INFORME DE EVALUACIÓN N° 15/2020

CONTRATACIÓN DIRECTA DINCAP N° 04/2020
"ADQUISICIÓN DE EQUIPOS DE COMPUTACIÓN"
ID Nº 384.396

En la ciudad de Asunción, capital de la República del Paraguay, se reúne el Comité de Evaluación conformado por Resolución Ministerial Nº 153 de fecha 13 de Febrero de 2020, *"Por la cual se aprueba la conformación del Comité de Evaluación permanente para los procedimientos de Licitaciones de la Dirección Nacional de Coordinación y Administración de Proyectos DINCAP"*, integrado por las siguientes personas: **Lic. SERGIO SUAREZ GUANES**, en representación de la Dirección General de la DINCAP, **Econ. RODY CENTURION y el Lic. SERGIO FIGUEREDO LEZCANO**, en representación de la Dirección de Administración Financiera (DAF) de la DINCAP; para iniciar la Evaluación y Comparación de Ofertas del llamado de referencia; de la Dirección Nacional De Coordinación y Administración de Proyectos (DINCAP) del Ministerio de Agricultura y Ganadería.-

Los integrantes del Comité se comprometen a la más estricta reserva, sin dar a conocer ninguna información relativa al análisis, aclaración y evaluación de las ofertas, ni sobre la recomendación de la adjudicación, sin antes obtener la resolución de adjudicación del llamado.

ANTECEDENTES

Se deja constancia que el Pedido de Inicio de Llamado fue realizado en fecha 22 de Julio de 2020, según Expediente Nº 19.961/2020, por la Coordinación TIC-DINCAP, luego de la verificación realizada por la Coordinación de Licitación y Compras de la SUOC-DINCAP fue publicado en el Portal de Contrataciones Públicas en fecha 17 de Agosto del corriente, donde fueron cursadas las invitaciones a las empresas que se detallan a continuación:

NOMBRE	RUC	TELEFONO	EMAIL
COMPUSAVER S.A.	80012343-3	228251	posta@compusaver.com.py
INFORMATION TECHNOLOGY CONSULTING SUPPORT SOCIEDAD ANONIMA	80046953-4	200-637 / 200-638/0981 100012	licitaciones@itcs.com.py
NETLOGIC S.R.L.	80015538-6	612227	lismael@netlogic.com.py
OFFICE COMPU SA	80013316-1	206176/0983-727543	belinda@officecompu.com.py
SDA PARAGUAY SA	80017709-6	021/908-462/0981/404-413	info@sda.com.py

APERTURA DE SOBRES

Se hace constar que por **Acta N° 16/2020** de fecha **25 de agosto del corriente**, se ha realizado una prórroga al acto de apertura, conforme lo estipula la RESOLUCION DNCP Nº 522/15 del 24 de febrero de 2015, *Artículo 2º "DISPONER que en las Contrataciones Directas en las cuales no se contare con un mínimo de 3 (tres) ofertas al vencimiento del plazo de entrega de sobres, la Autoridad Competente del Organismo, Entidad o Municipalidad, bajo su exclusiva responsabilidad podrá disponer, si lo considerase pertinente, la prórroga el tiempo límite para presentar ofertas o en su caso, la evaluación de las que se hubieren presentado, sin necesidad de contar con el mínimo de ofertas indicado, de conformidad a lo dispuesto en el Inc. "c" del Art. 34 de la Ley Nº 2051/03. La prórroga en su caso deberá fijar una fecha límite para la presentación y apertura de ofertas con un plazo mínimo de 5 (cinco) días corridos cuando se trate de contrataciones directas superiores a 200 (doscientos) jornales mínimos y de 3 (tres) días corridos cuando sean inferiores a 200 (doscientos) jornales mínimos. Estos plazos se computarán desde la fecha de difusión en el SICP (Sistema de Información de las Contrataciones Públicas) y deberán ser difundidas mediante sus respectivas adenda)".*

Que según Acta de Apertura N° 19/2020 de fecha 03 de Setiembre del corriente, se informa que se han presentado en tiempo y forma, al llamado "**ADQUISICIÓN DE EQUIPOS DE COMPUTACIÓN – ID 384.396"**, las siguientes firmas:

Oferentes	RUC	E-MAIL	Monto de la Oferta Gs.	Garantía de Mantenimiento de oferta Gs.	Poder de Representante (Persona Jurídica)	Fotocopia de Cedula del Firmante (Persona Física)	Constancia SIPE N°
COMPUSAVER S.A.	80012343-3	posta@compusaver.com.py	93.005.000.-	2.790.150.-	SIPE.-	No Aplica.-	1607918.-
PARASOFT S.R.L.	80000727-1	dpto.comercial@parasoft.com.py	77.638.000.-	7.500.000.-	SIPE.-	No Aplica.-	1609207.-
SOLUTEC de Fernando Ariel Cárdenas Galeano	3846758-5	armandorcgster@gmail.com; fac.cardenas@gmail.com	82.620.000.-	3.470.000.-	No Aplica.-	SIPE.-	1609083.-

EVALUACION DE LAS OFERTAS

El Comité procede al estudio y análisis de las ofertas presentadas por los citados oferentes que posibilite la elaboración del informe y la recomendación de adjudicación correspondiente, en cumplimiento a las disposiciones en los Art. 26, 27, 28 y 34 de la Ley N° 2051/03, como así también a los Art. 63, 64, 65, 66 y 67 del Decreto Reglamentario N° 2992/19 y los requisitos establecidos en la Carta de Invitación.

Al respecto en cumplimiento a lo que establece la Carta de Invitación, en concordancia a lo dispuesto en el Art. 61 del Decreto Reglamentario N° 2992/19, se procede a la verificación de los documentos sustanciales presentados por el oferente, en base a la cual se hace constar lo siguiente:

DOCUMENTOS SUSTANCIALES REQUERIDOS	COMPUSAVER S.A.	PARASOFT S.R.L.	SOLUTEC de Fernando Cárdenas
a) Formulario de Oferta y lista de precios, debidamente completado y firmado. El oferente deberá llenar en todos los ítems indicados en la planilla de precios. (*)	Presenta y Cumple	Presenta y Cumple	Presenta y Cumple
b) Garantía de Mantenimiento de Oferta debidamente extendida, bajo la forma de una declaración jurada. (*).	Presenta y Cumple	Presenta y Cumple	Presenta y Cumple
c) Declaración jurada de no hallarse comprendido en las prohibiciones o limitaciones para contratar establecidas en el artículo 40 y de integridad conforme al artículo 20, inc. "w", ambos de la Ley N° 2051/03 "De Contrataciones Públicas", de acuerdo con lo dispuesto en la Resolución N° 330/07 de la Dirección General de Contrataciones Públicas. (*).	Presenta y Cumple	Presenta y Cumple	Presenta y Cumple
d) Fotocopia simple de la cedula de identidad del firmante de la oferta, **Persona Física(*)**	No Aplica	No Aplica	Presenta SIPE y Cumple
e) En el caso que suscriba la oferta otra persona en su representación deberá acompañar una fotocopia simple de su Cédula de Identidad y una fotocopia autenticada del Poder suficiente otorgado por Escritura Pública para presentar la Oferta y representarlo en los actos de la Licitación. No es necesario que el Poder esté inscripto en el Registro de Poderes.(*) **Persona Física.**	No Aplica	No Aplica	No Aplica
f) Fotocopia simple de los documentos que acrediten las facultades del firmante de la oferta para comprometer al oferente. Estos documentos pueden consistir en: un poder suficiente otorgado por Escritura Pública (no es necesario que esté inscripto en el Registro de Poderes); ó los documentos societarios que justifiquen la representación del firmante, tales como las actas de asamblea y de directorio en el caso de las sociedades anónimas.(*) **Persona Jurídica.**	Presenta SIPE y Cumple	Presenta SIPE y Cumple	No Aplica
g) Fotocopia simple de los documentos que acrediten la existencia legal de la persona jurídica tales como la Escritura Pública de Constitución y protocolización de los Estatutos Sociales. Los estatutos deberán estar inscriptos en la Sección Personas Jurídicas de la Dirección de Registros Públicos.(*) **Persona Jurídica.**	Presenta SIPE y Cumple	Presenta SIPE y Cumple	No Aplica

OBS: Los documentos indicados con asterisco (*) son considerados documentos sustanciales a ser presentados con la oferta.

Analizada las documentaciones sustanciales de las firmas: **COMPUSAVER S.A., PARASOFT S.R.L., SOLUTEC de Fernando Cárdenas**; las mismas cumplen con los requisitos establecidos en la Carta de Invitación, por consiguiente son **"OFERTAS EVALUABLES".-**

Luego del examen de cumplimiento en la presentación de los documentos sustanciales, se procede a la elaboración y exposición a los efectos meramente comparativos del "**CUADRO COMPARATIVO DE PRECIOS"-**

Seguidamente y conforme al Art. 62 del Decreto N° 2.992/2019 y la Ley Nº 2051/03 "De Contrataciones Públicas" que expresa: *"Disconformidades, errores y omisiones. Siempre y cuando una oferta se ajuste sustancialmente al Pliego de Bases y Condiciones, el Comité podrá requerirá que cualquier disconformidad u omisión que no constituya una desviación significativa, se subsane en cuanto a la información o documentación que permita al Comité de Evaluación realizar la calificación de la oferta. Así mismo, y a los efectos de rectificar disconformidades u omisiones meramente formales y no sustanciales, el Comité emplazará por escrito al Oferente a que presente la información o documentación necesaria, dentro de un plazo razonable establecido por el mismo, bajo apercibimiento de rechazo de la oferta .....",* solicitando las siguientes documentaciones formales:

- Según **Nota SUOC Nº 108/2020** de fecha 03 de Setiembre del corriente se solicitaron documentos a la firma **COMPUSAVER S.A.,** conforme el siguiente detalle:

- *Certificado de cumplimiento tributario.*
- *Certificado de Producto y Empleo Nacional, emitido por el MIC.*
- *Constancia de presentación de la "Declaración Jurada de bienes y rentas, activos y pasivos" ante la Contraloría General de la República, para los sujetos obligados en el marco de la Ley N° 6355/19.*
- *Patente comercial del municipio en donde esté asentado el establecimiento principal del oferente.*
- *Copia del Balance General y Cuadro de Estado de Resultados de los años 2017 y 2018.*
- *Copia de facturaciones y/o recepciones finales de los años 2017, 2018 y 2019, que avalen la experiencia requerida.*

En fecha 07/09/2020, la firma **COMPUSAVER S.A.,** NO PRESENTA lo solicitado por esta Convocante, por lo tanto, este Comité procede a **RECHAZAR** dicha oferta, y se prosigue con la Evaluación del presente llamado.

- Según **Nota SUOC Nº 109/2020** de fecha 03 de Setiembre del corriente se solicitaron documentos a la firma **PARASOFT S.R.L.,** conforme el siguiente detalle:

- *Constancia de presentación de la "Declaración Jurada de bienes y rentas, activos y pasivos" ante la Contraloría General de la República, para los sujetos obligados en el marco de la Ley N° 6355/19.* ***Presenta Acción de Inconstitucionalidad N° 240/2020. Cumple.-***
- *Copia del Balance General y Cuadro de Estado de Resultados de los años 2017 y 2018.* ***Presenta y cumple.***
- *Copia de facturaciones y/o recepciones finales del año 2018, que avalen la experiencia requerida.* ***Presenta y cumple.***
- *Especificaciones Técnicas de los bienes o servicios a ser adquiridos.* ***Presenta y cumple.***

En fecha 07/09/2020, la firma **PARASOFT S.R.L.,** presenta en tiempo y forma, todo lo solicitado por esta Convocante, siendo una oferta ***EVALUABLE***, se prosigue con la Evaluación del presente llamado.

- Según **Nota SUOC Nº 110/2020** de fecha 03 de Setiembre del corriente se solicitaron documentos a la firma **SOLUTEC de Fernando Ariel Cárdenas Galeano,** conforme el siguiente detalle:

- *Certificado de Producto y Empleo Nacional, emitido por el MIC.* ***No presenta. Alega que no es motivo de descalificación.***
- *Copia del Balance General y Cuadro de Estado de Resultados de los años 2017 y 2018.* ***Presenta y cumple.***
- *Copia de facturaciones y/o recepciones finales del año 2017, 2018 y 2019, que avalen la experiencia requerida.* ***Presenta y cumple.***

En fecha 07/09/2020, la firma **SOLUTEC de Fernando Ariel Cárdenas Galeano,** presenta en tiempo y forma, lo solicitado por esta Convocante, siendo una oferta ***EVALUABLE***, y se prosigue con la Evaluación del presente llamado.

ESPECIFICACIONES TÉCNICAS REQUERIDAS

Según Providencia de fecha 08 de Setiembre del corriente, se solicitó a la Coordinación TIC de la DINCAP lo siguiente:

Se remiten copias de las especificaciones técnicas de los equipos solicitados por la convocante, recepcionados en fecha 03/09/2020 en la SUOC, en el marco del llamado ***CONTRATACION DIRECTA DINCAP N° 04/2019 "ADQUISICIÓN DE EQUIPOS DE COMPUTACIÓN" ID N° 384.396,*** a efectos de solicitar se realicen las verificaciones en cuanto a si se ajustan sustancialmente a las Especificaciones Técnicas requeridas en la Carta de Invitación, en donde por providencia de fecha 09 de setiembre del corriente, la Coordinación TIC de la DINCAP concluye lo siguiente:

Que las tres (3) empresas ***COMPUSAVER S.A.; PARASOFT S.R.L. y SOLUTEC de Fernando Cárdenas,*** cumplen con lo solicitado en el Anexo C – Especificaciones Técnicas de los bienes o servicios adquiridos, según el siguiente cuadro:

ROUTER		Marca: FORTINET Modelo: FORTIGATE 100E
1) Características Equipo tipo 1 (1 unidades)		**Cumple / No cumple**
1.1)	Throughput de firewall (medido con paquetes 512 bytes) por lo menos 7.4 Gbps, con tráfico IPv4 y IPv6	Cumple
1.2)	Soporte a por lo menos 2M sesiones simultaneas	Cumple
1.3)	Soporte a por lo menos 30,000 nuevas sesiones por segundo	Cumple
1.4)	Throughput de al menos 4 Gbps de VPN IPSec	Cumple
1.5)	Estar licenciado para, o soportar sin necesidad de licencia, 2K túneles de VPN IPSec site-to-site simultáneos	Cumple
1.6)	Estar licenciado para, o soportar sin necesidad de licencia, 1K túneles de clientes VPN IPSec simultáneos	Cumple
1.7)	Throughput de al menos 250 Mbps de VPN SSL	Cumple
1.8)	Soportar al menos 500 clientes de VPN SSL simultáneos	Cumple
1.9)	Soportar al menos 500 Mbps de throughput de IPS	Cumple
1.10)	Soportar al menos 130 Mbps de throughput de Inspección SSL	Cumple
1.11)	Soportar al menos 900 Mbps de throughput de Application Control	Cumple
1.12)	Soportar al menos 360 Mbps de throughput de NGFW	Cumple
1.13)	Soportar al menos 250 Mbps de throughput de Threat Protection	Cumple

1.14)	Permitir gestionar al menos 30 Access Points	Cumple
1.15)	Debe incluir al menos 16 interfaces 1Gbps con conector RJ45.	Cumple
1.16)	Además debe incluir: 2 interfaces dedicadas para HA, 1 interfaz dedicada para gestión, 1 interfaz dedicada para consola	Cumple
1.17)	Tener al menos 2 interfaces 1Gbps SFP	Cumple
1.18)	Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance	Cumple
1.19)	Soporte a por lo menos 10 sistemas virtuales lógicos (Contextos) por appliance	Cumple
1.20)	El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios y funcionalidades incluidas por el equipo, siendo el desempeño del equipo la única limitante para usar dichas funcionalidades.	Cumple
1.21)	La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS, URL Filtering y Sandbox en la nube del fabricante, debe proveerse para al menos 1 (un) año	Cumple
2) Requisitos Mínimos de Funcionalidad		
Características Generales		
2.1)	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.	Cumple
2.2)	Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;	Cumple
2.3)	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;	Cumple
2.4)	La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;	Cumple
2.5)	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;	Cumple
2.6)	La gestión del equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;	Cumple
2.7)	Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;	Cumple
2.8)	Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;	Cumple
2.9)	Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;	Cumple
2.10)	Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);	Cumple
2.11)	Los dispositivos de protección de red deben soportar DHCP Relay;	Cumple
2.12)	Los dispositivos de protección de red deben soportar DHCP Server;	Cumple
2.13)	Los dispositivos de protección de red deben soportar sFlow;	Cumple
2.14)	Los dispositivos de protección de red deben soportar Jumbo Frames;	Cumple
2.15)	Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;	Cumple
2.16)	Debe ser compatible con NAT dinámica (varios-a-1);	Cumple
2.17)	Debe ser compatible con NAT dinámica (muchos-a-muchos);	Cumple
2.18)	Debe soportar NAT estática (1-a-1);	Cumple

2.19)	Debe admitir NAT estática (muchos-a-muchos);	Cumple
2.20)	Debe ser compatible con NAT estático bidireccional 1-a-1;	Cumple
2.21)	Debe ser compatible con la traducción de puertos (PAT);	Cumple
2.22)	Debe ser compatible con NAT Origen;	Cumple
2.23)	Debe ser compatible con NAT de destino;	Cumple
2.24)	Debe soportar NAT de origen y NAT de destino de forma simultánea;	Cumple
2.25)	Debe soportar NAT de origen y NAT de destino en la misma política	Cumple
2.26)	Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;	Cumple
2.27)	Debe ser compatible con NAT64 y NAT46;	Cumple
2.28)	Debe implementar el protocolo ECMP;	Cumple
2.29)	Debe soportar SD-WAN de forma nativa	Cumple
2.30)	Debe soportar el balanceo de enlace hash por IP de origen;	Cumple
2.31)	Debe soportar el balanceo de enlace por hash de IP de origen y destino;	Cumple
2.32)	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;	Cumple
2.33)	Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;	Cumple
2.34)	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;	Cumple
2.35)	Enviar logs a sistemas de gestión externos simultáneamente;	Cumple
2.36)	Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;	Cumple
2.37)	Debe soporta protección contra la suplantación de identidad (anti-spoofing);	Cumple
2.38)	Implementar la optimización del tráfico entre dos dispositivos;	Cumple
2.39)	Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);	Cumple
2.40)	Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);	Cumple
2.41)	Soportar OSPF graceful restart;	Cumple
2.42)	Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;	Cumple
2.43)	Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;	Cumple
2.44)	Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;	Cumple
2.45)	Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;	Cumple
2.46)	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;	Cumple
2.47)	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;	Cumple
2.48)	Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;	Cumple
2.49)	La configuración de alta disponibilidad debe sincronizar: Sesiones;	Cumple

2.50)	La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;	Cumple
2.51)	La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;	Cumple
2.52)	La configuración de alta disponibilidad debe sincronizar: Tablas FIB;	Cumple
2.53)	En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;	Cumple
2.54)	Debe soportar la creación de sistemas virtuales en el mismo equipo;	Cumple
2.55)	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;	Cumple
2.56)	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;	Cumple
2.57)	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 configuración de sistemas virtuales (contextos) por ambos tipos de acceso;	Cumple
2.58)	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);	Cumple
2.59)	Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;	Cumple
2.60)	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;	Cumple
2.61)	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;	Cumple
2.62)	La consola de administración debe soportar como minimo, ingles, Español y Portugues.	Cumple
2.63)	La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad	Cumple
2.64)	La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.	Cumple
Control por Política de Firewall		
2.65)	Debe soportar controles de zona de seguridad;	Cumple
2.66)	Debe contar con políticas de control por puerto y protocolo;	Cumple
2.67)	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;	Cumple
2.68)	Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;	Cumple
2.69)	Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;	Cumple

2.70)	Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;	Cumple
2.71)	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.	Cumple
2.72)	Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);	Cumple
2.73)	Debe soportar integración de nubes publicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes	Cumple
2.74)	Debe soportar el protocolo estándar de la industria VXLAN;	Cumple
2.75)	La solución debe permitir la implementación sin asistencia de SD-WAN	Cumple
2.76)	En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por politicas, IPSEC VPN;	Cumple
2.77)	la solución debe soportar la integración nativa con solución de sandboxing, protección de correo electronico, cache y Web application firewall.	Cumple
Control de Aplicación		
2.78)	Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;	Cumple
2.79)	Detección de miles de aplicaciones en 18 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;	Cumple
2.80)	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;	Cumple
2.81)	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;	Cumple
2.82)	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;	Cumple
2.83)	Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;	Cumple
2.84)	Actualización de la base de firmas de la aplicación de forma automática;	Cumple
2.85)	Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por politica de usuarios y grupos;	Cumple
2.86)	Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;	Cumple
2.87)	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;	Cumple

2.88)	El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;	Cumple
2.89)	Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;	Cumple
2.90)	Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;	Cumple
2.91)	Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;	Cumple
2.92)	Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;	Cumple
2.93)	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);	Cumple
2.94)	Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;	Cumple
2.95)	Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;	Cumple
2.96)	Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente	Cumple
Prevención de Amenazas		
2.97)	Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;	Cumple
2.98)	Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);	Cumple
2.99)	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;	Cumple
2.100)	Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;	Cumple
2.101)	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;	Cumple
2.102)	Deber permitir el bloqueo de vulnerabilidades y exploits conocidos	Cumple
2.103)	Debe incluir la protección contra ataques de denegación de servicio;	Cumple
2.104)	Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;	Cumple
2.105)	Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;	Cumple
2.106)	Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;	Cumple
2.107)	Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;	Cumple
2.108)	Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);	Cumple

2.109)	Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc;	Cumple
2.110)	Detectar y bloquear los escaneos de puertos de origen;	Cumple
2.111)	Bloquear ataques realizados por gusanos (worms) conocidos;	Cumple
2.112)	Contar con firmas específicas para la mitigación de ataques DoS y DDoS;	Cumple
2.113)	Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);	Cumple
2.114)	Debe poder crear firmas personalizadas en la interfaz gráfica del producto;	Cumple
2.115)	Identificar y bloquear la comunicación con redes de bots;	Cumple
2.116)	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;	Cumple
2.117)	Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;	Cumple
2.118)	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;	Cumple
2.119)	Los eventos deben identificar el país que origino la amenaza;	Cumple
2.120)	Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);	Cumple
2.121)	Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;	Cumple
2.122)	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;	Cumple
2.123)	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;	Cumple
2.124)	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);	Cumple
Filtrado de URL		
2.125)	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);	Cumple
2.126)	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;	Cumple
2.127)	Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;	Cumple

2.128)	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;	Cumple
2.129)	Tener por lo menos 75 categorías de URL;	Cumple
2.130)	Debe tener la funcionalidad de exclusión de URLs por categoría;	Cumple
2.131)	Permitir página de bloqueo personalizada;	Cumple
2.132)	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);	Cumple
2.133)	Además del Explicit Web Proxy, soportar proxy web transparente;	Cumple
Identificación de Usuarios		
2.134)	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;	Cumple
2.135)	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;	Cumple
2.136)	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;	Cumple
2.137)	Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios;	Cumple
2.138)	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;	Cumple
2.139)	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);	Cumple
2.140)	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;	Cumple
2.141)	Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;	Cumple
2.142)	Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;	Cumple
2.143)	Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;	Cumple
QoS Traffic Shaping		

2.144)	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;	Cumple
2.145)	Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;	Cumple
2.146)	Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;	Cumple
2.147)	Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;	Cumple
2.148)	Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;	Cumple
2.149)	Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;	Cumple
2.150)	En QoS debe permitir la definición de tráfico con ancho de banda garantizado;	Cumple
2.151)	En QoS debe permitir la definición de tráfico con máximo ancho de banda;	Cumple
2.152)	En QoS debe permitir la definición de colas de prioridad;	Cumple
2.153)	Soportar marcación de paquetes DiffServ, incluso por aplicación;	Cumple
2.154)	Soportar la modificación de los valores de DSCP para Diffserv;	Cumple
2.155)	Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);	Cumple
2.156)	Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;	Cumple
Filtro de Datos		
2.157)	Permite la creación de filtros para archivos y datos predefinidos;	Cumple
2.158)	Los archivos deben ser identificados por tamaño y tipo;	Cumple
2.159)	Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones;	Cumple
2.160)	Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;	Cumple
2.161)	Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;	Cumple
2.162)	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;	Cumple
Geo Localización		
2.163)	Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;	Cumple
2.164)	Debe permitir la visualización de los países de origen y destino en los registros de acceso;	Cumple
2.165)	Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;	Cumple
VPN		
2.166)	Soporte VPN de sitio-a-sitio y cliente-a-sitio;	Cumple
2.167)	Soportar VPN IPSec;	Cumple
2.168)	Soportar VPN SSL;	Cumple

2.169)	La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512	Cumple
2.170)	La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;	Cumple
2.171)	La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);	Cumple
2.172)	La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);	Cumple
2.173)	Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;	Cumple
2.174)	Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;	Cumple
2.175)	Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting;	Cumple
2.176)	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;	Cumple
2.177)	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;	Cumple
2.178)	Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;	Cumple
2.179)	Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;	Cumple
2.180)	Deberá mantener una conexión segura con el portal durante la sesión;	Cumple
2.181)	El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.	Cumple
Wireless Controller		
2.182)	Solución de red inalámbrica que administre y controle de manera centralizada los puntos de acceso (AP);	Cumple
2.183)	Cualquier licencia y / o software necesario para la plena ejecución de todas las características descritas en este término de referencia deberá ser suministrada;	Cumple
2.184)	Debe permitir la conexión de dispositivos inalámbricos que implementen los estándares IEEE 802.11a / b / g / n / ac y que transmitan tráfico IPv4 e IPv6 a través del controlador;	Cumple
2.185)	La solución debe ser capaz de administrar puntos de acceso de tipo indoor y outdoor;	Cumple
2.186)	El controlador inalámbrico debe permitir ser descubierto automáticamente por los puntos de acceso a través de Broadcast, DHCP y consulta DNS;	Cumple
2.187)	La solución debe optimizar el rendimiento y la cobertura inalámbrica (RF) en los puntos de acceso administrados por ella, realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados. La solución debe permitir además deshabilitar el ajuste automático de potencia y canales cuando sea necesario;	Cumple
2.188)	Permitir programar día y hora en que ocurrirá la optimización del aprovisionamiento automático de canales en los Access Points;	Cumple

2.189)	El encaminamiento de 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 ser tunelados hasta el controlador inalámbrico;	Cumple
2.190)	Cuando tunelado, el tráfico debe ser encriptado a través de DTLS o IPSEC;	Cumple
2.191)	Debe permitir la administración de puntos de acceso conectados remotamente a través de WAN. En este escenario el encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe ocurrir de forma distribuida (local switching), o sea, el tráfico debe ser cambiado localmente en la interfaz LAN del punto de acceso y no necesitará de tunelamiento hasta el controlador inalámbrico;	Cumple
2.192)	Cuando el tráfico se conmuta directamente en los puertos Ethernet de los puntos de acceso (local switching) y la autenticación sea WPA/WPA2-Personal (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;	Cumple
2.193)	La solución debe permitir definir qué redes serán tuneladas hasta la controladora y qué redes serán conmutadas directamente por la interfaz del punto de acceso;	Cumple
2.194)	La solución debe soportar el recurso de Split-Tunneling de forma que sea posible definir, a través de las subredes de destino, qué paquetes serán tunelados hasta el controlador y cuáles serán conmutados localmente en la interfaz del punto de acceso;	Cumple
2.195)	La solución debe implementar recursos que posibiliten la identificación de interferencias provenientes de equipos que operen en las frecuencias de 2.4GHz y 5GHz;	Cumple
2.196)	La solución debe detectar Receiver Start of Packet (RX-SOP) en paquetes inalámbricos y ser capaz de omitir aquellos que están por debajo de determinado umbral especificado en dBm;	Cumple
2.197)	La solución debe permitir el equilibrio de carga de los usuarios conectados a la infraestructura inalámbrica de forma automática. La distribución de los usuarios entre los puntos de acceso cercanos debe ocurrir sin intervención humana y basada en criterios como número de dispositivos asociados en cada punto de acceso;	Cumple
2.198)	La solución debe tener mecanismos para detectar y mitigar los puntos de acceso no autorizados, también conocidos como Rogue AP. La mitigación debe realizarse de forma automática y batida en criterios tales como: intensidad de señal o SSID. Los puntos de acceso administrados por la solución deben evitar la conexión de clientes en puntos de acceso no autorizados;	Cumple
2.199)	La solución debe identificar automáticamente puntos de acceso intrusos que estén conectados a la red de cable (LAN). La solución debe ser capaz de identificar el punto de acceso intruso incluso cuando el MAC Address de la interfaz LAN es ligeramente diferente (adyacente) del MAC Address de la interfaz WLAN;	Cumple

2.200)	La solución debe detectar los puntos de acceso no autorizados y / o intrusos a través de radios dedicados a la función de análisis o a través de Off-channel / Background scanning. Cuando se realiza a través de Off-channel / Background scanning, la solución debe ser capaz de identificar el uso del punto de acceso para, en caso necesario, retrasar el análisis y de esta forma no perjudicar a los clientes conectados;	Cumple
2.201)	La solución debe permitir la configuración individual de las radios del punto de acceso para que operen en el modo monitor, o sea, con función dedicada para detectar amenazas en la red inalámbrica y con ello permitir mayor flexibilidad en el diseño de la red;	Cumple
2.202)	La solución debe permitir la adición de controlador redundante operando en N + 1. En este modo, el controlador redundante debe monitorear la disponibilidad y sincronizar la configuración del principal, además de asumir todas las funciones en caso de error del controlador principal. De esta forma, todos los puntos de acceso deben asociarse automáticamente al controlador redundante que pasará a tener función de primario de forma temporal;	Cumple
2.203)	La solución debe permitir el agrupamiento de VLANs para que se distribuyan múltiples subredes en un determinado SSID, reduciendo así el broadcast y aumentando la disponibilidad de direcciones IP;	Cumple
2.204)	La solución debe permitir la creación de múltiples dominios de movilidad (SSID) con configuraciones distintas de seguridad y red. Debe ser posible especificar en qué puntos de acceso o grupos de puntos de acceso que cada dominio estará habilitado;	Cumple
2.205)	La solución debe garantizar al administrador de la red determinar los horarios y días de la semana que las redes (SSID) estarán disponibles para los usuarios;	Cumple
2.206)	Debe permitir restringir el número máximo de dispositivos conectados por punto de acceso y por radio;	Cumple
2.207)	La solución debe implementar el estándar IEEE 802.11r para acelerar el proceso de roaming de los dispositivos a través de la función conocida como Fast Roaming;	Cumple
2.208)	La solución debe implementar el estándar IEEE 802.11k para permitir que un dispositivo conectado a la red inalámbrica identifique rápidamente otros puntos de acceso disponibles en su área para que ejecute la itinerancia;	Cumple
2.209)	La solución debe implementar el estándar IEEE 802.11v para permitir que la red influya en las decisiones de roaming del cliente conectada mediante el suministro de información complementaria, como la carga de utilización de los puntos de acceso cercanos;	Cumple
2.210)	La solución debe implementar el estándar IEEE 802.11w para prevenir ataques a la infraestructura inalámbrica;	Cumple
2.211)	La solución debe soportar priorización a través de WMM y permitir la traducción de los valores a DSCP cuando los paquetes se destinan a la red de cableado;	Cumple
2.212)	La solución debe implementar técnicas de Call Admission Control para limitar el número de llamadas simultáneas;	Cumple

2.213)	La solución debe mostrar información sobre los dispositivos conectados a la infraestructura inalámbrica e informar al menos la siguiente información: Nombre de usuario conectado al dispositivo, Fabricante y sistema operativo del dispositivo, Dirección IP, SSID al que está conectado, Punto de acceso al que está conectado , Canal al que está conectado, Banda transmitida y recibida (en Kbps), intensidad de la señal considerando el ruido en dB (SNR), capacidad MIMO y horario de la asociación;	Cumple
2.214)	Para garantizar una mejor distribución de dispositivos entre las frecuencias disponibles y mejorar la utilización de la radiofrecuencia, la solución debe ser capaz de distribuir automáticamente los dispositivos de banda dual para que se conecten primariamente a 5GHz a través del recurso conocido como Band Steering;	Cumple
2.215)	La solución debe permitir la configuración de los data rates que se activarán en la herramienta y las que se deshabilitar para las frecuencias de 2.4 y 5GHz y los estándares 802.11a / b / g / n / ac;	Cumple
2.216)	La solución debe tener capacidad capaz de convertir paquetes Multicast en paquetes Unicast cuando se reenvían a los dispositivos que están conectados a la infraestructura inalámbrica, mejorando así el consumo de Airtime;	Cumple
2.217)	La solución debe soportar la característica que ignore Probe Requests de clientes que tienen una señal débil o distante. Debe permitir definir el umbral para que los Probe Requests sean ignorados;	Cumple
2.218)	La solución debe permitir la configuración del valor de Short Guard Interval para 802.11n y 802.11ac en 5GHz;	Cumple
2.219)	La solución debe implementar una característica conocida como Airtime Fairness (ATF) para controlar el uso de airtime asignando porcentajes a utilizar en los SSID;	Cumple
2.220)	La solución debe implementar reglas de firewall (stateful) para controlar el tráfico permitiendo o descartando paquetes de acuerdo con la política configurada, reglas que deben utilizar como criterio direcciones de origen y destino (IPv4 e IPv6), puertos y protocolos;	Cumple
2.221)	La solución debe implementar la función de web filtering para controlar los sitios que se accede a la red inalámbrica. Debe poseer una base de conocimiento para categorizar los sitios y permitir configurar qué categorías de sitios serán permitidos y bloqueados para cada perfil de usuario y SSID;	Cumple
2.222)	La solución debe tener capacidad de reconocimiento de aplicaciones a través de la técnica de DPI (Deep Packet Inspection) que permita al administrador de la red monitorear el perfil de acceso de los usuarios e implementar políticas de control. Debe permitir el funcionamiento de esta característica y la actualización periódica de la base de aplicaciones durante todo el período de garantía de la solución;	Cumple
2.223)	La base de reconocimiento de aplicaciones a través de DPI debe identificar con al menos 1500 (mil y quinientas) aplicaciones;	Cumple
2.224)	La solución debe permitir la creación de reglas para el bloqueo y el límite de banda (en Mbps, Kbps ou Bps) para las aplicaciones reconocidas a través de la técnica de DPI;	Cumple
2.225)	La solución debe, a través de la técnica de DPI, reconocer aplicaciones sensibles al negocio y permitir la priorización de este tráfico con QoS;	Cumple

2.226)	La solución debe implementar mecanismos de protección para identificar ataques a la infraestructura inalámbrica. Al menos los siguientes ataques deben ser identificados: - Ataques de flood contra el protocolo EAPOL (EAPOL Flooding); - Los siguientes ataques de denegación de servicio: Association Flood, Authentication Flood, Broadcast Deauthentication y Spoofed Deauthentication; - ASLEAP; - Null Probe Response / Null SSID Probe Response; - Long Duration; - Ataques contra Wireless Bridges; - Weak WEP; - Invalid MAC OUI.	Cumple
2.227)	La solución debe implementar mecanismos de protección para mitigar ataques a la infraestructura inalámbrica. Al menos ataques de denegación de servicio deben ser mitigados por la infraestructura a través del envío de paquetes de authentication	Cumple
2.228)	La solución debe implementar mecanismos de protección contra ataques de ARP Poisoning en la red inalámbrica;	Cumple
2.229)	La solución debe monitorear y clasificar el riesgo de las aplicaciones accesadas por los clientes inalámbricos;	Cumple
2.230)	Permitir configurar el bloqueo en la comunicación entre los clientes inalámbricos conectados a un SSID;	Cumple
2.231)	Debe implementar la autenticación administrativa a través del protocolo RADIUS;	Cumple
2.232)	En combinación con los puntos de acceso, la solución debe implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES);	Cumple
2.233)	En combinación con los puntos de acceso, la solución debe ser compatible e implementar el método de autenticación WPA3;	Cumple
2.234)	La solución debe permitir la configuración de múltiples claves de autenticación PSK para su uso en un SSID determinado;	Cumple
2.235)	Cuando se utiliza la función de múltiples claves PSK, la solución debe permitir la definición de límite en cuanto al número de conexiones simultáneas para cada clave creada;	Cumple
2.236)	La solución debe implementar el protocolo IEEE 802.1X con la asociación dinámica de VLAN para los usuarios basados en los atributos proporcionados por los servidores RADIUS;	Cumple
2.237)	La solución debe implementar el mecanismo de cambio de autorización dinámica a 802.1X, conocido como RADIUS CoA (Change of Authorization) para autenticaciones 802.1X;	Cumple
2.238)	La solución debe admitir los siguientes métodos de autenticación EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP;	Cumple
2.239)	La solución debe implementar la característica de autenticación de los usuarios a través de la página web HTTPS, también conocido como Captive Portal. La solución debe limitar el acceso de los usuarios mientras éstos no informen las credenciales válidas para el acceso a la red;	Cumple
2.240)	La solución debe permitir el hospedaje del captive portal en la memoria interna del controlador inalámbrico;	Cumple

2.241)	La solución debe permitir la personalización de la página de autenticación, de forma que el administrador de red sea capaz de cambiar el código HTML de la página web con formato de texto e insertar imágenes;	Cumple
2.242)	La solución debe permitir la recopilación del correo electrónico de los usuarios como método de autorización para ingreso a la red;	Cumple
2.243)	La solución debe permitir que la página de autenticación se quede alojada en un servidor externo;	Cumple
2.244)	La solución debe permitir el registro de cuentas para usuarios visitantes en la memoria interna. La solución debe permitir que sea definido un período de validez para la cuenta creada;	Cumple
2.245)	La solución debe garantizar que los usuarios se autentiquen en el portal cautivo que utilice la dirección IPv6;	Cumple
2.246)	La solución debe tener interfaz gráfica para administrar y gestionar las cuentas de usuarios visitantes, no permitiendo acceso a las demás funciones de administración de la solución;	Cumple
2.247)	Después de la creación de un usuario visitante, la solución debe enviar las credenciales por e-mail al usuario registrado;	Cumple
2.248)	La solución debe implementar la función de DHCP Server (IPv4 y IPv6) para facilitar la configuración de las redes de visitantes;	Cumple
2.249)	La solución debe identificar automáticamente el tipo de equipo y sistema operativo utilizado por el dispositivo conectado a la red inalámbrica;	Cumple
2.250)	La solución debe permitir que los usuarios puedan acceder a los servicios disponibles a través del protocolo Bonjour (L2) y que estén alojados en otras subredes, como AirPlay y Chromecast. Debe ser posible especificar en qué VLANs el servicio estará disponible;	Cumple
2.251)	La solución debe permitir la configuración de redes Mesh entre los puntos de acceso administrados por ella;	Cumple
2.252)	La solución debe permitir la configuración de red Mesh entre puntos de acceso indoor y outdoor;	Cumple
2.253)	La solución debe permitir ser administrada a través de los protocolos HTTPS y SSH vía IPv4 e IPv6;	Cumple
2.254)	La solución debe permitir el envío de los Logs a múltiples servidores externos de syslog;	Cumple
2.255)	La solución debe permitir ser administrada a través del protocolo SNMP (v1, v2c y v3), además de emitir notificaciones a través de la generación de traps;	Cumple
2.256)	La solución debe permitir que los softwares de gestión realicen consultas directamente en los puntos de acceso a través del protocolo SNMP;	Cumple
2.257)	La solución debe incluir soporte para las RFC 1213 (MIB II) y RFC 2665 (Ethernet-like MIB);	Cumple
2.258)	La solución debe permitir la captura de paquetes en la red inalámbrica y exportarlos en archivos en formato .pcap;	Cumple
2.259)	La solución debe permitir la adición de planta baja del pavimento para ilustrar gráficamente la posición geográfica y el estado de operación de los puntos de acceso administrados por ella. Debe permitir la adición de plantas bajas en los siguientes formatos: JPEG, PNG, GIF o CAD;	Cumple
2.260)	La solución debe presentar gráficamente la topología lógica de la red, representar los elementos de la red gestionados, además de información sobre los usuarios conectados con la cantidad de datos	Cumple

	transmitidos y recibidos por ellos;	
2.261)	La solución debe implementar la administración unificada y de forma gráfica para redes WiFi y redes cableadas;	Cumple
2.262)	La solución debe permitir la actualización de firmware del controlador inalámbrico incluso cuando se conecta de forma remota;	Cumple
2.263)	La solución debe permitir la identificación del firmware utilizado por cada punto de acceso administrado y permitir la actualización individualizada a través de interfaz gráfica;	Cumple
2.264)	La solución debe tener herramientas de diagnóstico y depuración;	Cumple
2.265)	La solución debe soportar la comunicación con elementos externos a través de las API;	Cumple
2.266)	La solución deberá ser compatible y administrar los puntos de acceso de este proceso;	Cumple

Descripción	**Especificaciones Técnicas SWITCH** Especificaciones técnicas mínimas: - Switch L2/L3 básico - IPv4/IPv6 con enrutamiento estático. RIPv1/v2, OSPF, PIM, PBR - 24 puertos 1000Base-T - Con 4 puertos 1GbE SFP

Marca: ARUBA
Modelo: ARUBA 2930F 24 G PoE + 4SFP – JL255A

Descripción	Características Generales	Cumple / No Cumple
Formato	Fixed de 1 RU	Cumple
Interfaces en el chasís	Debe incluir mínimo: - 24 puertos 10/100/1000Base-T, Auto-MDIX y al menos 4 puertos de 1 GbE SFP - Un (1) puerto consola de personalidad dual (RJ-45 o USB micro-B)	Cumple
Stacking	Capacidad de conectarse en stack con otros equipos de la misma familia: - Los equipos que son parte del stack deberán comportarse como un único dispositivo virtual. - El stack debe ser capaz de crecer al menos hasta cuatro (4) equipos de la misma serie. - El stack debe poder ser configurado utilizando interfaces uplink de 1G	Cumple
Rendimiento	Al menos: - Rendimiento: 41 Mpps - Capacidad de conmutación: 56 Gbps. Latencia: - < 3.8 µs (64-byte packets) en 1000 Mb	Cumple
Memoria	Al menos: - RAM: 1 GB - FLASH: 4 GB - Buffer compartido: 12.3 MB.	Cumple
Sistema Operativo	El sistema operativo debe incluir la última versión completa (con todos los protocolos, servicios y funcionalidades que el equipo sea capaz de realizar) liberada por el fabricante a la fecha de la compra.	Cumple

Calidad de Servicio	- Al menos 8 colas por puerto - Priorización de tráfico (IEEE 802.1p) - Priorización de tráfico en L4, basado en puertos TCP/UDP - CoS (Class of Service) en base a la dirección IP, al ToS (Type of Service) IP, al protocolo Layer 3, al número de puerto TCP/UDP, al puerto de origen y a DiffServ - Función rate limiting que permita establecer máximos obligados de ingreso por puerto y mínimos por puerto, por cola - DSCP	Cumple
Conectividad	- Auto-MDIX en todos los puertos 10/100/1000 - Soporte de IEEE 802.3at y 802.3af - LLDP-MED (Media Endpoint Discovery) - IEEE 802.1AB LLDP (Link Layer Discovery Protocol) - IPv6 host permite que los switches se administren en una red IPv6 - Dual stack (IPv4 y IPv6) transiciona de IPv4 a IPv6, soportando conectividad para ambos protocolos - MLD snooping reenvía tráfico multicast IPv6 a la interface apropiada - IPv6 ACL/QoS soporta ACL y QoS para tráfico de red IPv6 - El enrutamiento IPv6 soporta los protocolos estático y RIPng - La seguridad proporciona RA guard, protección DHCPv6, dynamic IPv6 lockdown y ND snooping	Cumple
Consumo energético	- Fuente de alimentación certificada en 80 PLUS Silver (aumenta la eficiencia y el ahorro de energía). - Soporte para EEE (Energy-efficient Ethernet) reduce el consumo de potencia de conformidad con IEEE 802.3az	Cumple
Multicast	- IGMP (Internet Group Management Protocol) v1, v2 y v3 - IGMP Snooping - IGMP MLD - IP Multicast routing: PIM Sparse y Dense (hasta 16 interfaces)	Cumple
Resiliencia y Alta Disponibilidad	- STP - RSTP - MSTP - RPVST+ - STP Root guard - STP BPDU port protection - VRRP (Virtual Router Redundancy Protocol) para redes IPv4 y IPv6 (limitado a 128 VRs). - LACP (IEEE 802.3ad link aggregation control protocol). Soporta hasta 128 troncales estáticas, dinámicas, o distribuidas activas (por stack) y cada unos de estas troncales hasta 8 puertos.	Cumple
Administración	- SNMPv1, v2 y v3 - Manejo de al menos dos (2) imágenes de sistema operativo en modo primario y secundario. - Se permite almacenar multiples archivos de configuración en la memoria flash - RMON, XRMON y sFlow - UDLD (unidirectional link detection)	Cumple
Switching L2	- IEEE 802.1Q, Soporte de 4,094 VLAN Ids (2000 vlans en simultáneo) - Paquetes jumbo de hasta 9,220 bytes - IEEE 802.1v - GVRP y MVRP - Protocolo de encapsulación VxLAN (tunelización) - MAC Address table: 32,678	Cumple
Routing L3	- Enrutamiento estático - ECMP	Cumple

	- RIP (Routing Information Protocol) proporciona enrutamiento RIPv1, RIPv2 y RIPng - OSPF v2 y v3 - PBR (Policy Based Routing) hasta 16 rutas de siguiente salto - 2,000 rutas IPv4, 1,000 rutas IPv6 en hardware, 200 rutas OSPF, 256 estáticas y 10,000 rutas RIP	
Seguridad	- Configuración de políticas de plano de control que establecen rate limits que protegen a la sobrecarga del CPU originada por ataques DOS. - Múltiples métodos de autenticación de usuarios: - IEEE 802.1X utiliza un supplicant IEEE 802.1X en el cliente, en conjunto con un servidor RADIUS para autenticar de conformidad con las normas de la industria. - La autenticación basada en Web proporciona un ambiente basado en navegador, similar a IEEE 802.1X, para autenticar clientes que no soportan el supplicant IEEE 802.1X. - Autenticación basada en MAC autentica al cliente con el servidor RADIUS basado en la dirección MAC del cliente. - Flexibilidad de autenticación - Multiple IEEE 802.1X users per port proporciona autenticación de múltiples usuarios IEEE 802.1X por puerto y; evita que un usuario utilice la autenticación IEEE 802.1X de otro usuario. - Esquemas de autenticación concurrentes IEEE 802.1X, Web y MAC por cada switchport aceptarán hasta 32 sesiones de autenticaciones IEEE 802.1X, Web y MAC. - Las ACLs, listas de control de acceso, proporcionan filtrado IP de Capa 3 basado en dirección IP/subred de origen/destino y número de puerto TCP/UDP de origen/destino. - El filtrado de puertos de origen permite que únicamente puertos especificados se comuniquen entre sí. - RADIUS/TACACS+ facilita la administración de seguridad de cada switch, utilizando un servidor de autenticación de contraseñas. - Secure shell cifra todos los datos transmitidos para acceso remoto seguro a la CLI sobre redes IP. - SSL (Secure Sockets Layer) cifra todo el tráfico HTTP, permitiendo acceso seguro al GUI de administración basada en navegador del switch. - Port security permite acceso solamente a direcciones MAC especificadas, las cuales se pueden aprender o ser especificadas por el administrador. - MAC address lockout evita que direcciones MAC configuradas específicas se conecten a la red. - Secure FTP permite la transferencia segura de archivos hacia y desde el switch; protege contra descargas de archivos no deseadas o copiado no autorizado del archivo de configuración de un switch. - Switch management logon security ayuda a asegurar el inicio de sesión de la CLI de un switch, requiriendo opcionalmente autenticación de RADIUS o TACACS+. - STP BPDU port protection bloquea BPDUs (Bridge Protocol Data Units) en puertos que no requieren BPDUs, evitando ataques de BPDUs falsificadas. - DHCP protection bloquea paquetes DHCP desde servidores DHCP no autorizados, evitando ataques denial-of-service. - Dynamic ARP protection bloquea broadcasts ARP desde hosts no autorizados, evitando espionaje o robo de los datos de la red.	Cumple

	- STP root guard protege al puente raíz de ataques maliciosos o de errores de configuración. - Identity-driven ACL permite la implementación de una política de seguridad de acceso altamente granular y flexible y asignación de VLANs específicas a cada usuario autenticado en la red. - Per-port broadcast throttling configura el control de broadcasts selectivamente en puertos uplink con tráfico pesado.	
SDN	Soporte OpenFlow	Cumple
Montaje	Debe traer todos los accesorios para montaje y operación en rack estándar de 19".	Cumple
Alimentación eléctrica	Soporte: - 100 VAC a 240 VAC - 50 Hz a 60 Hz.	Cumple
Medio ambiente	Cumplir al menos: - RoHS - EEE con IEEE 802.3az. Temperatura de operación: - 0°C a 45°C (1500 m.s.n.m.) - 0°C a 40°C (3000 m.s.n.m.) Humedad relativa de operación: - 20% a 95%	Cumple
Simplicidad	- Aprovisionamiento sin intervención humana simplifica la instalación de la infraestructura del switch.	Cumple

Seguidamente y considerando que el sistema de adjudicación del presente llamado es por ***EL TOTAL***, en base al Art. 61 del Decreto Reglamentario Nº 21.909/03, se selecciona provisoriamente a la oferta de la empresa con el precio más bajo, siendo la misma **PARASOFT S.R.L.,** la que será analizada en detalle para verificar su cumplimiento con otros requisitos, como Capacidad Legal y su Experiencia para cumplir con el Contrato. Si dicha oferta cumple sustancialmente con todos los requerimientos será declarada calificada y propuesta para la adjudicación. En caso de no serlo, se procederá a rechazar dicha oferta.-

Firma	Monto
PARASOFT S.R.L.	77.638.000.-

A continuación y en base al Art. 61 inc. 3 del Decreto Reglamentario N° 21.909/03 y al Art. 63 del Decreto Reglamentario Nº 2992/19, el Comité procede a verificar las demás documentaciones requeridas en la Carta de Invitación que a continuación se detallan: -

DOCUMENTACIONES	PARASOFT S.R.L.
CAPACIDAD LEGAL	
Fotocopia simple de la cedula tributaria del oferente (RUC)	Presenta **Cumple**
Constancia de inscripción en el Registro Único de Contribuyentes.	Presenta **Cumple**
Certificado de Cumplimiento Tributario	Presenta **Cumple**
Patente comercial del municipio en donde esté asentado el establecimiento principal del oferente	Presenta **Cumple**

Declaración Jurada en la que se garantice que el Oferente no se encuentre involucrado en prácticas que violen los derechos de los menores estipulados en la Constitución Nacional, los Convenios 138 y 182 de la Organización Internacional del Trabajo (OIT), el Código del Trabajo, Código de la Niñez y la Adolescencia, demás leyes y normativas vigentes en la República del Paraguay, conforme al formato aprobado por la Dirección Nacional de Contrataciones Públicas en la Resolución DNCP Nº 941/2010.	Presenta **Cumple**
EXPERIENCIA y CAPACIDAD FINANCIERA	
Demostrar la experiencia en (tres) años como mínimo en provisión de equipos de computación con facturaciones de venta y/o recepciones finales por un monto equivalente al **30% como mínimo** del monto total ofertado en la presente licitación de los años: **2017, 2018, 2019 (Copias de facturaciones y/o recepciones).**	Presenta Año 2017 **Gs. 1.235.850.000** Año 2018 **Gs. 152.000.000** Año 2019 **Gs. 46.420.000** **Cumple**
a. **Ratio de Liquidez:** activo corriente / pasivo corriente Deberá ser igual o mayor que 1, en promedio, en los 2 últimos años (2017 - 2018). b. **Endeudamiento:** pasivo total / activo total No deberá ser mayor a 0,80 en promedio, en los 2 últimos años (2017 - 2018). c. **Rentabilidad:** Porcentaje de utilidad después de impuestos o pérdida con respecto al Capital. El promedio en los en los 2 últimos años, no deberá ser negativo (2017 - 2018).	**Cumple**
Copia del Balance General y Cuadro de Estado de Resultados de los años 2017 y 2018.	Presenta **Cumple**
OTROS DOCUMENTOS	
Certificado de Producto y Empleo Nacional, emitido por el MIC	Presenta Certificado Nº 85.021 Vencimiento 04/12/2020 **Cumple**
Constancia de presentación de la "Declaración Jurada de bienes y rentas, activos y pasivos" ante la Contraloría General de la República, para los sujetos obligados en el marco de la Ley N° 6355/19.	Presenta Acción de Inconsticucionalidad A.I. N° 240/2020 **Cumple**
Certificado de cumplimiento con el Seguro Social.	Presenta Certificado N° 269876 Vencimiento 20/09/2020 **Cumple**

Cuadro de Análisis Financiero

PARASOFT S.R.L.		2017		2018		PROMEDIO
Ratio de Liquidez: activo corriente / pasivo corriente - Deberá ser igual o mayor que 1, en promedio de los últimos 2 (dos) últimos ejercicios fiscales (2017 - 2018)	AC	20.065.276.330	1,5	16.158.568.608	2,2	1,85
	PC	13.477.111.284		7.315.060.671		
Endeudamiento: pasivo total / activo total - No deberá ser mayor a 0,80 en promedio de los últimos 2 (dos) últimos ejercicios fiscales (2017 - 2018)	PT	13.477.111.284	0,4	7.315.060.671	0,3	0,35
	AT	31.379.170.037		26.113.408.702		
Rentabilidad: Porcentaje de utilidad después de impuestos o pérdida con respecto al Capital - El promedio de los últimos 2 (dos) últimos ejercicios fiscales (2017 - 2018), no deberá ser negativo.	UTILIDAD	14.521.606.565	1116%	15.343.731.433	1180%	11,48
	CAPITAL	1.300.768.000		1.300.768.000		

Resumen de Facturación

PARASOFT S.R.L.

AÑO	*Nro*	*Monto*
2.017	3.384	1.235.850.000
2.018	4.266	152.000.000
2.019	4.623	46.420.000
Monto total		**1.434.270.000**

ORIGEN NACIONAL

La firma ***PARASOFT S.R.L.***, ha presentado con su oferta al momento de la Apertura, Certificado de Origen de Producto y Empleo Nacional Nº 85.021 con fecha de vencimiento 04/12/2020, por consiguiente cumple con las formalidades requeridas en la Carta de Invitación y conforme a las reglamentaciones legales vigentes.

MARGEN DE PREFERENCIA LOCAL

Para contrataciones realizadas por Unidades Operativas que se encuentren conformadas dentro de un municipio o departamento se deberá considerar que, si la oferta evaluada como las más baja pertenece una firma u empresa domiciliada fuera del territorio departamental de la convocante, ésta será comparada con la oferta más baja de la firma u empresa domiciliada dentro del territorio de la convocante agregándole al precio total de la oferta propuesta por la primera una suma del diez por ciento (10%) del precio. Si en dicha comparación adicional la oferta de la firma u empresa domiciliada dentro del territorio departamental de la convocante resultare ser la más baja, se la seleccionará para la adjudicación; en caso contrario se seleccionará la oferta de servicios de la firma u empresa domiciliada fuera del territorio departamental de la convocante.

En el caso de que el oferente, sea de la zona y además cuente con margen de preferencia nacional, se le aplicará únicamente el margen de este último.

Por lo tanto, este Comité no considera aplicar el Margen de Preferencia, atendiendo que no existen razones para la evaluación del punto mencionado, considerando que la firma ***PARASOFT S.R.L.,*** se encuentra dentro del territorio departamental.-

ANALISIS DE PRECIOS OFERTADOS

Con referencia al **Análisis de precios ofertados**: y teniendo en cuenta la **RESOLUCIÓN DNCP Nº 1890/2020:** "POR LA CUAL SE REGULA LA ESTIMACION DE PRECIOS Y SU PUBLICIDAD EN LOS PROCEDIMIENTOS DE CONTRATACIONES PUBLICAS EN EL MARCO DE LA LEY 2051/03"

Artículo 4º APROBACION DEL CRITERIO DE EVALUACION APLICABLE AL ANÁLISIS DE LOS PRECIOS DE REFERENCIA:

Análisis de precios ofertados: Durante la evaluación de las ofertas, luego de haber realizado la corrección de errores aritméticos y ordenar las ofertas presentadas de menor a mayor, el Comité de Evaluación procederá a solicitar a los eferentes una explicación detallada de la composición del precio ofertado de cada ítems, rubro o partida adjudicable, conforme a los siguientes parámetros:

1. En contrataciones en general: cuando la diferencia entre el precio ofertado y el precio referencial sea superior al 25% para ofertas por debajo del precio referencial y del 15% para ofertas que se encuentren por encima del referencial establecido por la convocante y difundido con el llamado a contratación.

Si el oferente no respondiese la solicitud, o la respuesta no sea suficiente para justificar el precio ofertado del bien o servicio, el precio será declarado inaceptable y la oferta rechazada.

El análisis de los precios, con esta metodología, será aplicado a cada ítem, rubro o partida que componga la oferta y en cada caso deberá ser debidamente fundada la decisión adoptada por la Convocante en el ejercicio de su facultad discrecional.

Seguidamente se procede a la comparación del precio ofertado y el precio de referencia de la firma ***PARASOFT S.R.L.,*** siendo cuanto sigue:

VARIACION - PARASOFT S.R.L.

Item	Código Catalogo	Descripción del Servicio	Unidad de Medida	Presentación	Cantidad	Precio Unitario (IVA incluido)	Precio Referencial	Variacion Gs.	Porcentaje Variacion
1	43222609-001	Routers de red	Unidad	Unidad	1	22.324.000	23.980.000	(1.656.000)	(7)
2	43201410-001	Switchs	Unidad	Unidad	9	6.146.000	8.020.000	(1.874.000)	(23)

Teniendo en cuenta que la firma ***PARASOFT S.R.L.,*** cumple con lo establecido en la Resolución DNCP Nº 1890/2020, con referencia al precio ofertado y el precio de referencia, este Comité de Evaluación NO ha procedido a solicitar una explicación detallada de la composición de los precios ofertados, por lo que es una oferta **"EVALUABLE"**, y se prosigue con la Evaluación del presente llamado.

ANALISIS DE CAPACIDAD LEGAL DE LOS OFERENTES RESPECTO A LA PROHIBICIÓN PREVISTA EN EL *Inc. "a y b" del Artículo 40.*

Seguidamente el Comité verifica la capacidad legal de los oferentes respecto a la prohibición prevista en el ***Inciso "a":*** *Verificará los registros del personal de la convocante para detectar si el Oferente o sus representantes, se hallan comprendidos en el presupuesto del inciso "a" del artículo 40 y* al ***Inciso b):*** *Verificará por los medios disponibles, si el Oferente y los demás sujetos individualizados en las prohibiciones contenidas en la Ley Nº 1626/00 "De la Función Pública", aparecen en la base de datos del SINARH* ***o bien*** *de la Secretaría de la Función Pública de los siguientes representantes:*

PARASOFT S.R.L.

CARLOS ARMANDO JORGE RAUL GUGGIARI DOUTRELEAU con CI Nº 636.489; *No Registra Datos ni Antecedentes*, según Certificado Nº 514108 de la Secretaria de la Función Pública; por tanto ***CUMPLE*** con lo establecido *para la Calificación de la Capacidad Legal del Oferente con respecto a la Prohibición Prevista en los* ***Incisos "a" y "b" del artículo 40*** *- de la Ley N° 2051/03 "De Contrataciones Públicas".-*

JUAN PABLO AGUILA BRAVO con CI Nº 1.341.894; *No Registra Datos ni Antecedentes*, según Certificado Nº 514118 de la Secretaria de la Función Pública; por tanto ***CUMPLE*** con lo establecido *para la Calificación de la Capacidad Legal del Oferente con respecto a la Prohibición Prevista en los* ***Incisos "a" y "b" del artículo 40*** *- de la Ley N° 2051/03 "De Contrataciones Públicas".-*

Teniendo en cuenta lo expuesto la firma **PARASOFT S.R.L.**, cumple con lo establecido en la Resolución DNCP N° 849/15, *Para la Calificación de la Capacidad Legal del Oferente con respecto a la Prohibición Prevista En Los Incisos "a" y "b" del artículo 40 - de la Ley N° 2051/03 "De Contrataciones Públicas", siendo una* ***OFERTA EVALUABLE;*** *y se prosigue con el evaluación del presente llamado*

ANALISIS DEL *Inc. "K" que dice... "las personas físicas o jurídicas que se encuentren en mora como deudores del fisco o la seguridad social"; del Artículo 40 de la Ley 2051/03 de Contrataciones Públicas.-*

Con relación a la Circular DNCP Nº 29/2017, y la Resolución C.A. N° 49 – 019/17 de fecha 18 de julio del corriente "POR LA CUAL SE ESTABLECE EL PROCEDIMIENTO A SER APLICADO POR LOS ORGANISMOS Y ENTIDADES DEL ESTADO PARA EL CUMPLIMIENTO DE LO ESTABLECIDO EN EL DECRETO Nº 6121/16 "POR EL CUAL SE REGLAMENTA EL INC. K) DEL ARTÍCULO 40º DE LA LEY Nº 2051/03 DE CONTRATACIONES PÚBLICAS:

La firma **PARASOFT S.R.L.**, presenta ***Constancia de SIPE Nº 1609207***, y Certificado de Cumplimiento con el Seguro Social Nº 269876 en la que se encuentra el *Estado de Cuenta de Patronal(es) del Instituto de Previsión Social (I.P.S.)*, con una Cantidad de Empleados de (12) doce, con vencimiento 20/09/2020, *el cual es proporcionada por la Institución Pública competente y extraída de su Base de Datos*.-

Teniendo en cuenta lo expresado la firma, **PARASOFT S.R.L.**, cumple con lo dispuesto en el **Inc. "K"** que dice... *"las personas físicas o jurídicas que se encuentren en mora como deudores del fisco o la seguridad social"*; del **Artículo 40 de la Ley 2051/03** de Contrataciones Públicas, *siendo una* ***OFERTA EVALUABLE.***-

DISPONIBILIDAD PRESUPUESTARIA

Para el presente llamado se ha previsto en el **PAC N° 384.396** un monto total de **Gs. 96.160.000 (Guaraníes Noventa y Seis Millones Ciento Sesenta Mil)** para el presente año fiscal, según Certificado de Disponibilidad Presupuestaria – CDP Nº 341/2020.-

Tip	Pro	Pry	Obj.	Fue.	Fin.	UnR.	Descripción	Certificación Actual
1	001	02	540	30	84	26	Adquisición de Equipos de Oficina y Computación	96.160.000.-

RECOMENDACIÓN

Del Análisis realizado, se concluye que la firma: **PARASOFT S.R.L.**, cumple con la totalidad de los requisitos establecidos en la Carta de Invitación, por ende resulta ser **"OFERTA CALIFICADA"** y propuesta para la Adjudicación.-

Conforme a lo dispuesto en el Art. 28 de la Ley 2051/03 de Contrataciones Públicas, y de acuerdo al Art. 65 del Decreto Reglamentario Nº 2.992/2019; "*....la adjudicación deberá recaer en el oferente cuya oferta: a) Cumpla con las condiciones legales y técnicas estipuladas en el PBC; b) Tenga las calificaciones y la Capacidad necesarias para ejecutar el Contrato; c) Presente el precio evaluado como el más bajo*", este Comité de Evaluación recomienda adjudicar "salvo otro parecer" de la máxima autoridad de la institución y, conforme al **"Cuadro de Precios Adjudicados"** a la firma **PARASOFT S.R.L.**, por un Monto Total de ***Gs. 77.638.000 (Guaraníes Setenta y Siete Millones Seiscientos Treinta y Ocho Mil) IVA Incluido.***

Forma parte integrante de este Informe los siguientes:

- Acta de Apertura N° 16/2020 (Prórroga)
- Acta de Apertura Nº 19/2020,
- Cuadro Comparativo de Precios,
- Cuadro de Precios Adjudicados,
- Certificado de Disponibilidad Presupuestaria Nº 341/2020

Se solicita realizar las gestiones pertinentes del presente llamado, Resolución Ministerial mediante, según la recomendación del Comité de Evaluación y comunicar oficialmente a quienes corresponda. -

Finalizado el acto, previa lectura y ratificación de su contenido, siendo las 11:00 hs. del 10 de Setiembre del corriente, suscriben las partes intervinientes en prueba de conformidad, en 2 (dos) ejemplares de un mismo tenor y a un solo efecto.-

Lic. SERGIO SUAREZ GUANES
Representante de la Dirección General de la DINCAP

Econ. RODY CENTURION
Representante de la Dirección de Administración Financiera (DAF) de la DINCAP-MAG

Lic. SERGIO FIGUEREDO LEZCANO
Representante de la Dirección de Administración Financiera (DAF) de la DINCAP-MAG

GOBIERNO NACIONAL

Secretaría de la Función Pública

https://www.sfp.gov.py

Constancia Nro.
514108
514108

Consulta de ser o no Funcionario/a Público/a

https://www.paraguay.gov.py

CERTIFICO, que CARLOS ARMANDO JORGE RAUL GUGGIARI DOUTRELEAU, ciudadano/a de nacionalidad PARAGUAYA, mayor de edad, con Cédula de identidad Civil N° 636489, se consta que los datos personales, en las bases de datos consultadas por la Secretaría de la Función Pública SFP a la fecha de expedición de la Constancia, como funcionario/a en situación permanente, o contratado/a en los Organismos de la Administración Central y Entes Descentralizados, salvo casos de homonimias.

BASES DE DATOS CONSULTADAS

Sistema Nacional de Administración de RRHH (SINARH)

Cédula	Institución	Cargo	Vínculo	Mes/Año	Objeto de Gasto

No registra datos

Nómina de Funcionarios Permanentes o Contratados (Altas y Bajas)

Cédula	Institución	Cargo	Vínculo	Mes/Año	Objeto de Gasto	Movimiento

No registra datos

AVISO LEGAL PARA TODAS LAS CONSTANCIAS DE SER O NO FUNCIONARIO PÚBLICO

Una de las atribuciones de la Secretaría de la Función Pública (SFP) es la de organizar y mantener actualizado un registro sexado de todos los funcionarios públicos tal como lo estipula la Ley 1626/2000 "De la Función Pública", en el inciso b) Artículo 96.

El Decreto 1212/2014 aprueba la implementación del Portal Único del Empleo Público Paraguay Concursa y la puesta en funcionamiento del Sistema Integrado Centralizado de la Carrera Administrativa – SICCA, bajo la administración de la SFP.

Los OEE deben remitir en forma mensual (hasta el decimoquinto día hábil de cada mes) un reporte de su institución sobre los registros del ingreso (altas) y desvinculación (bajas) de sus funcionarios públicos, dentro de los primeros quince (15) días hábiles de cada mes, según lo dispuesto en el Art. 109 del Decreto N° 3264/2020; sin embargo, no todas las instituciones públicas lo cumplen en los plazos establecidos, por lo que la información con la que cuenta la SFP no es absoluta. De las instituciones que cumplen con la remisión de sus altas y bajas en tiempo y forma no podemos certificar la información remitida, y se adjunta la que bajo responsabilidad sobre la correctitud y confiabilidad de cada Organismo y Entidad del Estado se ha enviado a la SFP.

Tanto el decreto reglamentario de la Ley de Presupuesto N° 3264/2020 como el Decreto N° 7792/2006 "Por la cual se dispone que las instituciones de la Administración Central, Entes Autónomos y Autárquicos, comuniquen a la Secretaría de la Función Pública, dependiente de la Presidencia de la República, los nombramientos, destituciones, renuncias, fallecimientos y permisos de los funcionarios públicos", se hallan vigentes a la fecha y disponen manifiestamente que todas las instituciones debe comunicar a la SFP datos estadísticos precisos concernientes a los nombramientos, desvinculaciones, renuncias o cualquier información relevante con respecto al movimiento de los recursos humanos; aún así, no todas lo cumplen, por lo que esta Secretaría Ejecutiva solo cuenta con información parcial, y la pertinente a la prensa consultada se halla en este extracto.

La SFP ha implementado en el SICCA un Sistema Online para la remisión de planillas de Altas y Bajas a través del cual todos los Organismos

Fecha de Emisión: 08/09/2020 14:10

GOBIERNO NACIONAL

Secretaría de la Función Pública a través del Sistema de Intercambio de Información
Decreto N° 3264/2020

Código de Verificación: **305632a6**
Verifique la validez de este documento
https://www.paraguay.gov.py/validar

GOBIERNO NACIONAL

Secretaría de la Función Pública

https://www.sfp.gov.py

Constancia Nro.
514108
514108

y Entidades del Estados (OEE) deben enviar en formato digital los datos de sus funcionarios PERMANENTES, CONTRATADOS y COMISIONADOS en el marco del cumplimiento de las leyes anuales de Presupuesto General de la Nación, en donde en concordancia con el Art. 96 inc b) de la Ley N° 1626/2000 "De la Función Pública", se dispone la obligatoriedad de la provisión de datos de funcionarios permanentes y contratados a la SFP dentro de los 15 días hábiles siguiente al cierre de cada mes calendario.

Los datos que se disponibilizan de las bases de Altas y Bajas para la funcionalidad de las constancias de ser o no funcionarios públicos, son datos que cada OEE ha remitido a la SFP a través del SICCA dando cumplimiento al marco normativo, según los procedimientos reglamentados por la SFP en su carácter de administrador del sistema, que se hallan debidamente publicados en www.paraguayconcursa.gov.py.

La SFP solamente es responsable por la actualización, veracidad, corrección, integridad y calidad los datos que corresponden a la administración del presupuesto y del talento humano de la propia SFP.

Todos los datos publicados por la SFP en el portal de Datos Abiertos deben ser corroborados por las personas físicas o jurídicas que accedan os mismos en los portales de cada institución o a través de las vías previstas para el acceso a la información pública, dispuestas en la ley N° 5282/2014, y reglamentada por Decreto 4064/2015.

La responsabilidad por el uso, manipulación y destino de los datos abiertos publicados por la SFP corresponden exclusivamente a los usuarios de los mismos, quienes pueden utilizarlos en el marco de investigación, información, publicaciones, o cualquier otra actividad lícita protegida o no por derechos de autor, reservándose la SFP en todos los casos la atribución de emitir comunicados valorando la coherencia de los datos manipulados por los usuarios del sistema con la base original administrada por esta institución.

Todos los derechos intelectuales sobre la producción del sistema utilizado para la publicación, así como del SICCA y los materiales publicados, son propiedad de la SFP y se hallan accesibles gratuitamente, con el reconocimiento de la fuente por los usuarios.

Las Constancias de ser o no funcionario público tendrá validez a fin de ser utilizada en los siguientes casos:

a) Incorporación de servidores públicos por nombramientos o contrataciones, y para los procesos de selección que correspondan, sin perjuicio de los demás requisitos para la validez de las vinculaciones; concordante con el Art. 164 del Decreto N° 3264/2020.
b) Para las personas seleccionadas a través de procesos de Concursos Públicos de Oposición y/o Concursos de Méritos.
c) En los procesos para la contratación de bienes y servicios en el marco de la Ley 2051/03, sin perjuicio del análisis que cada entidad adjudicataria y la Dirección Nacional de Contrataciones Públicas (DNCP) deban realizar sobre la pertinencia de la contratación;
d) Para lagestión de devolución de aportes jubilatorios en las Entidades Públicas de Seguridad Social, sin perjuicio de los tramites que para el efecto cada una de las Cajas prevea en caso de ser pertinente;
e) Para inscripción al Programa de Retiro Voluntario;
f) Para registro de profesionales Despachantes de Aduanas ante la Dirección Nacional de Aduanas, sin perjuicio de los demás requisitos previstos en la normativa vigente.
g) Para matriculación de Peritos ante la Corte Suprema de Justicia, sin perjuicio de los demás tramites a ser realizados para el efecto;
h) Para elacceso a dicha información de personas físicas, e instituciones públicas y privadas que los requieran para otros fines, incluyendo a Juzgados que dependan de la Corte Suprema de Justicia, Agentes Fiscales del Ministerio Público, acuerdos con Universidades Públicas y Privadas, Entidades Financieras y Cooperativas, entre otras.

Conforme a lo dispuesto en los Artículos 13 y 14 del Decreto N° 8709/2018, toda información y documentos obtenidos mediante el Servicio del Portal Único de Gobierno, proveniente del Sistema de Intercambio de Información, poseen plena validez para la gestión de servicios o trámites en la administración pública.

Fecha de Emisión: 08/09/2020 14:10

GOBIERNO NACIONAL

Secretaría de la Función Pública a través del Sistema de Intercambio de Información
Decreto N° 3264/2020

Código de Verificación: **305632a6**
Verifique la validez de este documento
https://www.paraguay.gov.py/validar

GOBIERNO NACIONAL

Secretaría de la Función Pública

https://www.sfp.gov.py

Constancia Nro. 514118

514118

Consulta de ser o no Funcionario/a Público/a

https://www.paraguay.gov.py

CERTIFICO, que JUAN PABLO AGUILA BRAVO, ciudadano/a de nacionalidad PARAGUAYA NATURALIZADA, mayor de edad, con Cédula de identidad Civil N° 1341894, se consta que los datos personales, en las bases de datos consultadas por la Secretaría de la Función Pública SFP a la fecha de expedición de la Constancia, como funcionario/a en situación permanente, o contratado/a en los Organismos de la Administración Central y Entes Descentralizados, salvo casos de homonimias.

BASES DE DATOS CONSULTADAS

Sistema Nacional de Administración de RRHH (SINARH)

Cédula	Institución	Cargo	Vínculo	Mes/Año	Objeto de Gasto

No registra datos

Nómina de Funcionarios Permanentes o Contratados (Altas y Bajas)

Cédula	Institución	Cargo	Vínculo	Mes/Año	Objeto de Gasto	Movimiento

No registra datos

AVISO LEGAL PARA TODAS LAS CONSTANCIAS DE SER O NO FUNCIONARIO PÚBLICO

Una de las atribuciones de la Secretaría de la Función Pública (SFP) es la de organizar y mantener actualizado un registro sexado de todos los funcionarios públicos tal como lo estipula la Ley 1626/2000 "De la Función Pública", en el inciso b) Artículo 96.

El Decreto 1212/2014 aprueba la implementación del Portal Único del Empleo Público Paraguay Concursa y la puesta en funcionamiento del Sistema Integrado Centralizado de la Carrera Administrativa – SICCA, bajo la administración de la SFP.

Los OEE deben remitir en forma mensual (hasta el decimoquinto día hábil de cada mes) un reporte de su institución sobre los registros del ingreso (altas) y desvinculación (bajas) de sus funcionarios públicos, dentro de los primeros quince (15) días hábiles de cada mes, según lo dispuesto en el Art. 109 del Decreto N° 3264/2020; sin embargo, no todas las instituciones públicas lo cumplen en los plazos establecidos, por lo que la información con la que cuenta la SFP no es absoluta. De las instituciones que cumplen con la remisión de sus altas y bajas en tiempo y forma no podemos certificar la información remitida, y se adjunta la que bajo responsabilidad sobre la correctitud y confiabilidad de cada Organismo y Entidad del Estado se ha enviado a la SFP.

Tanto el decreto reglamentario de la Ley de Presupuesto N° 3264/2020 como el Decreto N° 7792/2006 "Por la cual se dispone que las instituciones de la Administración Central, Entes Autónomos y Autárquicos, comuniquen a la Secretaría de la Función Pública, dependiente de la Presidencia de la República, los nombramientos, destituciones, renuncias, fallecimientos y permisos de los funcionarios públicos", se hallan vigentes a la fecha y disponen manifiestamente que todas las instituciones debe comunicar a la SFP datos estadísticos precisos concernientes a los nombramientos, desvinculaciones, renuncias o cualquier información relevante con respecto al movimiento de los recursos humanos; aún así, no todas lo cumplen, por lo que esta Secretaría Ejecutiva solo cuenta con información parcial, y la pertinente a la prensa consultada se halla en este extracto.

La SFP ha implementado en el SICCA un Sistema Online para la remisión de planillas de Altas y Bajas a través del cual todos los Organismos y Entidades del Estados (OEE) deben enviar en formato digital los datos de sus funcionarios PERMANENTES, CONTRATADOS y

Fecha de Emisión: 08/09/2020 14:12

GOBIERNO NACIONAL

Secretaría de la Función Pública a través del Sistema de Intercambio de Información
Decreto N° 3264/2020

Código de Verificación: **44051bc1**

Verifique la validez de este documento

https://www.paraguay.gov.py/validar

GOBIERNO NACIONAL

Secretaría de la Función Pública

https://www.sfp.gov.py

Constancia Nro.
514118
514118

COMISIONADOS en el marco del cumplimiento de las leyes anuales de Presupuesto General de la Nación, en donde en concordancia con el Art. 96 inc b) de la Ley N° 1626/2000 "De la Función Pública", se dispone la obligatoriedad de la provisión de datos de funcionarios permanentes y contratados a la SFP dentro de los 15 días hábiles siguiente al cierre de cada mes calendario.

Los datos que se disponibilizan de las bases de Altas y Bajas para la funcionalidad de las constancias de ser o no funcionarios públicos, son datos que cada OEE ha remitido a la SFP a través del SICCA dando cumplimiento al marco normativo, según los procedimientos reglamentados por la SFP en su carácter de administrador del sistema, que se hallan debidamente publicados en www.paraguayconcursa.gov.py.

La SFP solamente es responsable por la actualización, veracidad, corrección, integridad y calidad los datos que corresponden a la administración del presupuesto y del talento humano de la propia SFP.

Todos los datos publicados por la SFP en el portal de Datos Abiertos deben ser corroborados por las personas físicas o jurídicas que accedan a los mismos en los portales de cada institución o a través de las vías previstas para el acceso a la información pública, dispuestas en la ley N° 82/2014, y reglamentada por Decreto 4064/2015.

La responsabilidad por el uso, manipulación y destino de los datos abiertos publicados por la SFP corresponden exclusivamente a los usuarios de los mismos, quienes pueden utilizarlos en el marco de investigación, información, publicaciones, o cualquier otra actividad lícita protegida o no por derechos de autor, reservándose la SFP en todos los casos la atribución de emitir comunicados valorando la coherencia de los datos manipulados por los usuarios del sistema con la base original administrada por esta institución.

Todos los derechos intelectuales sobre la producción del sistema utilizado para la publicación, así como del SICCA y los materiales publicados, son propiedad de la SFP y se hallan accesibles gratuitamente, con el reconocimiento de la fuente por los usuarios.

Las Constancias de ser o no funcionario público tendrá validez a fin de ser utilizada en los siguientes casos:

a) Incorporación de servidores públicos por nombramientos o contrataciones, y para los procesos de selección que correspondan, sin perjuicio de los demás requisitos para la validez de las vinculaciones; concordante con el Art. 164 del Decreto N° 3264/2020.
b) Para las personas seleccionadas a través de procesos de Concursos Públicos de Oposición y/o Concursos de Méritos.
c) En los procesos para la contratación de bienes y servicios en el marco de la Ley 2051/03, sin perjuicio del análisis que cada entidad adjudicataria y la Dirección Nacional de Contrataciones Públicas (DNCP) deban realizar sobre la pertinencia de la contratación;
d) Para lagestión de devolución de aportes jubilatorios en las Entidades Públicas de Seguridad Social, sin perjuicio de los tramites que para el efecto cada una de las Cajas prevea en caso de ser pertinente;
e) Para inscripción al Programa de Retiro Voluntario;
f) Para registro de profesionales Despachantes de Aduanas ante la Dirección Nacional de Aduanas, sin perjuicio de los demás requisitos previstos en la normativa vigente.
g) Para matriculación de Peritos ante la Corte Suprema de Justicia, sin perjuicio de los demás tramites a ser realizados para el efecto;
h) Para elacceso a dicha información de personas físicas, e instituciones públicas y privadas que los requieran para otros fines, incluyendo a Juzgados que dependan de la Corte Suprema de Justicia, Agentes Fiscales del Ministerio Público, acuerdos con Universidades Públicas y Privadas, Entidades Financieras y Cooperativas, entre otras.

Conforme a lo dispuesto en los Artículos 13 y 14 del Decreto N° 8709/2018, toda información y documentos obtenidos mediante el Servicio del Portal Único de Gobierno, proveniente del Sistema de Intercambio de Información, poseen plena validez para la gestión de servicios o trámites en la administración pública.

Fecha de Emisión: 08/09/2020 14:12

GOBIERNO NACIONAL

Secretaría de la Función Pública a través del Sistema de Intercambio de Información
Decreto N° 3264/2020

Código de Verificación: **44051bc1**
Verifique la validez de este documento
https://www.paraguay.gov.py/validar