

TÉRMINOS DE REFERENCIA PARA LA CONTRATACIÓN DEL SERVICIO DE INTERNET PRINCIPAL PARA EL INSTITUTO PERUANO DEL DEPORTE

1. ÁREA SOLICITANTE

Unidad Funcional de Administración de Recintos Deportivos de Lima Metropolitana (UFARDELM) del Instituto Peruano del Deporte.

2. OBJETIVO DE LA CONVOCATORIA (SERVICIO)

Contratación de servicio de internet de alta disponibilidad, con solución de seguridad perimetral e interconexión con todas las sedes de IPD, por un periodo de 24 meses; este servicio debe permitir la interconexión entre la sede administrativa principal (Estadio Nacional), sedes deportivas y/o complejos deportivos (CD), mediante enlaces de fibra óptica LAN to LAN y brindar el servicio de acceso a Internet e incluir la gestión compartida de seguridad a través de un equipo de seguridad perimetral que permitan proteger la red institucional de accesos no deseados desde internet, control de spam de los correos y controlar los accesos del personal del IPD a internet mediante un equipo de seguridad perimetral.

3. FINALIDAD PÚBLICA

La Contratación del Servicio de Internet Principal para el Instituto Peruano del Deporte permitirá contar con un oportuno acceso a información y servicios informáticos en la institución, que permitan a los funcionarios y servidores públicos tener la disponibilidad de información para sus labores.

4. ESPECIFICACIONES DEL SERVICIO

4.1. Servicio de acceso a Internet

- i. El servicio de acceso a Internet a contratar, debe contar con un enlace principal y un enlace de contingencia, de acuerdo al siguiente cuadro:

N°	Dirección	Cantidad	Ancho de Banda	Enlace Dedicado
01	Estadio Nacional (Calle Madre de Dios N°463), Cercado de Lima	01	400 Mbps	Principal
02	Estadio Nacional (Calle Madre de Dios N°463), Cercado de Lima	01	400 Mbps	Contingencia

- ii. El enlace principal y el enlace secundario deben venir de diferentes nodos de comunicación para garantizar la continuidad de los servicios de Internet. Dicho requisito debe ser expresado por el postor adjudicado con la buena pro, para la firma de contrato, mediante una declaración jurada que indique: "Mi representada declara que el enlace principal y el enlace secundario (contingencia) vienen de diferentes nodos de comunicación para garantizar la continuidad de los servicios de Internet".
- iii. Acceso dedicado simétrico Carrier Class a internet, sin restricción de protocolo, puerto o aplicación; enlaces transparentes para todos los servicios IP; con un ancho

de banda 400 Mbps, con un Overbooking 1:1 en el enlace local e internacional. Este overbooking 1:1 en el enlace internacional hace referencia al overbooking 1:1 hasta el Router de acceso de salida Internacional a Internet.

- iv. La red Backbone del contratista deberá ser propia y con redundancia y debe emplear fibra óptica y el ancho de banda será exclusivo 1:1.
- v. El proveedor debe ser propietario de su backbone y últimas millas de fibra óptica; no se aceptarán propuestas que subcontraten o arrienden.
- vi. El proveedor del servicio para el enlace backup de 400 Mbps debe emplear fibra óptica y el ancho de banda será exclusivo 1:1.
- vii. El proveedor brindará un rango de treinta y dos (32) IPs públicas; de ser necesarios nuestros registros DNS y dominios podrán ser registrados en los servidores de comunicación del proveedor; el proveedor podrá entregar en un máximo de dos rangos de IPs distintas para cubrir la solicitud de treinta y dos (32) IPs públicas si es que el proveedor del servicio lo ve conveniente y necesario.
- viii. Para la asignación de los IPs para el Gateway, broadcast y red, el proveedor del servicio no debe hacer uso de ninguno de las treinta y dos (32) IPs públicas solicitadas; el proveedor debe dimensionar su propuesta en base a lo solicitado.
- ix. El proveedor debe asegurar la disponibilidad del servicio mayor o igual al 99.9% como requisito mínimo para el uso del servicio de Internet para los trabajos remotos que viene realizando la Entidad.
- x. El servicio de acceso a Internet deberá contar con una alta disponibilidad en modo activo /pasivo, que se activará de manera automática en caso de falla del enlace principal. El acceso de contingencia deberá garantizar el mismo ancho de banda contratado del acceso principal (400 Mbps) y el Router del enlace de contingencia debe tener las mismas características que el Router del enlace principal. La Salida a Internet será por la sede del Instituto Peruano del Deporte en Lima
- xi. El contratista debe tener redundancia de servidores DNS en arreglos de alta disponibilidad.
- xii. El contratista debe proveer una herramienta de Monitoreo, Gestión y Reporte en línea, del enlace y uso de ancho de banda. Así mismo deberá proveer reportes de tráfico diario, semanales y mensuales en línea, almacenando una bitácora de las últimas 8 semanas, para fines comparativos.
- xiii. El contratista deberá realizar los trabajos necesarios dentro o fuera del local, incluyendo su trámite de permisos municipales, obras civiles y otros necesarios sin que esto implique costo adicional para el Instituto Peruano del Deporte. El servicio es considerando llave en mano incluyendo todos los equipos necesarios para el cumplimiento del presente servicio.
- xiv. El contratista deberá implementar una línea de contingencia desde un nodo y ruta diferente para línea de la sede principal, con las mismas características, la configuración será Activo - Pasivo.
- xv. El contratista podrá hacer uso del equipo para proporcionar el servicio de transmisión de datos siempre y cuando garantice el ancho de banda requerido para el servicio de internet y para el servicio de transmisión de datos.
- xvi. El postor deberá tener conexión con 03 proveedores TIER-1 diferentes y deberá acreditarlo con la presentación de copia de constancias y/o contratos emitidos o suscritos con los proveedores de las salidas.

- xvii. La activación de la cabecera en el Datacenter del contratista será a petición del personal responsable del Instituto Peruano del Deporte y no de forma automática, este requerimiento se realizará vía correo electrónico, el cual tendrá un tiempo máximo de implementación desde su aviso de 6 horas.
- xviii. El Contratista deberá ofrecer una protección DDoS la cual puede ser implementada como funcionalidad del equipo NGFW en la policita de navegación
- xix. El proveedor debe llevar la señal de internet hasta el puerto RJ45 del switch core principal del IPD acondicionando adecuadamente el cableado de red y/o fibra óptica; el proveedor debe realizar las labores de conexiones físicas y configuración en los equipos de comunicación que permitan la comunicación y acceso a Internet a todos los equipos de cómputo del IPD. La entidad, en este caso IPD, se encargará de la configuración LAN y no el proveedor ganador.
- xx. El servicio es a todo costo; el proveedor debe dimensionar adecuadamente el uso desus recursos, equipos, componentes para la implementación de la conectividad a Internet vía fibra óptica.
- xxi. La última milla de conexión debe ser fibra óptica para el enlace principal y el de contingencia.
- xxii. El contratista, dentro de los cinco (05) días calendario siguientes de la firma del Contrato, deberá presentar su plan de implementación del servicio, debe presentar información con respecto a la tecnología que va utilizar, los equipos y accesorios que va a instalar y del diagrama de red propuesto, con lo que va garantizar el correcto funcionamiento del servicio que propone.
- xxiii. La instalación, implementación y puesta en marcha de la solución no debe exceder de un plazo máximo de hasta los cuarenta y cinco (45) días calendarios, contados apartir del día siguiente de aprobado el plan de implementación por la Unidad de Informática (UI).
- xxiv. El proveedor podrá realizar una visita técnica a las instalaciones del IPD para que pueda dimensionar su propuesta técnico económica adecuadamente.
- xxv. El proveedor deberá coordinar y solicitar los permisos correspondientes a la Municipales para las instalaciones de sus respectivas fibras ópticas hacia la sede administrativa principal (Estadio Nacional), sedes deportivas y/o complejos deportivos (CD) del Instituto Peruano del Deporte (IPD).

4.2. Servicio de Interconexión LAN to LAN

- i. El contratista debe brindar el servicio de Interconexión LAN to LAN entre las sedes del Instituto Peruano del Deporte hacia la sede principal, y ancho de banda de acuerdo al siguiente cuadro:

Nº	SEDE (Complejo Deportivo)	DIRECCION	ANCHO DE BANDA
1	Estadio Nacional	Estadio Nacional (Calle Madre de Dios N°463), Cercado de Lima	400 Mbps
2	Albergue Videna (Villa Deportiva)	Av. Aviación 2085 (referencia al costado de la federación peruana de futbol) ó Av. del Aire (referencia cd. 08) – Local administrado por el IPD	200 Mbps
3	San Juan de Miraflores	Av. San Juan N°640, San Juan de Miraflores	20 Mbps
4	Oscar Benavides	Av. 28 de Julio N°1699, La Victoria	20 Mbps

5	Chacarilla de Otero	Pasaje Mariano Melgar N°146 Urb. Chacarilla de Otero, San Juan de Lurigancho	20 Mbps
6	Piscina Canto Grande	Av. Héroes del Cenepa s/n - Av. Wiesse y Bayovar – Urb. Mariscal Cáceres, San Juan de Lurigancho	20 Mbps
7	Coliseo Cerrado Puente del Ejercito	Av. Alfonso Ugarte N°95 - Puente del Ejercito (Plaza Unión), Cercado de Lima.	20 Mbps
8	Los Olivos	Jr. Las Flores s/n Urb. Los Naranjos	20 Mbps
9	Carabayllo	Km. 22 Av. Tupac Amaru - Carabayllo	20 Mbps
10	Piscina 12 de octubre	Psje. 12 de octubre s/n - La Victoria	20 Mbps
11	Piscina Matute	Psje. Francia Cdra. 12 de Abtao	20 Mbps
12	Santa Anita	Coop. Vivienda Santa Aurelia - Santa Anita	20 Mbps
13	Coliseo Eduardo Dibos	Av. Angamos con Av. Aviación	20 Mbps
14	Estadio Tahuantinsuyo	Ca. Coricancha 4ta. Zona Tahuantinsuyo - Independencia	20 Mbps
15	Mangomarca	Jr. Mangomarca s/n - Urb. Mangomarca - San Juan de Lurigancho	20 Mbps

- ii. Los equipos locales del cliente - CPE que serán provistos en calidad de alquiler por parte del contratista, deberán contar con la última actualización de software, nuevos, de primer uso deberán soportar al menos el doble de Throughput contratado, para ampliaciones de ancho de banda en casos necesarios; el contratista deberá brindar hoja técnica y/o carta del fabricante donde indique el valor de Throughput que soporta el equipo.
- iii. Los equipos CPE, deberán tener habilitados los protocolos SNMP u otros similares, de manera tal que se puedan monitorear el consumo de ancho de banda (BW) y tráfico con las propias herramientas de gestión del Instituto Peruano del Deporte. Se deberá hacer entrega de las credenciales de acceso de solo lectura, definidas en los Routers instalados, a las sedes del Instituto Peruano del Deporte.
- iv. El servicio debe estar basado en líneas de enlace dedicados y debe ser una red privada y no debe ser compartida; y debe ser de uso exclusivo del IPD.
- v. La disponibilidad del servicio será como mínimo de 99.6%.
- vi. El proveedor deberá garantizar que el servicio solicitado para cada uno de sus sedes el acceso dedicado simétrico y con un Overbooking 1:1
- vii. El proveedor instalará sus equipos de comunicación en cada sede.
- viii. El enrutamiento de las comunicaciones estará a cargo del proveedor del servicio, y este enrutamiento debe permitir una comunicación fluida y sin interferencias entre todas las sedes; se debe considerar que el Estadio Nacional será el punto de concentración principal de conexión entre todas las sedes.
- ix. El proveedor de servicio debe llevar la señal de red hasta el puerto RJ45 de los equipos de comunicación del IPD de cada sede.
- x. El proveedor debe ser propietario de su backbone y últimas millas de fibra óptica; no se aceptarán propuestas que subcontraten o arrienden.
- xi. El contratista del servicio debe garantizar una transmisión segura, íntegra y confiable de la voz, video y datos desde las sedes remotas hacia la sede principal, considerando como factor crítico en el transporte de la información, una trayectoria privada separada de la red pública de Internet. Además, la conexión solicitada para cada local es de acceso dedicado simétrico y con un Overbooking 1:1
- xii. El contratista no podrá emplear el Internet como medio de transporte para la

interconexión de las sedes. No se aceptará una solución basada en túneles a través de Internet.

- xiii. El ancho de banda consumido por el Servicio de Interconexión LAN to LAN, no debe afectar al ancho de banda del Servicio de Acceso a Internet.
- xiv. El contratista debe asegurar el 100% del ancho de banda del enlace principal y de contingencia bajo cualquier circunstancia. El Instituto Peruano del Deporte podrá realizar pruebas de esfuerzo en las líneas dedicadas para verificar que se cumplan los valores solicitados.
- xv. El protocolo de la red de transporte deberá ser MPLS.
- xvi. El Instituto Peruano del Deporte proporcionará espacio en los gabinetes de comunicaciones (para el caso de la sede central) para alojar los equipos que serán instalados por el contratista, El Instituto Peruano del Deporte será responsable de brindar la energía para dichos equipos. La ubicación de todos los equipos en las sedes del El Instituto Peruano del Deporte a nivel nacional deberá ser aprobada antes de su instalación por el Instituto Peruano del Deporte.
- xvii. El contratista deberá implementar una línea de contingencia desde un NODO y ruta diferente solo para línea de la sede principal, con las mismas características, la configuración será Activo - Pasivo.
- xviii. El contratista podrá hacer uso del equipo para proporcionar el servicio de internet siempre y cuando garantice el ancho de banda requerido para el servicio de transmisión de datos y para el servicio de internet.
- xix. La medición de la latencia se realizará considerando la trayectoria de ida y vuelta entre el punto origen y destino. El tiempo máximo de latencia será de 80ms.
- xx. La instalación, implementación y puesta en marcha de la solución no debe exceder de un plazo máximo de hasta los cuarenta y cinco (45) días calendarios, contados apartir del día siguiente de aprobado el plan de implementación por la Unidad de Informática (UI).
- xxi. Tiempo de espera máximo (promedio) de enlaces terrestres de 5ms.

4.2.1. Características de los routers por sede

i. Router de enlace principal y contingencia (Estadio Nacional)

- Los routers deben emplear la tecnología VRRP o similar, debe soportar un ancho de banda mínima de 400 Mbps, con capacidad de crecimiento mínima 800 Mbps de ser necesario su crecimiento.
- Debe incluir como mínimo un (1) USB puertos, (1) puerto de consola, 2x GE RJ45 Puertos de Gestión, 8x GE SFP Slots, 8x puertos GE RJ45 , 2x 10 GE SFP+ Slots
- Todos los puertos solicitados podrán operar en capa tres (03) y capa dos (02)del modelo OSI.
- Soporte de protocolos de enrutamiento BGP, OSPF, RIP y rutas estáticas.
- Soporte para protocolos IPV4 e IPV6.
- Soporte para 802.1q VLAN, VRRP
- Los routers deben administrar configuraciones de calidad de servicios (QoS).
- Los routers podrán como mínimo siempre y cuando los equipos que proponga el proveedor sean estables, permita una comunicación fluida, sin latencia en las comunicaciones y permita una comunicación segura; sin que la entidad se vea perjudicada.

ii. Routers de las trece (13) sedes (complejos deportivos)

- Deben soportar un ancho de banda mínima de diez (20) Mbps y un máximo cincuenta (60) Mbps.
- Debe incluir como mínimo dos (2) puertos RJ-45 , (2) puertos Gigabit Ethernet 10/100/1000 WAN
- Se debe incluir servicio de WIFI para usuarios de estas sedes este red de wifi debe tener las mismas políticas de navegación que la red cableada para cada sede remota
- Todos los puertos solicitados podrán operar en capa tres (03) y capa dos (02) del modelo OSI.
- Soporte de protocolos de enrutamiento BGP, OSPF, RIP y rutas estáticas.
- Soporte para protocolos IPV4 e IPV6.
- Soporte para 802.1q VLAN, PPP y PPPoE., VRRP,
- Los routers deben administrar configuraciones de calidad de servicios (QoS).
- Memoria Flash de al menos 128 MB
- Memoria DRAM Máxima 2G

iii. Los routers deben tener habilitados la lectura SNMP.

iv. Debe priorizarse el tráfico basado en direcciones IP y/o puertos TCP/UDP según la configuración que se esté empleando.

v. Los equipos instalados deben permitir el transporte de tráfico ruteado en IP.

vi. Los equipos router proporcionados por el proveedor del servicio, deben ser de última generación y con capacidad de soportar el requerimiento de ampliación de ancho banda a emplear de ser solicitado por el IPD.

vii. El proveedor debe dimensionar su solución a todo costo que permita la interconexión entre las distintas sedes del IPD.

viii. El proveedor se encargará de toda la implementación que permita la interconexión entre todas las sedes con la sede principal; debe considerar todos los componentes necesarios que permitan instalar los equipos routers.

ix. La solución que proponga debe llegar hasta el puerto de red RJ45 de la red institucional del IPD.

4.3. Características del equipo de seguridad perimetral

El postor del servicio de telecomunicaciones deberá implementar un equipo de seguridad perimetral.

Se requieren (01) unidades de appliance físico, licenciados por el periodo que dure el contrato. El equipo debe ser nuevo y de primer uso. Dichos equipos deben incluir las siguientes capacidades como mínimo:

1. Características de rendimiento

- ✓ Soportar al menos 3.4 Gbps de throughput de NGFW, medido en EnterpriseMix.
- ✓ Soportar al menos 4.9 Gbps de throughput de IPS, medido en EnterpriseMix.
- ✓ Soportar al menos 2.9 Gbps de throughput de Threat Protection, medido en Enterprise Mix.
- ✓ Soporte a por lo menos 2.9 millones conexiones simultáneas TCP o conexiones concurrentes.
- ✓ Soporte a por lo menos 270 000 nuevas conexiones por segundo TCP
- ✓ Throughput de al menos 12 Gbps de VPN IPSec, medido con paquetes

de 512 bytes

- ✓ Estar licenciado para, o soportar sin necesidad de licencia, 1900 túneles de VPN IPSec site-to-site simultáneos o Gateway to Gateway.
- ✓ Estar licenciado para, o soportar sin necesidad de licencia, 15000 túneles de clientes VPN IPSec simultáneos
- ✓ Throughput de al menos 1.9 Gbps de VPN SSL
- ✓ Soportar al menos 500 clientes de VPN SSL simultáneos
- ✓ Soportar al menos 3.9 Gbps de throughput de Inspección SSL, medido con conexiones HTTPS
- ✓ Soportar al menos 12 Gbps de throughput de Application Control, medido en HTTP 64 KB
- ✓ Tener al menos 16 interfaces 1 Gbps RJ45, las cuales serán utilizadas exclusivamente para tráfico de red
- ✓ Tener al menos 8 slots de 1 Gbps SFP, las cuales serán utilizadas exclusivamente para tráfico de red
- ✓ Tener al menos 2 slots de 10 Gbps SFP+, las cuales serán utilizadas exclusivamente para tráfico de red
- ✓ Tener al menos 1 interfaz dedicada para gestión
- ✓ Tener al menos 1 interfaz dedicada para HA
- ✓ Tener al menos 2 fuentes de poder internas.
- ✓ Tener al menos 1 puerto de consola
- ✓ Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) o dominios virtuales por appliance.

2. 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;
- ✓ El sistema operativo debe contar con certificación USGv6 en la suite de Basic Interoperability.
- ✓ Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;
- ✓ 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;
- ✓ La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;
- ✓ 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;
- ✓ La gestión del equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;
- ✓ Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;
- ✓ Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;
- ✓ Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;

- ✓ Los dispositivos de protección de red deben soportar encaminamiento demulticast (PIM-SM y PIM-DM);
- ✓ Los dispositivos de protección de red deben soportar DHCP Relay y DHCP Server
- ✓ Los dispositivos de protección de red deben soportar sFlow;
- ✓ Los dispositivos de protección de red deben soportar Jumbo Frames;
- ✓ Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;
- ✓ Debe ser compatible con NAT dinámica (varios-a-1);
- ✓ Debe ser compatible con NAT dinámica (muchos-a-muchos);
- ✓ Debe soportar NAT estática (1-a-1);
- ✓ Debe admitir NAT estática (muchos-a-muchos);
- ✓ Debe ser compatible con NAT estático bidireccional 1-a-1;
- ✓ Debe ser compatible con la traducción de puertos (PAT);
- ✓ Debe ser compatible con NAT Origen;
- ✓ Debe ser compatible con NAT de destino;
- ✓ Debe soportar NAT de origen y NAT de destino de forma simultánea;
- ✓ Debe soportar NAT de origen y NAT de destino en la misma política
- ✓ Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;
- ✓ Debe ser compatible con NAT64 y NAT46;
- ✓ Debe implementar el protocolo ECMP;
- ✓ La solución debe incluir capacidades de SD-WAN durante la vigencia del contrato.
- ✓ Las capacidades de SD-WAN de la solución deben permitir monitorear el tráfico de aplicaciones desde un servicio en nube del fabricante.
- ✓ Debe soportar el balanceo de enlace por hash de IP de origen y destino;
- ✓ 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;
- ✓ Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;
- ✓ 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;
- ✓ Enviar logs a sistemas de gestión externos simultáneamente;
- ✓ Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;
- ✓ Debe soportar protección contra la suplantación de identidad (anti-spoofing);
- ✓ Implementar la optimización del tráfico entre dos dispositivos;
- ✓ Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);
- ✓ Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);
- ✓ Soportar OSPF graceful restart;
- ✓ Debe ser compatible con el modo Sniffer para la inspección a través del

puerto espejo del tráfico de datos de la red;

- ✓ Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;
- ✓ Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;
- ✓ Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;
- ✓ Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;
- ✓ Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;
- ✓ Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;
- ✓ La configuración de alta disponibilidad debe sincronizar: Sesiones, asociaciones de seguridad VPN y ablas FIB;
- ✓ La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;
- ✓ En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;
- ✓ Debe soportar la creación de sistemas virtuales en el mismo equipo;
- ✓ 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;
- ✓ 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;
- ✓ 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;
- ✓ 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);
- ✓ La consola de administración debe soportar como mínimo, inglés, español y Portugues.
- ✓ La solución debe incluir la capacidad de detectar al menos los siguientes valores dentro del tráfico analizado: nombre del host y sistema operativo.
- ✓ La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.

3. Control por Política de Firewall

- ✓ Debe soportar controles de zona de seguridad;
- ✓ Debe contar con políticas de control por puerto y protocolo;

- ✓ 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;
- ✓ Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;
- ✓ Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;
- ✓ Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;
- ✓ Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);
- ✓ Debe soportar el protocolo estándar de la industria VXLAN;
- ✓ La solución debe permitir la implementación sin asistencia de SD-WAN
- ✓ En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN;
- ✓ La solución debe soportar la integración nativa con una solución de sandboxing.

4. Control de Aplicación

- ✓ Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;
- ✓ 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;
- ✓ 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;
- ✓ 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;
- ✓ 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;
- ✓ Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;
- ✓ Actualización de la base de firmas de la aplicación de forma automática;
- ✓ Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos;
- ✓ Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;

- ✓ 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;
- ✓ El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
- ✓ Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;
- ✓ Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;
- ✓ Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitir a Hangouts el chat, pero impedir la llamada de video;
- ✓ Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;
- ✓ Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones, nivel de riesgo de la aplicación y categoría de aplicación.
- ✓ Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente

5. Prevención de Amenazas

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

intermedia (buffer overflow);

- ✓ Debe poder crear firmas personalizadas en la interfaz gráfica del producto;
- ✓ Identificar y bloquear la comunicación con redes de bots;
- ✓ 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;
- ✓ Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;
- ✓ 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;
- ✓ La capacidad de filtro de DNS debe ser alimentada por un servicio de inteligencia de amenazas de la propia marca.
- ✓ Debe permitir la translación en el firewall de una consulta de DNS, a fin de redirigir la resolución hacia otro destino diferente del original.
- ✓ Los eventos deben identificar el país que origino la amenaza;
- ✓ Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);
- ✓ Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;
- ✓ 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;
- ✓ Debe incluir la protección contra ataques de día cero a través de una estrecha integración con análisis Sandbox en nube;

6. 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);
- ✓ 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;
- ✓ Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;
- ✓ 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;
- ✓ Tener por lo menos 75 categorías de URL;
- ✓ Debe tener la funcionalidad de exclusión de URLs por categoría;
- ✓ Permitir página de bloqueo personalizada;
- ✓ 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);

7. 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 activo, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;
- ✓ Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / controles basados en usuarios y grupos de usuarios;
- ✓ Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/controles 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;
- ✓ Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / controles basados en usuarios y grupos de usuarios;
- ✓ Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/controles basados en usuarios y grupos de usuarios;
- ✓ 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);
- ✓ 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;
- ✓ Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;
- ✓ Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;
- ✓ Debe incluir al menos dos tokens dentro del servicio, permitiendo la autenticación de dos factores para los usuarios administradores del firewall;

8. QoS Traffic Shaping

- ✓ Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda
- ✓ máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming;
- ✓ Soportar la creación de políticas de QoS y Traffic Shaping por dirección

de origen, dirección de destino, por usuario y grupo.

- ✓ Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
- ✓ Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;
- ✓ En QoS debe permitir la definición de tráfico con ancho de banda garantizado, con máximo ancho de banda y colas de prioridad.
- ✓ Soportar marcación de paquetes DiffServ, incluso por aplicación;
- ✓ Soportar la modificación de los valores de DSCP para Diffserv;
- ✓ Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);
- ✓ Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;

9. Filtro de Datos

- ✓ Permite la creación de filtros para archivos y datos predefinidos;
- ✓ Los archivos deben ser identificados por tamaño y tipo;
- ✓ Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones;
- ✓ Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;
- ✓ Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;
- ✓ 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;

4.3.3 REGISTRO DE EVENTOS DE SEGURIDAD DEL FIREWALL

Deberá contar con las siguientes especificaciones mínimas:

- a. Generación de reportes personalizados a solicitud.
- b. Almacenamiento de log por últimos 30 días.
- c. Envío automático de reporte standard de forma semanal, el cual consta de los siguientes puntos:
 - Estado de recursos del Firewall
 - Recursos – promedio
 - Recursos - pico Estadísticas del Tráfico
 - Flujo de Tráfico (BW)
 - Número de Sesiones Top 10
 - Usuarios con mayor consumo de Bandwidth % Utilizado
 - Control de Aplicaciones
 - Top 20 Dominios web x visitas
 - Top 20 Usuarios x Bandwidth
 - Top 20 de intrusiones Bloqueadas
 - Malware Detectados y Bloqueados
 - Consumo de ancho de banda por sedes

5. CENTRAL TELEFONICA IP

- a. El servicio de telefonía IP para el IPD, deberá considerar la instalación, configuración y el soporte respectivo de los equipos necesarios para la implementación de la solución por un periodo de (24) veinticuatro meses contabilizados a partir del día siguiente de la firma del acta de inicio del servicio.
- b. Todos los equipos, elementos y/o accesorios que sean utilizados en la infraestructura de comunicaciones y enlace VPN, deberán ser de tecnología vigente. El proveedor garantizará el cumplimiento mediante documentación aplicable, la misma que será revisada y aprobada por la Oficina de Tecnologías de la Información de la entidad.
- c. El servicio debe proporcionar un nivel de operatividad no menor al 99.6% calculado mensualmente, para todos los componentes que formen parte de la plataforma.
- d. El servicio de telefonía IP deberá estar basado en una plataforma de arquitectura modular que deberá estar configurada para ser parte de la red privada del proveedor del servicio, la plataforma debe a su vez ser accesible a través de una conexión dedicada segura proveída por el contratista entre la entidad y el centro de datos del proveedor del servicio. La velocidad del enlace deberá soportar la cantidad de anexos y llamadas externas de manera concurrente.
- e. Se deberá habilitar el servicio de telefonía corporativa para la sede Estadio Nacional y sus sedes a través de 01 enlace para comunicación con la red de telefonía pública de 60 canales para llamadas entrantes y salientes desde y hacia los anexos internos; este enlace deberá ser habilitados y configurados en la arquitectura tecnológica del proveedor del servicio (red del proveedor).
- f. El proveedor deberá brindar el servicio para la interconexión del local de la sede de Estadio Nacional. Esta interconexión deberá ser brindada mediante un enlace de fibra óptica dedicado simétrico garantizado al 100%; asimismo, la solución de telefonía IP instalada deberá garantizar la calidad de la voz en sus comunicaciones internas, así como en las comunicaciones hacia la red pública de telefonía, el ancho de banda de este enlace deberá ser capaz de soportar las comunicaciones de los canales de voz.
- g. El proveedor será responsable de la configuración de las soluciones solicitadas.
- h. La solución deberá de utilizar como base el sistema de cableado estructurado existente, estas facilidades son responsabilidad de la entidad.
- i. La entidad brindará la infraestructura de switches capaces de asegurar la independencia de la red de voz con la red de datos.
- j. El contratista deberá incluir un enlace dedicado sobre Fibra Óptica para telefonía 10 Mbps simétrico, sin restricciones, de alta calidad, velocidad y disponibilidad utilizando como medio de acceso al backbone la red privada del proveedor.

De la Plataforma de telefonía IP

El sistema sobre el cual deberá estar montada la solución de telefonía IP deberá ser gestionada a través de una PBX en la nube.

- a. La plataforma de telefonía IP deberá ofrecer un alto grado de escalabilidad en el producto ofertado.

De las capacidades técnicas mínimas

- a. El sistema deberá de soportar 60 llamadas recurrentes.
El sistema deberá de soportar un mínimo de cien (100) anexos internos administrativos.
- b. 01 operadora automática con capacidad para atender hasta 15 accesos simultáneos.
- c. El sistema de telefonía IP debe soportar un IVR, el cual será configurado por el contratista.

- d. Se brindará 20 teléfonos IP como máximo del modelo administrativo los teléfonos influyen fuente de poder así mismo se debe contar con un punto de red cercano a donde se colocará el teléfono

De las Funcionalidades del sistema de telefonía IP

- a. Mensaje de bienvenida.
- b. Conferencia tripartita.
- c. Parqueo de llamadas.
- d. Llamadas internas
- e. Llamadas externas.
- f. Desvío de llamadas.
- g. Desvío de llamada en caso de ocupado
- h. Desvío de llamada en caso no contesta
- i. Transferencia directa.
- j. Marcación por tonos DTMF.
- k. Llamada en espera.
- l. Indicador de mensaje de espera.
- m. Historial de llamadas.
- n. Soporte de múltiples líneas.
- o. Identificación de llamadas.
- p. No molestar.
- q. Portal de voz con guías vocales en español
- r. Captura de llamadas
- s. Perifoneo.
- t. Monitoreo de status de presencia en el teléfono
- u. Voicemail
- v. Marcación abreviada
- w. Operadora automática
- x. Música en espera.
- y. Grupo de timbrado.

De las Terminales telefónicos físicos existentes

- a. La municipalidad cuenta con sus propios teléfonos IP que soportan protocolo SIP

De la bolsa de minutos

Destino de llamada*	Minutos Mensuales
Todo destino nacional	10 000

* Los minutos presentados no incluyen llamadas a teléfonos rurales y/o satelitales

6. CARACTERISTICAS DE LOS POSTES INTELIGENTES CON WIFI

- Se implementarán 03 postes inteligentes con acceso a internet WIFI de 20Mbps y punto de video vigilancia, en las siguientes ubicaciones:
 - 1.- Av. San Juan N°640, San Juan de Miraflores
 - 2.- Av. Héroes del Cenepa s/n - Av. Wiese y Bayovar Urb Mariscal Cáceres, San Juan de Lurigancho
 - 3.- Coop. Vivienda Santa Aurelia - Santa Anita
- El wifi de acceso público deberá contar con un portal cautivo para el acceso gratuito a internet.

- El poste inteligente contará con una cámara de video vigilancia implementada para los puntos de video vigilancia, los cuales deberán contar con las siguientes especificaciones mínimas:
 - ✓ Cámara domo IP HD PTZ (1920 X 1080P), formato panorámico (16:9).
 - ✓ Sensor de 1/1.9" CMOS Progresivo.
 - ✓ Tasa de imágenes: Hasta 30 cuadros por segundo en 1080p.
 - ✓ Rotación continua de 360°.
 - ✓ Función día/noche con filtro IR.
 - ✓ Debe contener infrarrojos adaptativos como mínimo 200 metros.
 - ✓ Iluminación mínima (noche): 0,0005 Lux (30 IRE).
 - ✓ Zoom óptico de 30x y digital 15x como mínimo.
 - ✓ WDR (wide Dynamic Range): 110dB.
 - ✓ Obturador de 1 a 1/30,000s.
 - ✓ Entradas Binarias: Debe tener mínimo 6 entradas binarias.
 - ✓ Inteligencia analítica: Detección de movimiento, Líneas de activación, Detección de intrusión.
 - ✓ Detección de objetos abandonados o desaparecidos, cambio en la escena.
 - ✓ Detección facial, alteración de video.
 - ✓ Múltiples transmisiones: Multicast ilimitados, mínimo cuatro conexiones Unicast disponible de 8Mbps.
 - ✓ Puerto de Red: 10BASE-T Ethernet/100BASE-T
 - ✓ Housing con protección al tiempo mínimo IP67, IK10
 - ✓ Soporte adecuado para montaje en poste.
 - ✓ Capacidad de conexiones en distintos protocolos, TCP, UDP, ICMP, IGMP,SNMP, HTTP, RTP, SSH, PPoE Y DHCP.
 - ✓ Velocidades de bits de video variable, seleccionable por el usuario desde 500Kps a 8 Mbps como mínimo.
 - ✓ Hora: Reloj en tiempo real incorporado, cliente NTP
 - ✓ Temperatura de funcionamiento entre -30°C y 65°C.
 - ✓ Posiciones predefinidas: 290.
 - ✓ Giros predeterminados: Mínimo 6.
 - ✓ Giros establecidos/mímicos: Mínimo 4.
 - ✓ Zonas de privacidad: Mínimo 20.
 - ✓ Rango de inclinación: mínimo 100°
 - ✓ Velocidad de función panorámica: Velocidad de giro: 0.1-240°/s
 - ✓ Velocidad de función inclinación: Velocidad de inclinación: 0.1-120°/s
 - ✓ Compatibilidad con sistemas de audio G.711
 - ✓ Debe ser compatible con estándar ONVIF Perfil S.
 - ✓ Deberá tener las siguientes certificaciones: FCC Part 15 Subpart B Class A, EN61000-4.
- El postor deberá adjuntar la ficha técnica de la cámara propuesta cumpliendo con las especificaciones técnicas mínimas indicadas.
- El área usuaria requerirá la presentación de la carta de garantía emitida por el fabricante, brindando por al menos 2 años de garantía del modelo propuesto de cámara a instalar.
- El postor deberá presentar una carta y/o constancia emitida por el fabricante de la solución de video vigilancia; acreditándolo como proveedor autorizado en la distribución de la cámara propuesta.
- La cámara de vigilancia deberá ser integrada a la Central de Cámaras de Video

Vigilancia del Estadio Nacional, la cual deberá ser compatible y contar con el software (licencias) respectivas para su operación.

- Para la instalación de la cámara el proveedor proporcionará el soporte para la misma, el cual deberá ser de acero galvanizado, y deberá tener como mínimo, 1.5 metros de longitud.

7. SERVICIO DE RESPALDO EN LA NUBE

El contratista deberá incluir un servicio de copia de seguridad en nube con una capacidad mínima de 500Mbps hasta para 3 dispositivos (servidor o laptop o desktop). El servicio brindado deberá tener las siguientes características:

- a) Deberá permitir copia de seguridad desde servidores basados en sistema operativos Windows o Linux.
- b) Deberá garantizar la seguridad del respaldo de los datos frente a malware.
- c) Deberá brindar una protección antiransomware con certificación mediante blockchain.
- d) Deberá permitir copia de seguridad de archivos y de imagen de disco.
- e) Deberá proporcionar almacenamiento altamente disponible, seguro, duradero, escalable y redundante
- f) Deben cifrar los datos en tránsito y en reposo
- g) Deberá permitir copia de seguridad desde sistemas VMware y desde máquinas virtuales.
- h) Deberá ser miembro del Cloud Security Alliance (CSA), miembro de la Antimalware Testing Standard Organization, miembro del APWG (Anti-Phishing Working Group) y miembro de la Biblioteca Criptográfica certificada por FIPS 140-2.
- i) Debe tener la herramienta de gestión de Backup para hacer la programación de Backup, encriptación de datos, compresión de datos, programa de retención de datos, almacenamiento seguro en línea, control de versiones de datos, copia de seguridad diferencial, capacidad de restaurar en una fecha en particular, la verificación de copia de seguridad y recursos compartidos de red de copia de seguridad, entre otros.
- j) Deberá permitir ingresos incrementales rápidamente ya sea en entornos físicos o virtuales, insitu o en la nube.
- k) Deberá brindar el análisis de malware integrado permitiendo una copia de seguridad limpia sin malware durante la restauración.
- l) Deberá almacenar los datos en un formato de copia de seguridad unificado que permita recuperar en cualquier plataforma, independientemente del sistema de origen.
- m) Deberá permitir restaurar los sistemas Windows o Linux en hardware diferente, incluidos equipos físicos sin sistema operativo, y entornos virtuales o en la nube.
- n) Deberá poder restaurar hacia VMWare.
- o) Restauración a nivel de archivo desde un Backup basado en una imagen.
- p) Deberá permitir la captura exclusiva de los bloques que contienen datos que han cambiado desde la copia de seguridad anterior.
- q) Debe incluir la restauración de la capacidad total del respaldo en nube por lo menos en 4 oportunidades como mínimo durante el período del contrato sin incurrir en costo adicional
- r) Debe incluir una herramienta para estadísticas de uso del servicio, reportes e indicadores
- s) Soporte presencial, vía teléfono, correo electrónico, Teams o cualquier otra herramienta de soporte remoto, en modalidad 24x7
- t) El tiempo de respuesta para la atención de averías debe ser como máximo de dos (02) horas, luego de registrada la avería.
- u) El tiempo de resolución de averías debe ser como máximo de doce (12) horas, luego

de registrada la avería. Para los casos especiales en los que el tiempo de resolución se estime mayor a 12 horas, sea o no responsabilidad del proveedor; la institución establecerá también un procedimiento especial para atender estos casos.

8. SERVICIO DE AV+EDR PARA DISPOSITIVOS FINALES Y SERVIDORES

- El postor debe proveer licencias para de antivirus para 850 PCs y laptops, y 50 licencias para 50 servidores con las siguientes características:
- Antivirus+EDR
 - ✓ Cortafuegos que prevea contra amenazas entrantes de manera bidireccional
 - ✓ Control de aplicaciones
 - ✓ Informes sobre el estado de todo el parque de dispositivos a través de una consulta de administrador
 - ✓ Gestor de informes esto para permitir crear informes personalizados sobre las estadísticas y eventos detectados
 - ✓ El servicio de EDR debe de proporcionar a través de IA análisis estático y basado de los patrones de amenazas emergentes

9. GARANTIA DE LOS EQUIPOS

El contratista deberá asegurar a la entidad (Instituto Peruano del Deporte) que si alguno de los equipos alquilados fallara y se requiera su cambio, este deberá ser realizado en un plazo máximo de 24 horas. Se aclara que estos días no incluye sábados y domingos.

El contratista para los cambios en el caso que los equipos de comunicación que instale e implemente presenten fallas de operatividad y funcionamiento, serán reemplazados en el tiempo de respuesta no mayor de cuatro (04) horas para los equipos que se instalen en el Estadio Nacional y para los complejos deportivos el plazo será no mayor de ocho (08) horas desde que se reporta el caso.

10. SOPORTE TÉCNICO

- a. El contratista debe contar con un Centro de Operaciones (SOC - NOC) propio para el servicio de monitoreo y soporte Técnico 24x7x365 con línea telefónica y correo electrónico para la atención de todas las solicitudes de soporte respecto al servicio solicitado a nivel nacional y los cambios de configuraciones de políticas en los dispositivos de seguridad perimetral.
- b. El contratista deberá escalar y abrir casos directamente con el fabricante, de requerirlo, por lo que EL contratista deberá brindarle los accesos correspondientes.
- c. El servicio de soporte técnico comprenderá la solución de cualquier tipo de evento (incidente y/o problema) que cause una interrupción parcial o total del servicio a nivel nacional solicitado por la entidad, así como a la pérdida de la calidad o degradación del mismo. A todo ello se le denominará "falla".
- d. El servicio de soporte técnico comprenderá consultas, solicitudes de reportes, y solicitudes de análisis de auditoría. A todo ello se le denominará "requerimiento".
- e. El contratista deberá brindar el soporte técnico in situ en caso se presenten fallas que no puedan ser solucionados de manera remota.
- f. El servicio de soporte técnico se efectuará a través de línea telefónica y correo electrónico. Una vez recibida tal notificación, El contratista, registrará el requerimiento y/o falla del servicio y proporcionará a la entidad un número de seguimiento al pedido.
- g. Se consideran los siguientes tiempos de respuesta:

Tiempo de resolución defalla o avería	No mayor de dos (02) horas
Tiempo de mantenimiento correctivo local	No mayor de seis (06) horas

h. Mantenimiento preventivo

Como parte del servicio, se realizara un mantenimiento preventivo a los seis (06) meses de iniciada las operaciones, el proveedor del servicio a fin de garantizar la óptima calidad de sus comunicaciones para el acceso a internet y los enlaces LAN to LAN entre las sedes; realizará un diagnóstico de la calidad de sus servicios de comunicación; y verificará si la calidad y rendimiento de la fibra óptica tiene los mismos valores a cuando se iniciaron las operaciones del servicio y de ser necesario realizará las acciones preventivas y correctivas necesarias para mejorar la calidad de las comunicaciones.

11. OBLIGACIONES DEL CONTRATISTA

El postor cumplirá con las siguientes obligaciones:

- Una vez que el contratista finalice con el despliegue de la fibra óptica en cada complejo debe presentar reportes de los enlaces implementados donde se pueda observar que los tiempos de respuestas desde las sedes a la sede principal son óptimos; estos reportes deben ser a nivel de pruebas con equipos de calibración de fibra óptica y de router a router; esto con la finalidad que se garantice una óptima y eficiente comunicación.
- El contratista debe entregar equipos nuevos y de primer uso para todo el proyecto a implementarse en el IPD.
- La garantía del servicio será durante todo el periodo contratado del servicio de Internet, conexión LAN to LAN y equipos de seguridad perimetral. El servicio será a todo costo y será empleado para el uso en la transmisión datos, voz y video.
- El postor debe contar con un centro de operaciones (SOC - NOC); que brinde las atenciones durante 24x7x365 del año ante cualquier solicitud de atención, eventualidad, y/o consulta del personal de la UI. Para la firma del contrato el postor debe indicar el o los números de atención telefónica (call center) y correo electrónico de contacto.
- El proveedor debe ofrecer flexibilidad y escalabilidad en su servicio; y estar en la capacidad de permitir a solicitud del IPD incrementar el ancho de banda contratado según necesidades de la institución, por periodos temporales o permanentes. La solicitud de crecimiento de ancho de banda podrá ser hasta de un 20% y se avisará con una anticipación de 15 días calendarios.
- El proveedor debe asegurar el monitoreo permanente del servicio de acceso a Internet y de los aspectos de la seguridad de los datos que circulan por él; para ello el proveedor debe contar con su centro de operación de red (NOC) propio y centro de operación de seguridad (SOC) propio que realice la gestión de los enlaces (principal y contingencia) del servicio de Internet y enlaces LAN to LAN y equipos de seguridad perimetral.
- La propuesta de la implementación de todo el servicio por parte del proveedor será a todo a todo costo.
- El proveedor "en el caso que los equipos de comunicación que instale e implemente presenten fallas de operatividad y funcionamiento, serán reemplazados en el tiempo de respuesta no mayor de cuatro (04) horas para los equipos que se instalen en el Estadio Nacional y para los complejos deportivos el plazo será no mayor de (08) ocho horas desde que se reporta el caso".
- El proveedor debe asegurar un tiempo de respuesta de hasta a los treinta (30) minutos como máximo para informar o dar solución a las consultas y/o solicitudes de apoyo, problemas originados por fallas de comunicación y/o enlaces. Las averías de mayor gravedad motivadas por problemas originados por fallas en planta externa y/o en la sede de la institución, serán atendidas y/o solucionadas de acuerdo a la gravedad de la

ocurrencia en el menor plazo; el proveedor emitirá un informe a la institución detallando las causas del incidente y las medidas correctivas realizadas para solucionarlo. El tiempo de atención de cualquier tipo de avería será computado a partir de la generación de un ticket de atención, luego de producido el incidente.

- j. El proveedor del servicio informará a la UI mediante carta enviada a la jefatura o al correo electrónico amosquera@ipd.gob.pe acerca de cualquier mantenimiento físico o lógico que afecte el desempeño del servicio que brinda.
- k. Las coordinaciones de las visitas a las sedes deben ser coordinadas y solicitadas mediante carta dirigida a la UI o mediante correo electrónico amosquera@ipd.gob.pe.
- l. Asimismo, se precisa que, para los trabajos de instalación que requieran hacerse de forma presencial, el contratista deberá aplicar el Protocolo Sanitarios Sectorial para la Prevención del COVID19 para los servicios de telecomunicaciones, aprobado por Resolución Ministerial N° 0258-2020-MTC/01, de acuerdo a las normativas recientemente dispuestas.

12. CAPACITACIÓN Y/O ENTRENAMIENTO

- a. La capacitación se brindará a un mínimo de tres (03) participantes de la Unidad de Informática (UI) dentro del plazo de sesenta (60) días calendario, luego de suscrita el acta de inicio del servicio; cabe señalar que las fechas y horarios tentativos de la capacitación serán coordinados previamente con la Unidad de Informática.
- b. La capacitación tendrá un mínimo de veinticuatro (24) horas, comprendidas en la aplicación del servicio implementado y la administración del equipo de seguridad perimetral:
 - Publicación de IP y/o nombres de dominio.
 - Políticas de bloqueo.
 - Políticas de DMZ.
 - Y otras políticas aplicables en materia de seguridad informática.
 - Generación de reportes de seguimiento del servicio.
- c. Al finalizar la capacitación, el postor deberá proporcionar el certificado de capacitación correspondiente a los participantes.
- d. Las capacitaciones podrán ser de manera virtual empleando herramientas colaborativas disponibles en el mercado y que el postor proponga y brinde el acceso correspondiente sin incurrir en gastos adicionales.

13. ENTREGABLES

i. Al inicio del Servicio

El proveedor deberá entregar los siguientes documentos por única vez, en un plazo máximo de diez (10) días calendario contabilizado, a partir del día siguiente de suscrita el acta de inicio del servicio:

El **informe de implementación del servicio** debe contener la información como mínimo:

- Detalle del servicio implementado.
- Diagrama de red (equipos, enlaces de datos, direccionamiento IP, Lan to Lan, gateways y la salida internacional)
- Listado completo de todos los equipos alquilados proporcionados por el proveedor, indicando su descripción, marca, modelo y número de serie, entre otros datos informativos. Asimismo, las guías de remisión de los citados equipos.
- Cuadro de escalamiento para el reporte de incidencias y/o solicitudes de atención.
- Resumen de la configuración y topología de los equipos empleados en el servicio.

ii. Durante el Servicio

El proveedor durante todo el servicio y de forma mensual dentro de los siete (7) días posteriores a la finalización de la prestación mensual del servicio, presentará para su conformidad, los siguientes documentos:

- a) Reporte detallado mensual del uso del servicio de internet y disponibilidad del servicio de interconexión Lan to Lan.
- b) Reporte detallado mensual de la información relacionada con los intentos de acceso no autorizados, ataque DDoS (Denegación de servicio Distribuido), entre los más importantes; que se den al enrutador de entrada de internet.
- c) Reporte detallado mensual de análisis del equipo de seguridad perimetral.

14. PLAZO DE PARA LA IMPLEMENTACIÓN DEL SERVICIO Y ACTA DE INICIO DEL SERVICIO

El proveedor dentro de los cinco (05) días calendario siguientes de la firma del Contrato, deberá presentar su plan de implementación del servicio, donde se proporcione información con respecto a la tecnología que va utilizar, los equipos y accesorios que va a instalar y del diagrama de red propuesto, con lo que va garantizar el correcto funcionamiento del servicio que propone.

El plan de implementación del servicio será revisado y aprobado por la Unidad de Informática (UI) en el plazo máximo de dos (02) días calendario de recibido el plan y de encontrarse algún tipo de observación, el proveedor debe subsanar las observaciones en el plazo máximo de hasta dos (02) días calendario.

Una vez aprobado el plan de implementación del servicio, se suscribirá el **acta de aprobación del plan de implementación del servicio**; el proveedor coordinará con el personal de la UI, a fin de empezar con la ejecución de las actividades de implementación del servicio.

El proveedor tendrá un plazo máximo de hasta cuarenta y cinco (45) días calendarios para realizar la implementación del servicio, contabilizado a partir del día siguiente de suscrito el **acta de aprobación del plan de implementación del servicio**.

Una vez culminada la implementación del servicio se suscribirá el **acta de inicio del servicio** entre la Unidad de Informática y el proveedor, previa verificación del cumplimiento de las condiciones establecidas.

Finalmente, **una vez suscrito el acta de inicio del servicio, al día siguiente se dará oficialmente el inicio de operaciones del servicio adjudicado al proveedor.**

15. PLAZO DE EJECUCIÓN DEL SERVICIO

El plazo de ejecución será de 24 meses, contabilizados a partir del día siguiente de suscrito el acta de inicio del servicio.

16. LUGAR DE LA PRESTACIÓN DEL SERVICIO

El lugar del servicio se realizará en el Centro de Datos del Instituto Peruano del Deporte, primer piso de la tribuna de oriente del Estadio Nacional. El acceso al recinto es en Calle Madre de Dios N° 463, Cercado de Lima. (Tribuna Sur, frente al Parque de las Aguas).

17. CONFORMIDAD DEL SERVICIO

La conformidad será otorgada por la Unidad Funcional de Administración de Recintos Deportivos de Lima Metropolitana (UFARDELM) previo informe de la Unidad de Informática.

18. FORMA DE PAGO

La forma de pago del servicio será en moneda nacional, de acuerdo a cada uno de los comprobantes de pago presentados por el contratista de forma mensual, previa conformidad, debiendo el contratista presentar mensualmente los documentos señalados en el ítem ii. de la sección 13. ENTREGABLES.

Dicha documentación se debe presentar en mesa de partes del IPD de la Ventanilla de Trámite Documentario, en sito en calle Madre de Dios N°463-Tribuna Sur del Estadio Nacional, Cercado de Lima-Lima, en el horario de 08:00 a 16:30 horas, o a través de la mesa de partes virtual del IPD, a través del siguiente enlace: <https://www.gob.pe/ipd>.

19. CONFIDENCIALIDAD

El proveedor del servicio se compromete a mantener en reserva y a no revelar a terceros, sin previa autorización escrita por el IPD, toda la información que le sea suministrada y/o sea obtenida en el ejercicio de las actividades a desarrollarse o conozca directa o indirectamente durante el proceso de selección o para la realización de sus tareas, excepto en cuanto resultare estrictamente necesario para el cumplimiento del contrato.

El proveedor del servicio deberá mantener a perpetuidad la confidencialidad y reserva absoluta en el manejo de cualquier información y documentación a la que se tenga acceso a consecuencia del procedimiento de selección y la ejecución del contrato, quedando prohibida de revelarlo a terceros. Dicha obligación comprende que la información que sea entregada, como también la que se genere durante las realizaciones de actividades previas a la ejecución del contrato, durante su ejecución y la producida una vez que haya concluido el contrato.

Asimismo, aun cuando sea índole pública, la información vinculada al procedimiento de contratación, incluyendo su ejecución y conclusión, no podrá ser utilizada por el contratista para fines publicitarios o de difusión por cualquier medio sin obtener la autorización correspondiente del IPD.

La obligación de confidencialidad no resulta aplicable en los siguientes supuestos:

1. Resulte accesible al público por causa distinta del incumplimiento de la obligación de confidencialidad por la parte receptora.
2. Haya sido publicada con anterioridad a la fecha de la firma de contrato.
3. Se encuentre en poder de la Parte receptora y no esté sujeta a cualquier otro impedimento o restricción puesto de manifiesto a la otra Parte en el momento de la revelación o luego de ella.
4. Sea recibida a través de terceros sin restricciones y sin que implique incumplimiento del Contrato.
5. Sea independientemente desarrollada por la Parte receptora, siempre que no se hubiese utilizado para ello la información confidencial proporcionada por la otra Parte.
6. Deba ser revelada para dar cumplimiento de una orden de naturaleza judicial o administrativa, en cuyo caso la Parte receptora deberá informar a la otra Parte en forma inmediata a la sola recepción de la citada orden.

20. RESPONSABILIDAD DEL CONTRATISTA

El Contratista es responsable por la calidad ofrecida y por los vicios ocultos de los servicios

ofertados por el plazo máximo de responsabilidad del contratista es de dos (02) años contados a partir de la conformidad del inicio del servicio otorgada por la entidad.

21. PENALIDADES APLICABLES

En caso de retraso en la ejecución de las contraprestaciones ejecutadas por el contratista, se aplicará una penalidad al contratista por cada día de retraso hasta por el monto máximo del 10% del monto según lo dispuesto en los artículos 162 y 163 del Reglamento de la Ley de Contrataciones del Estado vigente.

22. OTRAS PENALIDADES

De conformidad con el Artículo N° 163 Otras penalidades, del Reglamento de la Ley de Contrataciones del Estado:

ITEM	Supuestos de Aplicación de Penalidad	Forma de Calculo	Procedimiento
1	Por retraso en el dictado de la capacitación	1% del pago mensual / Por día	Según Informe de Encargado de UI
2	Incumplimiento de disponibilidad mínima requerida	5% del pago mensual/ cada vez que se presente	Según Informe de Encargado de UI
3	Por retraso en la generación de un ticket de atención, por un tiempo mayor de 30 minutos	2% de 31 minutos Hasta 45 Minutos	Según Informe de Encargado de UI
		3% de 46 minutos Hasta 60 Minutos	
		5% más de 60 minutos.	
4	Por la solución del contratista después de emitido el ticket, por un tiempo mayor a 2 horas	2% más de 2 Hasta 4 Horas	Según Informe de Encargado de UI
		3% más de 4 Hasta 6 Horas	
		5% más de 6 Horas	

PROCEDIMIENTO PARA APLICACIÓN DE LAS “OTRAS PENALIDADES”

- El Encargado de la Unidad de Informática al detectar la penalidad señalada en la Tabla de “Otras Penalidades”, remite el informe al área técnica del contratista, otorgándole un plazo máximo de 1 día hábil para que presente sus descargos.
- El Contratista dentro del plazo máximo de 1 día hábil, deberá de demostrar fehacientemente la improcedencia de la penalidad notificada, de no hacerlo o la subsanación resulte infundada, se procederá a imponer la penalidad incurrida y calcular el monto resultante; la sanción se descontará preferentemente del pago mensual más próximo.
- En caso que la penalidad sea reincidente, el encargado de la Unidad de Informática al detectar los supuestos de penalidad señalada en la Tabla de “Otras Penalidades”, deberá de comunicar el monto de la penalidad incurrida, la misma que será deducida preferentemente de la valorización más próxima.
- En los casos que el monto acumulado de las penalidades haya alcanzado el máximo

admisible del monto del contrato vigente conforme a lo establecido en la LCE y su Reglamento, Según Informe de Encargado de UI remitirán un informe a la Entidad recomendando las acciones que según su evaluación del estado situacional del servicio corresponda.

Las penalidades enumeradas se calcularán aplicando los indicadores señalados, las mismas que serán deducidas de los pagos mensuales, del pago final, o si fuese necesario se cobrará del monto resultante de la ejecución de la garantía de fiel cumplimiento.

23. FUNCIONES Y/O ACTIVIDADES DEL PERSONAL CLAVE

- **Gestor de Servicio de Telecomunicaciones**

- Realizar la verificación y control de indicadores del servicio.
- Proponer mejoras o valores agregados del servicio al área usuaria de la entidad.
- Transmitir los lineamientos del servicio al especialista para la implementación de la solución.
- Difundir al personal clave los alcances del servicio.

- **Especialista en Dirección de Proyectos de Telecomunicaciones**

- Elaborar la solución integral del servicio.
- Revisar de los alcances contractuales del servicio
- Realizar el diseño de topología de red para el servicio a implementar.
- Implementar los indicadores de gestión para el proyecto.

- **Jefe de Servicio**

- Dirigir los recursos necesarios para implementación del servicio.
- Elaborar la hoja de ruta para implementación de redes de fibra óptica, de acuerdo a la topología planteada para el servicio.
- Participar en reuniones con el cliente para revisión o consultas con respecto al desarrollo del servicio
- Elaborar informes y/o entregables del servicio brindado.

- **Coordinador de Soporte de servicio**

- Brindar soporte a nivel técnico, del servicio con la entidad.
- Realizar la programación de mantenimiento preventivo o correctivo.
- Realizar las coordinaciones con el personal técnico para el servicio de atención de averías.
- Realizar la logística de equipamiento y accesorios para reposiciones u averías durante el servicio.

24. REQUISITOS DE CALIFICACIÓN

A	CAPACIDAD LEGAL
	HABILITACIÓN
	<p><u>Requisitos:</u></p> <ul style="list-style-type: none"> El postor deberá contar con registro para brindar servicio de valor añadido, para la prestación del servicio de conmutación de datos por paquete, emitido por el Ministerio de Transportes y Comunicaciones con cobertura a nivel nacional. El postor deberá contar con concesión para brindar servicios de telecomunicaciones a nivel nacional, emitido por el Ministerio de Transportes y Comunicaciones. <div> <p>Importante</p> <p><i>De conformidad con la Opinión N° 186-2016/DTN, la habilitación de un postor, está relacionada con cierta atribución con la cual debe contar el proveedor para poder llevar a cabo la actividad materia de contratación, este es el caso de las actividades reguladas por normas en las cuales se establecen determinados requisitos que las empresas deben cumplir a efectos de estar habilitadas para la ejecución de determinado servicio o estar autorizadas para la comercialización de ciertos bienes en el mercado.</i></p> </div> <p><u>Acreditación:</u></p> <ul style="list-style-type: none"> Copia del certificado de registro para el servicio de valor añadido emitido por el Ministerio de Transportes y Comunicaciones. Copia simple de Resolución Ministerial otorgando Concesión para brindar servicios públicos de telecomunicaciones a nivel nacional, emitido por el Ministerio de Transportes y Comunicaciones con cobertura nacional. <div> <p>Importante</p> <p><i>En el caso de consorcios, cada integrante del consorcio que se hubiera comprometido a ejecutar las obligaciones vinculadas directamente al objeto de la convocatoria debe acreditar este requisito.</i></p> </div>
B	CAPACIDAD TÉCNICA Y PROFESIONAL
B.3	CALIFICACIONES DEL PERSONAL CLAVE
B.3.1	FORMACIÓN ACADÉMICA
	<p><u>Requisitos:</u></p> <p>(01) Gestor de Servicio de Telecomunicaciones: Título profesional en Ingeniería de Informática y/o Telecomunicaciones y/o Sistemas.</p> <p>(01) Especialista de Dirección de Proyectos de Telecomunicaciones: Título profesional en Ingeniería Electrónica y/o Telecomunicaciones. Maestría Universitaria y/o Master en Dirección de Empresas</p> <p>(01) Jefe de Servicio: Título profesional en Ingeniería Electrónica y/o Telecomunicaciones y/o Informática y/o Sistemas</p> <p>(01) Coordinador de Soporte de Servicio: Bachiller en Ingeniería Electrónica y/o Sistemas e Informática y/o Telecomunicaciones</p>

	<p><u>Acreditación:</u></p> <p>El grado o título profesional será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: https://titulosinstitutos.minedu.gob.pe/, según corresponda.</p> <p>En caso el grado o título profesional no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p>
B.1.2	CAPACITACIÓN
	<p><u>Requisitos:</u></p> <p>(01) Gestor de Servicio de Telecomunicaciones: Diplomado y/o Diploma en Gestión Estratégica de la Información, de mínimo de 34 horas. Curso PMP (Project Management Professional) o Profesional en Gestión de Proyectos o Gestión de Proyectos para Profesionales, de mínimo 34 horas.</p> <p>(01) Especialista de Dirección de Proyectos de Telecomunicaciones: Curso PMP (Project Management Professional) o Profesional en Gestión de Proyectos o Gestión de Proyectos para Profesionales, de mínimo 34 horas.</p> <p>(01) Jefe de Servicio: Curso PMP (Project Management Professional) o Profesional en Gestión de Proyectos o Gestión de Proyectos para Profesionales, de mínimo 34 horas. Certificación de capacitación de Cámaras IP Tipo PTZ y entre otros temas relacionados, emitido por fabricante de la solución propuesta, como mínimo 40 horas</p> <p>(01) Coordinador de Soporte de Servicio: Certificación de operación y mantenimiento de equipo de medición de fibra óptica, emitido por proveedor autorizado de equipamiento de medición, como mínimo de 20 horas. Certificación de capacitación de Cámaras IP Tipo PTZ y entre otros temas relacionados, emitido por fabricante de la solución propuesta, como mínimo 40 horas.</p> <p><u>Acreditación:</u></p> <p>Se acreditará con copia simple de constancias, certificados, u otros documentos.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Importante</p> <p><i>Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.</i></p> </div>
B.2	EXPERIENCIA DEL PERSONAL CLAVE
	<p><u>Requisitos:</u></p> <p>(01) Gestor de Servicio de Telecomunicaciones: Cuatro (04) años de experiencia mínima en gestión de servicios y/o producto de telecomunicaciones.</p> <p>(01) Especialista de Dirección de Proyectos de Telecomunicaciones: Dos (02) años de experiencia mínima en dirección y/o gestión de proyectos de telecomunicaciones.</p> <p>(01) Jefe de Servicio: Ocho (08) años de experiencia mínima en implementación y/o supervisión de servicios de internet y/o</p>

<p>seguridad perimetral por redes de fibra óptica.</p> <p>(01) Coordinador de Soporte de Servicio: Tres (03) años de experiencia mínima en soporte y/o mantenimiento de servicios de internet dedicado y seguridad de redes.</p> <p><u>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</u></p> <p><u>Acreditación:</u></p> <p>La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p> <div style="border: 1px solid black; padding: 5px;"> <p>Importante</p> <ul style="list-style-type: none"> • <i>Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.</i> • <i>En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.</i> • <i>Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.</i> <p><i>Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.</i></p> </div>
--

C	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 800,000.00 (Ochocientos mil con 00/100 soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>Se consideran servicios similares a los siguientes: servicio de acceso a internet y/o servicio de internet dedicado y/o internet dedicado y transmisión de datos y/o transporte de datos de enlace de fibra óptica y/o internet e interconexión de datos para entidades del estado.</p> <p><u>Acreditación:</u></p> <p>La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago¹, correspondientes a un máximo de</p>

¹ Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado:**

“... el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello

veinte (20) contrataciones.

En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo N° 8** referido a la Experiencia del Postor en la Especialidad.

En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.

En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.

Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva “Participación de Proveedores en Consorcio en las Contrataciones del Estado”, debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9**.

Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo N° 8** referido a la Experiencia del Postor en la Especialidad.

Importante

- *Al calificar la experiencia del postor, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del objeto contractual no coincida literalmente con el previsto en las bases, se deberá validar la experiencia si las actividades que ejecutó el postor corresponden a la experiencia requerida.*
- *En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva “Participación de Proveedores en Consorcio en las Contrataciones del Estado”.*

equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado”

(...)

“Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término “cancelado” o “pagado”] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia”.



PERÚ

Ministerio
de Educación

Instituto Peruano
del Deporte

"Decenio de la igualdad de oportunidades para mujeres y hombres"
"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la
conmemoración de las heroicas batallas de Junín y Ayacucho"

Importante

- *Si como resultado de una consulta u observación corresponde precisarse o ajustarse el requerimiento, se solicita la autorización del área usuaria y se pone de conocimiento de tal hecho a la dependencia que aprobó el expediente de contratación, de conformidad con el numeral 72.3 del artículo 72 del Reglamento.*
- *El cumplimiento de los Términos de Referencia se realiza mediante la presentación de una declaración jurada. De ser el caso, adicionalmente la Entidad puede solicitar documentación que acredite el cumplimiento del algún componente de estos. Para dicho efecto, consignará de manera detallada los documentos que deben presentar los postores en el literal e) del numeral 2.2.1.1 de esta sección de las bases.*
- *Los requisitos de calificación determinan si los postores cuentan con las capacidades necesarias para ejecutar el contrato, lo que debe ser acreditado documentalmente, y no mediante declaración jurada.*