ANEXO 3

Planilla de Capacidad Financiera

ANDE

MEMORÁNDUM

DTE/TI/16/2020

A : Departamento de Estudios Económico-Financieros y Bancarios

De : División de Tecnología y Desarrollo Informático

Lugar y Fecha : Asunción, 27 de Octubre de 2020

Objeto: Solicitud de Análisis de Estudios Económico-Financieros de los oferentes de la **Licitación Pública Nacional ANDE N° 1567/2020.**

Señor Jefe,

Por medio del presente, se remiten los documentos de las ofertas presentadas en la L.P.N. N° 1567/2020 **"Servicio de Actualización, Soporte Técnico y Mantenimiento de Equipo UTM Sonicwall"**, para el correspondiente estudio, con respecto a los **Criterios de Análisis Económico-Financieros**, conforme a lo requerido en la **Sección del pliego de Base y Condiciones** de la Licitación de referencia.

Copia de la Carpeta del Oferente remitida:

1. **INFORMATICA PARAGUAYA S.A.- INFOPAR**

Atentamente;

Lic. Gustavo Quiroga
Miembro de Comité.

CORRESPONDE AL MEMORANDUM DTE/TI/16/2020

AL: LIC. GUSTAVO QUIROGA

Se remite, a su consideración, la evaluación de la Capacidad Financiera de los Oferentes de la **LICITACIÓN PÚBLICA NACIONAL ANDE Nº 1567/2020 "SERVICIO DE ACTUALIZACIÓN, SOPORTE TÉCNICO Y MANTENIMIENTO DE EQUIPO UTM SONICWALL".**

La evaluación de la Capacidad Financiera de las empresas oferentes, ha sido realizada conforme a lo estipulado en el punto 7. Capacidad Financiera Requisitos de Participación y Criterios de Evaluación del Pliego de Bases y Condiciones de la Licitación de referencia. La evaluación del Ratio de Liquidez, Endeudamiento y Rentabilidad, fue realizada utilizando el promedio de los últimos 3 años, de los balances correspondientes a los ejercicios 2017 al 2019 según lo establecido en el Pliego de Bases y Condiciones.

Se presenta a continuación los resultados obtenidos:

EMPRESA	CONDICIONES DEL PLIEGO DE BASES Y CONDICIONES - CALIFICACIÓN		
	RATIO DE LIQUIDEZ	ENDEUDAMIENTO	RENTABILIDAD
1) INFORMATICA PARAGUAY S.A.	CUMPLE	CUMPLE	CUMPLE

Al mismo tiempo, adjuntamos las planillas de cálculos y procedemos a la devolución de las copias de los documentos de la mencionada Licitación.

Atentamente;

DA, jb

Econ. Denis Amarilla
Dpto. Estudios Económicos
Financieros y Bancarios

LICITACIÓN PÚBLICA NACIONAL ANDE Nº 1567/2020

"SERVICIO DE ACTUALIZACION, SOPORTE TÉCNICO Y MANTENIMIENTO DE EQUIPO UTM SONICWALL"

EVALUACIÓN DE LA CAPACIDAD FINANCIERA

1) INFORMATICA PARAGUAY S.A.

RATIO DE LIQUIDEZ

CUENTA	Año 2019	Año 2018	Año 2017	PROMEDIO
ACTIVO CORRIENTE	9.753.912.178	7.931.204.906	5.707.629.430	
PASIVO CORRIENTE	6.965.568.598	4.765.306.325	4.225.500.418	
INDICE DE LIQUIDEZ CORRIENTE	1,40	1,66	1,35	1,47
CONDICION >=1 en promedio Años 2017 al 2019				CUMPLE

ENDEUDAMIENTO

CUENTA	Año 2019	Año 2018	Año 2017	PROMEDIO
PASIVO TOTAL	11.825.513.515	11.277.418.703	4.225.500.418	
ACTIVO TOTAL	15.554.080.166	14.177.355.115	6.739.678.630	
INDICE DE ENDEUDAMIENTO	0,76	0,80	0,63	0,73
CONDICION < 0,80 en promedio Años 2017 al 2019				CUMPLE

RENTABILIDAD

CUENTA	Año 2019	Año 2018	Año 2017	PROMEDIO
UTILIDAD DESPUES DE IMPUESTOS	1.154.707.904	664.988.105	735.158.312	
PATRIMONIO NETO	3.728.566.651	2.899.936.407	2.514.178.212	
RENTABILIDAD	30,97%	22,93%	29,24%	27,71%
CONDICION (NO SER NEGATIVO), en promedio Años 2017 al 2019				CUMPLE

Elaborado por: Jorge Bordón R. Economista

Verificado por: Econ. Denis Amarilla Dpto. Estudios Económicos Financieros y Bancarios

ANEXO 4

Planilla de Verificación de Especificaciones Técnicas

ANDE

LICITACIÓN PUBLICA NACIONAL
Nro. 1565/2020.-
" SERVICIO DE ACTUALIZACIÓN, SOPORTE TÉCNICO Y MANTENIMIENTO DE EQUIPO UTM SONICWALL"

Comité de Evaluación de Ofertas Resolución N°: 44286

PLANILLA DE VERIFICACIÓN TÉCNICA

LOTE 1 : SERVICIO DE ACTUALIZACIÓN, SOPORTE TÉCNICO Y MANTENIMIENTO DE EQUIPO UTM SONICWALL		OFERENTES
		INFOPAR S.A.
	Descripcion	2.655.000.000
Situación actual	La institución cuenta con dos equipos Sonic Wall NSA los cuales operan en modalidad standalone conectados a proveedores de internet.	CUMPLE
	La institución tiene implementado ambos equipos en modalidad HA y pretende la actualización de las licencias que poseen los equipos, además de un servicio de soporte y mantenimiento que mejore la performance para hacer frente a los nuevos ciberataques en tiempo real.	CUMPLE
ITEM 1 - ACTUALIZACIÓN DE LICENCIAS		
Provisión de licencias	Firewall SSL VPN para la solución HA	CUMPLE
	Content Filtering	
	Capture Advanced Threat Protection	
	Gateway Anti-Virus / Anti- Spyware	
	Application Firewall Service and networking	
	Intrusion Prevention	
	App Control	
	Descifrado e inspección TLS/SSL/SSH	
	Anti Spam	
	High Availability – heredando el secundario toda la configuración del primero	
	Tecnología SD-WAN para interconectar sedes remotas	
	VPN SSL 3000 (tres mil)	
	VPN IPSec	
	Sistema de filtrado de navegación Web	
	Protección anti DoS	
	Antispam, antimalware de correos, protección de 3500 buzones	
	Analytics Software	
	Cantidad de Licencias para HA	
	Cantidad de Usuarios 3000 (tres mil)	
	Actualizaciones por 3 años	
ITEM 2 - SOPORTE Y MANTENIMIENTO		
Servicio de Actualización	SONICWALL COMPREHENSIVE GATEWAY SECURITY SUITE-W VIEWPOINT	CUMPLE
	SonicWALL Advanced Gateway Security Suite para la solución HA	CUMPLE
Soporte y Garantía	Se deberá ofrecer el servicio de soporte técnico local por parte del oferente con técnicos certificados por el fabricante por 36 meses en la modalidad 24x7. Como parte del contrato de soporte, el proveedor deberá incluir actualización de firmware a la última versión, recambio de partes dañadas por desperfectos de fabricación y/o desgaste por tiempo de uso. Todas las partes deberán ser nuevas. Si los equipos están descontinuados por el fabricante que impida la provisión de soporte, recambio de partes, actualización de firmware, o la activación de algunos de los servicios descriptos en estas especificaciones técnicas, el oferente deberá reemplazar los mismos por equipos iguales o de mayores prestaciones para poder mantener la cobertura de soporte por el fabricante sin costo adicional para la convocante. En caso de reemplazo, dichos hardware deberán ser instalados, y configurados por técnicos del oferente certificados por el fabricante. El tiempo de respuesta para el soporte deberá ser de 4 (cuatro) horas a partir del reclamo efectuado por la convocante.	CUMPLE

Certificación del Fabricante	El proveedor deberá presentar la Autorización del fabricante para proveer el software y brindar soporte específico para la presente licitación.	CUMPLE
Técnicos Certificados	El oferente deberá presentar con la oferta, al menos 2(dos) certificados SonicWall Network Security Administrador (SNSA) vigente a la fecha de presentación de la oferta en la marca, que avale la formación. Los técnicos deben formar parte del plantel de la empresa oferente, comprobable en IPS.	CUMPLE
Activación y configuración de Content Filtering	Control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 56 categorías y deberán actualizarse automáticamente.	CUMPLE
	Soporte a Youtube en modo restringido	CUMPLE
	Ser capaz de forzar el uso del safe search en google y bing	CUMPLE
	Evitar el uso de URLs embebidas (por ejemplo Google Translate) para evadir el filtrado web	CUMPLE
	Soportar mecanismos de Autenticación: RADIUS, TACACS+, Active Directory, LDAP, base de datos interna, Reconocimiento transparente de usuario del LDAP, reconocimiento de usuarios presentes en Terminal services (Windows y Citrix) y usuarios locales	CUMPLE
	Reconocimiento transparente (sin validación adicional) de los usuarios ya autenticados a través de un RADIUS server usando información de RADIUS accounting	CUMPLE
	Definición de cuota diaria, semanal o mensual de tiempo de conexión o de tráfico generado por cada usuario	CUMPLE
	Filtrado de páginas web sobre usuarios que no estén dentro de la red a través de un cliente de filtrado web	CUMPLE
Activación y configuración de Capture Advanced Threat Protection	Servicio online de detección de virus en la nube con capacidad de reconocimiento de más de 70 millones de amenazas el cual se puedan enviar muestras resumidas del tráfico para detectar códigos maliciosos	CUMPLE
	Filtrado de conexiones a centros de control de Botnets basado en reputación de direcciones IP	CUMPLE
	Controles de localización geográfica basados en la dirección IP de origen para hacer reglas de conexión por país bien sea de manera general o por reglas de firewall	CUMPLE
Activación y configuración de Gateway Anti-Virus Anti-Spyware	Rendimiento de Gateway Antivirus de 5 Gbps usando el modo de operación (Proxy o Flow) que brinda la máxima seguridad.	CUMPLE
	Analizar, tráfico entrante y saliente mínimo de los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP, CIFS/NETBIOS, y esta debe estar completamente integrada a la administración del dispositivo appliance	CUMPLE
	Escaneo de virus o spyware sobre protocolos basados en stream TCP, como Mensajería Instantánea y P2P	CUMPLE
	Análisis antivirus sin limitación del tamaño del archivo transferido y sin que esto afecte la efectividad de la detección de amenazas	CUMPLE
	El sistema antivirus deberá contar con la certificación Antivirus ICSA labs	CUMPLE
	Actualizaciones automáticas con un intervalo mínimo de búsqueda de actualizaciones de 1 hora	CUMPLE
	La Cantidad Mínima de sub-interfaces VLANs será de 500	CUMPLE
	Enrutamiento basado en políticas para que el tráfico sea enrutado a las diferentes interfaces basado en el servicio, la direcciones IP de origen o de destino	CUMPLE
	Enrutamiento basado en la aplicación, por ejemplo, Office 365 se encaminan por una interface de salida a internet mientras que YouTube se encamina por otra	CUMPLE
	Enrutamiento basado en políticas basado en el Full Qualified Domain Name – FQDN	CUMPLE
	Equal Cost Multipath para balanceo de rutas a través de múltiples canales	CUMPLE
	Tecnología SD-WAN para interconectar sedes remotas usando enlaces de internet de bajo costo pero con alta calidad de conexión	CUMPLE
	Enrutamiento: BGP, OSPF, RIPv1/v2, rutas estáticas y Multicast	CUMPLE

Mejora de perfomance y configuración de Application Firewall Service and networking	Link aggregation tanto estático como dinámico	CUMPLE
	Redundancia de puertos	CUMPLE
	Capacidad de realizar backups de la configuración automáticamente también respaldarlos en la nube	CUMPLE
	Port Mirroring	CUMPLE
	(QoS) Garantizar comunicaciones críticas con 802.1p, etiquetado DSCP y reasignación de tráfico VoIP en la red.	CUMPLE
	Protección contra ataques DoS	CUMPLE
	Balanceo de carga de múltiples interfaces WAN utilizando los métodos Round Robin, Spillover o Percentage.	CUMPLE
	El Rendimiento mínimo de Firewall de 17 Gbps usando la metodología de medición basada en el RFC 2544.	CUMPLE
	La cantidad mínima de conexiones que el sistema deberá soportar en modo firewall será de al menos 10 Millones	CUMPLE
	Soportar 130 mil conexiones por segundo	CUMPLE
	Cantidad mínima de conexiones del sistema con los módulos de IPS, Antivirus, Antispyware y Control de Aplicaciones activados (DPI) será de 4 millones	CUMPLE
	Certificación ICSSA Labs para Firewall	CUMPLE
	Certificación Common Criteria NDPP, Firewall e IPS	CUMPLE
	Certificación FIPS 140-2	CUMPLE
	Deberá soportar DNS Sinkhole	CUMPLE
	Deberá soportar DNS Tunnel Detection	CUMPLE
Activación y configuración de Intrusion Prevention System	Rendimiento mínimo en IPS : 10 Gbps	CUMPLE
	El sistema IPS contará con al menos 4.800 firmas de ataques	CUMPLE
	Protección de ataques de inundación (flood) a nivel de UDP, ICMP y el conocido SYN Flood	CUMPLE
	Permitir al administrador ejecutar acciones sobre los eventos de IPS como bloquear el tráfico, registrar o capturar el tráfico generado por el ataque	CUMPLE
	El IPS podrá inspeccionar el tráfico entre las zonas internas de la red	CUMPLE
	Deberá contar con mecanismos de antievasión	CUMPLE
	Filtro de bloqueo hacia centros de comando y control de botnets	CUMPLE
	Filtro de bloqueo por localización geográfica granular por cada regla de firewall	CUMPLE
Activación y Configuración de App Control	El rendimiento mínimo del sistema de control de aplicaciones será de 11 Gbps	CUMPLE
	identificar, categorizar y controlar y visualizar tráfico de más de 4300 aplicaciones agrupadas en al menos 25 Categorías	CUMPLE
	Las aplicaciones se deben identificar independientemente del Stack o del puerto (TCP, UDP, etc.) que usen	CUMPLE
	Las políticas de control de aplicaciones se podrán hacer granular por dirección IP, usuario, grupos de usuarios locales o de LDAP/Active Directory y basado en horarios.	CUMPLE
	Creación de reglas de control de ancho de banda de las aplicaciones soportadas	CUMPLE
	Reportar en tiempo real cuales de las aplicaciones soportadas están siendo usadas, que usuario o dirección IP lo está haciendo y cuánto tráfico está cursando	CUMPLE
Activación y configuración de Descifrado e inspección DPI-SSL/TLS/SSH	Inspección de Aplicaciones, IPS, antivirus y filtrado de páginas web sobre comunicaciones cifradas por TLS (Transport Layer Security) tales como HTTPS sin importar si opera sobre el puerto 443 u otro	CUMPLE
	El sistema de inspección profunda de paquetes deberá funcionar bidireccionalmente	CUMPLE
	El sistema de inspección profunda de paquetes deberá operar sin proxies para evitar problemas de latencia	CUMPLE
	El Rendimiento en Inspección SSL será mínimo de 2 Gbps	CUMPLE
	Manejar como mínimo 500000 conexiones concurrentes de tráfico cifrado usando los módulos de protección (IPS, Antimalware y control de aplicaciones)	CUMPLE
	Inspección de tráfico cifrado sobre SSH	CUMPLE
	Se podrán definir excepciones al tráfico cifrado por dominios o por categorías de páginas web	CUMPLE
	Soportar conexiones DPI SSL hasta 200 mil	CUMPLE
	El sistema deberá hacer inspección de Spam, Phishing y virus tanto a nivel de correos entrantes como salientes	CUMPLE

Activación y configuración de Anti Spam	El sistema deberá contar con actualizaciones automáticas de detección de Spam y Virus.	CUMPLE
	El sistema opcionalmente podrá hacer envío de correos de manera cifrada sin necesidad de usar software cliente de correo adicional	CUMPLE
	El sistema no deberá tener restricción de la cantidad de dominios a usar	CUMPLE
	El sistema deberá soportar autenticación a nivel de SMTP (SMTP AUTH)	CUMPLE
	Capacidad de liberar los correos de cuarentena que considere admisibles y podrá configurar la lista blanca o negra (dominios o correos permitidos o negados)	CUMPLE
	El Sistema deberá contar con cuarentena para el Almacenamiento de Virus, SPAM y mensajes sospechosos, con acceso desde la interfaz del usuario.	CUMPLE
	El usuario podrá acceder a su cuarentena y liberar los correos que considere adecuados	CUMPLE
	El usuario podrá recibir un resumen periódico de los correos que se han quedado en la cuarentena	CUMPLE
	Envío por correo electrónico de un resumen de los coreos llevados a cuarentena	CUMPLE
	Debe poder filtrar tipos de adjuntos en correo electrónico	CUMPLE
	Bloqueo de archivos adjuntos de acuerdo al asunto del mensaje (subject), texto del mensaje, extensión nombre de archivo y al usuario de destino	CUMPLE
	El sistema deberá hacer inspección de los correos adjuntos	CUMPLE
	El sistema deberá ser capaz de bloquear los archivos adjuntos por tipo de archivos y extensión.	CUMPLE
	El sistema deberá tener mecanismos de "Approval Boxes", el envío de correo luego que un delegado apruebe su envío, de acuerdo al origen y destino.	CUMPLE
	El sistema deberá tener diccionarios de palabras claves (términos financieros, términos médicos, entre otros)	CUMPLE
	El sistema deberá tener capacidad de detectar números de identificación de registros como números de identificación, números telefónicos, tarjetas de crédito, números bancarios entre otros	CUMPLE
	Proteger contra envío de reportes de no entrega (non delivery report –NDR) que permite conocer la existencia de direcciones de correo.	CUMPLE
	Deberá soportar SPF (Sender Policy Framework Verification)	CUMPLE
	Deberá soportar DKIM (DomainKeys Identified Mail)	CUMPLE
	Deberá soportar DMARC (Domain-based Message Authentication, Reporting & Conformance)	CUMPLE
	Debe poseer capacidad de identificación y bloqueo de SPAM en distintos idiomas.	CUMPLE
	La agresividad del sistema antispam podrá ser configurable por usuario y/o grupos de usuarios	CUMPLE
	El usuario final podrá contar con un botón de Spam en el cliente de correo Microsoft Outlook para clasificar cualquier correo basura que haya recibido	CUMPLE
	Deberá manejar al menos 04 (Cuatro) motores de antivirus embebidos en el sistema para análisis y detección de virus en los correos	CUMPLE
	El sistema debe ser capaz de detectar URLs maliciosas dentro de los mensajes	CUMPLE
	El sistema deberá soportar "Time-of-click URL protection", mecanismo que revisa las URL maliciosas en los mensajes cuando el usuario en su equipo hace click y no en el momento que el mensaje fue entregado.	CUMPLE
	El sistema deberá hacer detección de zombies, equipos que envían agresivamente correos electrónicos porque tienen instalados códigos maliciosos	CUMPLE
	El sistema deberá contar con tecnología de análisis de malware de códigos desconocidos en un sistema aislado (Sandbox) donde se ejecutará e inspeccionará el comportamiento del código	CUMPLE
	El sistema Sandbox operará como un servicio basado en la nube sin necesidad de hardware adicional	CUMPLE
	El sistema deberá contar con métodos de Sandboxing local o en nube para la detección de amenazas emergentes y amenazas de día cero	CUMPLE
	El sistema de Sandbox deberá contar con múltiples motores de detección para reducir las técnicas de evasión.	CUMPLE

	El sistema deberá usar al menos tres motores de Sandbox, incluyendo inspección en memoria en tiempo real.	CUMPLE
	El sistema deberá hacer un bloqueo del código que se está descargando hasta que se defina un veredicto	CUMPLE
	El sistema deberá analizar archivos ejectutables (PE), DLLs, PDFs, Archivos de Office, Comprimidos, JAR, APKs para múltiples sistemas operativos (Windows, Android, MAC OSX)	CUMPLE
	El sandbox deberá permitir excepciones por tipo de archivos y por su resumen MD5	CUMPLE
	El sistema deberá contar con reportes sobre los archivos enviados a análisis y su veredicto, el reporte deberá incluir sistema operativo y detalles del archivo analizado	CUMPLE
High Availability	Alta Disponibilidad (HA) entre 2 equipos - heredando el secundario toda la configuración del primero	CUMPLE
Upgrade de Licencias VPN SSL	La cantidad mínima de túneles VPN Site to Site soportados será 12.000	CUMPLE
	El Mínimo Rendimiento de VPNs 3DES/AES será de 10 Gbps usando la metodología de medición basada en el RFC 2544.	CUMPLE
	El sistema contará con mínimo 3000 Licencias de cliente VPN para acceso remoto	CUMPLE
	El sistema permitirá autenticación biométrica para las conexiones VPN	CUMPLE
Analytics Software	Deberá tener Capture Security Center	CUMPLE
	Capture Security Center:	CUMPLE
	Proporcionar un agente de informes de flujos para el análisis del tráfico de las aplicaciones y datos sobre el uso mediante protocolos IPFIX o NetFlow para ofrecer una supervisión en tiempo real e histórica. Ofrecer a los administradores una interfaz para supervisar visualmente su red en tiempo real. Identificar aplicaciones y páginas web con gran demanda de ancho de banda, visualizar el uso de las aplicaciones por usuarios y anticiparse a ataques y amenazas en la red.	CUMPLE
	• Visor en tiempo real personalizable mediante funciones de arrastrar y soltar.	CUMPLE
	• Pantalla de informes en tiempo real con filtrado de un solo clic.	CUMPLE
	• Dashboard de los flujos principales con botones de "Visualizar por" de un solo clic.	CUMPLE
	•Pantalla de informes de flujos con cinco pestañas de atributos de flujos adicionales.	CUMPLE
	• Pantalla de análisis de flujos con potentes funciones de correlación y dinamización.	CUMPLE
	•Visor de sesiones para el desglose profundo de sesiones individuales y paquetes.	CUMPLE
	Análisis del tráfico de aplicaciones, visión del tráfico de aplicaciones, del uso del ancho de banda y de las amenazas de seguridad, prestaciones de análisis forenses y resolución de problemas.	CUMPLE
Capacitación	Capacitación local del Oferente para administración y configuración para 2 técnicos. La carga horaria debe ser de 40 horas	CUMPLE