaciones sensibles, incluyendo, mas no limitando al número de tarjetas de crédito, permitiendo la creación de nuevos tipos de datos vía expresión regular	Exigido	
144		Permitir listar el número de aplicaciones soportadas para control de datos	Exigido	

145		Permitir listar el número de tipos de archivos soportados para el control de datos	Exigido	
146		Deberá traer por efecto al menos dos perfiles de bloqueo predefinidos	Exigido	
147		Deberá poder integrarse son soluciones de punto final de terceros para mejorar la política de DLP	Exigido	
148		Deberá poder integrarse con soluciones DLP suministradas por el mismo fabricante o compatibles.	Exigido	
149	**VPN**	Soportar VPN Site-to-Site y Cliente-To-Site	Exigido	
150		Soportar IPSec VPN	Exigido	
151		Soportar SSL VPN	Exigido	
152		La VPN IPSEc deberá soportar: DES y 3DES; Autenticación MD5 e SHA-1; Diffie-Hellman Group 1, Group 2, Group 5 y Group 14; Algoritmo Internet Key Exchange (IKEv1 & IKEv2); AES 128, 192 e 256 (Advanced Encryption Standard) Deberá permitir SSO via Kerberos Autenticación vía certificado IKE PKI. Deberá ser compatible con la Suite B de protocolos de NSA.	Exigido	
153		Las VPN SSL deberán soportar	Exigido	
154		Permitir que el usuario realice la conexión por medio de cliente instalado en el sistema operacional del equipamiento o por medio de interfaz WEB;	Exigido	
155		Las funcionalidades de VPN SSL deberán ser atendidas con o sin el uso de agente;	Exigido	
156		La asignación de dirección IP en los clientes remotos de VPN;	Exigido	
157		La asignación de DNS en los clientes remotos de VPN;	Exigido	
158		Deberá haber la opción de ocultar el agente de VPN instalado en el cliente remoto, tornando el mismo invisible para el usuario;	Exigido	
159		Deberá permitir criar políticas de control de aplicaciones, IPS, Antivirus, Antispyware para tráfico de los clientes remotos conectados en la VPN SSL;	Exigido	
160		Las VPN SSL deberán soportar proxy arp y el uso de interfaces PPPOE;	Exigido	
161		Soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;	Exigido	

162		Permitir establecer un túnel VPN client-to-site del cliente a la plataforma de seguridad, proveyendo una solución de single-sign-on a los usuarios, integrándose como las herramientas de Windows-logon;	Exigido	
163		Soporte de lectura y verificación de CRL (certificate revocation list);	Exigido	
164		Permitir la aplicación de políticas de seguridad y visibilidades para las aplicaciones que circulan dentro de los túneles SSL;	Exigido	
165		El agente de VPN a ser instalado en los equipamientos desktop y laptops, deberá ser capaz de ser distribuido de manera automática vía Microsoft SMS, Active Directory y ser descargado directamente desde su propio portal, en el cual residirá el centralizador de VPN;	Exigido	
166		El agente deberá comunicarse con el portal para determinar las políticas de seguridad del usuario	Exigido	
167		Deberá permitir que las conexiones como VPN SSL sean establecidas de las siguientes	Exigido	
168		Antes del usuario autenticarse en la estación;	Exigido	
169		Después de la autenticación del usuario en la estación;	Exigido	
170		Bajo demanda del usuario;	Exigido	
171		Deberá mantener una conexión segura con el portal durante la sesión.	Exigido	
172		El agente de VPN SSL client-to-site deberá ser compatible al menos con: Windows	Exigido	
173		XP, Vista, Windows 7, Windows 8, Windows 10, MacOS X;	Exigido	
174		El portal de VPN deberá enviar al cliente remoto la lista de gateways VPN activos para el establecimiento de la conexión, los cuales deben poder ser administrados centralizadamente	Exigido	
175	**Administración y Monitoreo**	La plataforma de seguridad deberá contar con una herramienta de administración centralizada, posibilitando dicha administración para varios equipos o Virtual Appliances, el cual deberá estar disponible para formar parte de la plataforma en cualquier momento del ciclo de vida de la solución.	Exigido	
176		La administración de la solución deberá posibilitar un conjunto de estadísticas de todo el tráfico que pasa por los equipos de la plataforma de seguridad.	Exigido	
177		Deberá controlar todos los dispositivos de la plataforma de seguridad en una única consola, con administración de roles, privilegios y funciones	Exigido	

178		La administración centralizada deberá ser entregada como appliance virtual, el oferente deberá proveer todos los equipos necesarios para la puesta en funcionamiento del appliance virtual.	Exigido	
179		No deberá estar limitado por la cantidad de logs a almacenar o espacio en disco, se tiene que poder asignar por lo menos 2 Tb en disco inicialmente para almacenamiento de Logs, reportes, configuraciones etc. En caso de disponer licenciamiento por espacio, se deberá disponer de la licencia ilimitada de almacenamiento o la más grande disponible por el fabricante.	Exigido	
180		Deberá permitir el control global de las políticas para todos los dispositivos que componen la plataforma de seguridad.	Exigido	
181		Deberá soportar organizar los dispositivos administrados en grupos: los sistemas virtuales deberán ser administrados como dispositivos individuales, los grupos pueden ser geográficos, por funcionalidad (por ejemplo, IPS), y distribuidos.	Exigido	
182		Deberá permitir la creación de objetos y políticas compartidas.	Exigido	
183		Deberá consolidar logs y reportes de todos los dispositivos administrados	Exigido	
184		Deberá permitir exportar backups de configuración automáticamente vía programación	Exigido	
185		Deberá permitir realizar RBAC (Rol based administration) desde el directorio activo	Exigido	
186		Deberá centralizar la administración de Reglas y políticas del cluster, usando una única interfaz de administración	Exigido	
187		La administración de la solución deberá soportar acceso vía SSH, cliente WEB (HTTPS) y API abierta	Exigido	
188		En el caso de que sea necesaria la instalación de cliente para administración de la solución, el mismo deberá ser compatible con sistemas operacionales Windows y Linux	Exigido	
189	**Administración y Monitoreo**	La administración deberá permitir/hacer:	Exigido	
190		Permitir creación y administración de políticas de firewall y control de aplicaciones;	Exigido	
191		Permitir creación y administración de políticas de IPS y Anti-Spyware;	Exigido	
192		Permitir creación y administración de políticas de filtro de URL	Exigido	
193		Permitir monitoreo de logs;	Exigido	
194		Permitir herramientas de investigación de logs;	Exigido	
195		Permitir debugging;	Exigido	

196		Permitir captura de paquetes.	Exigido	
197		Permitir el acceso concurrente de administradores;	Exigido	
198		Tener un mecanismo de búsqueda de comandos de administración vía SSH, facilitando la localización de los comandos;	Exigido	
199		Permitir usar palabras clave y distintos tags de colores para facilitar la identificación de Reglas;	Exigido	
200		Permitir el bloqueo de alteraciones, en el caso de acceso simultaneo de dos o más administradores;	Exigido	
201		Permitir la definición de perfiles de acceso a la consola con permisos granulares como: acceso de escritura, acceso de lectura, creación de usuarios, alteración de configuraciones;	Exigido	
202		Permitir la autenticación integrada con Microsoft Active Directory y servidor Radius;	Exigido	
203		Permitir la localización de donde están siendo utilizados objetos en: Reglas, dirección IP, Rango de IPs, subredes u objetos	Exigido	
204		Poder atribuir secuencialmente un número a cada regla de firewall, NAT, QOS y Reglas de DOS;	Exigido	
205		Permitir la creación de Reglas que estén activas en un horario definido;	Exigido	
206		Permitir la creación de Reglas con fecha de expiración;	Exigido	
207	**Administración y Monitoreo**	Poder realizar un backup de las configuraciones y rollback de configuración para la última configuración salvada;	Exigido	
208		Soportar el Rollback de Sistema operativo para la última versión local;	Exigido	
209		Poseer la habilidad del upgrade vía SCP, TFTP e interfaz de administración;	Exigido	
210		Poder validar las Reglas antes de las aplicaciones;	Exigido	
211		Permitir la validación de las políticas, avisando cuando haya Reglas que ofusquen o tengan conflicto con otras (shadowing);	Exigido	
212		Posibilitar la visualización y comparación de configuraciones actuales, la configuración anterior y configuraciones más antiguas.	Exigido	
213		Cosibilitar la integración con otras soluciones de SIEM del mercado (third-party SIEM vendors)	Exigido	
214		Permitirá la generación de logs de auditoria detallados, informando de la configuración realizada, el administrador que la realizo y el horario de la alteración;	Exigido	

215		Permitir la generación de mapas geográficos en tiempo real para la visualización de orígenes y destinos del tráfico generado en la institución;	Exigido	
216		Proveer resúmenes con la vista correlacionada de aplicaciones, amenazas (IPS, Antispyware) URLs y filtro de archivos, para un mejor diagnóstico y respuesta a incidentes;	Exigido	
217		Posibilitar la recolección de estadísticas de todo el tráfico que pasa por los dispositivos de seguridad (administración de la solución);	Exigido	
218		Proveer resúmenes de utilización de los recursos por aplicaciones, amenazas (IPS, Anti- Spyware y antivirus de la solución), etc.;	Exigido	
219	**Administración y Monitoreo**	Proveer de una visualización sumarizada de todas las aplicaciones, amenazas (IPS, Antivirus e Anti-Spyware) y URLs que pasan por la solución;	Exigido	
220		Poseer un mecanismo "Drill-Down" para navegación por los resúmenes en tiempo real;	Exigido	
221		Ser posible, en las listas de "Drill-Down", identificar el usuario que ha determinado el acceso;	Exigido	
222		Ser posible exportar los logs en CSV;	Exigido	
223		Ser posible acceder al equipamiento a aplicar configuraciones durante momentos donde el tráfico sea muy alto y la CPU y memoria del equipamiento este siendo totalmente utilizada.	Exigido	
224		Tener rotación de logs;	Exigido	
225		Tener presentaciones de las siguientes informaciones, de forma histórica y en tiempo real (actualizado de forma automática y continua cada 1 minuto):	Exigido	
226		Deberá mostrar la situación del dispositivo y del cluster;	Exigido	
227		Poder mostrar las principales aplicaciones;	Exigido	
228		Poder mostrar las principales aplicaciones por riesgo;	Exigido	
229		Poder mostrar los administradores autenticados en la plataforma de seguridad;	Exigido	
230		Poder mostrar el número de sesiones simultaneas;	Exigido	
231		Poder mostrar el estado de las interfaces;	Exigido	
232		Poder mostrar el uso de CPU;	Exigido	
233		Generar reportes. Como mínimo los siguientes reportes deberán poder ser generados:	Exigido	
234		- Resumen gráfico de las aplicaciones utilizadas;	Exigido	
235		- Principales aplicaciones por utilización de ancho de banda de entrada y salida;	Exigido	

236		- Principales aplicaciones por tasa de transferencia en bytes;	Exigido	
237		- Principales hosts por número de amenazas identificadas;	Exigido	
238		- Actividades de un usuario específico y grupo de usuarios del AD/LDAP, incluyendo aplicaciones accedidas y amenazas (IPS, y Anti-Spyware), de red vinculadas a este tráfico;	Exigido	
239		Permitir la creación de reportes personalizados;	Exigido	
240		En cada criterio de búsqueda del log deberá ser posible incluir múltiples entradas (ej. redes e IP's distintas; servicios HTTP, HTTPS y SMTP), excepto en el campo horario, donde debe ser posible definir un rango de tiempo como criterio de búsqueda;	Exigido	
241		Generar alertas automáticas vía: Email; SNMP; Script;	Exigido	
242	**SSL Inspection (inbound / outbound)**	La solución debe soportar inspección y descifrado de SSL a través de todas las tecnologías de mitigación de amenazas.	Exigido	
243		La solución debe soportar Perfecr Forward Secrecy (PFS , ECDHE cipher suites)	Exigido	
244	**Sandboxing**	Deberá soportar la inclusión de sandboxing con el agregado de licencias y esta debe permitir la integración con inspección SSL	Exigido	
245		La solución deberá proteger contra ataques de día cero y malware desconocido antes de que una firma de protección estática sea creada.	Exigido	
246		La solución debera soportar emulación basada en red. "Network based Threat emulation	Exigido	
247		La solución debera tener disponibilidad de despliegue en la nube y en sitio.	Exigido	
248		"La solución debe ser capaz de emular archivos ejecutables, documentos, java y flash. En específico: 7z cab csv doc docm docx dot dotm dotx exe jar pdf	Exigido	

	Sandboxing	potx pps ppsm ppsx ppt pptm pptx rar rtf scr swf tar tgz xla xls xlsb xlsm xlsx xlt xltm xltx xlw zip "		
249		El motor de emulación debe soportar múltiples sistemas operativos, tales como XP y Windows 7 y tener la capacidad de implementar imágenes a la medida del cliente.	Exigido	
250		El motor debe detectar llamadas API, cambios en el sistema de archivos, cambios en el registro, conexiones de red, procesos de sistema.	Exigido	
251		La solución debe soportar análisis estático para Windows, MAC OS-X, Linux o cualquier plataforma X86.	Exigido	
252		El motor de emulación debe ser capaz de inspeccionar, emular, prevenir y compartir los resultados de los eventos de sandboxing con la infraestructura anti malware.	Exigido	
253		La solución debe realizar una pre-emulación o validación a través de un filtrado estático, en donde se valide si es necesario enviar el archivo a emulación.	Exigido	
254	**Sandboxing**	La solución debe ser capaz de emular archivos de más de 10 MB	Exigido	
255		Detección y prevención inmediata. La solución debe detectar el ataque en la fase de exploit, por ejemplo antes de que se ejecute el Shell code y antes de que el malware se descargue/ejecute.	Exigido	
256		La solución debe ser capaz de detectar ROP y otras técnicas de explotación a través del monitoreo del flujo de la CPU.	Exigido	
257		La solución debe ser capaz de soportar escaneo de links dentro de correos para detección de Malware desconocido.	Exigido	

258		La solución de emulación debe permitir ´Geo Restriction para restringir la emulación a través de la nube únicamente a ciertos países.	Exigido	
259	**Detección de actividad del sistema**	La solución debe monitorear las actividades sospechosas en: Llamadas a la API Cambios en el sistema de archivos Registro del sistema Conexiones de red Procesos del sistema Creación de archivos y eliminación Modificación del archivo Inyección de código kernel Modificaciones del kernel (cambios de memoria realizadas por el código del kernel) Comportamiento código del kernel (monitorear actividad que se da sobre código en modo non user) La interacción directa en la CPU	Exigido	
260	**Garantías**	El oferente deberá presentar con su oferta las siguientes cartas de autorización dirigida a la convocante en donde haga referencia al presente llamado: • Carta del Fabricante de la marca ofertada. • Carta del Distribuidor local de la marca Ofertada.	Exigido	
261		Presentar respaldo por escrito del fabricante vía carta de autorización a la empresa oferente autorizándola a presentar oferta (según formulario 4), servicio técnico y el cambio de partes por garantía desde la remisión oficial del equipo. **Garantía del Fabricante de la solución ofertada: 36 meses** **Suscripciones de los servicios de actualización y acceso a repositorios de firmas: 36 meses.**	Exigido	
262		Deberá cumplir con lo solicitado en la Sección II. Criterios de Evaluación y Requisitos de calificación, Capacidad Técnica.	Exigido	
263		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, etc.).	Exigido	

Lote 2

Lote 2: Renovación de infraestructura de Seguridad Para el Centro de Datos.				
Marca:		Fortinet		**El bien ofertado cumple con los requerimientos**
Modelo:		FG-1000C		
Número de Serie:				
Cantidad:		**2 (Dos) Unidades**		
#	**Características técnicas**	**Especificaciones técnicas mínimas solicitadas**	**Carácter**	**Ofrecido**
1	**Generalidades**	Upgrade tecnológico y Renovación de licencias de software para dispositivos de seguridad de redes con plataforma UTM – Unified Threat Managment (Administración Unificada contra Amenazas) de la marca FORTINET modelo FortiGate 1000C Período: 3 (tres) años (36 meses) Efectivos posterior a 5 días luego de la firma del contrato.	Exigido	
2		Renovación de soporte ténico en modalidad 8x5 con reposición de Hardware para los equipos de la marca FORTINET modelo FortiGate 1000C Período: 3 (tres) años (36 meses) Efectivos posterior a 5 días luego de la firma del contrato.	Exigido	
3	**Componentes del Bundle Fortinet**	Módulo de control de aplicaciones para análisis del comportamiento de las mismas en tiempo real en el tráfico de red.	Exigido	
4		Módulo de seguridad de monitoreo del tráfico de red y/o las actividades en busca de actividad sospechosa/maliciosa.	Exigido	
5		Módulo para análisis, monitoreo y bloqueo de amenazas (malware/spam) en el tráfico de red	Exigido	
6		Módulo para filtrado de sitios web basado en definición de políticas.	Exigido	
7		Acceso a soporte técnico del fabricante vía portal web, chat on-line o telefónico (jornada de 8 horas diarios en los 5 días hábiles de la semana).	Exigido	
8		El bundle solicitado deberá ser del tipo Enterprises.	Exigido	
9	**Servicios Profesionales**	El oferente deberá incluir en su oferta la provisión de servicios profesionales para todas las tareas de activación de la suscripción adquirida, así como toda la configuración necesaria para la implementación de estos equipos para la capa de seguridad del centro de datos. Todos los servicios deberán quedar a entera satisfacción de la convocante y los mismos deberán ser definidos considerando una correcta implementación de políticas de seguridad y utilización de los recursos de Red.	Exigido	

10		El oferente deberá incluir en su oferta servicios profesionales de soporte técnico por el lapso de 3(Tres) años (36 meses) en modalidad 8x5x4 (Ocho Horas al día, 5 días a la semana y tiempo máximo de respuesta de 4 horas)	Exigido	
11	**Garantías**	El oferente deberá presentar con su oferta las siguientes cartas de autorización dirigida a la convocante en donde haga referencia al presente llamado: • Carta del Fabricante de la marca ofertada. • Carta del Distribuidor local de la marca Ofertada.		
12		Presentar respaldo por escrito del fabricante vía carta de autorización a la empresa oferente autorizándola a presentar oferta (según formulario 4), servicio técnico y el cambio de partes por garantía desde la remisión oficial del equipo. **Garantía del Fabricante de la solución ofertada: 36 meses** **Suscripciones de los servicios de actualización y acceso a repositorios de firmas: 36 meses.**	Exigido	
13		Deberá cumplir con lo solicitado en la Sección II. Criterios de Evaluación y Requisitos de calificación, Capacidad Técnica.	Exigido	
14		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, etc.).	Exigido	

LOTE 3: **COMPUTADORAS TIPO 1 – Mini AVANZADA**
LOTE 4: **NOTEBOOK TIPO 1 - AVANZADA**

Remitirse a las plantillas que se encuentran en el Sistema de Información de Contrataciones Públicas.

- **Sección VII – Anexo Nº I - Documentos que Componen la Oferta**

1. Fotocopia/s simple/s de referencias satisfactorias de clientes del sector financiero, formalizadas por notas que contengan la debida identificación del emisor, como mínimo 3 (tres), de haber provisto los equipamientos y servicios objetos del presente llamado entre los años 2015 al 2018, expedidas por Instituciones Públicas y/o Privadas con quienes mantiene y/o mantuvo relaciones comerciales.
2. Fotocopia/s simple/s de contrato/s ejecutado/s, y/o facturas, y/o recepciones finales de prestación de servicios de soporte técnico informático a Instituciones Públicas y/o Privadas, en el periodo comprendido entre los años (2015 a 2018), cuyos montos sumados representen un monto igual o superior al 30% del monto total ofertado en la presente licitación. Podrán presentarse la cantidad de fotocopia/s de contrato/s ejecutado/s, y/o factura/s, y/o recepciones finales que fueren necesarias para acreditar el monto solicitado, siempre y cuando dichas prestaciones hayan sido realizadas dentro del periodo mencionado. Serán aceptados Fotocopias de contratos ejecutados y/o facturas de recepciones finales donde se demuestre provisión del lote ofertado.

3. Para el Lote Nº 1, el oferente deberá contar con un mínimo de 3 (tres) años de experiencia con la marca ofertada en la provisión de Next Generation Firewall (NGFW) para la seguridad de la información perimetral en entidades financieras. (2015, 2016,2017) Mínimo 1(uno) por año. Para lo cual el oferente deberá presentar cartas de satisfacción del cliente, así como también contratos y/o facturas que avalen la solución entregada.
4. Para el Lote Nº 2, el oferente deberá contar con un mínimo de 3 (tres) años de experiencia en la marca fortinet en entidades financieras. (2015, 2016,2017). Mínimo 1 (uno) por año. Para lo cual el oferente deberá presentar cartas de satisfacción del cliente, así como también contratos y/o facturas que avalen la solución entregada.
5. Para el Lote Nº 1 y Nº2 el oferente deberá presentar con su oferta las siguientes cartas de autorización dirigida a la convocante en donde haga referencia al presente llamado:
   - Carta del Fabricante de la marca ofertada.
   - Carta del Distribuidor local de la marca Ofertada.
6. Para el Lote Nº 1 y Nº2 deberá presentar respaldo por escrito del fabricante vía carta de autorización a la empresa oferente autorizándola a presentar oferta (según formulario 4), servicio técnico y el cambio de partes por garantía desde la remisión oficial del equipo.
7. Para el LOTE Nº3 y Nº4 Licencia de Windows 10 PRO de 64 bits en español última versión, pre instalado y configurado con todas las actualizaciones y activaciones necesarias con posibilidad de Downgrade.
8. Para el Lote Nº 3 el oferente deberá presentar con su oferta los siguientes documentos:
   - Certificación de calidad ISO 90001:2008 o similar para todo el equipo en conjunto.
   - Carta de distribución del Representante
   - Carta de Autorización del Fabricante
   - Catálogo especificaciones originales del equipo Ofertado
9. Para el Lote Nº 4 el oferente deberá presentar con su oferta los siguientes documentos:
   - Certificación de calidad ISO 90001:2008 o similar para todo el equipo en conjunto.
   - Carta de distribución del Representante
   - Carta de Autorización del Fabricante
   - Catálogo especificaciones originales del equipo Ofertado

Observación: No serán aceptados Certificaciones que cubran solo ensamblados

Criterios de Calificación	
Para oferentes individuales (Físicas o Jurídicas)	
1	El profesional técnico solicitado podrá formar parte del staff permanente de la empresa oferente, debiendo presentarse en este caso certificado del IPS o el contrato de trabajo celebrado entre el oferente y el profesional, que deberá abarcar la vigencia del contrato a ser celebrado entre la convocante y el adjudicado.
2	Para el Lote Nº2: 1 (Un) Profesional Fortinet NSE4
3	Para el Lote Nº2: 1 (Un) Profesional Fortinet NSE5.
4	Para el Lote Nº1: 1 (Un) Profesional Técnico Certificado en la Solución de NGFW
5	Todo el personal técnico solicitado en el punto 2 deberán ser empleados de la empresa oferente con una antigüedad mínima de doce meses, para demostrar este requerimiento será aceptada la documentación que acredite la inclusión del profesional técnico al IPS o el contrato de trabajo celebrado entre la empresa oferente y el profesional técnico. El personal técnico deberá recidir en la República del Paraguay durante la vigencia del contrato del presente llamado, además deberá contar con documentación paraguaya.
6	Para el Lote 1 se deberá contar con al menos 2 profesionales con certificación oficial y vigente del fabricante del equipamiento (la certificación presentada deberá ser verificable vía web y estar vigente al momento de la presentación de oferta) por la criticidad del equipamiento requerido esta certificación deberá ser del máximo nivel que dispone el fabricante ofertado.

Para oferentes en Consorcio.		
1	Líder de Consorcio	El líder del consorcio deberá cumplir con todas las certificaciones técnicas requeridas.

Atentamente,

SUBGERENCIA OPERATIVA DE CONTRATACIONES
DIVISIÓN CONTRATACIONES

LIDIA CAMILA AQUINO NOGUERA
Func. Responsable Sección Compras Mayores

JAVIER RODRIGO ESTECHE
Jefe Sección Compras Mayores

MARIELA ALSINA
Jefa División Contrataciones

MÓNICA CORBETA
Encargada de Despacho
Subgerencia Operativa de Contrataciones