

PLIEGO DE BASES Y CONDICIONES

Convocante:

Corte Suprema de Justicia (CSJ)
Corte Suprema de Justicia

Nombre de la Licitación:

**ADQUISICIÓN DE EQUIPOS DE CONMUTACIÓN,
SEGURIDAD DE RED DE DATOS Y SOFTWARE DE
REPORTES - PLURIANUAL - AD REFERENDUM - S.B.E.**
(versión 6)

ID de Licitación:

416434



Modalidad:

Concurso de Ofertas

Publicado el:

15/11/2022

"Pliego para la Adquisición de Bienes - SBE"
Versión 1

RESUMEN DEL LLAMADO

Datos de la Convocatoria

ID de Licitación:	416434	Nombre de la Licitación:	ADQUISICIÓN DE EQUIPOS DE CONMUTACIÓN, SEGURIDAD DE RED DE DATOS Y SOFTWARE DE REPORTES - PLURIANUAL - AD REFERENDUM - S.B.E.
Convocante:	Corte Suprema de Justicia (CSJ)	Categoría:	24 - Equipos, accesorios y programas computacionales, de oficina, educativos, de imprenta, de comunicación y señalamiento
Unidad de Contratación:	Corte Suprema de Justicia	Tipo de Procedimiento:	CO - Concurso de Ofertas

Etapas y Plazos

Lugar para Realizar Consultas:	Consultas Virtuales a traves del portal	Fecha Límite de Consultas:	16/11/2022 13:00
Lugar de Entrega de Ofertas:	PALACIO DE JUSTICIA DE ASUNCIÓN - TORRE SUR - 4TO PISO - UOC	Fecha de Entrega de Ofertas:	24/11/2022 09:15
Lugar de Apertura de Ofertas:	PALACIO DE JUSTICIA DE ASUNCIÓN - TORRE SUR - 4TO PISO - UOC	Fecha de Apertura de Ofertas:	24/11/2022 09:30

Adjudicación y Contrato

Sistema de Adjudicación:	Por Total	Anticipo:	20%
Vigencia del Contrato:	Hasta Cumplimiento Total de Obligaciones		

Datos del Contacto

Nombre:	Lic. Liz Fátima Insfrán	Cargo:	DIRECTORA
Teléfono:	424460	Correo Electrónico:	CONTRATACIONES1@PJ.GOV.PY

ADENDA

Adenda

Las modificaciones al presente procedimiento de contratación son los indicados a continuación:

ADENDA N° 05

REF.: LICITACIÓN POR CONCURSO DE OFERTAS PAC N° 53/2022 "ADQUISICIÓN DE EQUIPOS DE CONMUTACIÓN, SEGURIDAD DE RED DE DATOS Y SOFTWARE DE REPORTES - PLURIANUAL - AD REFERENDUM - S.B.E." - ID N° 416.434.

Por la que se introducen modificaciones o enmiendas a las Bases y Condiciones de la contratación de referencia. Los cuales quedan redactados de la siguiente manera:

DATOS DE LA LICITACIÓN

1. COPIAS DE LA OFERTA - CPS

El oferente presentará su oferta original. En caso de que la convocante requiera la presentación de copias lo deberá indicar en este apartado, las copias deberán estar identificadas como tales. Cuando la presentación de ofertas se realice a través del sistema de Oferta Electrónica, la convocante no requerirá de copias.

Cantidad de copias requeridas: 0 copia.

2. PERIODO DE VALIDEZ DE LA GARANTÍA DE CUMPLIMIENTO DE CONTRATO

El plazo de vigencia de la Garantía de Fiel Cumplimiento de Contrato será de: 45 (CUARENTA Y CINCO) MESES, contados desde la entrada en vigor del contrato.

REQUISITOS DE CALIFICACIÓN Y CRITERIOS DE EVALUACIÓN

1. CAPACIDAD TÉCNICA

El oferente deberá proporcionar evidencia documentada que demuestre su cumplimiento con los siguientes requisitos de capacidad técnica:

1. Deberá contar con al menos 4 (cuatro) técnicos certificados en las marcas de los ítems ofertados, de los cuales, 2 (dos) técnicos con certificación de nivel superior y 2 (dos) técnicos con certificación de nivel medio. Los mismos deberán formar parte del plantel de la empresa.
2. La empresa oferente debe contar con autorización del fabricante para proveer los equipos de la marca ofertada, ser servicio técnico autorizado o estar debidamente autorizado por el fabricante o el representante para brindar asistencia para equipos de la marca ofertada.
3. Contar con el aval de al menos 2 (dos) clientes que demuestren haber recibido a satisfacción los trabajos realizados por el Oferente referente a la venta, instalación o configuración de equipos. Dichos documentos deberán corresponder a los años (2019, 2020, 2021).
4. Los equipos ofertados (ítems 1 y 3) deberán contar con Certificación de Calidad ISO 9001:2015 o similar. El mismo deberá ser mínimamente para fabricación. (No se aceptarán certificados de ensamblaje de equipos).
5. Especificaciones técnicas de los bienes ofertados.

- **OFERENTES EN CONSORCIO:** El socio líder debe cumplir al menos con el 60 % (SESENTA POR CIENTO) del requisito y los demás socios en su conjunto al menos el 40 % (CUARENTA POR CIENTO) de este requisito.

• REQUISITO DOCUMENTAL PARA EVALUAR LA CAPACIDAD TÉCNICA

1. Listado de 4 (cuatro) técnicos certificados en la marca de los ítems ofertado, acompañado de la Planilla de Instituto de Previsión Social correspondiente al mes de septiembre de 2022 donde figuren los técnicos propuestos.
 - a. 2 (dos) técnicos con certificación de nivel superior (Ej.: Cisco CCNP, Fortinet NSE7, Sonicwall SNSP), los mismos deberán acompañar la siguiente documentación:
 - Currículum Vitae

- Certificados por la marca de los ítems ofertados
 - Fotocopia de cédula de identidad de los técnicos
- b. 2 (dos) técnicos con certificación de nivel medio (Ej.: Cisco CCNA, Fortinet NSE4, Sonicwall SNSA), los mismos deberán acompañar la siguiente documentación:
- Currículum Vitae
 - Certificados por la marca de los ítems ofertados
 - Fotocopia de cédula de identidad de los técnicos

2. La empresa oferente deberá contar con autorización del fabricante para proveer, instalar y soportar los equipos adquiridos.

Para Representantes debe reunir los siguientes requisitos: Documentación expedida por el Fabricante que los acredite como representante de la marca ofertada y centro autorizado de servicios (CAS), dichos documentos deben estar debidamente legalizados por el Consulado Paraguayo del País de emisión del documento y del Ministerio de Relaciones Exteriores de la República del Paraguay. Los mismos deben ser originales o copias autenticadas por Escribano Público.

Para Distribuidor Autorizado debe reunir los siguientes requisitos: Documentación expedida por el Fabricante que los acredite como distribuidor autorizado de la marca ofertada y centro autorizado de servicios (CAS), para tal efecto debe presentar el documento original o copia autenticada por Escribano Público, y el mismo debe estar debidamente legalizado por el Consulado Paraguayo del País de emisión del documento y del Ministerio de Relaciones Exteriores de la República del Paraguay.

Para Sub-Distribuidor debe reunir los siguientes requisitos: Documento original o copia autenticada por Escribano Público de la autorización del Fabricante extendida al Representante, Distribuidor y/o Resellers para el PARAGUAY Y/O LATINOAMERICA que lo nombra como representante, o distribuidor autorizado de la marca ofertada y centro autorizado de servicios (CAS), en la cual lo autoriza a nombrar sub - distribuidores. Para tal efecto debe presentar el documento original o copia autenticada por Escribano Público, y el mismo debe estar debidamente legalizado por el Consulado Paraguayo del País de emisión del documento y del Ministerio de Relaciones Exteriores de la República del Paraguay.

Serán considerados válidos los documentos apostillados como los documentos legalizados por el Consulado y el Ministerio de Relaciones Exteriores en conformidad a la Ley N° 4987/13 QUE APRUEBA EL CONVENIO SUPRIMIENDO LA EXIGENCIA DE LA LEGALIZACIÓN DE LOS DOCUMENTOS PÚBLICOS EXTRANJEROS.

Cuando la convocante lo requiera, el oferente deberá acreditarse la cadena de autorizaciones, hasta el fabricante o productor.

- **OBSERVACIÓN:**
- La autorización del fabricante debe ser presentada indefectiblemente con la oferta estando o no este documento legalizado o apostillado.
- En caso de que el oferente no cuente con la autorización del fabricante legalizada o apostillada al momento de la presentación de la oferta, se aclara que, para firma del contrato, el oferente adjudicado deberá presentar el documento debidamente legalizado por el Consulado Paraguayo del país de emisión del documento y del Ministerio de Relaciones Exteriores de la República del Paraguay o apostillado en conformidad a la Ley N° 4987/13 QUE APRUEBA EL CONVENIO SUPRIMIENDO LA EXIGENCIA DE LA LEGALIZACIÓN DE LOS DOCUMENTOS PÚBLICOS EXTRANJEROS.
- El documento presentado con la oferta debe presentar identidad con el documento presentado para la firma del contrato.

3. Certificados o constancias de satisfacción de clientes, referente a la venta, instalación o configuración de equipos. Dichos documentos deberán corresponder a los años (2019, 2020, 2021).
4. Certificación de Calidad ISO 9001:2015 o similar. El mismo deberá ser mínimamente para fabricación. (No se aceptarán certificados de ensamble de equipos).
5. Especificaciones técnicas de los bienes ofertados acompañado de Catálogo de cada uno de los ítems ofertados.

SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS

DETALLE DE LOS PRODUCTOS CON LAS RESPECTIVAS ESPECIFICACIONES TÉCNICAS

Los productos a ser requeridos cuentan con las siguientes especificaciones técnicas:

ALCANCE DE LOS TRABAJOS Y SERVICIOS

Los oferentes deben entregar todos los subsistemas del presente llamado en la modalidad de llave en mano, por lo cual deben tener en cuenta todos los equipamientos, accesorios, materiales de instalación, horas de servicio técnico especializado para la correcta implementación de la solución ofertada, de acuerdo con los requerimientos técnicos del presente documento. A continuación, se listan de manera enunciativa y no limitativa algunas de las consideraciones dentro del alcance del presente llamado.

1. El sistema de seguridad perimetral para el Datacenter de la DGRP correspondiente a este documento comprende la provisión,

instalación y configuración del Firewall, Sistema de Reporte y Switches de Acceso para proveer seguridad, alta disponibilidad y gestión a la red de la DGRP.

2. Se deben proveer la cantidad de equipos necesarios que cumplan con los requerimientos mínimos de este documento para soportar los servicios actuales y futuros de voz, datos, video en todas las dependencias del edificio.
3. Se debe considerar que, para la correcta implementación de la solución e integración a los equipos existentes, serán necesarios realizar cambios en la infraestructura actual, para lo cual, la convocante prestará la asistencia necesaria.
4. Queda a cargo de los oferentes, la correcta configuración, implementación e integración de la solución ofertada con la infraestructura actual, de acuerdo a los más altos estándares y mejores prácticas de la industria, contemplando configuración, por mencionar apenas algunas de ellas, hardening, acceso a proveedores, ruteo dinámico y estático externo, ruteo interno local y entre vlans, integración con Active Directory mediante LDAP, políticas de acceso a Internet por usuario y grupos, filtrado web, VPNs, antivirus, IPS, anti malware, anti phishing, ACLs, NAT, port forwarding, publicación de servicios web. El tiempo máximo para el despliegue no deberá superar los 30 días hábiles.

La convocante se reserva el derecho de verificación in situ de las instalaciones de los oferentes de manera a corroborar que los oferentes cuentan con los recursos y capacidad necesaria para proveer este servicio.

Soporte

El soporte requerido deberá ser in-situ e incluir la configuración de los equipos en el formato que la convocante lo exija.

En caso de alguna falla en un equipo, que impida su correcto uso o funcionamiento, se deberá prever un tiempo máximo de respuesta de 4 horas a partir de la comunicación por correo electrónico de la convocante al proveedor. En caso de que el equipo no pueda ser reparado se deberá reemplazar por uno igual o de mayores prestaciones hasta la devolución del equipo reparado; se deberá dejar en funcionamiento todos los servicios con todas las configuraciones. Este soporte es solicitado por el tiempo que dure la Garantía.

La empresa oferente deberá contar con un Centro de Atención al Cliente propio de la empresa y que sea con funcionalidad operativa 7x24 (24 horas del día, los 365 días del año). Este centro de atención debe tener a disposición técnicos de guardia permanente para los casos de asistencia remota o in situ. Además, deberá anexar una documentación donde mencione niveles de escalamiento con números de teléfonos y direcciones de correo, y deberá garantizar que las solicitudes e incidencias sean gestionadas mediante un sistema de Tickets que permita el seguimiento y la gestión de los incidentes hasta su cierre (solución de los mismos). Igualmente, deberá anexar una Declaración Jurada indicando el cumplimiento, así como también la convocante se reserva el derecho de una verificación en sitio del oferente, en caso de que así se requiera.

Capacitación

El Oferente deberá prever, por cada ítem ofertado, la capacitación local corriendo con todos los gastos por cuenta propia, para 5 (cinco) funcionarios de la convocante con una duración mínima de 30 horas (reloj), en modalidad presencial en las oficinas de la Convocante en horario de oficina..

ÍTEM N°	BIEN	ESPECIFICACIONES TÉCNICAS	UNIDAD DE MEDIDA	PRESENTACIÓN	CANTIDAD
1	EQUIPOS DE SEGURIDAD DE REDES (UTM)	SEGÚN EETT	UNIDAD	EVENTO	2
2	SOFTWARE DE REGISTROS, ANÁLISIS Y REPORTES	SEGÚN EETT	UNIDAD	EVENTO	1
3	EQUIPOS DE CONMUTACIÓN (SWITCH)	SEGÚN EETT	UNIDAD	EVENTO	2
4	SERVICIO DE CAPACITACIÓN	SEGÚN EETT	UNIDAD	EVENTO	1

ESPECIFICACIONES TÉCNICAS

ITEM 1. EQUIPOS DE SEGURIDAD DE REDES (UTM)

Descripción	Requerimiento mínimo
Marca	indicar
Modelo	indicar
Procedencia	indicar
Cantidad	2 (dos)
Requisitos Mínimos	
NGFW en factor de forma appliance, rackeable de 1U	REQUERIDO
Throughput de por lo menos 25 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6	REQUERIDO
Soporte a por lo menos 3M conexiones simultaneas	REQUERIDO
Soporte a por lo menos 250K nuevas conexiones por segundo	REQUERIDO
Throughput de al menos 12 Gbps de VPN IPSec	REQUERIDO
Estar licenciado para, o soportar sin necesidad de licencia, 2K túneles de VPN IPSec site-to-site simultáneos	REQUERIDO
Estar licenciado para, o soportar sin necesidad de licencia, 15K túneles de clientes VPN IPSec simultáneos	REQUERIDO
Throughput de al menos 2 Gbps de VPN SSL	REQUERIDO
Soportar al menos 500 clientes de VPN SSL simultáneos	REQUERIDO
Soportar al menos 5 Gbps de throughput de IPS	REQUERIDO
Soportar al menos 4 Gbps de throughput de Inspección SSL	REQUERIDO
Soportar al menos 10 Gbps de throughput de Application Control	REQUERIDO
Soportar al menos 3 Gbps de throughput de NGFW	REQUERIDO
Soportar al menos 3 Gbps de throughput de Threat Protection	REQUERIDO

Permitir gestionar al menos 25 Access Points	REQUERIDO
Tener al menos 24 interfaces, 16 RJ45 y 8 SFP de 1 Gbps cada uno	REQUERIDO
Tener al menos 4 interfaces SFP+ de 10 Gbps cada uno	REQUERIDO
Estar licenciado y/o tener incluido sin costo adicional, al menos 9 sistemas virtuales lógicos (Contextos) por appliance	REQUERIDO
Soporte de por lo menos 10 sistemas virtuales lógicos (Contextos) por appliance	REQUERIDO
Fuente redundante	REQUERIDO
Al menos deberá contar con las siguientes certificaciones: FCC, CE, VCCI	REQUERIDO
Al menos deberá contar con las siguientes certificaciones: ISO 9001 y ICSA Labs	REQUERIDO
Requisitos Mínimos de Funcionalidad	
Características Generales	
La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo;	REQUERIDO
Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;	REQUERIDO
Las funcionalidades de protección de red que conforman la plataforma de seguridad, pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;	REQUERIDO
La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;	REQUERIDO
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;	REQUERIDO
La gestión del equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;	REQUERIDO
Los dispositivos de protección de red deben soportar mínimamente 4094 VLANs Tags 802.1q;	REQUERIDO
Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;	REQUERIDO

Los dispositivos de protección de red deben soportar policy based routing y policy based forwarding;	REQUERIDO
Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);	REQUERIDO
Los dispositivos de protección de red deben soportar DHCP Relay;	REQUERIDO
Los dispositivos de protección de red deben soportar DHCP Server;	REQUERIDO
Los dispositivos de protección de red deben soportar sFlow;	REQUERIDO
Los dispositivos de protección de red deben soportar Jumbo Frames;	REQUERIDO
Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;	REQUERIDO
Debe ser compatible con NAT dinámica (varios-a-1);	REQUERIDO
Debe ser compatible con NAT dinámica (muchos-a-muchos);	REQUERIDO
Debe soportar NAT estática (1-a-1);	REQUERIDO
Debe admitir NAT estática (muchos-a-muchos);	REQUERIDO
Debe ser compatible con NAT estático bidireccional 1-a-1;	REQUERIDO
Debe ser compatible con la traducción de puertos (PAT);	REQUERIDO
Debe ser compatible con NAT Origen;	REQUERIDO
Debe ser compatible con NAT de destino;	REQUERIDO
Debe soportar NAT de origen y NAT de destino de forma simultánea;	REQUERIDO
Debe soportar NAT de origen y NAT de destino en la misma política	REQUERIDO
Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;	REQUERIDO
Debe ser compatible con NAT64 y NAT46;	REQUERIDO
Debe implementar el protocolo ECMP;	REQUERIDO

Debe soportar SD-WAN de forma nativa	REQUERIDO
Debe soportar el balanceo de enlace hash por IP de origen;	REQUERIDO
Debe soportar el balanceo de enlace por hash de IP de origen y destino;	REQUERIDO
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;	REQUERIDO
Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;	REQUERIDO
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;	REQUERIDO
Enviar logs a sistemas de gestión externos simultáneamente;	REQUERIDO
Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;	REQUERIDO
Debe soportar protección contra la suplantación de identidad (anti-spoofing);	REQUERIDO
Implementar la optimización del tráfico entre dos dispositivos;	REQUERIDO
Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);	REQUERIDO
Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);	REQUERIDO
Soportar OSPF graceful restart;	REQUERIDO
Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;	REQUERIDO
Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;	REQUERIDO
Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;	REQUERIDO
Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;	REQUERIDO
Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;	REQUERIDO

Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;	REQUERIDO
Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;	REQUERIDO
La configuración de alta disponibilidad debe sincronizar: Sesiones;	REQUERIDO
La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;	REQUERIDO
La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;	REQUERIDO
La configuración de alta disponibilidad debe sincronizar: Tablas FIB;	REQUERIDO
En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;	REQUERIDO
Debe soportar la creación de sistemas virtuales en el mismo equipo;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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);	REQUERIDO
Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
La consola de administración debe soportar como mínimo, inglés y español.	REQUERIDO

La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad	REQUERIDO
La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.	REQUERIDO
Control por Política de Firewall	
Debe soportar controles de zona de seguridad;	REQUERIDO
Debe contar con políticas de control por puerto y protocolo;	REQUERIDO
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;	REQUERIDO
Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;	REQUERIDO
Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;	REQUERIDO
Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;	REQUERIDO
Debe soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.	REQUERIDO
Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);	REQUERIDO
Debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes	REQUERIDO
Debe soportar el protocolo estándar de la industria VXLAN;	REQUERIDO
La solución debe permitir la implementación sin asistencia de SD-WAN	REQUERIDO
En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN;	REQUERIDO
la solución debe soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall.	REQUERIDO
Control de Aplicación	

Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;	REQUERIDO
Detección de miles de aplicaciones en 18 categorías, 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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
Para tráfico 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;	REQUERIDO
Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;	REQUERIDO
Actualización de la base de firmas de la aplicación de forma automática;	REQUERIDO
Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos;	REQUERIDO
Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;	REQUERIDO
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;	REQUERIDO
El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;	REQUERIDO
Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;	REQUERIDO
Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;	REQUERIDO
Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitir a Hangouts el chat, pero impedir la llamada de video;	REQUERIDO

Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;	REQUERIDO
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);	REQUERIDO
Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;	REQUERIDO
Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;	REQUERIDO
Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente	REQUERIDO
Prevención de Amenazas	
Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;	REQUERIDO
Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);	REQUERIDO
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;	REQUERIDO
Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;	REQUERIDO
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;	REQUERIDO
Debe permitir el bloqueo de vulnerabilidades y exploits conocidos	REQUERIDO
Debe incluir la protección contra ataques de denegación de servicio;	REQUERIDO
Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;	REQUERIDO
Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;	REQUERIDO
Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;	REQUERIDO

Debe tener los siguientes mecanismos de inspección IPS: Reensamblado de paquetes TCP;	REQUERIDO
Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);	REQUERIDO
Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc;	REQUERIDO
Detectar y bloquear los escaneos de puertos de origen;	REQUERIDO
Bloquear ataques realizados por gusanos (worms) conocidos;	REQUERIDO
Contar con firmas específicas para la mitigación de ataques DoS y DDoS;	REQUERIDO
Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);	REQUERIDO
Debe poder crear firmas personalizadas en la interfaz gráfica del producto;	REQUERIDO
Identificar y bloquear la comunicación con redes de bots;	REQUERIDO
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;	REQUERIDO
Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;	REQUERIDO
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;	REQUERIDO
Los eventos deben identificar el país que origino la amenaza;	REQUERIDO
Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);	REQUERIDO
Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;	REQUERIDO
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;	REQUERIDO

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;	REQUERIDO
Proporcionar 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);	REQUERIDO
Filtrado de URL	
Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora);	REQUERIDO
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;	REQUERIDO
Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;	REQUERIDO
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;	REQUERIDO
Tener por lo menos 75 categorías de URL;	REQUERIDO
Debe tener la funcionalidad de exclusión de URLs por categoría;	REQUERIDO
Permitir página de bloqueo personalizada;	REQUERIDO
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);	REQUERIDO
Además del Explicit Web Proxy, soportar proxy web transparente;	REQUERIDO
Identificación de Usuarios	
Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;	REQUERIDO
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;	REQUERIDO

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;	REQUERIDO
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;	REQUERIDO
Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/control basados en usuarios y grupos de usuarios;	REQUERIDO
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 autenticación residente en el equipo de seguridad (portal cautivo);	REQUERIDO
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;	REQUERIDO
Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;	REQUERIDO
Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;	REQUERIDO
Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;	REQUERIDO
QoS Traffic Shaping	
Capacidad de controlar el ancho de banda máximo utilizado, por usuario o aplicación, tanto audio como vídeo sobre demanda	REQUERIDO
Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;	REQUERIDO
Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;	REQUERIDO
Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;	REQUERIDO
Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;	REQUERIDO
Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;	REQUERIDO
En QoS debe permitir la definición de tráfico con ancho de banda garantizado;	REQUERIDO

En QoS debe permitir la definición de tráfico con máximo ancho de banda;	REQUERIDO
En QoS debe permitir la definición de colas de prioridad;	REQUERIDO
Soportar marcación de paquetes DiffServ, incluso por aplicación;	REQUERIDO
Soportar la modificación de los valores de DSCP para Diffserv;	REQUERIDO
Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);	REQUERIDO
Debe soportar QoS (traffic-shaping) en las interfaces agregadas o redundantes;	REQUERIDO
Filtro de Datos	
Permite la creación de filtros para archivos y datos predefinidos;	REQUERIDO
Los archivos deben ser identificados por tamaño y tipo;	REQUERIDO
Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones;	REQUERIDO
Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;	REQUERIDO
Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;	REQUERIDO
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;	REQUERIDO
Geo Localización	
Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;	REQUERIDO
Debe permitir la visualización de los países de origen y destino en los registros de acceso;	REQUERIDO
Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;	REQUERIDO
VPN	

Soporte VPN de sitio-a-sitio y cliente-a-sitio;	REQUERIDO
Soportar VPN IPSec;	REQUERIDO
Soportar VPN SSL;	REQUERIDO
La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512	REQUERIDO
La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;	REQUERIDO
La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);	REQUERIDO
La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);	REQUERIDO
Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;	REQUERIDO
Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;	REQUERIDO
Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución.	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;	REQUERIDO
Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;	REQUERIDO
Deberá mantener una conexión segura con el portal durante la sesión;	REQUERIDO
El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.	REQUERIDO
Wireless Controller	

Solución de red inalámbrica que administre y controle de manera centralizada los puntos de acceso (AP);	REQUERIDO
Cualquier licencia y / o software necesario para la plena ejecución de todas las características descritas en este término de referencia deberá ser suministrada;	REQUERIDO
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;	REQUERIDO
La solución debe ser capaz de administrar puntos de acceso de tipo indoor y outdoor;	REQUERIDO
El controlador inalámbrico debe permitir ser descubierto automáticamente por los puntos de acceso a través de Broadcast, DHCP y consulta DNS;	REQUERIDO
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;	REQUERIDO
Permitir programar día y hora en que ocurrirá la optimización del aprovisionamiento automático de canales en los Access Points;	REQUERIDO
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;	REQUERIDO
Cuando tunelado, el tráfico debe ser encriptado a través de DTLS o IPSEC;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO

La solución debe implementar recursos que posibiliten la identificación de interferencias provenientes de equipos que operen en las frecuencias de 2.4GHz y 5GHz;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO

Debe permitir restringir el número máximo de dispositivos conectados por punto de acceso y por radio;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
La solución debe implementar el estándar IEEE 802.11v para permitir que la red influya en las decisiones de roaming de la cliente conectada mediante el suministro de información complementaria, como la carga de utilización de los puntos de acceso cercanos;	REQUERIDO
La solución debe implementar el estándar IEEE 802.11w para prevenir ataques a la infraestructura inalámbrica;	REQUERIDO
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;	REQUERIDO
La solución debe implementar técnicas de Call Admission Control para limitar el número de llamadas simultáneas;	REQUERIDO
La solución debe mostrar información sobre los dispositivos conectados a la infraestructura inalámbrica y presentar 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;	REQUERIDO
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;	REQUERIDO
La solución debe permitir la configuración de los data rates que se activarán en la herramienta y las que se deshabilitan para las frecuencias de 2.4 y 5GHz y los estándares 802.11a / b / g / n / ac;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
La solución debe permitir la configuración del valor de Short Guard Interval para 802.11n y 802.11ac en 5GHz;	REQUERIDO

La solución debe implementar una característica conocida como Airtime Fairness (ATF) para controlar el uso de airtime asignando porcentajes a utilizar en los SSID;	REQUERIDO
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;	REQUERIDO
La solución debe implementar la función de web filtering para controlar los sitios que se accede a la red. 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;	REQUERIDO
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;	REQUERIDO
La base de reconocimiento de aplicaciones a través de DPI debe identificar con al menos 1500 (mil quinientas) aplicaciones;	REQUERIDO
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;	REQUERIDO
La solución debe, a través de la técnica de DPI, reconocer aplicaciones sensibles al negocio y permitir la priorización de este tráfico con QoS;	REQUERIDO
La solución debe implementar mecanismos de protección para identificar ataques a la infraestructura inalámbrica. Al menos los siguientes ataques deben ser identificados:	REQUERIDO
- 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.	

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 deauthentication	REQUERIDO
La solución debe implementar mecanismos de protección contra ataques de ARP Poisoning en la red inalámbrica;	REQUERIDO
La solución debe monitorear y clasificar el riesgo de las aplicaciones accedidas por los clientes inalámbricos;	REQUERIDO
Permitir configurar el bloqueo en la comunicación entre los clientes inalámbricos conectados a un SSID;	REQUERIDO
Debe implementar la autenticación administrativa a través del protocolo RADIUS;	REQUERIDO
En combinación con los puntos de acceso, la solución debe implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES);	REQUERIDO
En combinación con los puntos de acceso, la solución debe ser compatible e implementar el método de autenticación WPA3;	REQUERIDO
La solución debe permitir la configuración de múltiples claves de autenticación PSK para su uso en un SSID determinado;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
La solución debe admitir los siguientes métodos de autenticación EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP;	REQUERIDO
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;	REQUERIDO
La solución debe permitir el hospedaje del portal cautivo (captive portal) en la memoria interna del controlador inalámbrico;	REQUERIDO
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;	REQUERIDO

La solución debe permitir la recopilación del correo electrónico de los usuarios como método de autorización para ingreso a la red;	REQUERIDO
La solución debe permitir que la página de autenticación se quede alojada en un servidor externo;	REQUERIDO
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;	REQUERIDO
La solución debe garantizar que los usuarios se autenticuen en el portal cautivo que utilice la dirección IPv6;	REQUERIDO
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;	REQUERIDO
Después de la creación de un usuario visitante, la solución debe enviar las credenciales por e-mail al usuario registrado;	REQUERIDO
La solución debe implementar la función de DHCP Server (IPv4 y IPv6) para facilitar la configuración de las redes de visitantes;	REQUERIDO
La solución debe identificar automáticamente el tipo de equipo y sistema operativo utilizado por el dispositivo conectado a la red inalámbrica;	REQUERIDO
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;	REQUERIDO
La solución debe permitir la configuración de redes Mesh entre los puntos de acceso administrados por ella;	REQUERIDO
La solución debe permitir la configuración de red Mesh entre puntos de acceso indoor y outdoor;	REQUERIDO
La solución debe permitir ser administrada a través de los protocolos HTTPS y SSH vía IPv4 e IPv6;	REQUERIDO
La solución debe permitir el envío de los Logs a múltiples servidores externos de syslog;	REQUERIDO
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;	REQUERIDO
La solución debe permitir que los softwares de gestión realicen consultas directamente en los puntos de acceso a través del protocolo SNMP;	REQUERIDO

La solución debe incluir soporte para las RFC 1213 (MIB II) y RFC 2665 (Ethernet-like MIB);	REQUERIDO
La solución debe permitir la captura de paquetes en la red inalámbrica y exportarlos en archivos en formato. pcap;	REQUERIDO
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;	REQUERIDO
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 transmitidos y recibidos por ellos;	REQUERIDO
La solución debe implementar la administración unificada y de forma gráfica para redes WiFi y redes cableadas;	REQUERIDO
La solución debe permitir la actualización de firmware del controlador inalámbrico incluso cuando se conecta de forma remota;	REQUERIDO
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;	REQUERIDO
La solución debe tener herramientas de diagnóstico y depuración;	REQUERIDO
La solución debe soportar la comunicación con elementos externos a través de las API;	REQUERIDO
La solución deberá ser compatible y administrar los puntos de acceso de este proceso;	REQUERIDO
Instalación, configuración y garantía	
El plazo de garantía será de 36 meses, se entiende por garantía el mantenimiento preventivo y correctivo del software en la modalidad de al menos 24x7 incluyendo el reemplazo del software en caso de necesidad, solución de errores debido a algún incidente o corrupción en el software, así como la instalación de las actualizaciones que pudieran surgir durante el referido periodo.	REQUERIDO
El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo. La validez de las licencias debe ser por un periodo de mínimo 36 meses.	REQUERIDO

ITEM 2. SOFTWARE DE REGISTROS, ANÁLISIS Y REPORTES

Descripción	Requerimiento mínimo
Software de Reporte	REQUERIDO
Denominación	indicar
Versión	indicar
Procedencia	indicar
Cantidad	1 (uno)
Requisitos Mínimos	
Sistema de Reportería en formato Virtualizado (VM) para instalación en ambientes virtualizados	REQUERIDO
Funcionalidades Generales	
Compatible con el ambiente VMware ESXi 5.0/5.1/5.5/6.0/6.5/6.7;	REQUERIDO
Compatible con el ambiente Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2/2016	REQUERIDO
Compatible con el ambiente Citrix XenServer 6.0+	REQUERIDO
Compatible con el ambiente Open Source Xen 4.1+	REQUERIDO
Compatible con el ambiente KVM on Redhat 6.5+ and Ubuntu 17.04	REQUERIDO
Compatible con el ambiente Nutanix AHV (AOS 5.10.5)	REQUERIDO
Compatible con el ambiente Amazon Web Services (AWS)	REQUERIDO
Compatible con el ambiente Microsoft Azure.	REQUERIDO
Compatible con el ambiente Google Cloud (GCP)	REQUERIDO
Compatible con el ambiente Oracle Cloud Infrastructure (OCI)	REQUERIDO
Compatible con el ambiente Alibaba Cloud (AliCloud)	REQUERIDO
No debe haber límites a la cantidad de múltiples vCPU	REQUERIDO

No debe haber límites a la expansión de memoria RAM	REQUERIDO
Debe soportar acceso vía SSH, WEB (HTTPS) para la gestión de la solución	REQUERIDO
Contar con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interface gráfica (GUI) como vía línea de comandos en consola de gestión.	REQUERIDO
Permitir acceso simultáneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.	REQUERIDO
Soporte SNMP versión 2 y 3	REQUERIDO
Permitir virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.	REQUERIDO
Debe permitir la creación de administrador general, que tenga acceso general a todas las instancias de virtualización de la solución.	REQUERIDO
Debe permitir activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH	REQUERIDO
Autenticación de usuarios de acceso a la plataforma vía LDAP	REQUERIDO
Autenticación de usuarios de acceso a la plataforma vía Radius	REQUERIDO
Autenticación de usuarios de acceso a la plataforma vía TACACS+	REQUERIDO
Generación de informes en tiempo real de tráfico, en formato de gráfica de mapas geográficos	REQUERIDO
Generación de informes en tiempo real de tráfico, en formato de gráfica de burbuja.	REQUERIDO
Generación de informes en tiempo real de tráfico, en formato de gráfica tabla	REQUERIDO
Definición de perfiles de acceso a consola con permiso granulares, tales como: acceso de escritura, de lectura, de creación de nuevos usuarios y cambios en configuraciones generales.	REQUERIDO
Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña del mismo.	REQUERIDO
Debe ser posible ver la cantidad de logs enviados desde cada dispositivo supervisado	REQUERIDO
Contar con mecanismos de borrado automático de logs antiguos.	REQUERIDO

Permitir la importación y exportación de reportes	REQUERIDO
Debe contar con la capacidad de crear informes en formato HTML	REQUERIDO
Debe contar con la capacidad de crear informes en formato PDF	REQUERIDO
Debe contar con la capacidad de crear informes en formato XML	REQUERIDO
Debe contar con la capacidad de crear informes en formato CSV	REQUERIDO
Debe permitir exportar los logs en formato CSV	REQUERIDO
Generación de logs de auditoría, con detalle de la configuración realizada, el administrador que realizó el cambio y hora del mismo.	REQUERIDO
Los logs generados por los dispositivos administrados deben ser centralizados en los servidores de la plataforma, pero la solución debe ofrecer también la posibilidad de utilizar un servidor externo de Syslog o similar.	REQUERIDO
La solución debe contar con reportes predefinidos	REQUERIDO
Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución	REQUERIDO
Debe ser posible la duplicación de reportes existentes para su posterior edición.	REQUERIDO
Debe tener la capacidad de personalizar la portada de los reportes obtenidos.	REQUERIDO
Permitir centralmente la visualización de logs recibidos por uno o más dispositivos, incluido la capacidad de uso de filtros para facilitar la búsqueda dentro de los mismos logs.	REQUERIDO
Los logs de auditoría de cambios de configuración de reglas y objetos deben ser visualizados en una lista distinta a la de los logs relacionados a tráfico de datos.	REQUERIDO
Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas	REQUERIDO
Debe poseer mecanismo de Drill-Down para navegar en los reportes de tiempo real.	REQUERIDO
Debe permitir descargar de la plataforma los archivos de logs para uso externo.	REQUERIDO
Tener la capacidad de generar y enviar reportes periódicos automáticamente.	REQUERIDO

Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.	REQUERIDO
Permitir el envío por email de manera automática de reportes.	REQUERIDO
Debe permitir que el reporte a enviar por email sea al destinatario específico.	REQUERIDO
Permitir la programación de la generación de reportes, conforme a un calendario definido por el administrador.	REQUERIDO
Debe ser posible visualizar gráficamente en tiempo real la tasa de generación de logs por cada dispositivo gestionado.	REQUERIDO
Debe permitir el uso de filtros en los reportes.	REQUERIDO
Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros.	REQUERIDO
Permitir especificar el idioma de los reportes creados	REQUERIDO
Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.	REQUERIDO
Debe permitir el envío automático de reportes a un servidor externo SFTP o FTP.	REQUERIDO
Debe ser capaz de crear consultas SQL o similar dentro de las bases de datos de logs, para uso en gráficas y tablas en reportes.	REQUERIDO
Tener la capacidad de visualizar en GUI de reportes de información del Sistema, como licencias, memoria, disco duro, uso de CPU, tasa de logs por segundo recibidos, total de logs diarios recibidos, alertas del sistema, entre otros.	REQUERIDO
Debe contar con una herramienta que permita analizar el rendimiento en la generación de reportes, con el objetivo de detectar y arreglar problemas en generación de los mismos.	REQUERIDO
Que la solución sea capaz de importar archivos con logs de dispositivos compatibles conocido y no conocidos por la plataforma, para posterior generación de reportes.	REQUERIDO
Debe ser posible poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.	REQUERIDO
Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.	REQUERIDO
Debe ser compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.	REQUERIDO

Debe permitir aplicar políticas para el uso de contraseñas para los administradores de la plataforma, como tamaño mínimo y caracteres permitidos	REQUERIDO
Debe permitir visualizar en tiempo real los logs recibidos.	REQUERIDO
Debe permitir el reenvío de logs en formato syslog.	REQUERIDO
Debe permitir el reenvío de logs en formato CEF (Common Event Format).	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea las principales amenazas de seguridad para su red	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea comprometimiento de usuarios y uso sospechoso de la web en su red.	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea el tráfico en su red.	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea el tráfico de aplicaciones y sitios web en su red	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea detecciones de amenazas de día cero en su red (sandboxing).	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea actividad de endpoints en su red.	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea actividad VPN en su red.	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea puntos de acceso WiFi y SSIDs	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea rendimiento de recursos local de la solución (CPU, Memoria)	REQUERIDO
Debe permitir crear dashboards personalizados para monitoreo de operaciones SOC	REQUERIDO
Debe soportar configuración de alta disponibilidad Master/Slave en la capa 3	REQUERIDO
Debe permitir generar alertas de eventos a partir de logs recibidos	REQUERIDO
Debe permitir crear incidentes a partir de alertas de eventos para endpoint	REQUERIDO
Debe permitir la integración al sistema de tickets ServiceNow	REQUERIDO

Debe soportar servicio de Indicadores de Compromiso (IoC) del mismo fabricante, que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas.	REQUERIDO
Debe permitir respaldar logs en nube publica de Amazon S3	REQUERIDO
Debe permitir respaldar logs en nube publica de Microsoft Azure	REQUERIDO
Debe permitir respaldar logs en nube publica de Google Cloud	REQUERIDO
Debe soportar el estándar SAML para autenticación de usuarios administradores	REQUERIDO
Reportes de Firewall	
Debe contar con reporte de cumplimiento de PCI DSS	REQUERIDO
Debe contar con reporte de utilización de aplicaciones SaaS	REQUERIDO
Debe contar con reporte de prevención de pérdida de datos (DLP)	REQUERIDO
Debe contar con reporte de VPN	REQUERIDO
Debe contar con reporte de Sistema de prevención de intrusos (IPS)	REQUERIDO
Debe contar con reporte de reputación de cliente	REQUERIDO
Debe contar con reporte de análisis de seguridad de usuario	REQUERIDO
Debe contar con reporte de análisis de amenaza cibernética	REQUERIDO
Debe contar con reporte de breve resumen diario de eventos e incidentes de seguridad	REQUERIDO
Debe contar con reporte de tráfico DNS	REQUERIDO
Debe contar con reporte tráfico de correo electrónico	REQUERIDO
Debe contar con reporte de Top 10 de Aplicaciones utilizadas en la red	REQUERIDO
Debe contar con reporte de Top 10 de Websites utilizadas en la red	REQUERIDO
Debe contar con reporte de uso de redes sociales	REQUERIDO

Compatibilidad con ITEM 1 Firewall e ÍTEM 3 Switch	
Para garantizar la compatibilidad de las funciones requeridas, el sistema deberá ser del mismo fabricante del Ítem 1 y del Ítem 3 o en su defecto contar con un respaldo documental de interoperabilidad de las funciones solicitadas del sistema de reporte, tanto del Fabricante del ITEM 1, como del Fabricante del ITEM 3. Es decir, ambos fabricantes deberán garantizar mediante nota dirigida a la Convocante la interoperabilidad.	REQUERIDO
Instalación, configuración y garantía.	
El plazo de garantía será de 36 meses, se entiende por garantía el mantenimiento preventivo y correctivo del software en la modalidad de al menos 24x7 incluyendo el reemplazo del software en caso de necesidad, solución de errores debido a algún incidente o corrupción en el software, así como la instalación de las actualizaciones que pudieran surgir durante el referido periodo.	REQUERIDO
El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo. La validez de las licencias debe ser por un periodo de mínimo 36 meses.	REQUERIDO

ITEM 3. EQUIPOS DE CONMUTACIÓN (SWITCH)	
Descripción	Requerimiento mínimo
Marca	indicar
Modelo	indicar
Procedencia	indicar
Cantidad	2 (dos)
Descripción	Switch de Acceso
Tipo de configuración	Fija
Stacking/Apilamiento: máximos equipos apilables	4
Tipo de uso	Acceso a Proveedores
Interfaces y rendimiento	

Interfaces independientes 10/100/1000BaseT-Cobre UTP RJ45	24 puertos RJ45
Interfaces SFP+ independientes (1/10Gbps)	4 puertos SFP+
Puerto 10/100 BaseT Ethernet adicional e independiente para administración del equipo (Out of Band Management)	1 puerto RJ45
Puerto SERIAL RS-232 para ser usado como consola de administración.	1 puerto serial
Puerto USB para el almacenado y descarga de configuraciones y sistema operativo	Opcional
Capacidad de conmutación de paquetes unidireccional	64 Gbps
Capacidad de conmutación de paquetes bidireccional	128 Gbps
Throughput de Capa 2/Capa 3 (Mbps)	95 Mbps
Stacking/Apilamiento	
Capacidad de backplane del Stack utilizando los puertos de UPLINK	Opcional
Equipos agrupados para administrar con un único acceso administrativo	Opcional
Cables de stacking proporcionados para la interconexión de equipos	Opcional
Deberá soportar el protocolo Link Aggregation Control Protocol (LACP) IEEE 802.3ad.	Opcional
Número de grupos a soportar por todo el STACK	Opcional
Calidad de Servicio	
Encolamiento basado en clases de servicio con priorización de tráfico Strick priority en egreso	Exigido
Soporte de Port Shaping: puede ser usados para manejar el exceso de tráfico, esta característica define el ancho de banda maximo alojado en un puerto	Exigido
Soporte de queuing shaping: puede ser usados para manejar el exceso de tráfico, esta característica define el ancho de banda maximo alojado en cada cola	Exigido
Soporte de QoS en puertos LAG	Exigido
L2 QoS (classification, rewrite, queuing) Permite la clasificacion re-escritura y encolamiento de CoS en interfaces de layer 2.	Exigido

L3 QoS (classification, rewrite, queuing) Permite la clasificacion re-escritura y encolamiento de CoS en interfaces de layer 3	Exigido
Soporte de QoS Clasificacion, re-write y queueing en interfaces RVI (Interface VLANs)	Exigido
Soporta el tratamiento de las colas ante congestión con los mecanismos SDWRR (Shaped deficit Weighted Round Robin) y SPQ (Strict Priority).	Opcional
Soporta el protocolo LLDP (Link Layer Discovery Protocol) IEEE 802.1AB y LLDP-MED (LLDP for Media Endpoint Device) ANSI/TIA-1057 integrado para Voice sobre IP (VoIP)	Exigido
Soporte de priorización de tráfico de salida por hardware mínimo ocho (8) colas de servicio por puerto.	Exigido
Políticas de tráfico de red que limitan la velocidad de entrada y salida de una clase de tráfico con base en el criterio establecido por el usuario. Permite controlar la velocidad máxima de tráfico enviado o recibido en una interfaz y particionar una red en múltiples niveles de clase de servicio	Exigido
Encolado estricto y de baja latencia (Strict priority queuing or Low Latency Queuing (LLQ)) Strict priority queuing, or low latency queuing (LLQ): es una característica usada para reenviar de forma más rápida ciertos tipos de tráfico sensible a retardos (voz, video etc).	Opcional
Trust 802.1p/DSCP/IP Prec (ingress)	Exigido
Soporte de limitación de tráfico mediante lista de control de acceso (ACL) aplicable en los puertos físicos o VLANs por:	
Filtros basados en direcciones MAC origen o destino	Exigido
Filtros basados en direcciones IP origen o destino	Exigido
Filtros basados en número de puerto TCP/UDP	Exigido
Cantidad de filtros de tráfico (ACL)	Al menos 1000
Spanning Tree Protocol	
IEEE 802.1d.	Exigido
Rapid Spanning Tree IEEE 802.1w	Exigido
Multiple Spanning Tree Protocol IEEE 802.1s.	Exigido
Soporte de Time Domain Reflectometry para detectar las fallas en cables UTP	Exigido

Soporte de ruteo layer 3 por medio de los siguientes protocolos:	
Rutas Estáticas	Exigido
Soporte máximo de rutas IPv4	Al menos 100
Soporte de IEEE802.1ag Ethernet OAM connectivity fault management (CFM)	Opcional
Soporte de Ethernet ring protection switching (ERPS, G.8032/Y.1344)	Opcional
Soporte de TDR (Time Domain Reflectometry). Una tecnología que permite el seguimiento y señalización de fallas en los cables o conectores de redes de computadoras. Los puertos deben ser capaces de generar un pulso electromagnético, cuando este pulso alcanza un obstáculo o el fin del cable se genera un eco que es traducido en la distancia a la falla.	Exigido
RIP v1/v2	Exigido
RIPng	Exigido
Soporte OSPF	Exigido
Soporte de Layer 2 protocol tunneling (L2PT)	Opcional
Soporte de ARP (número de entradas)	Opcional
Funcionalidades layer 2	
Soporte máximo de direcciones MAC de red.	16000
Soporte de tramas Jumbo	Exigido
Soporte de IEEE 802.1X para VLAN VoIP.	Exigido
Port-based VLAN	Exigido
MAC-based VLAN	Exigido
Soporte IEEE 802.1Q-in-Q: VLAN Stacking	Exigido
IEEE 802.1ak: Multiple VLAN Registration Protocol (MVRP)	Opcional

Compatible con Per-VLAN Spanning Tree Plus	Opcional
Soporte de interfaces RVI (Routed VLAN Interfaces)	Exigido
Capacidad de soportar definición de dominios de broadcast VLANs (Virtual LANs) en todos los puertos según IEEE 802.1 p/Q.	Exigido
Numero de VLANs configurables en el Virtual Chasis	Opcional
VLANs en equipo individual	4092
Posible rango de VLAN-ID para configurar	1 - 4092
Soporte de DHCP Relay y DHCP helper	Exigido
Soporte de DHCP Server sobre interfaces RVI	Opcional
Voice VLAN fallback	Opcional
Multicast	
Soporte protocolo IGMP-Snooping	Exigido
Soporte PIM-SM, PIM-SSM, PIM-DM	Opcional
Soporte IGMP: v1, v2, v3	Exigido
Administracion / Management	
Deberá soportar Simple Network Management Protocol versión SNMP v2c, SNMP v3.	Exigido
Capacidad de proveer los bloques de información de management (MIBs) necesarios.	Exigido
Capacidad de Remote Monitoring (RMON), deberá soportar al menos cuatro (4) grupos (statistics, history, alarm, events).	Exigido
sFlow	Exigido
Soporte de registro remoto (SysLog).	Exigido
Soporte de traffic mirroring por puerto o por VLAN.	Exigido

Deberá soportar Network Timing Protocol (NTP).	Exigido
Creación de 20 perfiles de administrador con facultadas específicas de modificar la configuración o solo acceder a vistas de la misma y listado de comandos disponibles para ejecutar por cada perfil	Exigido
Las passwords (claves) de administrador almacenadas localmente deben estar encriptadas usando hash MD5 o SHA1	Exigido
Soporte de MIB para la información de media attachment unit (MAU)	Opcional
Fuente para AC	Exigido
Accesorios necesarios para montar en racks estándar de 19".	Exigido
Seguridad, mecanismos soportados	
Central Web authentication	Exigido
Deberá soportar autenticación 802.1X. para diferentes VLANs por puerto.	Exigido
Soporte de IEEE 802.1X con soporte de VLANs de invitados (Guest VLAN)	Exigido
MAC Radius Authentication con 802.1X	Exigido
Soporte de protocolo EAP-PAP para MAC RADIUS authentication	Exigido
Soporte de seguridad del puerto mediante filtrado por dirección MAC. En caso de violación del puerto deberá poder enviarse una alerta al administrador y deshabilitar el puerto.	Exigido
Soporte de limitación de direcciones MAC por puerto.	Exigido
Soporte de Persistent MAC learning o sticky MAC	Exigido
DHCP Snooping.	Exigido
Dynamic ARP inspection (DAI)	Exigido
Proxy ARP	Exigido
Static ARP support	Exigido
IP source guard	Exigido

Orden de autenticación flexible	Exigido
IPv6 Neighbor Discovery inspection	Exigido
Servicio de configuración por medios seguros:	
Soporte Telnet / Secure Shell (SSH) versión 2 para conexión remota vía interfaz línea de comando (CLI).	Exigido
Soporte vía Web con SSL. (HTTPS)	Exigido
Soporte de creación de Certificados locales para conexión HTTPs	Exigido
Almacenamiento de sistema operativo y configuración en memoria Flash reescribible.	Al menos 256 MB
Roll-back a varias configuraciones anteriores almacenadas en el equipo (mínimo 3 configuraciones) o una configuración de rescate almacenada especialmente por el administrador	Opcional
Mecanismos de automatización mediante scripts o similares que permitan chequear el cumplimiento y administrar los cambios de configuraciones, aplicar configuraciones predefinidas, visualizar conjuntos de comandos para el diagnóstico, análisis y administración de eventos, y generar respuestas predefinidas a eventos.	Opcional
Servicio de configuración por medio de consola serial RS-232 asincrónica	Opcional
La unidad deberá ser entregada con 1 (un) juego de manuales de configuración de hardware y software. Estos manuales podrán ser entregados de manera impresa o bien en medio digital.	Exigido
Equipos alimentados con 220 V - 50 Hz, monofásico con toma de 3 patas, sin necesidad de requerir un transformador adicional.	Exigido
Troubleshooting	
Debugging: CLI via console, telnet, or SSH	Exigido
Diagnostics: Show and debug command statistics	Exigido
Traffic mirroring (port)	Exigido
Traffic mirroring (VLAN)	Exigido
ACL-based mirroring	Opcional

Mirroring destination ports per system	Opcional
LAG port monitoring	Opcional
Multiple destination ports monitored to 1 mirror (N:1)	Exigido
Maximum number of mirroring sessions	Exigido
Mirroring to remote destination (over L2)	Exigido
IP tools: Extended ping and trace	Exigido
Alta disponibilidad	
Soporte de Link Aggregation	Exigido
802.3ad (LACP) support: Number of LAGs supported	24
Maximum number of ports per LAG	8
LAG sharing algorithm—Routed Multicast Traffic:	
Tagged ports support in LAG	Exigido
Uplink Failure Detection (UFD)	Opcional
Soporte para equipos con dos Routing engines, configurar al Routing engine de respaldo para asumir el rol de master sin causar interrupcion en el reenvio.	Opcional
Soporte VRRP (Virtual Router Redundancy Protocol)	Exigido
Alimentación Eléctrica, Ventilación y dimensiones.	
Tensión de operación Fuente de Alimentación 100-120V / 200-240V auto detectable.	Exigido
Cumplimiento de ROHS	Exigido
Temperatura de operación: 0°C a 45°C	Exigido
Humedad de operación: 10% a 85% de humedad relativa máxima, sin condensación.	Exigido
Montaje en rack de 19"	Exigido

Cantidad de Unidad de Rack del Equipo	1U
MTBF	87.000 hs.
Instalación, configuración y garantía.	
Instalación: El equipo deberá ser configurado, instalado y probado de acuerdo a las indicaciones de la Convocante, por personal técnico del oferente.	Exigido
Actualización de software: El sistema operativo deberá ser actualizado a la última versión disponible a pedido del cliente durante la duración del contrato.	Exigido
Plazo de garantía del fabricante	36 meses

ITEM 4. SERVICIO DE CAPACITACIÓN	
Descripción	Requerimiento mínimo
Servicio de capacitación, para al menos 5 (CINCO) funcionarios, con una duración mínima de 30 horas (reloj), por cada ítem solicitado (1, 2 y 3), en modalidad presencial, en las oficinas de la Convocante y en horario de oficina.	REQUERIDO

ESQUEMA ACTUAL DE RED <https://ibb.co/M6WYjQE>

ESQUEMA REQUERIDO DE RED <https://ibb.co/DwXYfBg>

Switch de acceso a Proveedores

Equipos dedicados a concentrar los servicios de los proveedores. Los mismos estarán en redundancia, garantizando alta disponibilidad, distribuyendo las conexiones hasta los equipos de borde.

Enrutador / Firewall UTM de Borde

Dispositivo del tipo UTM en el esquema borde; el cual pueda gestionar todo el tráfico interno y externo, brindando de esta manera una capa de seguridad mejorada. Los mismos estarán en redundancia, garantizando alta disponibilidad.

Software de Reportes

Herramienta dedicada a la gestión de registros, análisis e informes, con capacidad de permitir operaciones de seguridad, identificación proactiva y corrección de riesgos, y visibilidad completa de todo el panorama de ataques en la red.

SON PROVEEDORES EN EL BORDE DE COMUNICACIONES:

PROVEEDOR DE INTERNET A

Acceso a Internet

Enlace punto a punto entre la DGRP y la CSJ

PROVEEDOR DE INTERNET B

Acceso a Internet

CSJ

Enlace propio que conecta a la DGRP con la CSJ.

MITIC

Enlace para el Servicio de Intercambio de Información (SII) entre Organismos y Entidades del Estado (OEE)

SNC

Enlace propio que conecta a la DGRP con la SNC.

PLAN DE ENTREGA DE LOS BIENES

La entrega de los bienes se realizará de acuerdo al Plan de Entrega y Cronograma de Cumplimiento, indicado en el presente apartado. Así mismo, de los documentos de embarque y otros que deberá suministrar el Proveedor indicados a continuación:

Ítem	Descripción del bien	Cantidad	Unidad de medida	Lugar de entrega de los bienes	Fecha(s) final(es) de ejecución de los bienes
1	TODOS LOS ÍTEMS	SEGÚN LAS EETT	SEGÚN LAS EETT	<p>El oferente adjudicado deberá entregar los bienes (equipos de conmutación, seguridad de red de datos y software de reportes), como también, el cronograma, contenido y fechas tentativas para la realización de la capacitación dentro de los 90 (noventa) días hábiles posteriores a la firma del contrato, y dispondrá, de otros 30 (treinta) días hábiles, posteriores a la entrega de los bienes, para realizar la planificación, instalación, configuración e implementación de los ítems adjudicados.</p> <p>Todo esto, debe ser entregado, instalado, configurado, implementado y realizado en el edificio de la Dirección General de los Registros Públicos, sito en Avda. Eusebio Ayala casi Capitán Román García, de lunes a viernes de 07:15 hs a 13:00 hs, salvo los feriados oficiales y de conformidad al horario normal y diferenciado de los funcionarios de la DGRP.</p> <p>La emisión del Acta de Recepción Total dada por la Contratante, significará el cumplimiento por parte del Proveedor de sus obligaciones contractuales y le facultará a solicitar el pago de la misma.</p>	36 (TREINTA Y SEIS) MESES, CONTADOS DESDE LA FIRMA DEL CONTRATO.

INDICADOR DE CUMPLIMIENTO DE CONTRATO

- El documento requerido para acreditar el cumplimiento contractual, será: **Acta de recepción Definitiva.**
- **Serán presentados:** 1 (un) Acta Final por la entrega efectuada.
- **Frecuencia:** Conforme se establece en el Plan de Entrega de bienes establecido en el PBC.

INDICADOR	TIPO	FECHA DE PRESENTACIÓN PREVISTA
Acta de Recepción Definitiva.	Acta	120 (ciento veinte) días hábiles, computados a partir de la fecha de la firma del contrato

- Se modifican los plazos de la subasta en el SICP.

- Fecha Tope de Consulta

OBSERVACIÓN: Solo se modifican los puntos citados en la presente Adenda, quedando invariable los demás puntos del Pliego de Bases y Condiciones.

Se detectaron modificaciones en las siguientes cláusulas:

Sección: Datos de la licitación

- Copias de la oferta - CPS
- Periodo de validez de la Garantía de Cumplimiento de Contrato

Sección: Requisitos de calificación y criterios de evaluación

- Capacidad Técnica
- Requisito documental para evaluar la capacidad técnica

Sección: Suministros requeridos - especificaciones técnicas

- Detalle de los productos con las respectivas especificaciones técnicas
- Plan de entrega de los bienes
- Indicadores de Cumplimiento

Se puede realizar una comparación de esta versión del pliego con la versión anterior en el siguiente enlace:
<https://www.contrataciones.gov.py/licitaciones/convocatoria/416434-adquisicion-equipos-conmutacion-seguridad-red-datos-software-reportes-plurianual-ad-1/pliego/6/diferencias/5.html?seccion=adenda>

La adenda es el documento emitido por la convocante, mediante la cual se modifican aspectos establecidos en la convocatoria y/o en las bases de la licitación y/o en los contratos suscritos. La adenda será considerada parte integrante del documento cuyo contenido modifique.

DATOS DE LA LICITACIÓN

Los Datos de la Licitación constituye la información proporcionada por la convocante para establecer las condiciones a considerar del proceso particular, y que sirvan de base para la elaboración de las ofertas por parte de los potenciales oferentes.

Contratación Pública Sostenibles - CPS

Las compras públicas juegan un papel fundamental en el desarrollo sostenible, así como en la promoción de estilos de vida sostenibles.

El Estado, por medio de las actividades de compra de bienes y servicios sostenibles, busca incentivar la generación de nuevos emprendimientos, modelos de negocios innovadores y el consumo sostenible. La introducción de criterios y especificaciones técnicas con consideraciones sociales, ambientales y económicas tiene como fin contribuir con el Desarrollo Sostenible en sus tres dimensiones.

El símbolo “CPS” en este pliego de bases y condiciones, es utilizado para indicar criterios o especificaciones sostenibles.

Criterios sociales y económicos:

- Los oferentes deberán indicar bajo declaración jurada el pago del salario mínimo a sus colaboradores, además de garantizar la no contratación de menores.
- Los oferentes deberán dar cumplimiento a las disposiciones legales vigentes asegurando a los trabajadores dependientes condiciones de trabajo dignas y justas en lo referente al salario, cargas sociales, provisión de uniformes, provisión de equipos de protección individual, bonificación familiar, jornada laboral, asegurar condiciones especiales a trabajadores expuestos a trabajos insalubres y peligrosos, remuneración por jornada nocturna.
- Las deducciones al salario, anticipos y préstamos a los trabajadores no podrán exceder los límites legales. Los términos y condiciones relacionados a los mismos deberán comunicarse de manera clara, para que los trabajadores los entiendan.
- Los oferentes adjudicados deberán fomentar en la medida de lo posible, la creación de empleo local y el uso de suministros locales.

Criterios ambientales:

- El oferente adjudicado deberá utilizar en la medida de lo posible, insumos cuyo embalaje pueda ser reutilizado o reciclado.
- El oferente adjudicado deberá cumplir con los lineamientos ambientales, incluidos en el ordenamiento jurídico o dictado por la institución, tales como: cooperación en acciones de recolección, separación de residuos sólidos, disposición adecuada de los residuos, participación del personal en actividades de capacitación impartidas por la institución, entre otros.
- El oferente adjudicado deberá asegurar que todos los residuos generados por sus actividades sean adecuadamente gestionados (identificados, segregados y destinados) y buscar su reducción o eliminación en la fuente, por medio de prácticas como la modificación de los procesos de producción, manutención y de las instalaciones utilizadas, además de la sustitución, conservación, reciclaje o reutilización de materiales.

Conducta empresarial responsable:

Los oferentes deberán observar los más altos niveles de integridad, así como altos estándares de conducta de negocios, ya sea durante el procedimiento de licitación o la ejecución de un contrato. Asimismo, se comprometen a:

- No ofrecer, prometer, dar ni solicitar, directa o indirectamente, pagos ilícitos u otras ventajas indebidas para obtener o conservar un contrato u otra ventaja ilegítima.
- No ofrecer, prometer o conceder ventajas indebidas, pecuniarias o de otro tipo a funcionarios públicos. Tampoco deberán solicitar, recibir o aceptar ventajas indebidas, pecuniarias o de otro tipo, de funcionarios públicos o empleados de sus socios comerciales.
- Introducir políticas y programas contra la corrupción e implementarlas dentro de sus operaciones.
- Garantizar que todos los recursos a ser empleados en la ejecución de un contrato público sean de origen lícito.
- Garantizar que los fondos obtenidos de una licitación pública no sean destinados a fines ilícitos.

Difusión de los documentos de la licitación

Todos los datos y documentos de esta licitación deben ser obtenidos directamente del Sistema de Información de Contrataciones Públicas (SICP). Es responsabilidad del oferente examinar todos los documentos y la información de la licitación que obren en el mismo.

Aclaración de los documentos de la licitación

Todo oferente potencial que necesite alguna aclaración del pliego de bases y condiciones podrá solicitarla a la convocante. El medio por el cual se recibirán las consultas es el Sistema de Información de Contrataciones Públicas (SICP), y/o si es el caso, en la Junta de Aclaraciones que se realice en la fecha, hora y dirección indicados por la convocante.

La convocante responderá por escrito a toda solicitud de aclaración del pliego de bases y condiciones que reciba dentro del plazo establecido o que se derive de la Junta de Aclaraciones.

La convocante publicará una copia de su respuesta, incluida una explicación de la consulta, pero sin identificar su procedencia, a través del Sistema de Información de Contrataciones Públicas (SICP), dentro del plazo tope.

La inasistencia a la Junta de Aclaraciones no será motivo de descalificación de la oferta.

La convocante podrá optar por responder las consultas en la Junta de Aclaraciones o podrá diferirlas, para que sean respondidas conforme con los plazos de respuestas o emisión de adendas. En todos los casos se deberá levantar acta circunstanciada.

Documentos de la oferta

El pliego, sus adendas y aclaraciones no forman parte de la oferta, por lo que no se exigirá la presentación de copias de los mismos con la oferta.

Los oferentes inscriptos en el Sistema de Información de Proveedores del Estado (SIPE) de la DNCP, podrán presentar con su oferta, la constancia firmada emitida a través del SIPE, que reemplazará a los documentos solicitados por la convocante en el anexo pertinente del presente pliego.

Los oferentes deberán indicar en su oferta, que documentos que forman parte de la misma son de carácter confidencial e invocar la norma que ampara dicha reserva, para así dar cumplimiento a lo estipulado en la Ley N° 5282/14 "DE LIBRE ACCESO CIUDADANO A LA INFORMACIÓN PÚBLICA Y TRANSPARENCIA GUBERNAMENTAL". Si el oferente no hace pronunciamiento expreso amparado en la Ley, se entenderá que toda su oferta y documentación es pública.

Oferentes en consorcio

Dos o más interesados que no se encuentren comprendidos en las inhabilidades para presentar ofertas o contratar, podrán unirse temporalmente para presentar una oferta sin crear una persona jurídica.

Para ello deberán presentar escritura pública de constitución del consorcio o un acuerdo con el compromiso de formalizar el consorcio por escritura pública en caso de resultar adjudicados, antes de la firma del contrato.

Los integrantes de un consorcio no podrán presentar ofertas individuales ni conformar más de un consorcio en un mismo lote o ítem, lo que no impide que puedan presentarse individualmente o conformar otro consorcio que participe en diferentes partidas.

Aclaración de las ofertas

Con el objeto de facilitar el proceso de revisión, evaluación, comparación y posterior calificación de ofertas, el Comité de Evaluación solicitará a los oferentes, aclaraciones respecto de sus ofertas, dichas solicitudes y las respuestas de los oferentes se realizarán por escrito.

A los efectos de confirmar la información o documentación suministrada por el oferente, el Comité de Evaluación, podrá solicitar aclaraciones a cualquier fuente pública o privada de información.

Las aclaraciones de los oferentes que no sean en respuesta a aquellas solicitadas por la convocante, no serán consideradas.

No se solicitará, ofrecerá, ni permitirá ninguna modificación a los precios ni a la sustancia de la oferta, excepto para confirmar la corrección de errores aritméticos.

Disconformidad, errores y omisiones

Siempre y cuando una oferta se ajuste sustancialmente al pliego de bases y condiciones, el Comité de Evaluación, requerirá que cualquier disconformidad u omisión que no constituya una desviación significativa, sea subsanada en cuanto a la información o documentación que permita al Comité de Evaluación realizar la calificación de la oferta.

A tal efecto, el Comité de Evaluación 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. El Comité de Evaluación, podrá reiterar el pedido cuando la respuesta no resulte satisfactoria, toda vez que no viole el principio de igualdad.

Con la condición de que la oferta cumpla sustancialmente con los Documentos de la Licitación, la Convocante corregirá errores aritméticos de la siguiente manera y notificará al oferente para su aceptación:

1. Si hay una discrepancia entre un precio unitario y el precio total obtenido al multiplicar ese precio unitario por las cantidades correspondientes, prevalecerá el precio total y el precio unitario será corregido.
2. Los precios subtotales podrán ser corregidos siempre que se mantenga inalterable el precio total obtenido en la SBE.
3. En ambos casos, los precios unitarios modificados no podrán ser superiores a los precios unitarios iniciales que figuran en el Acta de Sesión Pública Virtual de la SBE.
4. En caso de que el oferente haya cotizado su precio en guaraníes con décimos y céntimos, la convocante procederá a realizar el redondeo hacia abajo, aun cuando el resultado varíe del precio total que se encuentra en el Acta de Sesión Pública Virtual de la SBE como precio final.
5. Si hay una discrepancia entre palabras y cifras, prevalecerá el monto expresado en palabras a menos que la cantidad expresada en palabras corresponda a un error aritmético, en cuyo caso prevalecerán las cantidades en cifras de conformidad con los párrafos (1) y (2) mencionados.

Idioma de la oferta

La oferta deberá ser presentada en idioma castellano o en su defecto acompañado de su traducción oficial, realizada por un traductor público matriculado en la República del Paraguay.

La convocante permitirá con la oferta, la presentación de catálogos, anexos técnicos o folletos en idioma distinto al castellano y sin traducción:

SI, EN IDIOMA INGLÉS.

Idioma del contrato

El contrato, así como toda la correspondencia y documentos relativos al Contrato, deberán ser escritos en idioma castellano. Los documentos de sustento y material impreso que formen parte del contrato, pueden estar redactados en otro idioma siempre que estén acompañados de una traducción realizada por traductor matriculado en la República del Paraguay, en sus partes pertinentes al idioma castellano y, en tal caso, dicha traducción prevalecerá para efectos de interpretación del contrato.

El proveedor correrá con todos los costos relativos a las traducciones, así como todos los riesgos derivados de la exactitud de dicha traducción.

Moneda de la oferta y pago

La moneda de la oferta y pago será:

En Guaraníes para todos los oferentes

La cotización en moneda diferente de la indicada en este apartado será causal de rechazo de la oferta. Si la oferta seleccionada es en Guaraníes, la oferta se deberá expresar en números enteros, no se aceptarán cotizaciones en decimos y céntimos.

Visita al sitio de ejecución del contrato

La convocante dispone la realización de una visita al sitio con las siguientes indicaciones:

No Aplica

Al culminar la o las visitas, se labrará acta en la cual conste, la fecha, lugar y hora de realización, en la cual se identifique el nombre de las personas que asistieron en calidad de potenciales oferentes, así como del funcionario encargado de dicho acto.

Los gastos relacionados con dicha visita correrán por cuenta del oferente.

Cuando la convocante haya establecido que no será requisito de participación, el oferente podrá declarar bajo fe de juramento conocer el sitio y que cuenta con la información suficiente para preparar la oferta y ejecutar el contrato.

Precio y formulario de la oferta

El oferente indicará el precio total de su oferta y los precios unitarios de los bienes que se propone suministrar, utilizando para ello el formulario de oferta y lista de precios, disponibles para su descarga a través del SICP, formando ambos un único documento.

1. Para la cotización el oferente deberá ajustarse a los requerimientos que se indican a continuación:

- a) El precio cotizado deberá ser el mejor precio posible, considerando que en la oferta no se aceptará la inclusión de descuentos de ningún tipo.
- b) En el caso del sistema de adjudicación por la totalidad de los bienes requeridos, el oferente deberá cotizar en la lista de precios todos los ítems, con sus precios unitarios y totales correspondientes.
- c) En el caso del sistema de adjudicación por lotes, el oferente cotizará en la lista de precios uno o más lotes, e indicará todos los ítems del lote ofertado con sus precios unitarios y totales correspondientes. En caso de no cotizar uno o más lotes, los lotes no cotizados no requieren ser incorporados a la planilla de precios.
- d) En el caso del sistema de adjudicación por ítems, el oferente podrá ofertar por uno o más ítems, en cuyo caso deberá cotizar el precio unitario y total de cada uno o más ítems, los ítems no cotizados no requieren ser incorporados a la planilla de precios.

2. En caso de que se establezca en las bases y condiciones, los precios indicados en la lista de precios serán consignados separadamente de la siguiente manera:

- a) El precio de bienes cotizados, incluidos todos los derechos de aduana, los impuestos al valor agregado o de otro tipo pagados o por pagar sobre los componentes y materia prima utilizada en la fabricación o ensamblaje de los bienes;
- b) Todo impuesto al valor agregado u otro tipo de impuesto que obligue la República del Paraguay a pagar sobre los bienes en caso de ser adjudicado el contrato; y
- c) El precio de otros servicios conexos (incluyendo su impuesto al valor agregado), si lo hubiere, enumerados en los datos de la licitación.

3. En caso de indicarse en el SICP, que se utilizará la modalidad de contrato abierto, cuando se realice por montos mínimos y máximos deberán indicarse el precio unitario de los bienes ofertados; y en caso de realizarse por cantidades mínimas y máximas, deberán cotizarse los precios unitarios

y los totales se calcularán multiplicando los precios unitarios por la cantidad máxima correspondiente.

4. El precio del contrato que cobre el proveedor por los bienes suministrados en virtud del contrato no podrá ser diferente a los precios unitarios cotizados en su oferta, excepto por cualquier ajuste previsto en el mismo.

5. En caso que se requiera el desglose de los componentes de los precios será con el propósito de facilitar a la convocante la comparación de las ofertas.

Abastecimiento simultáneo

El sistema de abastecimiento simultáneo para esta licitación será:

No Aplica

Incoterms

La edición de incoterms para esta licitación será:

No Aplica

Las expresiones DDP, CIP, FCA, CPT y otros términos afines, se regirán por las normas prescriptas en la edición vigente de los Incoterms publicada por la Cámara de Comercio Internacional.

Durante la ejecución contractual, el significado de cualquier término comercial, así como los derechos y obligaciones de las partes serán los prescritos en los Incoterms, a menos que sea inconsistente con alguna disposición del Contrato.

Autorización del Fabricante

Los productos a los cuales se le requerirá Autorización del Fabricante son los indicados a continuación:

SI, PARA TODOS LOS ÍTEMS SOLICITADOS.

Cuando la convocante lo requiera, el oferente deberá acreditar la cadena de autorizaciones, hasta el fabricante o productor.

Muestras

Se requerirá la presentación de muestras de los siguientes productos y en las siguientes condiciones:

No Aplica

En caso de ser solicitadas, las muestras deberán ser presentadas junto con la oferta, o bien en el plazo fijado por la convocante en este apartado, la cual será considerada requisito indispensable para la evaluación de la oferta. La falta de presentación en la forma y plazo establecido por la convocante será causal de descalificación de la oferta.

Copias de la oferta - CPS

El oferente presentará su oferta original. En caso de que la convocante requiera la presentación de copias lo deberá indicar en este apartado, las copias deberán estar identificadas como tales.

Cuando la presentación de ofertas se realice a través del sistema de Oferta Electrónica, la convocante no requerirá de copias.

Cantidad de copias requeridas:

0 copias

Formato y firma de la oferta

1. El formulario de oferta y la lista de precios serán firmados, física o electrónicamente, según corresponda por el oferente o por las personas debidamente facultadas para firmar en nombre del oferente.
2. No serán descalificadas las ofertas que no hayan sido firmadas en documentos considerados no sustanciales.
3. Los textos entre líneas, tachaduras o palabras superpuestas serán válidos solamente si llevan la firma de la persona que firma la Oferta.
4. La falta de foliatura no podrá ser considerada como motivo de descalificación de las ofertas.

Periodo de validez de las ofertas

Las ofertas deberán mantenerse válidas (en días calendarios) por:

120

Las ofertas se deberán mantener válidas por el periodo indicado en el presente apartado, que se computará a partir del inicio de la etapa competitiva. Toda oferta con un periodo menor será rechazada.

La convocante en circunstancias excepcionales podrá solicitar, por escrito, al oferente que extienda el periodo de validez de la oferta, por lo tanto la Garantía de Mantenimiento de la Oferta deberá ser también prorrogada.

El oferente puede rehusarse a tal solicitud sin que se le haga efectiva su Garantía de Mantenimiento de Oferta. A los oferentes que acepten la solicitud de prórroga no se les pedirá ni permitirá que modifiquen sus ofertas.

Garantías: instrumentación, plazos y ejecución.

1. La garantía de mantenimiento de oferta deberá expedirse en un monto en guaraníes que no deberá ser inferior al porcentaje especificado en el SICP. El oferente puede adoptar cualquiera de las formas de instrumentación de las garantías dispuestas por las normativas vigentes.
2. La garantía de mantenimiento de ofertas presentada en los términos del párrafo anterior, deberá cubrir el precio total de la oferta en la etapa de recepción de propuestas.
3. En los contratos abiertos, el porcentaje de las garantías a ser presentado por los oferentes que participen, deberá ser aplicado sobre el monto máximo del llamado; si la adjudicación fuese por lote o ítem ofertado, deberán sumarse los valores máximos de cada lote o ítem ofertado, a fin de obtener el monto sobre el cual se aplicará el porcentaje de la citada garantía.

4. En caso de instrumentarse a través de Garantía Bancaria, deberá estar sustancialmente de acuerdo con el formulario de Garantía de Mantenimiento de oferta incluido en la Sección "Formularios".
5. La garantía de mantenimiento de oferta en caso de oferentes en consorcio deberá ser presentado de la siguiente manera:
- Consorcio constituido por escritura pública: deberán emitir a nombre del consorcio legalmente constituido por escritura pública, del líder del consorcio o de todos los socios que la integran;
 - Consorcio en proceso de formación con acuerdo de intención: deberán emitir a nombre del líder del consorcio en proceso de formación con acuerdo de intención o de todos los miembros que la integran.
6. La garantía de mantenimiento de ofertas podrá ser ejecutada:
- a) Si el oferente altera las condiciones de su oferta,
 - b) Si el oferente retira su oferta durante el período de validez de la oferta,
 - c) Si no acepta la corrección aritmética del precio de su oferta, en caso de existir,
 - d) Si el oferente no presentare su oferta en la fecha y hora señaladas, previo requerimiento por parte de la convocante,
 - e) Si el adjudicatario no procede, por causa imputable al mismo a:
 - e.1. suministrar los documentos indicados en el pliego de bases y condiciones para la firma del contrato,
 - e.2. firmar el contrato,
 - e.3. suministrar en tiempo y forma la garantía de cumplimiento de contrato,
 - e.4. se comprobe que las declaraciones juradas presentadas por el oferente adjudicado con su oferta sean falsas,
 - e.5. el adjudicatario no presentare las legalizaciones correspondientes para la firma del contrato, cuando éstas sean requeridas, o
 - e.6. no se formaliza el consorcio por escritura pública, antes de la firma del contrato.
7. Las garantías tanto de Mantenimiento de Oferta, Cumplimiento de Contrato o de Anticipo, sea cual fuere la forma de instrumentación adoptada, deberá ser pagadera ante solicitud escrita de la convocante donde se haga constar el monto reclamado, cuando se tenga acreditada una de las causales de ejecución de la póliza. En estos casos será requisito que previamente el oferente sea notificado del incumplimiento y la intimación de que se hará efectiva la ejecución del monto asegurado.
8. Si la entrega de los bienes o la prestación de los servicios se realizare en un plazo menor o igual a diez (10) días calendario, posteriores a la firma del contrato, la garantía de cumplimiento deberá ser entregada antes del cumplimiento de la prestación.
9. La garantía de Fiel Cumplimiento de Contrato será liberada y devuelta al proveedor, a requerimiento de parte, a más tardar treinta (30) días contados a partir de la fecha de cumplimiento de las obligaciones del proveedor en virtud de contrato, incluyendo cualquier obligación relativa a la garantía de los bienes.

Periodo de Validez de la Garantía de Mantenimiento de Oferta

El plazo de validez de la Garantía de Mantenimiento de Oferta (en días calendario) será de:

150

El oferente deberá presentar como parte de su oferta una Garantía de Mantenimiento de acuerdo al porcentaje indicado para ello en el SICP y por el plazo indicado en este apartado. Cuando la competencia se desarrolle por más de un día, la garantía de mantenimiento de oferta deberá cubrir a partir del primer día del inicio de la etapa competitiva.

Porcentaje de Garantía de Fiel Cumplimiento de Contrato

El Porcentaje de Garantía de Fiel Cumplimiento de Contrato es de:

5,00 %

La garantía de Cumplimiento de Contrato deberá ser presentada por el proveedor, dentro de los 10 días calendarios siguientes a partir de la fecha de

suscripción del contrato, de conformidad con lo dispuesto en el artículo 39 de la Ley N° 2051/2003.

Periodo de validez de la Garantía de Cumplimiento de Contrato

El plazo de vigencia de la Garantía de Fiel Cumplimiento de Contrato será de:

45 (CUARENTA Y CINCO) MESES, contados desde la entrada en vigor del contrato.

Periodo de validez de la Garantía de los bienes

El periodo de validez de la Garantía de los bienes será el siguiente:

Para los mantenimientos correctivos, el servicio, las piezas y elementos utilizados para las operaciones respectivas deben contar con una garantía de funcionamiento de al menos 6 (seis) meses.

Tiempo de funcionamiento de los bienes

El periodo de tiempo estimado de funcionamiento de los bienes, para los efectos de repuestos será de:

No Aplica

Plazo de reposición de bienes

El plazo de reposición de bienes para reparar o reemplazar será de:

3 (tres) días hábiles, desde el momento de la identificación y comunicación del problema ya sea vía nota, fax o correo electrónico.

El proveedor garantiza que todos los bienes suministrados están libres de defectos derivados de actos y omisiones que este hubiera incurrido, o derivados del diseño, materiales o manufactura, durante el uso normal de los bienes en las condiciones que imperen en la República del Paraguay.

1. La Contratante comunicará al proveedor la naturaleza de los defectos y proporcionará toda evidencia disponible, inmediatamente después de haberlos descubierto. La contratante otorgará al proveedor facilidades razonables para inspeccionar tales defectos.

Tan pronto reciba ésta comunicación, y dentro del plazo establecido en este apartado, deberá reparar o reemplazar los bienes defectuosos, o sus partes sin ningún costo para la contratante.

2. Si el proveedor después de haber sido notificado, no cumple dentro del plazo establecido, la contratante, procederá a tomar medidas necesarias para remediar la situación, por cuenta y riesgo del proveedor y sin perjuicio de otros derechos que la contratante pueda ejercer contra el proveedor en virtud del contrato.

Cobertura de Seguro de los bienes

La cobertura de seguro requerida a los bienes será:

No Aplica

A menos que se disponga otra cosa en este apartado, los bienes suministrados deberán estar completamente asegurados en guaraníes, contra riesgo de extravío o daños incidentales ocurridos durante la fabricación, adquisición, transporte, almacenamiento y entrega, de acuerdo a los incoterms aplicables.

Sistema de presentación de ofertas

Las ofertas serán presentadas en un solo sobre y deberán:

1. Indicar el nombre y la dirección del oferente;
2. Estar dirigidos a la convocante;
3. Llevar la identificación específica del proceso de licitación indicado en el SICP;
4. Llevar una advertencia de no abrir antes de la hora y fecha de apertura de ofertas.

Si los sobres no están cerrados e identificados como se requiere, la convocante no se responsabilizará en caso de que la oferta se extravíe o sea abierta prematuramente.

Plazo para presentar las ofertas

Culminada la etapa competitiva, presentarán las ofertas físicas en la dirección y hasta la fecha y hora que se indican en el SICP, los siguientes participantes requeridos:

TODOS LOS OFERENTES.

Las ofertas deberán ser recibidas por la convocante en la dirección y hasta la fecha y hora que se indican en el SICP.

La convocante podrá a su discreción, extender el plazo originalmente establecido para la presentación de ofertas mediante una adenda. En este caso todos los derechos y obligaciones de la convocante y de los oferentes previamente sujetos a la fecha límite original para presentar las ofertas quedarán sujetos a la nueva fecha prorrogada.

Cuando la presentación de oferta sea electrónica la misma deberá sujetarse a la reglamentación vigente.

Retiro, sustitución y modificación de las ofertas

1. Un Oferente podrá retirar, sustituir o modificar su oferta después de presentada mediante el envío de una comunicación por escrito, debidamente firmada por el representante autorizado. La sustitución o modificación correspondiente de la oferta deberá acompañar dicha comunicación por escrito.

2. Todas las comunicaciones deberán ser:

a) presentadas conforme a la forma de presentación e identificación de las ofertas y además los respectivos sobres deberán estar marcados "RETIRO", "SUSTITUCION" o "MODIFICACION";

b) recibidas por la Convocante antes del plazo límite establecido para la presentación de las ofertas;

Las ofertas cuyo retiro, sustitución o modificación fuere solicitada serán devueltas sin abrir a los oferentes remitentes, durante el acto de apertura de ofertas.

3. Ninguna oferta podrá ser retirada, sustituida o modificada durante el intervalo comprendido entre la fecha límite para presentar ofertas y la expiración del período de validez de las ofertas indicado en el Formulario de Oferta, o cualquier extensión si la hubiere, caso contrario, se hará efectiva la Garantía de Mantenimiento de Oferta.

Apertura de ofertas

1. La convocante abrirá las ofertas y en caso de que hubiere notificaciones de retiro, sustitución y modificación de ofertas presentadas, las leerá en el acto público con la presencia de los oferentes o sus representantes a la hora, en la fecha y el lugar establecidos en el SICP.

2. Cuando la presentación de oferta sea electrónica, el acto de apertura deberá sujetarse a la reglamentación vigente.

3. Primero se procederá a verificar de entre las ofertas recibidas por courier o entregadas personalmente, los sobres marcados como:

a) "RETIRO". Se leerán en voz alta y el sobre con la oferta correspondiente no será abierto sino devuelto al oferente remitente. No se permitirá el retiro de ninguna oferta a menos que la comunicación de retiro pertinente contenga la autorización válida para solicitar el retiro y sea leída en voz alta en el acto de apertura de las ofertas.

b) "SUSTITUCION" se leerán en voz alta y se intercambiará con la oferta correspondiente que está siendo sustituida; la oferta sustituida no se abrirá y se devolverá al oferente remitente. No se permitirá ninguna sustitución a menos que la comunicación de sustitución correspondiente contenga una autorización válida para solicitar la sustitución y sea leída en voz alta en el acto de apertura de las ofertas.

c) "MODIFICACION" se abrirán y leerán en voz alta con la oferta correspondiente. No se permitirá ninguna modificación a las ofertas a menos que la comunicación de modificación correspondiente contenga la autorización válida para solicitar la modificación y sea leída en voz alta en el acto de apertura de las ofertas. Solamente se considerarán en la evaluación los sobres que se abren y leen en voz alta durante el Acto de Apertura de las Ofertas.

4. Los representantes de los oferentes que participen en la apertura de las ofertas deberán contar con autorización suficiente para suscribir el acta y los documentos que soliciten, bastando para ello la presentación de una autorización escrita del firmante de la oferta, esta autorización podrá ser incluida en el sobre oferta o ser portado por el representante.

5. Se solicitará a los representantes de los oferentes que estén presentes que firmen el acta. La omisión de la firma por parte de un Oferente no invalidará el contenido y efecto del acta. Se distribuirá una copia del acta a todos los presentes.

6. Las ofertas sustituidas y modificadas presentadas, que no sean abiertas y leídas en voz alta durante el acto de apertura no podrán ser consideradas para la evaluación sin importar las circunstancias y serán devueltas sin abrir a los oferentes remitentes.

7. La falta de firma en un documento sustancial, es considerada una omisión sustancial que no podrá ser subsanada en ninguna oportunidad una vez abiertas las ofertas.

8. El acta de apertura deberá ser comunicada al Sistema de Información de Contrataciones Públicas para su difusión, dentro de los dos (02) días hábiles de la realización del acto de apertura.

REQUISITOS DE CALIFICACIÓN Y CRITERIOS DE EVALUACIÓN

Esta sección contiene los criterios que la convocante utilizará para evaluar la oferta y determinar si un oferente cuenta con las calificaciones requeridas. Ningún otro factor, método o criterio será utilizado.

Condición de Participación

Podrán participar de ésta licitación, individualmente o en forma conjunta (consorcio), los oferentes domiciliados en la República del Paraguay, que no se encuentren comprendidos en las prohibiciones o limitaciones para presentar propuestas y contratar con el Estado, establecidas en la Ley N° 2051/03 "De Contrataciones Públicas".

Adicionalmente a lo establecido en el párrafo anterior el oferente deberá considerar las siguientes condiciones de participación:

Que se encuentren registrados/as en el Sistema de Información de Proveedores del Estado (SIPE), debiendo suscribir ante el mismo una Declaración Jurada en la cual manifiesta que tiene pleno conocimiento y acepta las reglas del proceso para su activación como oferente. La Declaración Jurada referida, podrá ser descargada desde el SICP, módulo del SIPE.

Que activados/as conforme al SIPE posean su Usuario y Contraseña, personal e intransferible, salvo que los mismos hayan sido cancelados por el Sistema, de conformidad a la reglamentación específica. La pérdida del usuario y contraseña deberá ser comunicada a la DNCP para que, a través del Sistema, sea bloqueado el acceso inmediatamente; y

Como requisito para la participación en la Subasta a la Baja Electrónica, el oferente deberá manifestar en el campo previsto en el Sistema Electrónico, que cumple plenamente los requisitos de habilitación y que su propuesta de precios está conforme con las exigencias del pliego de bases y condiciones.

Requisitos de Calificación

Capacidad Legal

Los oferentes deberán declarar que no se encuentran comprendidos en las limitaciones o prohibiciones para contratar con el Estado, contempladas en el artículo 40 de la Ley N° 2051/03, modificado por Ley N° 6716/2021, declaración que forma parte del formulario de oferta.

Serán desechadas las ofertas de los oferentes que se encuentren comprendidos en las prohibiciones o limitaciones para contratar a la hora y fecha límite de presentación de ofertas o a la fecha de firma del contrato.

A los efectos de la verificación de la existencia de prohibiciones o limitaciones contenidas en los incisos a) y b), m) y n) del artículo 40 de la Ley N° 2051/03, modificado por Ley N° 6716/2021, el comité de evaluación realizará el siguiente análisis:

1. Verificará que el oferente haya proporcionado el formulario de ofertas que incluye la declaratoria debidamente firmada.
2. 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 de la Ley N° 2051/03, modificado por Ley N° 6716/2021.
3. Verificará por los medios disponibles, si el oferente y los demás sujetos individualizados en las prohibiciones o limitaciones contenidas en los incisos a) y b), m) y n) del artículo 40 de la Ley N° 2051/03, modificado por Ley N° 6716/2021, aparecen en la base de datos del SINARH o de la Secretaría de la Función Pública.
4. Si se constata que alguno de las personas mencionadas en el párrafo anterior figura en la base de datos del SINARH o de la Secretaría de la Función Pública, el comité analizará acabadamente si tal situación le impedirá ejecutar el contrato, exponiendo los motivos para aceptar o rechazar la oferta, según sea el caso.
5. Verificará que el oferente haya proporcionado el formulario de Declaración de Miembros, de conformidad a estándar debidamente firmado en su oferta y cotejará los datos con las personas físicas inhabilitadas que constan en el registro de "Sanciones a Proveedores" del SICP a fin de detectar si directores, gerentes, socios gerentes, quienes ejerzan la administración, accionistas, cuotapartistas o propietarios se hallan comprendidos en el presupuesto del inciso m) y n) del artículo 40 de la Ley N° 2051/03, modificado por Ley N° 6716/2021.

El comité podrá recurrir a fuentes públicas o privadas de información, para verificar los datos proporcionados por el oferente.

6. Si el Comité confirma que el oferente o sus integrantes poseen impedimentos, la oferta será rechazada y se remitirán los antecedentes a la Dirección Nacional de Contrataciones Públicas (DNCP) para los fines pertinentes.

Análisis de precios ofertados

Durante la evaluación de ofertas, luego de haber realizado la corrección de errores aritméticos y de ordenar las ofertas presentadas de menor a mayor, el Comité de Evaluación procederá a solicitar a los oferentes una explicación detallada de la composición del precio ofertado de cada ítem, 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, 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.

Certificado de Producto y Empleo Nacional - CPS

A los efectos de acogerse al beneficio de la aplicación del margen de preferencia, el oferente deberá contar con el Certificado de Producto y Empleo Nacional (CPEN). El certificado debe ser emitido como máximo a la fecha y hora de la etapa competitiva.

La falta del CPEN no será motivo de descalificación de la oferta, sin embargo, el oferente no podrá acogerse al beneficio.

El comité de evaluación verificará en el portal oficial indicado por el Ministerio de Industria y Comercio (MIC) la emisión en tiempo y forma del CPEN declarado por los oferentes. No será necesaria la presentación física del Certificado de Producto y Empleo Nacional.

Independientemente al sistema de adjudicación, el margen de preferencia será aplicado a cada bien o servicio objeto de contratación que se encuentre indicado en la planilla de precios.

a) Consorcios:

a.1. Provisión de Bienes

El CPEN debe ser expedido a nombre del oferente que fabrique o produzca los bienes objeto de la contratación. En el caso que ninguno de los oferentes consorciados fabrique o produzca los bienes ofrecidos, el consorcio deberá contar con el CPEN correspondiente al bien ofertado, debiendo encontrarse debidamente autorizado por el fabricante. Esta autorización podrá ser emitida a nombre del consorcio o de cualquiera de los integrantes del mismo.

Margen de preferencia local - CPS

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 la más baja pertenece a 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, se le aplicará únicamente el margen de este último.

Las convocantes deberán acogerse a las condiciones específicas para la aplicación del Margen de Preferencia Local establecidas en la reglamentación emitida por la DNCP.

Requisitos documentales para evaluación de las condiciones de participación

1. Formulario de Oferta (*) SUSTANCIAL

[El formulario de oferta y lista de precios, generados electrónicamente a través del SICP, deben ser completados y firmados por el oferente.]

2. Garantía de Mantenimiento de Oferta (*) SUSTANCIAL

La garantía de mantenimiento de oferta debe ser extendida, bajo la forma de una garantía bancaria o póliza de seguro de caución.

3. Certificado de Cumplimiento con la Seguridad Social. ()**

4. Certificado de Producto y Empleo Nacional, emitido por el MIC, en caso de contar. ()**

5. 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 según los incisos a) y b) del numeral 2 del art. 1 de la Ley N° 6355/19. (**) **NO APLICA.**

6. Declaración Jurada de Declaración de Miembros, de conformidad con el formulario estándar Sección Formularios ()**

7. Certificado de Cumplimiento Tributario ()**

8. Patente Comercial del municipio en donde esté asentado el establecimiento principal del oferente. ()**

9. Documentos legales

9.1. Oferentes Individuales. Personas Físicas.

- Fotocopia simple de la Cédula de Identidad del firmante de la oferta. (**) **SUSTANCIAL**

- Constancia de inscripción en el Registro Único de Contribuyentes - RUC. (**) **SUSTANCIAL**

- 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 simple 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. (**) **SUSTANCIAL**

9.2. Oferentes Individuales. Personas Jurídicas.

- 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. (**) **SUSTANCIAL**

- Constancia de inscripción en el Registro Único de Contribuyentes y fotocopia simple de los documentos de identidad de los representantes o apoderados de la sociedad.

- 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); o 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. (**) **SUSTANCIAL**

9.3. Oferentes en Consorcio.

1. Cada integrante del consorcio que sea una persona física domiciliada en la República del Paraguay deberá presentar los documentos requeridos para Oferentes Individuales especificados en el apartado Oferentes individuales. Personas Físicas. Cada integrante del consorcio que sea una persona jurídica domiciliada en Paraguay deberá presentar los documentos requeridos para Oferentes Individuales Personas Jurídicas. (*) **SUSTANCIAL**
2. Original o fotocopia del consorcio constituido o del acuerdo de intención de constituir el consorcio por escritura pública en caso de resultar adjudicados y antes de la firma del contrato. Las formalidades de los acuerdos de intención y de los consorcios serán determinadas por la Dirección Nacional de Contrataciones Públicas (DNCP). (*) **SUSTANCIAL**
3. Fotocopia simple de los documentos que acrediten las facultades de los firmantes del acuerdo de intención de consorciarse. Estos documentos pueden consistir en (*) **SUSTANCIAL**:
 - Un poder suficiente otorgado por escritura pública por cada miembro del consorcio (no es necesario que esté inscripto en el Registro de Poderes); o
 - Los documentos societarios de cada miembro del consorcio, que justifiquen la representación del firmante, tales como actas de asamblea y de directorio en el caso de las sociedades anónimas.
4. Fotocopia simple de los documentos que acrediten las facultades del firmante de la oferta para comprometer al consorcio, cuando se haya formalizado el consorcio. Estos documentos pueden consistir en (*) **SUSTANCIAL**:
 1. Un poder suficiente otorgado por escritura pública por la Empresa Líder del consorcio (no es necesario que esté inscripto en el Registro de Poderes); o
 2. Los documentos societarios de la Empresa Líder, que justifiquen la representación del firmante, tales como actas de asamblea y de directorio en el caso de las sociedades anónimas.

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

Los documentos indicados con doble asterisco (**) deberán estar vigentes al inicio de la etapa competitiva.

Capacidad Financiera

Con el objetivo de calificar la situación financiera del oferente, se considerarán los siguientes índices:

a. Para contribuyente de IRE.

Deberán cumplir con los siguientes parámetros:

Ratio de Liquidez: activo corriente / pasivo corriente

Deberá ser igual o mayor que 1, en promedio, en los años 2019, 2020, 2021.

Endeudamiento: pasivo total/ activo total

No deberá ser mayor a 0,80 en promedio, en los años 2019, 2020, 2021.

Rentabilidad: Porcentaje de utilidad después de impuestos o pérdida con respecto al Capital.

El promedio de la sumatoria de los años 2019, 2020, 2021, no deberá ser negativo.

b. Para contribuyentes de IRE SIMPLE.

Deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso) Deberá ser igual o mayor que 1, el promedio de la sumatoria de los años 2019, 2020, 2021.

c. Para contribuyentes de IRP

Deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso).

Deberá ser igual o mayor que 1, el promedio de la sumatoria de los años 2019, 2020, 2021.

d. Para contribuyentes de exclusivamente IVA General

Deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso). Deberá ser igual o mayor que 1, el promedio de la sumatoria de los años 2019, 2020, 2021.

- **OFERENTES EN CONSORCIO:** Cada miembro debe cumplir con el requisito.

Requisitos documentales para la evaluación de la capacidad financiera

a. Balance General y Estados de Resultados (comparativo) de los años 2019, 2020, 2021, firmados por el contador, propietario y/o representante legal si correspondiere, acorde a las normas contables y a los modelos establecidos en las Normativas Vigentes de la Sub Secretaría de Estado de Tributación, que se encuentran en la página web de la SET (www.set.gov.py).

b. Formulario 101 para el año 2019 y Formulario 500 para los años 2020 y 2021, correspondientes a la Declaración Jurada del Impuesto a la Renta.

c. Formulario 106 para el año 2019, y Formulario 501 para los años 2020, 2021 correspondientes a contribuyentes del IRE SIMPLE.

d. Formulario 104 del año 2019, Formulario 515 para contribuyentes de Renta Personal y Formulario 516 IRP RGC para los años 2020, 2021.

e. Formulario 120 para contribuyentes del IVA General de los últimos 36 (TREINTA Y SEIS) meses, correspondiente a los años 2019, 2020 y 2021.

Experiencia requerida

Con el objetivo de calificar la experiencia del oferente, se considerarán los siguientes índices:

1. Demostrar la experiencia en **VENTA, INSTALACIÓN O CONFIGURACIÓN DE LOS EQUIPOS OFERTADOS** con copias de contratos ejecutados y/o facturas anteriores ya sea en entidades públicas y/o privadas. Los contratos y/o facturas deberán ser de los últimos tres años (2019, 2020, 2021) y la sumatoria deberá ser como mínimo el 50% (CINCUENTA POR CIENTO) del monto total de la oferta. No es necesario contar con un contrato por año.

2. El oferente deberá contar con al menos 5 años de experiencia en el mercado de las Telecomunicaciones.

OFERENTES EN CONSORCIO: El socio líder debe cumplir al menos con el 60% (SESENTA POR CIENTO) del requisito y los demás socios en su conjunto al menos el 40% (CUARENTA POR CIENTO) de este requisito.

Requisitos documentales para la evaluación de la experiencia

1. Copias de contratos ejecutados anteriores demostrando la experiencia en **VENTA, INSTALACIÓN O CONFIGURACIÓN DE LOS EQUIPOS OFERTADOS**, ya sea en entidades públicas y/o privadas. Los contratos y/o facturas deberán ser de los últimos tres años (2019, 2020, 2021) y la sumatoria deberá ser como mínimo el 50% (CINCUENTA POR CIENTO) del monto total de la oferta. No es necesario contar con un contrato por año.
2. Copia del Estatuto de Conformación de la empresa, que demuestre que cuentan con -al menos- 5 (cinco) años de experiencia en el rubro de las telecomunicaciones.

Capacidad Técnica

El oferente deberá proporcionar evidencia documentada que demuestre su cumplimiento con los siguientes requisitos de capacidad técnica:

1. Deberá contar con al menos 4 (cuatro) técnicos certificados en las marcas de los ítems ofertados, de los cuales, 2 (dos) técnicos con certificación de nivel superior y 2 (dos) técnicos con certificación de nivel medio. Los mismos deberán formar parte del plantel de la empresa.
 2. La empresa oferente debe contar con autorización del fabricante para proveer los equipos de la marca ofertada, ser servicio técnico autorizado o estar debidamente autorizado por el fabricante o el representante para brindar asistencia para equipos de la marca ofertada.
 3. Contar con el aval de al menos 2 (dos) clientes que demuestren haber recibido a satisfacción los trabajos realizados por el Oferente referente a la venta, instalación o configuración de equipos. Dichos documentos deberán corresponder a los años (2019, 2020, 2021).
 4. Los equipos ofertados (ítems 1 y 3) deberán contar con Certificación de Calidad ISO 9001:2015 o similar. El mismo deberá ser mínimamente para fabricación. (No se aceptarán certificados de ensamblaje de equipos).
 5. Especificaciones técnicas de los bienes ofertados.
- **OFERENTES EN CONSORCIO:** El socio líder debe cumplir al menos con el 60 % (SESENTA POR CIENTO) del requisito y los demás socios en su conjunto al menos el 40 % (CUARENTA POR CIENTO) de este requisito.

Requisito documental para evaluar la capacidad técnica

1. Listado de 4 (cuatro) técnicos certificados en la marca de los ítems ofertado, acompañado de la Planilla de Instituto de Previsión Social correspondiente al mes de septiembre de 2022 donde figuren los técnicos propuestos.
 - a. 2 (dos) técnicos con certificación de nivel superior (Ej.: Cisco CCNP, Fortinet NSE7, Sonicwall SNSP), los mismos deberán acompañar la siguiente documentación:
 - Currículum Vitae
 - Certificados por la marca de los ítems ofertados
 - Fotocopia de cédula de identidad de los técnicos
 - b. 2 (dos) técnicos con certificación de nivel medio (Ej.: Cisco CCNA, Fortinet NSE4, Sonicwall SNSA), los mismos deberán acompañar la siguiente documentación:
 - Currículum Vitae
 - Certificados por la marca de los ítems ofertados
 - Fotocopia de cédula de identidad de los técnicos
2. La empresa oferente deberá contar con autorización del fabricante para proveer, instalar y soportar los equipos adquiridos.

Para Representantes debe reunir los siguientes requisitos: Documentación expedida por el Fabricante que los acredite como

representante de la marca ofertada y centro autorizado de servicios (CAS), dichos documentos deben estar debidamente legalizados por el Consulado Paraguayo del País de emisión del documento y del Ministerio de Relaciones Exteriores de la República del Paraguay. Los mismos deben ser originales o copias autenticadas por Escribano Público.

Para Distribuidor Autorizado debe reunir los siguientes requisitos: Documentación expedida por el Fabricante que los acredite como distribuidor autorizado de la marca ofertada y centro autorizado de servicios (CAS), para tal efecto debe presentar el documento original o copia autenticada por Escribano Público, y el mismo debe estar debidamente legalizado por el Consulado Paraguayo del País de emisión del documento y del Ministerio de Relaciones Exteriores de la República del Paraguay.

Para Sub-Distribuidor debe reunir los siguientes requisitos: Documento original o copia autenticada por Escribano Público de la autorización del Fabricante extendida al Representante, Distribuidor y/o Resellers para el PARAGUAY Y/O LATINOAMERICA que lo nombra como representante, o distribuidor autorizado de la marca ofertada y centro autorizado de servicios (CAS), en la cual lo autoriza a nombrar sub - distribuidores. Para tal efecto debe presentar el documento original o copia autenticada por Escribano Público, y el mismo debe estar debidamente legalizado por el Consulado Paraguayo del País de emisión del documento y del Ministerio de Relaciones Exteriores de la República del Paraguay.

Serán considerados válidos los documentos apostillados como los documentos legalizados por el Consulado y el Ministerio de Relaciones Exteriores en conformidad a la **Ley N° 4987/13 QUE APRUEBA EL CONVENIO SUPRIMIENDO LA EXIGENCIA DE LA LEGALIZACIÓN DE LOS DOCUMENTOS PÚBLICOS EXTRANJEROS.**

Cuando la convocante lo requiera, el oferente deberá acreditar la cadena de autorizaciones, hasta el fabricante o productor.

• **OBSERVACIÓN:**

- La autorización del fabricante debe ser presentada indefectiblemente con la oferta estando o no este documento legalizado o apostillado.
- En caso de que el oferente no cuente con la autorización del fabricante legalizada o apostillada al momento de la presentación de la oferta, se aclara que, para firma del contrato, el oferente adjudicado deberá presentar el documento debidamente legalizado por el Consulado Paraguayo del país de emisión del documento y del Ministerio de Relaciones Exteriores de la República del Paraguay o apostillado en conformidad a la Ley N° 4987/13 QUE APRUEBA EL CONVENIO SUPRIMIENDO LA EXIGENCIA DE LA LEGALIZACIÓN DE LOS DOCUMENTOS PÚBLICOS EXTRANJEROS.
- El documento presentado con la oferta debe presentar identidad con el documento presentado para la firma del contrato.

3. Certificados o constancias de satisfacción de clientes, referente a la venta, instalación o configuración de equipos. Dichos documentos deberán corresponder a los años (2019, 2020, 2021).
4. Certificación de Calidad ISO 9001:2015 o similar. El mismo deberá ser mínimamente para fabricación. (No se aceptarán certificados de ensamblaje de equipos).
5. Especificaciones técnicas de los bienes ofertados acompañado de Catálogo de cada uno de los ítems ofertados.

Criterio de desempate de ofertas

El vencedor de cada grupo subastado será el oferente que ingresó el menor precio. En los casos de igualdad de precios, queda como vencedor el que lo haya ingresado primero.

Siempre que el criterio de desempate establecido, no sea aplicable, el comité de evaluación determinará cuál de ellas es la mejor calificada para ejecutar el contrato utilizando los criterios dispuestos para el efecto por la DNCP.

Nota1: Conforme a lo previsto en el Decreto reglamentario de la Ley de Contrataciones los adjudicatarios de los contratos resultantes de los procesos licitatorios, deberán inscribirse en el Sistema de Información de Proveedores del Estado - SIPE, como requisito previo a la emisión del Código de Contratación respectivo, no siendo la inscripción una exigencia para participar en el proceso tradicional.

SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS

Esta sección constituye el detalle de los bienes con sus respectivas especificaciones técnicas - EETT, de manera clara y precisa para que el oferente elabore su oferta. Salvo aquellas EETT de productos ya determinados por plantillas aprobadas por la DNCP.

Suministros y Especificaciones técnicas

El Suministro deberá incluir todos aquellos ítems que no hubiesen sido expresamente indicados en la presente sección, pero que pueda inferirse razonablemente que son necesarios para satisfacer el requisito de suministro indicado, por lo tanto, dichos bienes serán suministrados por el Proveedor como si hubiesen sido expresamente mencionados, salvo disposición contraria en el Contrato.

Los bienes suministrados deberán ajustarse a las especificaciones técnicas y las normas estipuladas en este apartado. En caso de que no se haga referencia a una norma aplicable, la norma será aquella que resulte equivalente o superior a las normas oficiales de la República del Paraguay. Cualquier cambio de dichos códigos o normas durante la ejecución del contrato se aplicará solamente con la aprobación de la contratante y dicho cambio se registrará de conformidad a la cláusula de adendas y cambios.

El Proveedor tendrá derecho a rehusar responsabilidad por cualquier diseño, dato, plano, especificación u otro documento, o por cualquier modificación proporcionada o diseñada por o en nombre de la Contratante, mediante notificación a la misma de dicho rechazo.

Detalle de los productos con las respectivas especificaciones técnicas

Los productos a ser requeridos cuentan con las siguientes especificaciones técnicas:

ALCANCE DE LOS TRABAJOS Y SERVICIOS

Los oferentes deben entregar todos los subsistemas del presente llamado en la modalidad de llave en mano, por lo cual deben tener en cuenta todos los equipamientos, accesorios, materiales de instalación, horas de servicio técnico especializado para la correcta implementación de la solución ofertada, de acuerdo con los requerimientos técnicos del presente documento. A continuación, se listan de manera enunciativa y no limitativa algunas de las consideraciones dentro del alcance del presente llamado.

1. El sistema de seguridad perimetral para el Datacenter de la DGRP correspondiente a este documento comprende la provisión, instalación y configuración del Firewall, Sistema de Reporte y Switches de Acceso para proveer seguridad, alta disponibilidad y gestión a la red de la DGRP.
2. Se deben proveer la cantidad de equipos necesarios que cumplan con los requerimientos mínimos de este documento para soportar los servicios actuales y futuros de voz, datos, video en todas las dependencias del edificio.
3. Se debe considerar que, para la correcta implementación de la solución e integración a los equipos existentes, serán necesarios realizar cambios en la infraestructura actual, para lo cual, la convocante prestará la asistencia necesaria.
4. Queda a cargo de los oferentes, la correcta configuración, implementación e integración de la solución ofertada con la infraestructura actual, de acuerdo a los más altos estándares y mejores prácticas de la industria, contemplando configuración, por mencionar apenas algunas de ellas, hardening, acceso a proveedores, ruteo dinámico y estático externo, ruteo interno local y entre vlans, integración con Active Directory mediante LDAP, políticas de acceso a Internet por usuario y grupos, filtrado web, VPNs, antivirus, IPS, anti malware, anti phishing, ACLs, NAT, port forwarding, publicación de servicios web. El tiempo máximo para el despliegue no deberá superar los 30 días hábiles.

La convocante se reserva el derecho de verificación in situ de las instalaciones de los oferentes de manera a corroborar que los oferentes cuentan con los recursos y capacidad necesaria para proveer este servicio.

Soporte

El soporte requerido deberá ser in-situ e incluir la configuración de los equipos en el formato que la convocante lo exija.

En caso de alguna falla en un equipo, que impida su correcto uso o funcionamiento, se deberá prever un tiempo máximo de respuesta de 4 horas a partir de la comunicación por correo electrónico de la convocante al proveedor. En caso de que el equipo no pueda ser reparado se deberá reemplazar por uno igual o de mayores prestaciones hasta la devolución del equipo reparado; se deberá dejar en funcionamiento todos los servicios con todas las configuraciones. Este soporte es solicitado por el tiempo que dure la Garantía.

La empresa oferente deberá contar con un Centro de Atención al Cliente propio de la empresa y que sea con funcionalidad operativa 7x24 (24 horas del día, los 365 días del año). Este centro de atención debe tener a disposición técnicos de guardia permanente para los casos de

asistencia remota o in situ. Además, deberá anexar una documentación donde mencione niveles de escalamiento con números de teléfonos y direcciones de correo, y deberá garantizar que las solicitudes e incidencias sean gestionadas mediante un sistema de Tickets que permita el seguimiento y la gestión de los incidentes hasta su cierre (solución de los mismos). Igualmente, deberá anexar una Declaración Jurada indicando el cumplimiento, así como también la convocante se reserva el derecho de una verificación en sitio del oferente, en caso de que así se requiera.

Capacitación

El Oferente deberá prever, por cada ítem ofertado, la capacitación local corriendo con todos los gastos por cuenta propia, para 5 (cinco) funcionarios de la convocante con una duración mínima de 30 horas (reloj), en modalidad presencial en las oficinas de la Convocante en horario de oficina.

ÍTEM N°	BIEN	ESPECIFICACIONES TÉCNICAS	UNIDAD DE MEDIDA	PRESENTACIÓN	CANTIDAD
1	EQUIPOS DE SEGURIDAD DE REDES (UTM)	SEGÚN EETT	UNIDAD	EVENTO	2
2	SOFTWARE DE REGISTROS, ANÁLISIS Y REPORTES	SEGÚN EETT	UNIDAD	EVENTO	1
3	EQUIPOS DE CONMUTACIÓN (SWITCH)	SEGÚN EETT	UNIDAD	EVENTO	2
4	SERVICIO DE CAPACITACIÓN	SEGÚN EETT	UNIDAD	EVENTO	1

ESPECIFICACIONES TÉCNICAS

ITEM 1. EQUIPOS DE SEGURIDAD DE REDES (UTM)	
Descripción	Requerimiento mínimo
Marca	indicar
Modelo	indicar
Procedencia	indicar
Cantidad	2 (dos)
Requisitos Mínimos	
NGFW en factor de forma appliance, rackeable de 1U	REQUERIDO

Throughput de por lo menos 25 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6	REQUERIDO
Soporte a por lo menos 3M conexiones simultaneas	REQUERIDO
Soporte a por lo menos 250K nuevas conexiones por segundo	REQUERIDO
Throughput de al menos 12 Gbps de VPN IPSec	REQUERIDO
Estar licenciado para, o soportar sin necesidad de licencia, 2K túneles de VPN IPSec site-to-site simultáneos	REQUERIDO
Estar licenciado para, o soportar sin necesidad de licencia, 15K túneles de clientes VPN IPSec simultáneos	REQUERIDO
Throughput de al menos 2 Gbps de VPN SSL	REQUERIDO
Soportar al menos 500 clientes de VPN SSL simultáneos	REQUERIDO
Soportar al menos 5 Gbps de throughput de IPS	REQUERIDO
Soportar al menos 4 Gbps de throughput de Inspección SSL	REQUERIDO
Soportar al menos 10 Gbps de throughput de Application Control	REQUERIDO
Soportar al menos 3 Gbps de throughput de NGFW	REQUERIDO
Soportar al menos 3 Gbps de throughput de Threat Protection	REQUERIDO
Permitir gestionar al menos 25 Access Points	REQUERIDO
Tener al menos 24 interfaces, 16 RJ45 y 8 SFP de 1 Gbps cada uno	REQUERIDO
Tener al menos 4 interfaces SFP+ de 10 Gbps cada uno	REQUERIDO
Estar licenciado y/o tener incluido sin costo adicional, al menos 9 sistemas virtuales lógicos (Contextos) por appliance	REQUERIDO
Soporte de por lo menos 10 sistemas virtuales lógicos (Contextos) por appliance	REQUERIDO
Fuente redundante	REQUERIDO
Al menos deberá contar con las siguientes certificaciones: FCC, CE, VCCI	REQUERIDO

Al menos deberá contar con las siguientes certificaciones: ISO 9001 y ICSA Labs	REQUERIDO
Requisitos Mínimos de Funcionalidad	
Características Generales	
La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo;	REQUERIDO
Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;	REQUERIDO
Las funcionalidades de protección de red que conforman la plataforma de seguridad, pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;	REQUERIDO
La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;	REQUERIDO
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;	REQUERIDO
La gestión del equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;	REQUERIDO
Los dispositivos de protección de red deben soportar mínimamente 4094 VLANs Tags 802.1q;	REQUERIDO
Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;	REQUERIDO
Los dispositivos de protección de red deben soportar policy based routing y policy based forwarding;	REQUERIDO
Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);	REQUERIDO
Los dispositivos de protección de red deben soportar DHCP Relay;	REQUERIDO
Los dispositivos de protección de red deben soportar DHCP Server;	REQUERIDO
Los dispositivos de protección de red deben soportar sFlow;	REQUERIDO
Los dispositivos de protección de red deben soportar Jumbo Frames;	REQUERIDO

Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;	REQUERIDO
Debe ser compatible con NAT dinámica (varios-a-1);	REQUERIDO
Debe ser compatible con NAT dinámica (muchos-a-muchos);	REQUERIDO
Debe soportar NAT estática (1-a-1);	REQUERIDO
Debe admitir NAT estática (muchos-a-muchos);	REQUERIDO
Debe ser compatible con NAT estático bidireccional 1-a-1;	REQUERIDO
Debe ser compatible con la traducción de puertos (PAT);	REQUERIDO
Debe ser compatible con NAT Origen;	REQUERIDO
Debe ser compatible con NAT de destino;	REQUERIDO
Debe soportar NAT de origen y NAT de destino de forma simultánea;	REQUERIDO
Debe soportar NAT de origen y NAT de destino en la misma política	REQUERIDO
Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;	REQUERIDO
Debe ser compatible con NAT64 y NAT46;	REQUERIDO
Debe implementar el protocolo ECMP;	REQUERIDO
Debe soportar SD-WAN de forma nativa	REQUERIDO
Debe soportar el balanceo de enlace hash por IP de origen;	REQUERIDO
Debe soportar el balanceo de enlace por hash de IP de origen y destino;	REQUERIDO
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;	REQUERIDO
Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;	REQUERIDO

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;	REQUERIDO
Enviar logs a sistemas de gestión externos simultáneamente;	REQUERIDO
Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;	REQUERIDO
Debe soportar protección contra la suplantación de identidad (anti-spoofing);	REQUERIDO
Implementar la optimización del tráfico entre dos dispositivos;	REQUERIDO
Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);	REQUERIDO
Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);	REQUERIDO
Soportar OSPF graceful restart;	REQUERIDO
Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;	REQUERIDO
Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;	REQUERIDO
Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;	REQUERIDO
Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;	REQUERIDO
Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;	REQUERIDO
Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;	REQUERIDO
Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;	REQUERIDO
La configuración de alta disponibilidad debe sincronizar: Sesiones;	REQUERIDO
La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;	REQUERIDO
La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;	REQUERIDO

La configuración de alta disponibilidad debe sincronizar: Tablas FIB;	REQUERIDO
En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;	REQUERIDO
Debe soportar la creación de sistemas virtuales en el mismo equipo;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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);	REQUERIDO
Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
La consola de administración debe soportar como mínimo, inglés y español.	REQUERIDO
La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad	REQUERIDO
La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.	REQUERIDO
Control por Política de Firewall	
Debe soportar controles de zona de seguridad;	REQUERIDO
Debe contar con políticas de control por puerto y protocolo;	REQUERIDO

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;	REQUERIDO
Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;	REQUERIDO
Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;	REQUERIDO
Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;	REQUERIDO
Debe soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.	REQUERIDO
Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);	REQUERIDO
Debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes	REQUERIDO
Debe soportar el protocolo estándar de la industria VXLAN;	REQUERIDO
La solución debe permitir la implementación sin asistencia de SD-WAN	REQUERIDO
En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN;	REQUERIDO
la solución debe soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall.	REQUERIDO
Control de Aplicación	
Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;	REQUERIDO
Detección de miles de aplicaciones en 18 categorías, 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;	REQUERIDO
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;	REQUERIDO

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;	REQUERIDO
Para tráfico 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;	REQUERIDO
Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;	REQUERIDO
Actualización de la base de firmas de la aplicación de forma automática;	REQUERIDO
Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos;	REQUERIDO
Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;	REQUERIDO
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;	REQUERIDO
El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;	REQUERIDO
Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;	REQUERIDO
Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;	REQUERIDO
Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitir a Hangouts el chat, pero impedir la llamada de video;	REQUERIDO
Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;	REQUERIDO
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);	REQUERIDO
Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;	REQUERIDO
Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;	REQUERIDO

Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente	REQUERIDO
Prevención de Amenazas	
Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;	REQUERIDO
Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);	REQUERIDO
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;	REQUERIDO
Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;	REQUERIDO
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;	REQUERIDO
Debe permitir el bloqueo de vulnerabilidades y exploits conocidos	REQUERIDO
Debe incluir la protección contra ataques de denegación de servicio;	REQUERIDO
Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;	REQUERIDO
Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;	REQUERIDO
Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;	REQUERIDO
Debe tener los siguientes mecanismos de inspección IPS: Reensamblado de paquetes TCP;	REQUERIDO
Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);	REQUERIDO
Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc;	REQUERIDO
Detectar y bloquear los escaneos de puertos de origen;	REQUERIDO
Bloquear ataques realizados por gusanos (worms) conocidos;	REQUERIDO
Contar con firmas específicas para la mitigación de ataques DoS y DDoS;	REQUERIDO

Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);	REQUERIDO
Debe poder crear firmas personalizadas en la interfaz gráfica del producto;	REQUERIDO
Identificar y bloquear la comunicación con redes de bots;	REQUERIDO
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;	REQUERIDO
Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;	REQUERIDO
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;	REQUERIDO
Los eventos deben identificar el país que origino la amenaza;	REQUERIDO
Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);	REQUERIDO
Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
Proporcionar 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);	REQUERIDO
Filtrado de URL	
Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora);	REQUERIDO

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;	REQUERIDO
Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;	REQUERIDO
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;	REQUERIDO
Tener por lo menos 75 categorías de URL;	REQUERIDO
Debe tener la funcionalidad de exclusión de URLs por categoría;	REQUERIDO
Permitir página de bloqueo personalizada;	REQUERIDO
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);	REQUERIDO
Además del Explicit Web Proxy, soportar proxy web transparente;	REQUERIDO
Identificación de Usuarios	
Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/control basados en usuarios y grupos de usuarios;	REQUERIDO

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 autenticación residente en el equipo de seguridad (portal cautivo);	REQUERIDO
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;	REQUERIDO
Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;	REQUERIDO
Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;	REQUERIDO
Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;	REQUERIDO
QoS Traffic Shaping	
Capacidad de controlar el ancho de banda máximo utilizado, por usuario o aplicación, tanto audio como vídeo sobre demanda	REQUERIDO
Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;	REQUERIDO
Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;	REQUERIDO
Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;	REQUERIDO
Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;	REQUERIDO
Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;	REQUERIDO
En QoS debe permitir la definición de tráfico con ancho de banda garantizado;	REQUERIDO
En QoS debe permitir la definición de tráfico con máximo ancho de banda;	REQUERIDO
En QoS debe permitir la definición de colas de prioridad;	REQUERIDO
Soportar marcación de paquetes DiffServ, incluso por aplicación;	REQUERIDO
Soportar la modificación de los valores de DSCP para Diffserv;	REQUERIDO
Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);	REQUERIDO

Debe soportar QoS (traffic-shaping) en las interfaces agregadas o redundantes;	REQUERIDO
Filtro de Datos	
Permite la creación de filtros para archivos y datos predefinidos;	REQUERIDO
Los archivos deben ser identificados por tamaño y tipo;	REQUERIDO
Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones;	REQUERIDO
Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;	REQUERIDO
Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;	REQUERIDO
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;	REQUERIDO
Geo Localización	
Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;	REQUERIDO
Debe permitir la visualización de los países de origen y destino en los registros de acceso;	REQUERIDO
Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;	REQUERIDO
VPN	
Soporte VPN de sitio-a-sitio y cliente-a-sitio;	REQUERIDO
Soportar VPN IPSec;	REQUERIDO
Soportar VPN SSL;	REQUERIDO
La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512	REQUERIDO
La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;	REQUERIDO

La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);	REQUERIDO
La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);	REQUERIDO
Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;	REQUERIDO
Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;	REQUERIDO
Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución.	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;	REQUERIDO
Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;	REQUERIDO
Deberá mantener una conexión segura con el portal durante la sesión;	REQUERIDO
El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.	REQUERIDO
Wireless Controller	
Solución de red inalámbrica que administre y controle de manera centralizada los puntos de acceso (AP);	REQUERIDO
Cualquier licencia y / o software necesario para la plena ejecución de todas las características descritas en este término de referencia deberá ser suministrada;	REQUERIDO
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;	REQUERIDO
La solución debe ser capaz de administrar puntos de acceso de tipo indoor y outdoor;	REQUERIDO
El controlador inalámbrico debe permitir ser descubierto automáticamente por los puntos de acceso a través de Broadcast, DHCP y consulta DNS;	REQUERIDO

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;	REQUERIDO
Permitir programar día y hora en que ocurrirá la optimización del aprovisionamiento automático de canales en los Access Points;	REQUERIDO
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;	REQUERIDO
Cuando tunelado, el tráfico debe ser encriptado a través de DTLS o IPSEC;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
La solución debe implementar recursos que posibiliten la identificación de interferencias provenientes de equipos que operen en las frecuencias de 2.4GHz y 5GHz;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO

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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
Debe permitir restringir el número máximo de dispositivos conectados por punto de acceso y por radio;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO

La solución debe implementar el estándar IEEE 802.11v para permitir que la red influya en las decisiones de roaming de la cliente conectada mediante el suministro de información complementaria, como la carga de utilización de los puntos de acceso cercanos;	REQUERIDO
La solución debe implementar el estándar IEEE 802.11w para prevenir ataques a la infraestructura inalámbrica;	REQUERIDO
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;	REQUERIDO
La solución debe implementar técnicas de Call Admission Control para limitar el número de llamadas simultáneas;	REQUERIDO
La solución debe mostrar información sobre los dispositivos conectados a la infraestructura inalámbrica y presentar 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;	REQUERIDO
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;	REQUERIDO
La solución debe permitir la configuración de los data rates que se activarán en la herramienta y las que se deshabilitan para las frecuencias de 2.4 y 5GHz y los estándares 802.11a / b / g / n / ac;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
La solución debe permitir la configuración del valor de Short Guard Interval para 802.11n y 802.11ac en 5GHz;	REQUERIDO
La solución debe implementar una característica conocida como Airtime Fairness (ATF) para controlar el uso de airtime asignando porcentajes a utilizar en los SSID;	REQUERIDO
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;	REQUERIDO

La solución debe implementar la función de web filtering para controlar los sitios que se accede a la red. 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;	REQUERIDO
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;	REQUERIDO
La base de reconocimiento de aplicaciones a través de DPI debe identificar con al menos 1500 (mil quinientas) aplicaciones;	REQUERIDO
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;	REQUERIDO
La solución debe, a través de la técnica de DPI, reconocer aplicaciones sensibles al negocio y permitir la priorización de este tráfico con QoS;	REQUERIDO
La solución debe implementar mecanismos de protección para identificar ataques a la infraestructura inalámbrica. Al menos los siguientes ataques deben ser identificados:	REQUERIDO
- 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.	
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 deauthentication	REQUERIDO
La solución debe implementar mecanismos de protección contra ataques de ARP Poisoning en la red inalámbrica;	REQUERIDO

La solución debe monitorear y clasificar el riesgo de las aplicaciones accedidas por los clientes inalámbricos;	REQUERIDO
Permitir configurar el bloqueo en la comunicación entre los clientes inalámbricos conectados a un SSID;	REQUERIDO
Debe implementar la autenticación administrativa a través del protocolo RADIUS;	REQUERIDO
En combinación con los puntos de acceso, la solución debe implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES);	REQUERIDO
En combinación con los puntos de acceso, la solución debe ser compatible e implementar el método de autenticación WPA3;	REQUERIDO
La solución debe permitir la configuración de múltiples claves de autenticación PSK para su uso en un SSID determinado;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
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;	REQUERIDO
La solución debe admitir los siguientes métodos de autenticación EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP;	REQUERIDO
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;	REQUERIDO
La solución debe permitir el hospedaje del portal cautivo (captive portal) en la memoria interna del controlador inalámbrico;	REQUERIDO
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;	REQUERIDO
La solución debe permitir la recopilación del correo electrónico de los usuarios como método de autorización para ingreso a la red;	REQUERIDO
La solución debe permitir que la página de autenticación se quede alojada en un servidor externo;	REQUERIDO

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;	REQUERIDO
La solución debe garantizar que los usuarios se autenticuen en el portal cautivo que utilice la dirección IPv6;	REQUERIDO
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;	REQUERIDO
Después de la creación de un usuario visitante, la solución debe enviar las credenciales por e-mail al usuario registrado;	REQUERIDO
La solución debe implementar la función de DHCP Server (IPv4 y IPv6) para facilitar la configuración de las redes de visitantes;	REQUERIDO
La solución debe identificar automáticamente el tipo de equipo y sistema operativo utilizado por el dispositivo conectado a la red inalámbrica;	REQUERIDO
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;	REQUERIDO
La solución debe permitir la configuración de redes Mesh entre los puntos de acceso administrados por ella;	REQUERIDO
La solución debe permitir la configuración de red Mesh entre puntos de acceso indoor y outdoor;	REQUERIDO
La solución debe permitir ser administrada a través de los protocolos HTTPS y SSH vía IPv4 e IPv6;	REQUERIDO
La solución debe permitir el envío de los Logs a múltiples servidores externos de syslog;	REQUERIDO
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;	REQUERIDO
La solución debe permitir que los softwares de gestión realicen consultas directamente en los puntos de acceso a través del protocolo SNMP;	REQUERIDO
La solución debe incluir soporte para las RFC 1213 (MIB II) y RFC 2665 (Ethernet-like MIB);	REQUERIDO
La solución debe permitir la captura de paquetes en la red inalámbrica y exportarlos en archivos en formato .pcap;	REQUERIDO

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;	REQUERIDO
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 transmitidos y recibidos por ellos;	REQUERIDO
La solución debe implementar la administración unificada y de forma gráfica para redes WiFi y redes cableadas;	REQUERIDO
La solución debe permitir la actualización de firmware del controlador inalámbrico incluso cuando se conecta de forma remota;	REQUERIDO
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;	REQUERIDO
La solución debe tener herramientas de diagnóstico y depuración;	REQUERIDO
La solución debe soportar la comunicación con elementos externos a través de las API;	REQUERIDO
La solución deberá ser compatible y administrar los puntos de acceso de este proceso;	REQUERIDO
Instalación, configuración y garantía	
El plazo de garantía será de 36 meses, se entiende por garantía el mantenimiento preventivo y correctivo del software en la modalidad de al menos 24x7 incluyendo el reemplazo del software en caso de necesidad, solución de errores debido a algún incidente o corrupción en el software, así como la instalación de las actualizaciones que pudieran surgir durante el referido periodo.	REQUERIDO
El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo. La validez de las licencias debe ser por un periodo de mínimo 36 meses.	REQUERIDO

ITEM 2. SOFTWARE DE REGISTROS, ANÁLISIS Y REPORTE	
Descripción	Requerimiento mínimo
Software de Reporte	REQUERIDO
Denominación	indicar

Versión	indicar
Procedencia	indicar
Cantidad	1 (uno)
Requisitos Mínimos	
Sistema de Reportería en formato Virtualizado (VM) para instalación en ambientes virtualizados	REQUERIDO
Funcionalidades Generales	
Compatible con el ambiente VMware ESXi 5.0/5.1/5.5/6.0/6.5/6.7;	REQUERIDO
Compatible con el ambiente Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2/2016	REQUERIDO
Compatible con el ambiente Citrix XenServer 6.0+	REQUERIDO
Compatible con el ambiente Open Source Xen 4.1+	REQUERIDO
Compatible con el ambiente KVM on Redhat 6.5+ and Ubuntu 17.04	REQUERIDO
Compatible con el ambiente Nutanix AHV (AOS 5.10.5)	REQUERIDO
Compatible con el ambiente Amazon Web Services (AWS)	REQUERIDO
Compatible con el ambiente Microsoft Azure.	REQUERIDO
Compatible con el ambiente Google Cloud (GCP)	REQUERIDO
Compatible con el ambiente Oracle Cloud Infrastructure (OCI)	REQUERIDO
Compatible con el ambiente Alibaba Cloud (AliCloud)	REQUERIDO
No debe haber límites a la cantidad de múltiples vCPU	REQUERIDO
No debe haber límites a la expansión de memoria RAM	REQUERIDO
Debe soportar acceso vía SSH, WEB (HTTPS) para la gestión de la solución	REQUERIDO
Contar con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interface gráfica (GUI) como vía línea de comandos en consola de gestión.	REQUERIDO

Permitir acceso simultáneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.	REQUERIDO
Soporte SNMP versión 2 y 3	REQUERIDO
Permitir virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.	REQUERIDO
Debe permitir la creación de administrador general, que tenga acceso general a todas las instancias de virtualización de la solución.	REQUERIDO
Debe permitir activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH	REQUERIDO
Autenticación de usuarios de acceso a la plataforma vía LDAP	REQUERIDO
Autenticación de usuarios de acceso a la plataforma vía Radius	REQUERIDO
Autenticación de usuarios de acceso a la plataforma vía TACACS+	REQUERIDO
Generación de informes en tiempo real de tráfico, en formato de gráfica de mapas geográficos	REQUERIDO
Generación de informes en tiempo real de tráfico, en formato de gráfica de burbuja.	REQUERIDO
Generación de informes en tiempo real de tráfico, en formato de gráfica tabla	REQUERIDO
Definición de perfiles de acceso a consola con permiso granulares, tales como: acceso de escritura, de lectura, de creación de nuevos usuarios y cambios en configuraciones generales.	REQUERIDO
Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña del mismo.	REQUERIDO
Debe ser posible ver la cantidad de logs enviados desde cada dispositivo supervisado	REQUERIDO
Contar con mecanismos de borrado automático de logs antiguos.	REQUERIDO
Permitir la importación y exportación de reportes	REQUERIDO
Debe contar con la capacidad de crear informes en formato HTML	REQUERIDO
Debe contar con la capacidad de crear informes en formato PDF	REQUERIDO

Debe contar con la capacidad de crear informes en formato XML	REQUERIDO
Debe contar con la capacidad de crear informes en formato CSV	REQUERIDO
Debe permitir exportar los logs en formato CSV	REQUERIDO
Generación de logs de auditoría, con detalle de la configuración realizada, el administrador que realizó el cambio y hora del mismo.	REQUERIDO
Los logs generados por los dispositivos administrados deben ser centralizados en los servidores de la plataforma, pero la solución debe ofrecer también la posibilidad de utilizar un servidor externo de Syslog o similar.	REQUERIDO
La solución debe contar con reportes predefinidos	REQUERIDO
Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución	REQUERIDO
Debe ser posible la duplicación de reportes existentes para su posterior edición.	REQUERIDO
Debe tener la capacidad de personalizar la portada de los reportes obtenidos.	REQUERIDO
Permitir centralmente la visualización de logs recibidos por uno o más dispositivos, incluido la capacidad de uso de filtros para facilitar la búsqueda dentro de los mismos logs.	REQUERIDO
Los logs de auditoría de cambios de configuración de reglas y objetos deben ser visualizados en una lista distinta a la de los logs relacionados a tráfico de datos.	REQUERIDO
Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas	REQUERIDO
Debe poseer mecanismo de Drill-Down para navegar en los reportes de tiempo real.	REQUERIDO
Debe permitir descargar de la plataforma los archivos de logs para uso externo.	REQUERIDO
Tener la capacidad de generar y enviar reportes periódicos automáticamente.	REQUERIDO
Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.	REQUERIDO
Permitir el envío por email de manera automática de reportes.	REQUERIDO
Debe permitir que el reporte a enviar por email sea al destinatario específico.	REQUERIDO

Permitir la programación de la generación de reportes, conforme a un calendario definido por el administrador.	REQUERIDO
Debe ser posible visualizar gráficamente en tiempo real la tasa de generación de logs por cada dispositivo gestionado.	REQUERIDO
Debe permitir el uso de filtros en los reportes.	REQUERIDO
Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros.	REQUERIDO
Permitir especificar el idioma de los reportes creados	REQUERIDO
Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.	REQUERIDO
Debe permitir el envío automático de reportes a un servidor externo SFTP o FTP.	REQUERIDO
Debe ser capaz de crear consultas SQL o similar dentro de las bases de datos de logs, para uso en gráficas y tablas en reportes.	REQUERIDO
Tener la capacidad de visualizar en GUI de reportes de información del Sistema, como licencias, memoria, disco duro, uso de CPU, tasa de logs por segundo recibidos, total de logs diarios recibidos, alertas del sistema, entre otros.	REQUERIDO
Debe contar con una herramienta que permita analizar el rendimiento en la generación de reportes, con el objetivo de detectar y arreglar problemas en generación de los mismos.	REQUERIDO
Que la solución sea capaz de importar archivos con logs de dispositivos compatibles conocido y no conocidos por la plataforma, para posterior generación de reportes.	REQUERIDO
Debe ser posible poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.	REQUERIDO
Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.	REQUERIDO
Debe ser compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.	REQUERIDO
Debe permitir aplicar políticas para el uso de contraseñas para los administradores de la plataforma, como tamaño mínimo y caracteres permitidos	REQUERIDO
Debe permitir visualizar en tiempo real los logs recibidos.	REQUERIDO
Debe permitir el reenvío de logs en formato syslog.	REQUERIDO

Debe permitir el reenvío de logs en formato CEF (Common Event Format).	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea las principales amenazas de seguridad para su red	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea comprometimiento de usuarios y uso sospechoso de la web en su red.	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea el tráfico en su red.	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea el tráfico de aplicaciones y sitios web en su red	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea detecciones de amenazas de día cero en su red (sandboxing).	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea actividad de endpoints en su red.	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea actividad VPN en su red.	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea puntos de acceso WiFi y SSIDs	REQUERIDO
Debe incluir dashboard para operaciones SOC que monitorea rendimiento de recursos local de la solución (CPU, Memoria)	REQUERIDO
Debe permitir crear dashboards personalizados para monitoreo de operaciones SOC	REQUERIDO
Debe soportar configuración de alta disponibilidad Master/Slave en la capa 3	REQUERIDO
Debe permitir generar alertas de eventos a partir de logs recibidos	REQUERIDO
Debe permitir crear incidentes a partir de alertas de eventos para endpoint	REQUERIDO
Debe permitir la integración al sistema de tickets ServiceNow	REQUERIDO
Debe soportar servicio de Indicadores de Compromiso (IoC) del mismo fabricante, que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas.	REQUERIDO
Debe permitir respaldar logs en nube publica de Amazon S3	REQUERIDO
Debe permitir respaldar logs en nube publica de Microsoft Azure	REQUERIDO

Debe permitir respaldar logs en nube publica de Google Cloud	REQUERIDO
Debe soportar el estándar SAML para autenticación de usuarios administradores	REQUERIDO
Reportes de Firewall	
Debe contar con reporte de cumplimiento de PCI DSS	REQUERIDO
Debe contar con reporte de utilización de aplicaciones SaaS	REQUERIDO
Debe contar con reporte de prevención de perdida de datos (DLP)	REQUERIDO
Debe contar con reporte de VPN	REQUERIDO
Debe contar con reporte de Sistema de prevención de intrusos (IPS)	REQUERIDO
Debe contar con reporte de reputación de cliente	REQUERIDO
Debe contar con reporte de análisis de seguridad de usuario	REQUERIDO
Debe contar con reporte de análisis de amenaza cibernética	REQUERIDO
Debe contar con reporte de breve resumen diario de eventos e incidentes de seguridad	REQUERIDO
Debe contar con reporte de tráfico DNS	REQUERIDO
Debe contar con reporte tráfico de correo electrónico	REQUERIDO
Debe contar con reporte de Top 10 de Aplicaciones utilizadas en la red	REQUERIDO
Debe contar con reporte de Top 10 de Websites utilizadas en la red	REQUERIDO
Debe contar con reporte de uso de redes sociales	REQUERIDO
Compatibilidad con ÍTEM 1 Firewall e ÍTEM 3 Switch	
Para garantizar la compatibilidad de las funciones requeridas, el sistema deberá ser del mismo fabricante del Ítem 1 y del Ítem 3 o en su defecto contar con un respaldo documental de interoperabilidad de las funciones solicitadas del sistema de reporte, tanto del Fabricante del ÍTEM 1, como del Fabricante del ÍTEM 3. Es decir, ambos fabricantes deberán garantizar mediante nota dirigida a la Convocante la interoperabilidad.	REQUERIDO
Instalación, configuración y garantía.	

El plazo de garantía será de 36 meses, se entiende por garantía el mantenimiento preventivo y correctivo del software en la modalidad de al menos 24x7 incluyendo el reemplazo del software en caso de necesidad, solución de errores debido a algún incidente o corrupción en el software, así como la instalación de las actualizaciones que pudieran surgir durante el referido periodo.	REQUERIDO
El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo. La validez de las licencias debe ser por un periodo de mínimo 36 meses.	REQUERIDO

ITEM 3. EQUIPOS DE CONMUTACIÓN (SWITCH)	
Descripción	Requerimiento mínimo
Marca	indicar
Modelo	indicar
Procedencia	indicar
Cantidad	2 (dos)
Descripción	Switch de Acceso
Tipo de configuración	Fija
Stacking/Apilamiento: máximos equipos apilables	4
Tipo de uso	Acceso a Proveedores
Interfaces y rendimiento	
Interfaces independientes 10/100/1000BaseT-Cobre UTP RJ45	24 puertos RJ45
Interfaces SFP+ independientes (1/10Gbps)	4 puertos SFP+
Puerto 10/100 BaseT Ethernet adicional e independiente para administración del equipo (Out of Band Management)	1 puerto RJ45
Puerto SERIAL RS-232 para ser usado como consola de administración.	1 puerto serial

Puerto USB para el almacenado y descarga de configuraciones y sistema operativo	Opcional
Capacidad de conmutación de paquetes unidireccional	64 Gbps
Capacidad de conmutación de paquetes bidireccional	128 Gbps
Throughput de Capa 2/Capa 3 (Mbps)	95 Mbps
Stacking/Apilamiento	
Capacidad de backplane del Stack utilizando los puertos de UPLINK	Opcional
Equipos agrupados para administrar con un único acceso administrativo	Opcional
Cables de stacking proporcionados para la interconexión de equipos	Opcional
Deberá soportar el protocolo Link Aggregation Control Protocol (LACP) IEEE 802.3ad.	Opcional
Número de grupos a soportar por todo el STACK	Opcional
Calidad de Servicio	
Encolamiento basado en clases de servicio con priorización de tráfico Strick priority en egreso	Exigido
Soporte de Port Shaping: puede ser usados para manejar el exceso de tráfico, esta característica define el ancho de banda maximo alojado en un puerto	Exigido
Soporte de queuing shaping: puede ser usados para manejar el exceso de tráfico, esta característica define el ancho de banda maximo alojado en cada cola	Exigido
Soporte de QoS en puertos LAG	Exigido
L2 QoS (classification, rewrite, queuing) Permite la clasificacion re-escritura y encolamiento de CoS en interfaces de layer 2.	Exigido
L3 QoS (classification, rewrite, queuing) Permite la clasificacion re-escritura y encolamiento de CoS en interfaces de layer 3	Exigido
Soporte de QoS Clasificacion, re-write y queueing en interfaces RVI (Interface VLANs)	Exigido
Soporta el tratamiento de las colas ante congestión con los mecanismos SDWRR (Shaped deficit Weighted Round Robin) y SPQ (Strict Priority).	Opcional

Soporta el protocolo LLDP (Link Layer Discovery Protocol) IEEE 802.1AB y LLDP-MED (LLDP for Media Endpoint Device) ANSI/TIA-1057 integrado para Voice sobre IP (VoIP)	Exigido
Soporte de priorización de tráfico de salida por hardware mínimo ocho (8) colas de servicio por puerto.	Exigido
Políticas de tráfico de red que limitan la velocidad de entrada y salida de una clase de tráfico con base en el criterio establecido por el usuario. Permite controlar la velocidad máxima de tráfico enviado o recibido en una interfaz y particionar una red en múltiples niveles de clase de servicio	Exigido
Encolado estricto y de baja latencia (Strict priority queuing or Low Latency Queuing (LLQ)) Strict priority queuing, or low latency queuing (LLQ): es una característica usada para reenviar de forma más rápida ciertos tipos de tráfico sensible a retardos (voz, video etc).	Opcional
Trust 802.1p/DSCP/IP Prec (ingress)	Exigido
Soporte de limitación de tráfico mediante lista de control de acceso (ACL) aplicable en los puertos físicos o VLANs por:	
Filtros basados en direcciones MAC origen o destino	Exigido
Filtros basados en direcciones IP origen o destino	Exigido
Filtros basados en número de puerto TCP/UDP	Exigido
Cantidad de filtros de tráfico (ACL)	Al menos 1000
Spanning Tree Protocol	
IEEE 802.1d.	Exigido
Rapid Spanning Tree IEEE 802.1w	Exigido
Multiple Spanning Tree Protocol IEEE 802.1s.	Exigido
Soporte de Time Domain Reflectometry para detectar las fallas en cables UTP	Exigido
Soporte de ruteo layer 3 por medio de los siguientes protocolos:	
Rutas Estáticas	Exigido
Soporte máximo de rutas IPv4	Al menos 100
Soporte de IEEE802.1ag Ethernet OAM connectivity fault management (CFM)	Opcional

Soporte de Ethernet ring protection switching (ERPS, G.8032/Y.1344)	Opcional
Soporte de TDR (Time Domain Reflectometry). Una tecnología que permite el seguimiento y señalización de fallas en los cables o conectores de redes de computadoras. Los puertos deben ser capaces de generar un pulso electromagnético, cuando este pulso alcanza un obstáculo o el fin del cable se genera un eco que es traducido en la distancia a la falla.	Exigido
RIP v1/v2	Exigido
RIPng	Exigido
Soporte OSPF	Exigido
Soporte de Layer 2 protocol tunneling (L2PT)	Opcional
Soporte de ARP (número de entradas)	Opcional
Funcionalidades layer 2	
Soporte máximo de direcciones MAC de red.	16000
Soporte de tramas Jumbo	Exigido
Soporte de IEEE 802.1X para VLAN VoIP.	Exigido
Port-based VLAN	Exigido
MAC-based VLAN	Exigido
Soporte IEEE 802.1Q-in-Q: VLAN Stacking	Exigido
IEEE 802.1ak: Multiple VLAN Registration Protocol (MVRP)	Opcional
Compatible con Per-VLAN Spanning Tree Plus	Opcional
Soporte de interfaces RVI (Routed VLAN Interfaces)	Exigido
Capacidad de soportar definición de dominios de broadcast VLANs (Virtual LANs) en todos los puertos según IEEE 802.1 p/Q.	Exigido
Numero de VLANs configurables en el Virtual Chasis	Opcional
VLANs en equipo individual	4092

Posible rango de VLAN-ID para configurar	1 - 4092
Soporte de DHCP Relay y DHCP helper	Exigido
Soporte de DHCP Server sobre interfaces RVI	Opcional
Voice VLAN fallback	Opcional
Multicast	
Soporte protocolo IGMP-Snooping	Exigido
Soporte PIM-SM, PIM-SSM, PIM-DM	Opcional
Soporte IGMP: v1, v2, v3	Exigido
Administracion / Management	
Deberá soportar Simple Network Management Protocol versión SNMP v2c, SNMP v3.	Exigido
Capacidad de proveer los bloques de información de management (MIBs) necesarios.	Exigido
Capacidad de Remote Monitoring (RMON), deberá soportar al menos cuatro (4) grupos (statistics, history, alarm, events).	Exigido
sFlow	Exigido
Soporte de registro remoto (SysLog).	Exigido
Soporte de traffic mirroring por puerto o por VLAN.	Exigido
Deberá soportar Network Timing Protocol (NTP).	Exigido
Creación de 20 perfiles de administrador con facultadas específicas de modificar la configuración o solo acceder a vistas de la misma y listado de comandos disponibles para ejecutar por cada perfil	Exigido
Las passwords (claves) de administrador almacenadas localmente deben estar encriptadas usando hash MD5 o SHA1	Exigido
Soporte de MIB para la información de media attachment unit (MAU)	Opcional
Fuente para AC	Exigido

Accesorios necesarios para montar en racks estándar de 19".	Exigido
Seguridad, mecanismos soportados	
Central Web authentication	Exigido
Deberá soportar autenticación 802.1X. para diferentes VLANs por puerto.	Exigido
Soporte de IEEE 802.1X con soporte de VLANs de invitados (Guest VLAN)	Exigido
MAC Radius Authentication con 802.1X	Exigido
Soporte de protocolo EAP-PAP para MAC RADIUS authentication	Exigido
Soporte de seguridad del puerto mediante filtrado por dirección MAC. En caso de violación del puerto deberá poder enviarse una alerta al administrador y deshabilitar el puerto.	Exigido
Soporte de limitación de direcciones MAC por puerto.	Exigido
Soporte de Persistent MAC learning o sticky MAC	Exigido
DHCP Snooping.	Exigido
Dynamic ARP inspection (DAI)	Exigido
Proxy ARP	Exigido
Static ARP support	Exigido
IP source guard	Exigido
Orden de autenticación flexible	Exigido
IPv6 Neighbor Discovery inspection	Exigido
Servicio de configuración por medios seguros:	
Soporte Telnet / Secure Shell (SSH) versión 2 para conexión remota vía interfaz línea de comando (CLI).	Exigido
Soporte vía Web con SSL. (HTTPS)	Exigido

Soporte de creación de Certificados locales para conexión HTTPs	Exigido
Almacenamiento de sistema operativo y configuración en memoria Flash reescribible.	Al menos 256 MB
Roll-back a varias configuraciones anteriores almacenadas en el equipo (mínimo 3 configuraciones) o una configuración de rescate almacenada especialmente por el administrador	Opcional
Mecanismos de automatización mediante scripts o similares que permitan chequear el cumplimiento y administrar los cambios de configuraciones, aplicar configuraciones predefinidas, visualizar conjuntos de comandos para el diagnóstico, análisis y administración de eventos, y generar respuestas predefinidas a eventos.	Opcional
Servicio de configuración por medio de consola serial RS-232 asincrónica	Opcional
La unidad deberá ser entregada con 1 (un) juego de manuales de configuración de hardware y software. Estos manuales podrán ser entregados de manera impresa o bien en medio digital.	Exigido
Equipos alimentados con 220 V - 50 Hz, monofásico con toma de 3 patas, sin necesidad de requerir un transformador adicional.	Exigido
Troubleshooting	
Debugging: CLI via console, telnet, or SSH	Exigido
Diagnostics: Show and debug command statistics	Exigido
Traffic mirroring (port)	Exigido
Traffic mirroring (VLAN)	Exigido
ACL-based mirroring	Opcional
Mirroring destination ports per system	Opcional
LAG port monitoring	Opcional
Multiple destination ports monitored to 1 mirror (N:1)	Exigido
Maximum number of mirroring sessions	Exigido
Mirroring to remote destination (over L2)	Exigido
IP tools: Extended ping and trace	Exigido

Alta disponibilidad	
Soporte de Link Aggregation	Exigido
802.3ad (LACP) support: Number of LAGs supported	24
Maximum number of ports per LAG	8
LAG sharing algorithm—Routed Multicast Traffic:	
Tagged ports support in LAG	Exigido
Uplink Failure Detection (UFD)	Opcional
Soporte para equipos con dos Routing engines, configurar al Routing engine de respaldo para asumir el rol de master sin causar interrupcion en el reenvio.	Opcional
Soporte VRRP (Virtual Router Redundancy Protocol)	Exigido
Alimentación Eléctrica, Ventilación y dimensiones.	
Tensión de operación Fuente de Alimentación 100-120V / 200-240V auto detectable.	Exigido
Cumplimiento de ROHS	Exigido
Temperatura de operación: 0°C a 45°C	Exigido
Humedad de operación: 10% a 85% de humedad relativa máxima, sin condensación.	Exigido
Montaje en rack de 19"	Exigido
Cantidad de Unidad de Rack del Equipo	1U
MTBF	87.000 hs.
Instalación, configuración y garantía.	
Instalación: El equipo deberá ser configurado, instalado y probado de acuerdo a las indicaciones de la Convocante, por personal técnico del oferente.	Exigido
Actualización de software: El sistema operativo deberá ser actualizado a la última versión disponible a pedido del cliente durante la duración del contrato.	Exigido

Plazo de garantía del fabricante	36 meses
----------------------------------	----------

ITEM 4. SERVICIO DE CAPACITACIÓN	
Descripción	Requerimiento mínimo
Servicio de capacitación, para al menos 5 (CINCO) funcionarios, con una duración mínima de 30 horas (reloj), por cada ítem solicitado (1, 2 y 3), en modalidad presencial, en las oficinas de la Convocante y en horario de oficina.	REQUERIDO

ESQUEMA ACTUAL DE RED <https://ibb.co/M6WYjQF>

ESQUEMA REQUERIDO DE RED <https://ibb.co/DwXYfBg>

Switch de acceso a Proveedores

Equipos dedicados a concentrar los servicios de los proveedores. Los mismos estarán en redundancia, garantizando alta disponibilidad, distribuyendo las conexiones hasta los equipos de borde.

Enrutador / Firewall UTM de Borde

Dispositivo del tipo UTM en el esquema borde; el cual pueda gestionar todo el tráfico interno y externo, brindando de esta manera una capa de seguridad mejorada. Los mismos estarán en redundancia, garantizando alta disponibilidad.

Software de Reportes

Herramienta dedicada a la gestión de registros, análisis e informes, con capacidad de permitir operaciones de seguridad, identificación proactiva y corrección de riesgos, y visibilidad completa de todo el panorama de ataques en la red.

SON PROVEEDORES EN EL BORDE DE COMUNICACIONES:

PROVEEDOR DE INTERNET A

Acceso a Internet

Enlace punto a punto entre la DGRP y la CSJ

PROVEEDOR DE INTERNET B

Acceso a Internet

CSJ

Enlace propio que conecta a la DGRP con la CSJ.

MITIC

Enlace para el Servicio de Intercambio de Información (SII) entre Organismos y Entidades del Estado (OEE)

SNC

Enlace propio que conecta a la DGRP con la SNC.

Identificación de la unidad solicitante y justificaciones

Identificar el nombre, cargo y la dependencia de la Institución de quien solicita el llamado a ser publicado.

Abg. y N.P. Lourdes Gonzales Directora General

Dirección General de los Registros Públicos Corte Suprema de Justicia.

Justificar la necesidad que se pretende satisfacer mediante la contratación a ser realizada.

La presente licitación se hace necesaria a fin de dotar a la infraestructura de red y servidores de equipos capacidad de brindar seguridad de acceso y filtrado de contenidos. Se pretende, de esta manera minimizar las intrusiones en la red local de la Institución, mediante la aplicación

de políticas de seguridad y filtrados respectivos.

Estos equipos pretenden coadyuvar a lograr los propósitos de la Institución y dar respuestas a las exigencias tecnológicas y diarias, por tanto, de la ciudadanía y de otras Instituciones

Además, se pretende responder a la necesidad de contar con la infraestructura física para soportar sistemas de misión crítica, en alta disponibilidad mediante redundancia, manteniendo las aplicaciones disponibles y resguardadas durante las 24 horas. (7x24x365).

Justificar la planificación. (si se trata de un llamado periódico o sucesivo, o si el mismo responde a una necesidad temporal)

Responde a la necesidad de adquisición de los referidos equipos que permitirán asegurar los servicios actuales y adecuarse a los nuevos servicios a ser ofrecidos, atendiendo a que tanto los enrutadores como firewalls -aún en funcionamiento- ya han sido discontinuados por la fábrica

Justificar las especificaciones técnicas establecidas.

Estas corresponden a equipos de gama media/alta, teniendo en cuenta las importantes funciones que le serán asignadas y al tiempo de reposición de estos equipos, por tanto, estas especificaciones apuntan a equipos que puedan estar operativos por varios años.

Plan de entrega de los bienes

La entrega de los bienes se realizará de acuerdo al Plan de Entrega y Cronograma de Cumplimiento, indicado en el presente apartado. Así mismo, de los documentos de embarque y otros que deberá suministrar el Proveedor indicados a continuación:

Ítem	Descripción del bien	Cantidad	Unidad de medida	Lugar de entrega de los bienes	Fecha(s) final(es) de ejecución de los bienes
1	TODOS LOS ÍTEMS	SEGÚN LAS EETT	SEGÚN LAS EETT	<p>El oferente adjudicado deberá entregar los bienes (equipos de conmutación, seguridad de red de datos y software de reportes), como también, el cronograma, contenido y fechas tentativas para la realización de la capacitación dentro de los 90 (noventa) días hábiles posteriores a la firma del contrato, y dispondrá, de otros 30 (treinta) días hábiles, posteriores a la entrega de los bienes, para realizar la planificación, instalación, configuración e implementación de los ítems adjudicados.</p> <p>Todo esto, debe ser entregado, instalado, configurado, implementado y realizado en el edificio de la Dirección General de los Registros Públicos, sito en Avda. Eusebio Ayala casi Capitán Román García, de lunes a viernes de 07:15 hs a 13:00 hs, salvo los feriados oficiales y de conformidad al horario normal y diferenciado de los funcionarios de la DGRP.</p> <p>La emisión del Acta de Recepción Total dada por la Contratante, significará el cumplimiento por parte del Proveedor de sus obligaciones contractuales y le facultará a solicitar el pago de la misma.</p>	36 (TREINTA Y SEIS) MESES, CONTADOS DESDE LA FIRMA DEL CONTRATO.

Planos y diseños

Para la presente contratación se pone a disposición los siguientes planos o diseños:

No Aplica

Embalajes y documentos

El embalaje, la identificación y la documentación dentro y fuera de los paquetes serán como se indican a continuación:

No Aplica

Inspecciones y pruebas

Las inspecciones y pruebas serán como se indica a continuación:

No Aplica

Indicadores de Cumplimiento

El documento requerido para acreditar el cumplimiento contractual, será:

- El documento requerido para acreditar el cumplimiento contractual, será: **Acta de recepción Definitiva.**
- **Serán presentados:** 1 (un) Acta Final por la entrega efectuada.
- **Frecuencia:** Conforme se establece en el Plan de Entrega de bienes establecido en el PBC.

INDICADOR	TIPO	FECHA DE PRESENTACIÓN PREVISTA
Acta de Recepción Definitiva.	Acta	120 (ciento veinte) días hábiles, computados a partir de la fecha de la firma del contrato

De manera a establecer indicadores de cumplimiento, a través del sistema de seguimiento de contratos, la convocante deberá determinar el tipo de documento que acredite el efectivo cumplimiento de la ejecución del contrato, así como planificar la cantidad de indicadores que deberán ser presentados durante la ejecución. Por lo tanto, la convocante en este apartado y de acuerdo al tipo de contratación de que se trate, deberá indicar el documento a ser comunicado a través del módulo de Seguimiento de Contratos y la cantidad de los mismos.

Criterios de Adjudicación

La Convocante adjudicará el contrato al oferente cuya oferta haya sido evaluada como la más baja y cumpla sustancialmente con los requisitos de las bases y condiciones, siempre y cuando la convocante determine que el oferente está calificado para ejecutar el contrato satisfactoriamente.

1. La adjudicación en los procesos de contratación en los cuales se aplique la modalidad de contrato abierto, se efectuará por las cantidades o montos máximos solicitados en el llamado, sin que ello implique obligación de la convocante de requerir la provisión de esa cantidad o monto durante de la vigencia del contrato, obligándose sí respecto de las cantidades o montos mínimos establecidos.
2. En caso de que la convocante no haya adquirido la cantidad o monto mínimo establecido, deberá consultar al proveedor si desea ampliarlo para el siguiente ejercicio fiscal, hasta cumplir el mínimo.
3. Al momento de adjudicar el contrato, la convocante se reserva el derecho a disminuir la cantidad de bienes requeridos, por razones de disponibilidad presupuestaria u otras razones debidamente justificadas. Estas variaciones no podrán alterar los precios unitarios u otros términos y condiciones de la oferta y de los documentos de la licitación.

En aquellos llamados en los cuales se aplique la modalidad de contrato abierto, cuando la convocante deba disminuir cantidades o montos a ser adjudicados, no podrá modificar el monto o las cantidades mínimas establecidas en las bases de la contratación.

Notificaciones

La comunicación de la adjudicación a los oferentes será como sigue:

1. Dentro de los cinco (5) días corridos de haberse resuelto la adjudicación, la convocante comunicará a través del Sistema de Información de Contrataciones Públicas, copia del informe de evaluación y del acto administrativo de adjudicación, los cuales serán puestos a disposición pública en el referido sistema. Adicionalmente el sistema generará una notificación a los oferentes por los medios remotos de comunicación electrónica pertinentes, la cual será reglamentada por la DNCP.
2. En sustitución de la notificación a través del Sistema de Información de Contrataciones Públicas, las convocantes podrán dar a conocer la adjudicación por cédula de notificación a cada uno de los oferentes, acompañados de la copia íntegra del acto administrativo y del informe de evaluación. La no entrega del informe en ocasión de la notificación, suspende el plazo para formular protestas hasta tanto la convocante haga entrega de dicha copia al oferente solicitante.
3. En caso de la convocante opte por la notificación física a los oferentes participantes, deberá realizarse únicamente con el acuse de recibo y en el mismo con expresa mención de haber recibido el informe de evaluación y la resolución de adjudicación.
4. Las cancelaciones o declaraciones desiertas deberán ser notificadas a todos los oferentes, según el procedimiento indicado precedentemente.
5. Las notificaciones realizadas en virtud al contrato, deberán ser por escrito y dirigirse a la dirección indicada en el contrato.

Audiencia Informativa

Una vez notificado el resultado del proceso, el oferente tendrá la facultad de solicitar una audiencia a fin de que la convocante explique los fundamentos que motivan su decisión.

La solicitud de audiencia informativa no suspenderá ni interrumpirá el plazo para la interposición de protestas.

La misma deberá ser solicitada dentro de los dos (2) días hábiles siguientes en que el oferente haya tomado conocimiento de los términos del Informe de Evaluación de Ofertas.

La convocante deberá dar respuesta a dicha solicitud dentro de los dos (2) días hábiles de haberla recibido y realizar la audiencia en un plazo que no exceda de dos (2) días hábiles siguientes a la fecha de respuesta al oferente.

Documentación requerida para la firma del contrato

Luego de la notificación de adjudicación, el proveedor deberá presentar en el plazo establecido en las reglamentaciones vigentes, los documentos indicados en el presente apartado.

1. Personas Físicas / Jurídicas

- Certificado de no encontrarse en quiebra o en convocatoria de acreedores expedido por la Dirección General de Registros Públicos;
- Certificado de no hallarse en interdicción judicial expedido por la Dirección General de Registros Públicos;
- Constancia de no adeudar aporte obrero patronal expedida por el Instituto de Previsión Social;
- Certificado laboral vigente expedido por la Dirección de Obrero Patronal dependiente del Viceministerio de Trabajo, siempre que el sujeto esté obligado a contar con el mismo, de conformidad a la reglamentación pertinente - CPS;
- En el caso que suscriba el contrato otra persona en su representación, acompañar poder suficiente del apoderado para asumir todas las obligaciones emergentes del contrato hasta su terminación;
- Certificado de cumplimiento tributario vigente a la firma del contrato.

2. Documentos. Consorcios

- Cada integrante del consorcio que sea una persona física o jurídica deberá presentar los documentos requeridos para oferentes individuales especificados en los apartados precedentes.
- Original o fotocopia del consorcio constituido.
- Documentos que acrediten las facultades del firmante del contrato para comprometer solidariamente al consorcio.
- En el caso que suscriba el contrato otra persona en su representación, acompañar poder suficiente del apoderado para asumir todas las obligaciones emergentes del contrato hasta su terminación.

CONDICIONES CONTRACTUALES

Esta sección constituye las condiciones contractuales a ser adoptadas por las partes para la ejecución del contrato.

Interpretación

Interpretación

1. Si el contexto así lo requiere, el singular significa el plural y viceversa; y "día" significa día calendario, salvo que se haya indicado expresamente que se trata de días hábiles.

2. Condiciones prohibidas, inválidas o inejecutables

Si cualquier provisión o condición del Contrato es prohibida o resultase inválida o inejecutable, dicha prohibición, invalidez o falta de ejecución no afectará la validez o el cumplimiento de las otras provisiones o condiciones del Contrato.

3. Limitación de Dispensas:

a) Toda dispensa a los derechos o facultades de una de las partes en virtud del Contrato, deberá ser documentada por escrito, indicar la fecha, estar firmada por un representante autorizado de la parte que otorga dicha dispensa y deberá especificar la obligación que está dispensando y el alcance de la dispensa.

b) Sujeto a lo indicado en el inciso precedente, ningún retraso, prórroga, demora o aprobación por cualquiera de las partes al hacer cumplir algún término y condición del contrato o el otorgar prórrogas por una de las partes a la otra, perjudicará, afectará o limitará los derechos de esa parte en virtud del Contrato. Asimismo, ninguna prórroga concedida por cualquiera de las partes por un incumplimiento del Contrato, servirá de dispensa para incumplimientos posteriores o continuos del Contrato.

Subcontratación

El porcentaje permitido para la subcontratación será de:

No Aplica

La subcontratación del contrato deberá ser realizada conforme a las disposiciones contenidas en la Ley, el Decreto Reglamentario y la reglamentación que emita para el efecto la DNCP.

Derechos Intelectuales

1. Los derechos de propiedad intelectual de todos los planos, documentos y otros materiales conteniendo datos e información proporcionada a la contratante por el proveedor, seguirán siendo salvo prueba en contrario de propiedad del proveedor. Si esta información fue suministrada a la contratante directamente o a través del proveedor por terceros, incluyendo proveedores de materiales, los derechos de propiedad intelectual de dichos materiales seguirá siendo de propiedad de dichos terceros

2. Sujeto al cumplimiento por parte de la contratante del párrafo siguiente, el proveedor indemnizará y liberará de toda responsabilidad a la contratante, sus empleados y funcionarios en caso de pleitos, acciones o procedimientos administrativos, reclamaciones, demandas, pérdidas, daños, costos y gastos de cualquier naturaleza, incluyendo gastos y honorarios por representación legal, que la contratante tenga que incurrir como resultado de la transgresión o supuesta transgresión de derechos de propiedad intelectual como patentes, dibujos y modelos industriales registrados, marcas registradas, derechos de autor u otro derecho de propiedad intelectual registrado o ya existente en la fecha del contrato debido a:

a) La instalación de los bienes por el proveedor o el uso de los bienes en la República del Paraguay; y

b) La venta de los productos producidos por los bienes en cualquier país.

Dicha indemnización no procederá si los bienes o una parte de ellos fuesen utilizados para fines no previstos en el Contrato o para fines que no pudieran inferirse razonablemente del Contrato. La indemnización tampoco cubrirá cualquier transgresión que resultara del uso de los bienes o parte de ellos, o de cualquier producto producido como resultado de asociación o combinación con otro equipo, planta o materiales no suministrados por el proveedor en virtud del Contrato.

3. Si se entablara un proceso legal o una demanda contra la Contratante como resultado de alguna de las situaciones indicadas en la cláusula anterior, la Contratante notificará prontamente al proveedor y éste por su propia cuenta y en nombre de la Contratante responderá a dicho proceso o demanda, y realizará las negociaciones necesarias para llegar a un acuerdo de dicho proceso o demanda.

4. Si el Proveedor no notifica a la Contratante dentro de treinta (30) días a partir del recibo de dicha comunicación de su intención de proceder con tales procesos o reclamos, la Contratante tendrá derecho a emprender dichas acciones en su propio nombre.

5. La Contratante se compromete, a solicitud del proveedor, a prestarle toda la asistencia posible para que el proveedor pueda contestar las citadas acciones legales o reclamaciones. La Contratante será reembolsada por el proveedor por todos los gastos razonables en que hubiera incurrido.

6. La Contratante deberá indemnizar y eximir de culpa al proveedor y a sus empleados, funcionarios y subcontratistas, por cualquier litigio, acción legal o procedimiento administrativo, reclamo, demanda, pérdida, daño, costo y gasto, de cualquier naturaleza, incluyendo honorarios y gastos de abogado, que pudieran afectar al proveedor como resultado de cualquier transgresión o supuesta transgresión de patentes, modelos de aparatos, diseños registrados, marcas registradas, derechos de autor, o cualquier otro derecho de propiedad intelectual registrado o ya existente a la fecha del Contrato, que pudieran suscitarse con motivo de cualquier diseño, datos, planos, especificaciones, u otros documentos o materiales que hubieran sido suministrados o diseñados por la Contratante o a nombre suyo.

Transporte

La responsabilidad por el transporte de los bienes será según se establece en los Incoterms.

Si las mismas no está de acuerdo con los Incoterms, el transporte deberá ser como sigue:

No Aplica

Confidencialidad de la información

1. No deberá darse a conocer información alguna acerca del análisis, aclaración y evaluación de las ofertas ni sobre las recomendaciones relativas a la adjudicación, después de la apertura en público de las ofertas, a los oferentes ni a personas no involucradas en el proceso de evaluación, hasta que haya sido dictada la Resolución de Adjudicación.

2. La contratante y el proveedor deberán mantener confidencialidad y en ningún momento divulgarán a terceros, sin el consentimiento de la otra parte, documentos, datos u otra información que hubiera sido directa o indirectamente proporcionada por la otra parte en conexión con el contrato, antes, durante o después de la ejecución del mismo. No obstante, el proveedor podrá proporcionar a sus subcontratistas los documentos, datos e información recibidos de la contratante para que puedan cumplir con su trabajo en virtud del contrato. En tal caso, el proveedor obtendrá de dichos subcontratistas un compromiso de confidencialidad similar al requerido al proveedor en la presente cláusula.

3. La Contratante no utilizará dichos documentos, datos u otra información recibida del proveedor para ningún uso que no esté relacionado con el contrato. Así mismo el proveedor no utilizará los documentos, datos u otra información recibida de la contratante para ningún otro propósito diferente al de la ejecución del contrato.

4. La obligación de las partes arriba mencionadas, no aplicará a la información que:

- a) La contratante o el proveedor requieran compartir con otras instituciones que participan en el financiamiento del Contrato;
- b) Actualmente o en el futuro se hace de dominio público sin culpa de ninguna de las partes;
- c) Puede comprobarse que estaba en posesión de esa parte en el momento que fue divulgada y no fue previamente obtenida directa o indirectamente de la otra parte; o
- d) Que de otra manera fue legalmente puesta a la disponibilidad de esa parte por un tercero que no tenía obligación de confidencialidad.

5. Las disposiciones precedentes no modificarán de ninguna manera ningún compromiso de confidencialidad otorgado por cualquiera de las partes a quien esto compete antes de la fecha del contrato con respecto a los suministros o cualquier parte de ellos.

6. Las disposiciones de esta cláusula permanecerán válidas después del cumplimiento o terminación del contrato por cualquier razón.

Obligatoriedad de declarar información del personal del contratista en el SICP

1. El proveedor deberá proporcionar los datos de identificación de sus subproveedores, así como de las personas físicas por medio de las cuales propone cumplir con las obligaciones del contrato, dentro de los treinta días posteriores a la obtención del código de contratación, y con anterioridad al primer pago que vaya a percibir en el marco de dicho contrato, con las especificaciones respecto a cada una de ellas. A ese respecto, el Contratista deberá consignar dichos datos en el Formulario de Información del Personal (FIP) y en el Formulario de Informe de Servicios Personales (FIS), a través del SIPE.

2. Cuando ocurra algún cambio en la nómina del personal o de los subcontratistas propuestos, el proveedor o contratista está obligado a actualizar el FIP.

3. Como requerimiento para efectuar los pagos a los proveedores o contratistas, la contratante, a través del procedimiento establecido para el efecto por la entidad previsional, verificará que el proveedor o contratista se encuentre al día en el cumplimiento con sus obligaciones para con el Instituto de Previsión Social (IPS).

4. La Contratante podrá realizar las diligencias que considere necesarias para verificar que la totalidad de las personas que prestan servicios personales en relación de dependencia para la contratista y eventuales subcontratistas se encuentren debidamente individualizados en los listados recibidos.

5. El proveedor o contratista deberá permitir y facilitar los controles de cumplimiento de sus obligaciones de aporte obrero patronal, tanto los que fueran realizados por la contratante como los realizados por el IPS y por funcionarios de la DNCP. La negativa expresa o tácita se considerará incumplimiento del contrato por causa imputable al proveedor o contratista.

6. En caso de detectarse que el proveedor o contratista o alguno de los subcontratistas, no se encontraran al día con el cumplimiento de sus obligaciones para con el IPS, deberán ser emplazados por la contratante para que en diez (10) días hábiles cumplan con sus obligaciones pendientes con la previsional. En el caso de que no lo hiciera, se considerará incumplimiento del contrato por causa imputable al proveedor o contratista.

Formas y condiciones de pago

El adjudicado para solicitar el pago de las obligaciones deberá presentar la solicitud acompañada de los siguientes documentos:

1. Documentos Genéricos:

1. Nota de remisión;
2. La factura de pago, con timbrado vigente, la cual deberán expresar claramente por separado el Impuesto al Valor Agregado (IVA) de conformidad con las disposiciones tributarias aplicables. En ningún caso el valor total facturado podrá exceder el valor adjudicado o las adendas aprobadas;
3. REPSE (registro de prestadores de servicios) todos los que son prestadores de servicios;
4. Certificado de Cumplimiento Tributario;
5. Constancia de Cumplimiento con la Seguridad Social;
6. Formulario de Informe de Servicios Personales (FIS).

f. Formulario de Informe de Servicios Personales (FIS). **NO APLICA.**

Otras formas y condiciones de pago al proveedor en virtud del contrato serán las siguientes: **NO APLICA.**

2. La Contratante efectuará los pagos, dentro del plazo establecido en este apartado, sin exceder sesenta (60) días después de la presentación de una factura por el proveedor, y después de que la contratante la haya aceptado. Dicha aceptación o rechazo, deberá darse a más tardar en quince (15) días posteriores a su presentación.

3. De conformidad a las disposiciones del Decreto N° 7781/2006, del 30 de Junio de 2006 y modificatoria, en las contrataciones con Organismos de la Administración Central, el proveedor deberá habilitar su respectiva cuenta corriente o caja de ahorro en un Banco de plaza y comunicar a la Contratante para que ésta gestione ante la Dirección General del Tesoro Público, la habilitación en el Sistema de Tesorería (SITE).

Solicitud de suspensión de la ejecución del contrato

Si la mora en el pago por parte de la contratante fuere superior a sesenta (60) días, el proveedor, consultor o contratista, tendrá derecho a solicitar por escrito la suspensión de la ejecución del contrato por causas imputables a la contratante.

La solicitud deberá ser respondida por la contratante dentro de los 10 (diez) días calendario de haber recibido por escrito el requerimiento. Pasado dicho plazo sin respuesta se considerará denegado el pedido, con lo que se agota la instancia administrativa quedando expedita la vía contencioso administrativa.

Solicitud de Pago de Anticipo

El plazo dentro del cual se solicitará el anticipo será (en días corridos) de:

EL PLAZO DENTRO DEL CUAL SE SOLICITARA EL ANTICIPO SERA DE 10 (DIEZ) DÍAS CALENDARIO LUEGO DE LA FIRMA DEL CONTRATO.
SERÁ DEL 20% (VEINTE PORCIENTO) DEL MONTO TOTAL DEL CONTRATO.

1. El anticipo es la suma de dinero que se entrega al proveedor, consultor o contratista destinada al financiamiento de los costos en que este debe incurrir para iniciar la ejecución del objeto contractual. El mismo no constituye un pago por adelantado; debe estar amparado con una garantía correspondiente al cien por ciento de su valor y deberá ser amortizado durante la ejecución del contrato y durante la ejecución de contrato demostrar el debido uso. La Garantía de Anticipo deberá mantener su vigencia hasta su total amortización.

Los recursos entregados en calidad de anticipo no podrán destinarse a fines distintos a los relacionados con el objeto del contrato.

En caso de extensión de la Garantía de Anticipo, la misma deberá cubrir el saldo pendiente de amortización.

2. Si se establece en el SICP el otorgamiento de anticipos, no podrá superar en ningún caso el porcentaje establecido en la legislación vigente.

3. La solicitud de pago del anticipo deberá ser presentada por escrito, con la factura, el plan de inversiones y la Garantía de Anticipo.

4. El proveedor podrá remitir una comunicación por escrito a la contratante, en la cual informe que rechaza el anticipo previsto en el PBC. La falta de solicitud de anticipo en el plazo previsto en el PBC será considerado como un rechazo del mismo. En estos casos podrá darse inicio al cómputo de la ejecución contractual en las condiciones establecidas en el pliego de bases y condiciones.

5. El Pago del Anticipo debe ser total. En el caso que se realizare el pago de un porcentaje inferior al 100% del mismo, el proveedor podrá rechazarlo en el plazo de cinco (5) días hábiles mediante una nota de reclamo remitida a la Contratante. Transcurrido dicho plazo, se considerará que el Anticipo ha sido aceptado por el proveedor y podrá darse inicio al cronograma de ejecución contractual en las condiciones establecidas en el pliego de bases y condiciones.

6. En el caso de que el proveedor haya solicitado el anticipo en las condiciones establecidas en la presente clausula y la convocante no ha procedido al pago, el oferente no está obligado a iniciar la ejecución del contrato hasta tanto el pago se haya efectuado de forma total o de acuerdo a lo dispuesto en el punto 5.

7. La amortización del anticipo se realizará de acuerdo con lo establecido en el contrato, en la proporción que éste indique.

8. Para la ejecución de esta garantía, especialmente cuando sea instrumentada a través de Póliza de Seguro de caución, será requisito que previamente el proveedor sea notificado del incumplimiento y la intimación de que se hará efectiva la ejecución del monto asegurado.

9. A menos que se indique otra cosa en este apartado, la Garantía de Anticipo será liberada por la contratante y devuelta al proveedor, a requerimiento de parte, a más tardar treinta (30) días contados a partir de la fecha de cumplimiento de las obligaciones del proveedor en virtud del contrato, pudiendo ajustarse por el saldo adeudado.

10. En el caso de rescisión o terminación anticipada del contrato, los proveedores o contratistas deberán reintegrar a la contratante el saldo por amortizar.

Reajuste

El precio del contrato estará sujeto a reajustes. La fórmula y el procedimiento para el reajuste serán los siguientes:

El precio de los bienes se reajustará durante el periodo de ejecución del contrato, a partir de una variación significativa de precios ocurrida en la economía nacional, que será medida a través del Índice de Precios al Consumo, publicado por el Banco Central del Paraguay, en una relación porcentual igual o mayor al 15% (quince por ciento) del mencionado Índice acumulado a partir de la fecha de presentación de la

Oferta. Los ajustes deberán corresponder a los bienes pendientes de entrega y aplicados sobre el importe facturado y presentado para su pago.

El precio del contrato será reajutable, conforme a la siguiente fórmula:

$$A = \frac{P \times I.I.B.C.P.}{15\%}$$

Dónde:

A= Precio ajustado de los bienes facturados.

P= Precio facturado de los bienes ofertados.

I.I.B.C.P. = Índice de Inflación emitido por el Banco Central del Paraguay.

15% (quince por ciento) = Mínimo necesario para reajuste del precio.

No se reconocerá reajuste de precios si el Proveedor se encuentra atrasado respecto a la provisión de los bienes o la Contratante haya podido constatar fehacientemente que el Proveedor se encuentra en incumplimiento de las obligaciones patronales de seguridad social.

Porcentaje de multas

El valor del porcentaje de multas que será aplicado por el atraso en la entrega de los bienes, prestación de servicios será de:

0,50 %

La contratante podrá deducir en concepto de multas una suma equivalente al porcentaje del precio de entrega de los bienes atrasados, por cada día de atraso indicado en este apartado. La contratante podrá rescindir administrativamente el contrato cuando el valor de las multas supere el monto de la Garantía de Cumplimiento de Contrato.

La aplicación de multas no libera al proveedor del cumplimiento de sus obligaciones contractuales.

Tasa de interés por Mora

En caso de que la contratante incurriera en mora en los pagos, se aplicará una tasa de interés por cada día de atraso, del:

0,01

La mora será computada a partir del día siguiente del vencimiento del pago y no incluye el día en el que la contratante realiza el pago.

Si la Contratante no efectuara cualquiera de los pagos al proveedor en las fechas de vencimiento correspondiente o dentro del plazo establecido en la presente cláusula, la Contratante pagará al proveedor interés sobre los montos de los pagos morosos a la tasa establecida en este apartado, por el período de la demora hasta que haya efectuado el pago completo, ya sea antes o después de cualquier juicio.

Impuestos y derechos

En el caso de bienes de origen extranjero, el Proveedor será totalmente responsable del pago de todos los impuestos, derechos, gravámenes, timbres, comisiones por licencias y otros cargos similares que sean exigibles fuera y dentro de la República del Paraguay, hasta el momento en que los bienes contratados sean entregados al contratante.

En el caso de origen nacional, el Proveedor será totalmente responsable por todos los impuestos, gravámenes, comisiones por licencias y otros cargos similares incurridos hasta el momento en que los bienes contratados sean entregados a la contratante.

El Proveedor será responsable del pago de todos los impuestos y otros tributos o gravámenes con excepción de los siguientes:

No Aplica

Convenios Modificatorios

La Contratante podrá acordar modificaciones al contrato conforme al artículo N° 63 de la Ley N° 2051/2003.

1. Cuando el sistema de adjudicación adoptado sea de abastecimiento simultáneo las ampliaciones de los contratos se regirán por las disposiciones contenidas en la Ley N° 2051/2003, sus modificaciones y reglamentaciones, que para el efecto emita la DNCP.
2. Tratándose de contratos abiertos, las modificaciones a ser introducidas se regirán atendiendo a la reglamentación vigente.
3. La celebración de un Convenio Modificatorio conforme a las reglas establecidas en el artículo N° 63 de la Ley 2051/2003, que constituyan condiciones de agravación del riesgo cuando la Garantía de Cumplimiento de Contrato sea formalizada a través de póliza de caución, obliga al proveedor a informar a la compañía aseguradora sobre las modificaciones a ser realizadas y en su caso, presentar ante la contratante los endosos por ajustes que se realicen a la póliza original en razón al convenio celebrado con la contratante.

Limitación de responsabilidad

Excepto en casos de negligencia grave o actuación de mala fe, el proveedor no tendrá ninguna responsabilidad contractual de agravio o de otra índole frente a la Contratante por pérdidas o daños indirectos o consiguientes, pérdidas de utilización, pérdidas de producción, o pérdidas de ganancias o por costo de intereses, estipulándose que esta exclusión no se aplicará a ninguna de las obligaciones del proveedor de pagar a la Contratante las multas previstas en el Contrato.

Responsabilidad del proveedor

El proveedor deberá suministrar todos los bienes o servicios de acuerdo con las condiciones establecidas en el pliego de bases y condiciones.

Fuerza mayor

El proveedor no estará sujeto a la ejecución de su Garantía de Cumplimiento, liquidación por daños y perjuicios o terminación por incumplimiento en la medida en que la demora o el incumplimiento de sus obligaciones en virtud del contrato sea el resultado de un evento de Fuerza Mayor.

1. Para fines de esta cláusula, "Fuerza Mayor" significa un evento o situación fuera del control del proveedor que es imprevisible, inevitable y no se origina por descuido o negligencia del mismo. Tales eventos pueden incluir sin que éstos sean los únicos actos de la autoridad en su capacidad soberana, guerras o revoluciones, incendios, inundaciones, epidemias, pandemias, restricciones de cuarentena, y embargos de cargamentos.
2. El proveedor deberá demostrar el nexo existente entre el caso notorio y la obligación pendiente de cumplimiento. La fuerza mayor solamente podrá afectar a la parte del contrato cuyo cumplimiento imposible fue probado.
3. No se considerarán casos de Fuerza Mayor los actos o acontecimientos que hagan el cumplimiento de una obligación únicamente más difícil o más onerosa para la parte correspondiente.
4. Si se presentara un evento de Fuerza Mayor, el proveedor notificará por escrito a la contratante sobre dicha condición y causa, en el plazo de siete (7) días calendario a partir del día siguiente en que el proveedor haya tenido conocimiento del evento o debiera haber tenido conocimiento del evento. Transcurrido el mencionado plazo, sin que el proveedor o contratista haya notificado a la convocante la situación que le impide cumplir con las condiciones contractuales, no podrá invocar caso fortuito o fuerza mayor. Excepcionalmente, la convocante bajo su responsabilidad, podrá aceptar la notificación del evento de caso fortuito en un plazo mayor, debiendo acreditar el interés público comprometido.

5. La fuerza mayor debe ser invocada con posterioridad a la suscripción del contrato y con anterioridad al vencimiento del plazo de cumplimiento de las obligaciones contractuales.
6. A menos que la contratante disponga otra cosa por escrito, el proveedor continuará cumpliendo con sus obligaciones en virtud del contrato en la medida que sea razonablemente práctico, y buscará todos los medios alternativos de cumplimiento que no estuviesen afectados por la situación de fuerza mayor existente.

Causales de terminación del contrato

1. Terminación por Incumplimiento

a) La Contratante, sin perjuicio de otros recursos a su disposición en caso de incumplimiento del contrato, podrá terminar el contrato, en cualquiera de las siguientes circunstancias:

i. Si el proveedor no entrega parte o ninguno de los bienes dentro del período establecido en el contrato, o dentro de alguna prórroga otorgada por la contratante; o

ii. Si el proveedor no cumple con cualquier otra obligación en virtud del contrato; o

iii. Si el proveedor, a juicio de la contratante, durante el proceso de licitación o de ejecución del contrato, ha participado en actos de fraude y corrupción;

iv. Cuando las multas por atraso superen el monto de la Garantía de Cumplimiento de Contrato;

v. Por suspensión de los trabajos, imputable al proveedor o al contratista, por más de sesenta días calendarios, sin que medie fuerza mayor o caso fortuito;

vi. En los demás casos previstos en este apartado.

2. Terminación por Insolvencia o quiebra

La Contratante podrá rescindir el contrato mediante comunicación por escrito al proveedor si éste se declarase en quiebra o en estado de insolvencia.

3. Terminación por conveniencia

a) La contratante podrá en cualquier momento terminar total o parcialmente el contrato por razones de interés público debidamente justificada, mediante notificación escrita al proveedor. La notificación indicará la razón de la terminación así como el alcance de la terminación con respecto a las obligaciones del proveedor, y la fecha en que se hace efectiva dicha terminación.

b) Los bienes que ya estén fabricados y estuviesen listos para ser enviados a la contratante dentro de los treinta (30) días siguientes a la fecha de recibo de la notificación de terminación del contrato deberán ser aceptados por la contratante de acuerdo con los términos y precios establecidos en el contrato. En cuanto al resto de los bienes la contratante podrá elegir entre las siguientes opciones:

i. Que se complete alguna porción y se entregue de acuerdo con las condiciones y precios del contrato; y/o

ii. Que se cancele la entrega restante y se pague al proveedor una suma convenida por aquellos bienes que hubiesen sido parcialmente completados y por los materiales y repuestos adquiridos previamente por el proveedor.

Otras causales de terminación del contrato

Además de las ya indicadas en la cláusula anterior, otras causales de terminación de contrato son:

No Aplica

Resolución de Conflictos a través del Arbitraje

Las partes se someterán a Arbitraje:

No

En caso que la Convocante adopte el arbitraje como mecanismo de resolución de conflicto, la cláusula arbitral que regirá a las partes es la siguiente:

"Todas las controversias que deriven del presente contrato o que guarden relación con éste serán resueltas definitivamente por arbitraje, conforme con las disposiciones de la ley N° 2051/03 "De Contrataciones Públicas", de la ley N° 1879/02 "De arbitraje y mediación" y las condiciones del Contrato. El procedimiento arbitral se llevará a cabo ante el Centro de Arbitraje y Mediación del Paraguay (en adelante, "CAMP"). El tribunal estará conformado por tres árbitros designados de la lista del cuerpo arbitral del CAMP, que decidirá conforme a derecho, siendo el laudo definitivo y vinculante para las partes. Se aplicará el reglamento respectivo y demás disposiciones que regule dicho procedimiento al momento de ser requerido, declarando las partes conocer y aceptar los vigentes, incluso en orden a su régimen de gastos y costas, considerándolos parte integrante del presente Contrato. Para la ejecución del laudo arbitral, o para dirimir cuestiones que no sean arbitrables, las partes se someterán a la jurisdicción de los tribunales de la ciudad de Asunción, República del Paraguay".

Fraude y Corrupción

1. La Convocante exige que los participantes en los procedimientos de contratación, observen los más altos niveles éticos, ya sea durante el proceso de licitación o de ejecución de un contrato. La Convocante actuará frente a cualquier hecho o reclamación que se considere fraudulento o corrupto.

2. Si se comprueba que un funcionario público, o quien actúe en su lugar, y/o el oferente o adjudicatario propuesto en un proceso de contratación, hayan incurrido en prácticas fraudulentas o corruptas, la Convocante deberá:

(i) En la etapa de oferta, se descalificará cualquier oferta del oferente y/o rechazará cualquier propuesta de adjudicación relacionada con el proceso de adquisición o contratación de que se trate; y/o

(ii) Durante la ejecución del contrato, se rescindirá el contrato por causa imputable al proveedor;

(iii) Se remitirán los antecedentes del oferente o proveedor directamente involucrado en las prácticas fraudulentas o corruptivas, a la Dirección Nacional de Contrataciones Públicas, a los efectos de la aplicación de las sanciones previstas.

(iv) Se presentará la denuncia penal ante las instancias correspondientes si el hecho conocido se encontrare tipificado en la legislación penal.

Fraude y corrupción comprenden actos como:

(i) Ofrecer, dar, recibir o solicitar, directa o indirectamente, cualquier cosa de valor para influenciar las acciones de otra parte;

(ii) Cualquier acto u omisión, incluyendo la tergiversación de hechos y circunstancias, que engañen, o intenten engañar, a alguna parte para obtener un beneficio económico o de otra naturaleza o para evadir una obligación;

(iii) Perjudicar o causar daño, o amenazar con perjudicar o causar daño, directa o indirectamente, a cualquier parte o a sus bienes para influenciar las acciones de una parte;

(iv) Colusión o acuerdo entre dos o más partes realizado con la intención de alcanzar un propósito inapropiado, incluyendo influenciar en forma inapropiada las acciones de otra parte.

(v) Cualquier otro acto considerado como tal en la legislación vigente.

3. Los Oferentes deberán declarar que por sí mismos o a través de interpósita persona, se abstendrán de adoptar conductas orientadas a que los funcionarios o empleados de la convocante induzcan o alteren las evaluaciones de las propuestas, el resultado del procedimiento u otros aspectos que les otorguen condiciones más ventajosas con relación a los demás participantes (Declaratoria de Integridad).

MODELO DE CONTRATO

Este modelo de contrato, constituye la proforma del contrato a ser utilizado una vez adjudicado al proveedor y en los plazos dispuestos para el efecto por la normativa vigente.

EL MODELO DE CONTRATO SE ENCUENTRA EN UN ARCHIVO ANEXO A ESTE DOCUMENTO.

FORMULARIOS

Los formularios dispuestos en esta sección son los estándar a ser utilizados por los potenciales oferentes para la preparación de sus ofertas.

ESTA SECCIÓN DE FORMULARIOS SE ENCUENTRA EN UN ARCHIVO ANEXO A ESTE DOCUMENTO, DEBIENDO LA CONVOCANTE MANTENERLO EN FORMATO EDITABLE A FIN DE QUE EL OFERENTE LO PUEDA UTILIZAR EN LA PREPARACION DE SU OFERTA.

