ESPECIFICACIONES TÉCNICAS MÍNIMAS REQUERIDAS
LICITACIÓN PÚBLICA LP-CC-005-2026
"CONTRATACIÓN DE SERVICIO DE TELECOMUNICACIONES Y TELEFONÍA IP EN LA NUBE"

Información mínima indispensable para el llenado de los anexos *Anexo 1 Propuesta Técnica* y *Anexo 5 Propuesta Económica* e integración de proposición.

Todas las especificaciones señaladas en este anexo son mínimas, por lo tanto, el licitante podrá ofertar especificaciones superiores, si así lo considera conveniente.

I. Requerimiento:

Partida 1: Servicio de conectividad: Internet dedicado con UTM [1] y Seguridad Administrada por 36 meses contados a partir del 01 de abril de 2026 y hasta el 31 de marzo de 2029.

Servicio telefónico: Telefonía IP y Comunicaciónes Unificadas basado en la nube, por 36 meses contados a partir del 01 de abril de 2026 y hasta el 31 de marzo de 2029.

Partida 2: Contratación de un segundo enlace de Internet por 36 meses, contados a partir del 01 de abril de 2026 y hasta el 31 de marzo de 2029.

Las partidas serán adjudicadas a licitantes diferentes.

II. Especificaciones técnicas mínimas requeridas:

1. Partida 1. Servicio De Conectividad y Telefonía IP Basada En La Nube:

Ancho de banda:	300 Mbps.
Servicios:	Internet Dedicado con Seguridad Administrada y Telefonía IP basada en la Nube.
Medio de Entrega:	Fibra Óptica.
Troncales:	30 troncales SIP con portabilidad.
IP´s Públicas:	5.

[1] Unidad de Gestión Unificada (UTM) por sus siglas en inglés, se refiere a un dispositivo de seguridad que combina múltiples funciones las cuales se enlistan de manera enunciativa mas no limitativa, como cortafuegos, antivirus, detección de intrusos, filtrado de contenido, etc.

Equipo Cortafuegos de Últitma Generación (NGFW):	Marca Fortinet o equivalente para 300 Mbps.

1.1 Especificaciones del servicio de Internet dedicado con UTM y Seguridad Administrada:

a) El servicio de Internet debe garantizar un retraso o latencia no mayor 50 mseg. por servicio tanto para la trasmisión como para la recepción y deben ser cubiertos desde la central del licitante hacia el CPE[2] instalado por el proveedor en el sitio de la convocante.

b) El servicio de Internet debe tener una pérdida de paquetes ≤1%.

c) El servicio de Internet debe ser suministrado en su última milla por medio de fibra óptica exclusiva (conexión directa y privada) para el proyecto de Auditoría Superior del Estado de Jalisco.

d) La fibra óptica con la que serán entregados los servicios debe ser propiedad del licitante, por ningún motivo podrá ser rentada o provista por un tercero.

e) Una vez terminado el plazo del servicio, si es decisición de la convocante, ser reásponsabilidad del licitante retirarla de las instalaciones para reutilizarla según le convenga.

f) El licitante debe tener un monitoreo constante de la red de fibra óptica provista para el servicio de internet.

g) El licitante debe tener cuadrillas las 24 horas, de manera que cualquier falla reportada por parte de la convocante sea reparada en un máximo de 6 horas.

h) La red de Internet del participante debe tener un backbone dedicado exclusivamente a transporte IP (*Internet Protocol*), el cual cuente con al menos 3 nodos *CORE*, para tener un esquema de alta redundancia.

i) La ruta del anillo de fibra óptica que sea provista por ningún motivo debe tener puntos de acceso de multiplexación o demultiplexación de servicios residenciales o algún otro tipo de servicios.

j) El servicio de internet, a través de su ruta desde la central del proveedor hasta el punto de demarcación, no debe contener ningún punto de sobresuscripción en el medio de acceso ni en la red dorsal del licitante.

k) El *backbone* debe contar al menos con 4 salidas de interconexión directa al backbone de Internet, de las cuales al menos 1 de ellas deben tener la capacidad de cruzar tráfico IPv6 hacia diferentes *carriers* de Tier 1 en los Estados Unidos cada una con capacidad de 30 Gbps, hacía al menos 3 ciudades en EUA. Esto para ofrecer redundancia geográfica con conexiones

[2] Equipo en las instalaciones del cliente (CPE) por sus siglas en inglés.

próximas a sus nodos en México, debe incluir en su propuesta técnica un documento que demuestre esquemáticamente a manera general las pruebas de

l) *traceroute*, topología de trayectorias y rutas, especificando la velocidad mínima y máxima en cada interconexión, asimismo debe de contar con tres salidas al TIER 1.

m) Debe demostrar mediante un diagrama los 3 nodos *CORE*, así como las 5 salidas de interconexión al *backbone* de internet mencionadas en los puntos anteriores.

n) El tráfico nacional debe estar optimizado con acuerdos de *peering* con al menos 3 diferentes proveedores, los cuales deben de estar conectados por lo menos a 2 nodos *CORE* del participante, mismos que deben de encontrarse en diferentes zonas geográficas, las capacidades de las conexiones de *peering* deben ser de al menos 1 Gbps con cada uno de ellos, con el fin de que el tráfico nacional no tenga que ser intercambiado en EUA.

o) El participante debe tener una cobertura a nivel nacional y conexión de manera local en las principales ciudades del país.

p) El servicio de internet se debe entregar en una interfaz RJ45 GigaEthernet.

q) El equipamiento a través del cual el servicio de internet será provisto, debe contar con certificación MEF (Metro Ethernet Forum).

r) Para comprobar el cumplimiento de la certificación MEF, el licitante deberá presentar documento que avale dicha información de los equipos a instalar.

s) De igual manera el *CORE* del licitante por donde se entregan los servicios a nivel local deberá ser cursando a través de equipos que cuenten con certificación MEF con la finalidad de garantizar la entrega de servicios en el formato Ethernet solicitado y con la calidad que se establecer en la normatividad emitida por la MEF, lo cual se verificará entregando los certificados de cumplimiento indicando un diagrama y equipos instalados en el *CORE*.

t) El diseño de la red del licitante debe estar basado en una serie de “mejores prácticas” orientadas a mejorar la seguridad de los servicios para enfrentar tanto ataques cibernéticos como contingencias físicas o tecnológicas.

u) Todas las plataformas utilizadas por el licitante deben ser redundantes, desde la red de anillos de transmisión a cada uno de los equipos CPE de cada sitio.

v) Durante el proceso de instalación y para su gestión es necesario contar y coordinar las actividades con un Ingeniero certificado por el Project Management Institute (PMI) por lo que debe integrar el comprobante en copia simple en su oferta técnica que compruebe la certificación.

w) Al momento de la entrega del enlace se debe entregar un reporte técnico que incluya pruebas de desempeño del mismo, las cuales deben ser realizadas por al menos 24 horas consecutivas. Entre los parámetros a medir están:

i. Ancho de banda.
ii. Delay.
iii. RFC 2544

1.1.1 Especificaciones mínimas del equipo NGFW (Firewall de proxima generaciòn):

a) Rendimiento de FW (64 bytes) [Gbps]: 70
b) Sesiones Concurrentes (TCP): 7.8 Millones
c) Nuevas Sesiones/Secundo (TCP): 500 000
d) Rendimiento de VPN IPsec (512 bytes) [Gbps]: 55
e) Túneles VPN IPsec de Puerta a Puerta: 2000
f) Túneles VPN IPsec de Cliente a Puerta: 50,000
g) Rendimiento de SSL-VPN [Gbps]: 3.6
h) Usuarios Concurrentes de SSL-VPN: 5000
i) Rendimiento de IPS (Mezcla Empresarial) [Gbps]: 12
j) Rendimiento de Inspección SSL (IPS, promedio HTTPS) [Gbps]: 8
k) Rendimiento de Control de Aplicaciones (HTTP 64K) [Gbps]: 28
l) Rendimiento de NGFW [Gbps]: 10
m) Rendimiento de Protección contra Amenazas [Gbps]: 9
n) Dominios Virtuales (Por Defecto): 10
o) Dominios Virtuales (Máximo): 10
p) Interfaces GE: 26
q) Interfaces 10GE: 8

1.1.2 Características principales del equipo NGFW:

a) El equipo debe crear una solución que debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de NGFW, así como consola de gestión y monitoreo;

b) Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;

c) Las funcionalidades de protección de red que conforman la plataforma de seguridad, puede ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;

d) La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;

e) Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si es necesario) y los cables de alimentación;

f) La gestión del equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;

g) Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;

h) Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;

i) Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;

j) Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);

k) Los dispositivos de protección de red deben soportar DHCP Relay;

l) Los dispositivos de protección de red deben soportar DHCP Server;

m) Los dispositivos de protección de red deben soportar sFlow;

n) Los dispositivos de protección de red deben soportar Jumbo Frames;

o) Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;

p) Debe ser compatible con NAT dinámica (varios-a-1);

q) Debe ser compatible con NAT dinámica (muchos-a-muchos);

r) Debe soportar NAT estática (1-a-1);

s) Debe admitir NAT estática (muchos-a-muchos);

t) Debe ser compatible con NAT estático bidireccional 1-a-1;

u) Debe ser compatible con la traducción de puertos (PAT);

v) Debe ser compatible con NAT Origen;

w) Debe ser compatible con NAT de destino;

x) Debe soportar NAT de origen y NAT de destino de forma simultánea;

y) Debe soportar NAT de origen y NAT de destino en la misma política;

z) Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;

aa) Debe ser compatible con NAT64 y NAT46;

bb) Debe implementar el protocolo ECMP;

cc) Debe soportar SD-WAN de forma nativa;

dd) Debe soportar el balanceo de enlace hash por IP de origen;

ee) Debe soportar el balanceo de enlace por hash de IP de origen y destino;

ff) 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.

gg) Debe ser compatible con el balanceo en al menos tres enlaces;

hh) Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;

ii) 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;

jj) Enviar logs a sistemas de gestión externos simultáneamente;

kk) Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;

ll) Debe soporta protección contra la suplantación de identidad (anti-spoofing);

mm) Implementar la optimización del tráfico entre dos dispositivos;

nn) Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);

oo) Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);

pp) Soportar OSPF graceful restart;

qq) Debe ser compatible con el modo *Sniffer* para la inspección a través del puerto espejo del tráfico de datos de la red;

rr) Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;

ss) Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;

tt) Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;

uu) Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;

vv) Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;

ww) Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;

xx) La configuración de alta disponibilidad debe sincronizar: Sesiones;

yy) La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;

zz) La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;

aaa) La configuración de alta disponibilidad debe sincronizar: Tablas FIB;

bbb) En modo HA (Alta Disponibilidad) debe permitir la supervisión de fallos de enlace;

ccc) Debe soportar la creación de sistemas virtuales en el mismo equipo;

ddd) Para una HA, 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;

eee) Debe permitir la creación de administradores independientes para cada uno de lo sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales;

fff) 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;

ggg) 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, es decir, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos);

hhh) Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;

iii) 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;

jjj) 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;

kkk) La consola de administración debe soportar como mínimo, inglés y español;

lll) La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad;

mmm) La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.

1.1.3 Gestión y Administración del Dispositivo UTM requerida:

a) Gestión y administración del servicio 24x7x365 días, instalación, configuración y puesta en operación con dirección IP fija;

b) Seguridad informática: control y políticas de acceso, firewall, sistema de prevención de intrusos (IPS), seguridad multifunción, seguridad de la red, administración de seguridad, clientes de seguridad de terminales y redes VPN, seguridad en la Web, detección de vulnerabilidades, detección de actividades sospechosas y anomalías en la red, así como el análisis de vulnerabilidades y políticas;

c) Monitoreo en tiempo real: Herramienta de análisis de seguridad a través de un NOC-SOC propio del licitante, construido con perspectiva de operaciones, con vistas orientadas a la acción y profundas capacidades de análisis. Deberá no solo brindar visión crítica de las amenazas, sino también abordar con precisión los riesgos en la superficie del ataque, señalando dónde se necesita una respuesta. Anexar evidencia fotográfica;

d) Administración centralizada: el proveedor deberá contar con herramienta de operaciones NOC- SOC propio construido con perspectiva de seguridad, para administrar los dispositivos de red y seguridad. Los equipos incluidos en la solución deberán proporcionar mejoras significativas en el desempeño. Con las versiones de consola central y el tablero de analíticos, se deberán realizar eficientes análisis de seguridad por evento.

1.1.4 Características del servicio de Seguridad Administrada provista por el Proveedor:

El proveedor deberá considerar un servicio continuo en el que se incluya tiempo, recursos y las mejores herramientas de revisión constante de redes al integrar altas, bajas y cambios, para

lograr que el sistema siempre opere al nivel óptimo, debiendo considerar que el servicio cuente con las siguientes características:

a) Firewall. Dispositivo de seguridad de la red que monitorea el tráfico de red - entrante y saliente- y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad;

b) VPN Red Privada Virtual;

c) Control de Aplicaciones. Que pueda crear rápidamente políticas para permitir, denegar o restringir el acceso a aplicaciones o categorías completas de aplicaciones;

d) IPS. Sistema de prevención de intrusos;

e) Web Filtering. Filtro de contenido, controla que contenido se permite mostrar, especialmente para restringir el acceso a ciertos materiales de la Web;

f) Anti-malware. Un tipo de programa diseñado para prevenir, detectar y remediar software malicioso en los dispositivos informáticos individuales y sistemas TI;

g) WAN Acceleration. Mecanismo que optimiza el ancho de banda para mejorar la experiencia del usuario final en una red de área amplia (WAN);

h) Advanced Threat Protection. Protección avanzada contra amenazas. Detección integrada de amenazas avanzadas para una respuesta y mitigación automatizadas.

1.1.5 Para garantizar la correcta gestión y administración del dispositivo UTM el proveedor debe considerar lo siguiente:

a) Instalación física de equipo de seguridad (NGFW) en las instalaciones de la Convocante.

b) Conexión de cables de red y energía.

c) Configuración modo bridge en caso de requerirse.

d) Actualización a la última versión soportada por el fabricante.

e) Configuración de NAT.

f) Configuración de rutas requeridas.

g) Configuración de puerta de enlace.

h) Revisión de políticas de red.

i) Configuración de políticas de seguridad necesarias.

j) Configuración de perfiles de seguridad de aplicaciones y de filtrado Web.

k) Configuración de VPNs necesarias en Interfaces.

l) Puesta en operación.

m) Documentación y reportes.

El proveedor adjudicado deberá entregar este servicio funcionando y operando correctamente dentro de las siguientes 4 semanas posterior al fallo.

1.1.6 Operación del servicio:

a) El licitante debe entregar el servicio operando en la capa 2 del modelo OSI.

b) El servicio entregado por el licitante deberá tener la capacidad de agregar más servicios sin que esto represente la necesidad de agregar otro equipamiento o actualizar el entregado inicialmente.

c) El licitante debe de incluir para la operación del servicio un equipo terminal con capacidad suficiente para el enlace y funcionalidades requeridas, el cual será responsabilidad del licitante la operación como en el mantenimiento.

1.1.7 Nivel de servicio:

a) El servicio de enlace a internet debe contar con un tiempo promedio de solución de fallas (MTTR) menor o igual a seis horas, contados a partir del reporte de falla.

b) El licitante debe mantener un nivel de disponibilidad de 99.8% en el *backbone* y 99.2% al incluir la última milla de acuerdo a la siguiente formula.

Donde: $$Disponibilidad\ (Mensual) = \frac{Ttotal - Tnodisp}{Ttotal} * 100(\%)$$

Ttotal = 43,200 minutos (30 días de mes base).
Tnodisp = Tiempo en el que no se entregó el servicio en minutos.

1.1.8 Consideraciones generales:

El licitante debe considerar todo el equipo activo necesario para la prestación del servicio enlace de internet dedicado con UTM y seguridad administrada.

1.2 Especificaciones del Servicio de Telefonía:

El Licitante deberá considerar ofrecer una solución habilitada 100% en la nube, donde se alojan los aplicativos y se integren las herramientas de comunicación y colaboración requeridas para servir a las distintas áreas de la Convocante, bajo un equema de alta disponibilidad, calidad y seguridad.

Deberá permitir la implementación de multiples escenarios de movilidad utilizando solamente una conexión de internet, de manera adicional, deberá soportar la habilitación de accesos a diferentes servicios de colaboración y telefonía desde varios dispositivos, como pueden ser *Softphones* instalados en equipos de cómputo Portatiles/Escritorio con sistemas operativos (MacOS, Windows11), teléfonos móviles (IoS, Android) y *Hardphone* (tecnología SIP). Deberá ser compatible para integrarse con aplicaciones de terceros (Office 365, Outlook add-in, Outlook Directory Integration, Google Drive, Skype for Business y Microsoft Teams como add on).

1.2.1 Tabla de Licencias:

La solución deberá incluir para cada extensión, una la licencia de integración al equipo PBX IP, conforme a la tabla anexa:

Características	Licenciamiento	Cantidad
Aplicación que integre funciones de comunicaciones Unificadas (video, mensajería, colaboración, integración con otras apps, llamadas VoIP)	**Básica**	**180**
Movilidad		
Historial de Llamadas		
Registros de Llamadas con Marcado Rápido		
Notificación de Llamadas		
Directorio Telefónico Empresarial		
Apariencia de Múltiples Líneas		
Directorio Telefónico Personal		
Llamadas con múltiples participantes (N-way)		
Buzón de Voz		
Recogida de Llamadas		
Llamada Tripartita		
Monitoreo de Lámpara Ocupado	**Profesional, Estandar y Workspace**	**40**
Desvío de Llamadas Siempre		
Desvío de Llamadas por Ocupado		
Desvío de Llamadas por No Contestar		
Espera de Llamadas y Reanudación		
Remarcado (Repetir Llamada)		
Transferencia de Llamadas (Asistida y Ciega)		
ID de Llamador Entrante (Nombre)		
ID de Llamador Entrante (Nombre y Número)		

El proveedor deberá considerar los modelos de teléfonos con los que cuenta actualmente la ASEJ para integrarse de forma transparente a la solucion de ToIP en la nube, el listado de los equipos y modelos se presenta a continuación, los números de serie e información extra requerida será proporcionada únicamente al proveedor adjudicado.

Modelo	Cantidad
CP-7821	41
CP-7841	100
CP-8811	42
CP-8841	5
CP-8845	11
CP-8851	3

De manera adicional se deberá considerar el suministro de 10 equipos telefónicos IP tipo sobremesa, de la misma marca que tiene actualmente la Convocante, el costo de la renta de cada equipo se integrará en la renta mensual del servicio y deberán cumplir con las siguientes especificiaciones: diseño ergonómico y características avanzadas de telefonía IP, que ofrezcan audio de banda ancha para garantizar la calidad del sonido, deberá incorporar 2 puertos RJ45 10/100/1000 Base-T y teclas BLF(lámpara ocupada) y de función fijas brindando un acceso a las funciones de servicio: mensajería, directorio, transferencia, etc.

El teléfono deberá contar con las siguientes características mínimas:

1. *Firmware* MPP, soporta 2 registros SIP.
2. Retroiluminación blanca, escala de grises, 2,5 pulg. (6.4 cm) Pantalla de 240 X 120 píxeles.
3. Soporte IEEE 802.3af PoE (Clase 2), el consumo de energía no supera los 6,49 W.
4. Full duplex.
5. G.711a, G.722, G.729a, ILBC.
6. 2 puertos RJ45 10/100/1000Base-T.

El proveedor adjudicado deberá aprovisionar la solución ofertada dentro de la organización para este mismo propósito, la cual ya se encuentra funcionando y operando. El proveedor adjudicado deberá entregar la solución en un periodo no mayor a 4 semanas posterior al fallo.

1.2.2 Servicio, gestión, reportes y atención de fallas:

El proveedor proporcionará una herramienta Web en la cual permita el monitoreo 24x7 (veinticuatro por siete) del ancho de banda utilizado. El usuario y contraseña serán entregados al personal asignado por la Convocante.

a) El proveedor proporcionará acceso a la herramienta de gestión de telefonía en la nube para que la convocante pueda realizar ajustes básicos como altas, bajas y cambios;

b) El proveedor se compromete a que la utilización de los elementos de red requeridos para la entrega de los enlaces solicitados, serán monitoreados y actualizados continuamente. Esto con el fin de asegurar que en ningún momento se alcance el máximo permitido de utilización, para este caso se considerará el 99.98% (noventa y nueve puntos noventa y ocho por ciento). Anexar carta bajo protesta de decir verdad;

c) El proveedor, proporcionará un portal donde sea posible dar de alta, así como dar seguimiento a los reportes levantados en el sistema;

d) El proveedor proporcionará un número telefónico único para levantar reportes de fallas en un esquema 24x7x365 (veinticuatro por siete por trescientos sesenta y cinco);

e) El proveedor deberá proporcionar el procedimiento de escalación de fallas, sin exceder de 4 (cuatro) niveles. El primer nivel de escalación no debe exceder de 30 (treinta) minutos, esto se refiere a la atención para el levantamiento del reporte de la falla;

f) El proveedor deberá contar con un centro de monitoreo que opere de manera continua las 24 (veinticuatro) horas del día los 365 (trescientos sesenta y cinco) días del año;

g) El proveedor deberá incluir como parte de esta propuesta un escrito bajo protesta de decir verdad, que cuenta con un centro de monitoreo conocido como NOC (por sus siglas en ingles “network operation center”), que es propio y no depende de un tercero (outsourcing);

h) El NOC del proveedor podrá ser visitado en diferentes ocasiones durante la vigencia del contrato, para verificar la capacidad de administración y monitoreo;

i) En las visitas el proveedor mostrará las herramientas de hardware/software con que cuenta el NOC para el monitoreo de la infraestructura;

j) El personal del proveedor deberá contar con certificación Scrum Máster para poder iniciar, planear y ejecutar cualquier proyecto. Anexar mínimo 3 certificados;

k) El personal del NOC del proveedor deberá contr con procesos eficientes basados en las mejores prácticas del mercado a través de ITIL v3.0 o superior para la atención de incidentes, deberá incluir como parte de su propuesta las constancias de al menos dos ingenieros certificados en ITIL Foundation y al menos uno certidicado como ITIL Expert;

l) Para una adecudada gestión durante el proceso de instalación, el provedor adjudicado deberá contar con un ingeniero certificado por el Project Management Institute (PMI) que se encargará de coordinar las actividades, por lo que deberá integrar el comprobante o certificado en su oferta;

m) Para asegurar la correcta integración de los servicios con la infraestructura, el proveedor deberá contar por lo menos con 2 (dos) ingenieros certificados CCIE en R&S o Enterprise, 2 (dos) CCNP en R&S o Enterprise y 2 (dos)ingenieros certificados en NSE7, por lo que deberá integrar los comprobantes o certificados en su oferta;

n) Para todo el personal certificado requerido, se deberá entregar una carta bajo protesta de decir verdad donde indique que laboran directamente para el proveedor o en el mismo grupo empresarial;

o) El proveedor deberá entregar el proceso para verificar la validez ante la entidad certificadora, de los certificados solicitados en ITIL, PMI, CCIE y CCNP;

p) El proveedor deberá contar con un tiempo promedio de solución de fallas (mttr) de 6 (seis) horas o menor para el servicio de internet simétrico dedicado, contados a partir del reporte de falla.

q) El proveedor mantendrá un nivel de disponibilidad de 99.8% (noventa y nueve punto ocho por ciento) en el *backbone* y 99.20% (noventa y nueve punto veinte por ciento) en la última milla;

r) El proveedor deberá considerar todo el equipo activo necesario para la prestación del servicio;

s) El servicio para entregar por parte del proveedor incluye todos los gastos de instalación y puesta en operación del mismo;

t) Para considerar como entregados los servicios, el proveedor, una vez adjudicado, realizará las pruebas correspondientes para demostrar la calidad en el servicio entregado adjuntando un reporte por escrito;

u) El proveedor entregará por escrito los números de sistema autónomo propios y de sus proveedores de internet (Tier-1), así como de otros 2 (dos) ISP´s con los que está haciendo *peering* nacional, como parte de la presente oferta;

v) Las conexiones *peering* nacional del proveedor con sus ISPs deberá de ser de al menos 10Gbps cada una;

w) El proveedor deberá contar con al menos 5 salidas a Tier1;

x) El proveedor entregará un diagrama de sus conexiones hacia proveedores internacionales (Tier-1) indicando la capacidad de ancho de banda en cada enlace cuya sumatoria deberá superar 1Tbps entre todos;

y) El proveedor deberá avalar con documentación (carta y diagrama) que cuenta con conexiones *peer* dedicado con Akamai, Amazon, Facebook, Google, Microsoft y Twitch donde dichas conexiones deben ser de al menos 100Gbps cada una;

z) Para asegura una correcta gestión de calidad, el proveedor deberá presentar certificado vigente ISO 9001:2015 a su nombre o a nombre de una empresa de su mismo grupo;

aa) Para asegurar una correcta integración de aplicación de procesos el proveedor deberá presentar certificado vigente ISO 20000-1 2018 a su nombre o a nombre de una empresa de su mismo grupo;

bb) Para asegurar la confidencialidad e integridad de los datos e información el proveedor deberá presentar certificado vigente ISO 27001-2013 a su nombre o a nombre de una empresa de su mismo grupo;

cc) Toda la solución deberá contar con una vigencia de 36 meses para servicio, soporte, licencias y todo lo necesario para su correcta operación;

2. Partida 2. Enlace De Internet Secundario

Ancho de banda:	300 Mbps
Servicio:	Internet Dedicado Simetrico
Medio de Entrega:	Fibra Óptica
IP´s Públicas:	5

2.1 Especificaciones del servicio de Internet para el segundo enlace debe ser simétrico y dedicado. El ancho de banda a suministrar para el servicio debe ser de acuerdo a las siguientes especificaciones:

El servicio de internet para el segundo enlace debe ser simétrico y dedicado. El ancho de banda a suministrar para el servicio debe ser de acuerdo a las siguientes especificaciones:

a) El servicio de Internet debe garantizar un retraso o latencia no mayor a 50 ms por servicio tanto para la trasmisión como para la recepción y deben ser cubiertos desde la central del licitante hacia el CPE instalado por el proveedor en el sitio de la convocante;

b) El servicio de Internet debe tener una pérdida de paquetes ≤1%;

c) El servicio de Internet debe ser suministrado en su última milla por medio de fibra óptica exclusiva (conexión directa y privada) para el proyecto de Auditoría Superior del Estado de Jalisco;

d) La fibra óptica con la que serán entregados los servicios debe ser propiedad del licitante, por ningún motivo podrá ser rentada o provista por un tercero;

e) El licitante debera tener la capacidad de instalar, mantener y reparar su red de fibra óptica en caso de ser necesario;

f) Toda la fibra óptica utilizada para el proyecto objeto de esta licitación, será propiedad del licitante, una vez terminado el plazo del servicio, si es decisión de la convocante, será responsabilidad del licitante retirarla o reutilizarla según le convenga;

g) El licitante debe tener un monitoreo constante de la red de fibra óptica provista para el servicio de Internet;

h) El licitante debe tener cuadrillas todo el tiempo, de manera que cualquier falla reportada por parte de la convocante sea reparada en máximo 6 horas;

i) El diseño de la red de fibra óptica del licitante debe contar anillos metropolitanos que aseguren la alta disponibilidad del servicio a contratar;

j) La ruta del anillo de fibra óptica que sea provista por ningún motivo debe tener puntos de acceso de multiplexación o demultiplexación de servicios residenciales o algún otro tipo de servicios;

k) El servicio de internet, a través de su ruta desde la central del proveedor hasta el punto de demarcación, no debe contener ningún punto de sobresuscripción en el medio de acceso en la red del licitante;

l) El servicio de internet se debe entregar en una interfaz RJ45 GigaEthernet;

m) El equipamiento a través del cual el servicio de internet será provisto, debe contar con certificación MEF;

n) Para comprobar el cumplimiento de la certificación MEF, el licitante deberá presentar documento que avale dicha información de los equipos a instalar;

o) De igual manera el *CORE* del licitante por donde se entregan los servicios a nivel local deberá ser cursando a través de equipos que cuenten con certificación MEF con la finalidad de garantizar la entrega de servicios en el formato Ethernet solicitado y con la calidad que se establecer en la normatividad emitida por la MEF, lo cual se verificará entregando los certificados de cumplimiento indicando un diagrama y equipos instalados en el *CORE*;

p) El diseño de la red del licitante debe estar basado en una serie de “mejores prácticas” orientadas a mejorar la seguridad de los servicios para enfrentar tanto ataques cibernéticos como contingencias físicas o tecnológicas;

q) Todas las plataformas utilizadas por el licitante deben ser redundantes, desde la red de anillos de transmisión a cada uno de los equipos CPE de cada sitio;

r) Durante el proceso de instalación y para su gestión es necesario contar y coordinar las actividades con un Ingeniero certificado por el Project Management Institute (PMI) por lo que debe integrar el comprobante en copia simple en su oferta técnica que compruebe la certificación;

s) Al momento de la entrega del enlace se debe entregar un reporte técnico que incluya pruebas de desempeño del mismo, las cuales deben ser realizadas por al menos 24 horas consecutivas. Entre los parámetros a medir están:

   i. Ancho de banda.

ii. Delay.
iii. RFC 2544

2.1.1 Operación de servicio:

a) El licitante debe entregar el servicio operando en la capa 2 del modelo OSI;

b) El servicio entregado por el licitante deberá tener la capacidad de agregar más servicios sin que esto represente la necesidad de agregar otro equipamiento o actualizar el entregado inicialmente;

c) El licitante debe de incluir para la operación del servicio un equipo terminal con capacidad suficiente para el enlace y funcionalidades requeridas, el cual será responsabilidad del licitante la operación como en el mantenimiento.

2.1.2 Nivel de servicio:

a) El servicio de enlace a internet debe contar con un tiempo promedio de solución de fallas (MTTR) menor o igual a seis horas, contados a partir del reporte de falla;

b) El licitante debe mantener un nivel de disponibilidad de 99.8% en el backbone y 99.2% al incluir la última milla de acuerdo a la siguiente formula;

Donde: $$Disponibilidad\ (Mensual) = \frac{Ttotal - Tnodisp}{Ttotal} * 100(\%)$$

Ttotal = 43,200 minutos (30 días de mes base).
Tnodisp = Tiempo en el que no se entregó el servicio en minutos.

2.1.3 Consideraciones generales:

El licitante debe considerar todo el equipo activo necesario para la prestación del servicio enlace de internet.

El tiempo de implementación del servicio deberá ser de 20 días hábiles.

2.1.4 Fase de Instalación

El licitante adjudicado deberá asignar un líder de proyecto para que coordine el proceso de instalación mediante una herramienta electrónica de administración de proyectos en la que deberá realizarse las siguientes acciones:

a) Validar que la información entregada por el personal de ASEJ es correcta a fin de realizar las configuraciones correspondientes;

b) Plan de trabajo realizado de manera conjunta entre el licitante adjudicado y la convocante donde se verán reflejadas las entregas en esta etapa;

c) Todos los entregables y documentación que se requiera deberá de ser desarrollado por el licitante adjudicado, con el personal necesario para entregar en tiempo y forma cada una de las etapas;

d) El licitante adjudicado deberá realizar una coordinación previa a la entrega de los equipos, cambios de configuración y puesta en operación con el personal de ASEJ, a fin de coordinarse con el personal de los diversos inmuebles para la instalación de los servicios, lo anterior previo a la configuración de los equipos, debiéndose coordinar de manera directa con el responsable del sitio, esto vía correo indicando la fecha, hora de implementación, así como la fecha y hora de las pruebas de recepción de los servicios en sitio. Cabe mencionar que los servicios y configuraciones realizadas al equipo deberán estar validadas por el personal que ASEJ designe para este efecto;

e) El licitante adjudicado deberá contar con su propio equipo de cómputo para la implementación del proyecto en cuestión;

f) El licitante adjudicado está sujeto a los reglamentos, esquemas de seguridad y normatividad de Auditoría Superior del Estado de Jalisco, aplicables en la materia;

g) Se deberán entregar las actas de recepción a la Auditoría Superior del Estado de Jalisco, a fin de dar como aceptados los puestos de servicios. La falta de estos documentos, se considerarán como puestos de servicios no entregados.

2.1.5 Entregables

El licitante entregará a la ASEJ la documentación y manuales de uso que permita al usuario final lo siguiente (aplica para todas las partidas):

a) Se deberá entregar el procedimiento de escalación y mesa de ayuda para el soporte del servicio.

b) Se deberá entregar la matriz de escalamiento que indique los responsables, datos del contacto y número telefónico.

c) Una vez adjudicado, el proveedor deberá presentar un listado de personal de atención en sus áreas de ingeniería, reportes y post venta, para conocimiento de la Auditoría Superior del Estado de Jalisco.

d) Plan de trabajo, el cual deberá incluir al menos:

i. Fecha de inicio.

ii. Fechas de instalación.

iii. Fecha de pruebas de los puestos de servicio.

iv. Fecha de liberación y anexar la documentación comprobatoria.

v. Descripcion de tareas-tareas y sub realizadas.

vi. Cuadro de Gantt con detalle de las actividades de implementación, migración, operación y liberación de los puestos de servicios, configuración de equipos, este se deberá presentar de manera impresa y en un USB.

vii. Ruta crítica del proyecto a fin de prever posibles retrasos.

viii. Fecha de término.

ix. Responsables por parte del proveedor adjudicado y de la convocante.

2.1.6 Memoria Técnica dirigida al área administradora del contrato, deberá incluir como mínimo:

a) Portada interior con datos del integrador y generales de proyecto.

b) Portada interior con la información de la empresa.

c) Índice de contenido.

d) Descripción general del proyecto.

e) Diagrama detallado del proyecto.

f) Diagrama de flujo de la atención.

g) Matriz de estalación.

h) Base de los activos administrados.

i) Relación de ubicación física del equipo posterior al Roll In.

j) Tabla de direccionamiento, referencia, número de serie, ubicación, y lo relacionado a la información técnica de cada dispositivo.

k) Directorio para reporte de servicios y plan de escalación.

l) Inventario de hardware.

Se deberá entregar una relación con los contratos o ID de cada servicio habilitados con los datos completos.

Se deberá de entregar el reporte total de servicios contratados, de manera mensual, incluyendo las incidencias solicitadas en la mesa de ayuda y su estado actual.

2.1.7 Gestión, monitoreo del servicio y reportes de atención de fallas para servicios de fibra óptica

La gestión, monitoreo y reporte de fallas deberá de aplicar a los servicios descritos anteriormente, con las siguientes especificaciones:

a) El licitante deberá proporcionar una herramienta en la cual permita el monitoreo 24x7 del ancho de banda utilizado.

b) El licitante deberá comprometerse a que la utilización de todos los elementos de red deberá ser monitoreada y actualizada continuamente.

c) El licitante deberá proporcionar un portal donde sea posible dar seguimiento a los reportes levantados en el sistema.

d) El licitante deberá proporcionar un número local para levantar reportes de fallas en un esquema 24x7x365.

e) El licitante deberá proporcionar procedimiento de escalación de fallas, sin exceder de 4 niveles.

f) El licitante deberá contar con un centro de monitoreo que opere continuamente las 24 horas del día los 365 días del año dentro de la zona metropolitana de Guadalajara, anexando comprobante de domicilio. Esto solo aplica para la Partida 1, correspondiente a un enlace de internet y telefonía y no para el enlace adicional de Internet.

g) El licitante deberá presentar carta o escrito bajo protesta de decir verdad que cuenta con un centro de monitoreo conocido como NOC (por sus siglas en inglés).

h) El NOC deberá ser una infraestructura 100% parte del licitante, es decir; que no podrá ser proporcionada por un tercero (outsourcing).

i) El NOC podrá ser visitado en diferentes ocasiones por personal de la Auditoría Superior del Estado de Jalisco durante la vigencia del contrato, para verificar la capacidad del licitante de administración y monitoreo.

j) En las visitas se deberán mostrar las herramientas de hardware/software con que cuenta el NOC del licitante para el monitoreo de la infraestructura de ASEJ.

Nota: Todos los puntos aplican para la partida 1, y solo los puntos del 1 al 5 aplican para la partida 2.

El licitante deberá de presentar copias de los siguientes documentos:

a) Certificación MEF.

b) Certificación ISO 9001.

c) Certificación ISO 20000.

d) 1 Ingenieros con certificado CCNA o equivalente.

e) 1 Ingenieros con certificado CCNP o equivalente.

f) 1 Ingenieros certificados en ITIL FOUNDATION V4 IT Service Management.

g) 1 Ingenieros certificados en PMI.

h) 1 Ingenieros certificados en la marca del NGFW ofertado.

i) Presentar carta del fabricante del NGFW como distribuidor tipo Carrier.

j) Presentar carta del fabricante de la ToIP como distribuidor Gold

III. Tiempo y lugar de entrega:

1. El servicio deberá iniciar y/o entregarse a más tardar el día 01 de abril de 2026, previa entrega de la orden de compra, en las instalaciones de la Auditoría Superior del Estado de Jalisco, ubicada en la avenida Niños Héroes número 2409, en la colonia Moderna, C. P. 44190, Guadalajara, Jalisco, México, y concluirá el 31 de marzo de 2029.

IV. Garantías:

1. El Licitante debe presentar por escrito en hoja membretada carta bajo protesta de decir verdad, donde manifieste que se cuenta con la capacidad para prestar el servicio de conectividad en la modalidad *dual stack* utilizando direcciones IPv4 e IPv6.

2. Fianza de cumplimiento, según lo establecido en las bases de la convocatoria.

3. Fianza de fidelidad.

Lo anterior se deberá asentar por escrito en el Anexo 14 o en hoja(s) aparte que se deberá(n) incluir en el sobre 1 de la proposición.

V. Normas:

No aplica.

VI. Vigencia de precios:

Según lo establecido en las bases de la convocatoria.

VII. Forma de pago:

El pago del servicio se realizará parcialmente en 36 mensualidades, impactando la partida presupuestal correspondiente. El pago del servicio se realizará dentro de los 05 días hábiles siguientes a la entrega del reporte de asistencia y factura por parte del licitante adjudicado a entera satisfacción de la Auditoría Superior del Estado de Jalisco.

Los pagos que se tengan que erogar con cargo a ejercicios presupuestales futuros, estarán sujetos a la aprobación del presupuesto de egresos correspondiente, ello con fundamento en el artículo 42, numeral 1, fracción X de la Ley, y el artículo 76 y 77 de la Ley del Presupuesto, Contabilidad y Gasto Público del Estado de Jalisco.

VIII. Anticipo:

No aplica.