UNIVERSIDAD AUTÓNOMA DE NAYARIT

ANEXO 1

INVITACIÓN A CUANDO MENOS TRES PERSONAS
IA-77-018-918038999-N-68-2026

	Descripción de la partida, conforme Anexo 01	Cantidad	Unidad de Medida	Vigencia del Servicio.
1.1	CONTRATACIÓN DE UN ENLACE DE 4000 MBPS (4 GBPS) DE SERVICIO DE INTERNET DEDICADO EN FIBRA ÓPTICA SIMÉTRICA CON ENLACE REDUNDANTE DE 1000 MBPS (1GBPS) Y SEGURIDAD APLICADA, PARA LA UNIVERSIDAD AUTÓNOMA DE NAYARIT.	1	Servicio	Del 01 de enero al 31de diciembre del 2027.

DESCRIPCIÓN TÉCNICA PARA LA CONTRATACIÓN DE UN ENLACE DE 4000 MBPS (4 Gbps Full-Dúplex) DE SERVICIO DE INTERNET DEDICADO EN FIBRA ÓPTICA SIMÉTRICA CON ENLACE REDUNDANTE DE 1000 MBPS (1Gbps Full-Dúplex), SEGURIDAD (Anti DDoS/DoS), ADQUISICIÓN DE HARDWARE FORTIGATE 400G Y LICENCIAMIENTO DE UN FIREWALL FORTINET MODELO FORTIGATE 600E PARA LA UNIVERSIDAD AUTÓNOMA DE NAYARIT.

PARTIDA	DESCRIPCION	UNIDAD	CANTIDAD
Única	Enlace de 4000 Mbps (4Gbps) con el servicio de Internet dedicado en fibra óptica con enlace redundante de 1000 Mbps (1Gbps).	Servicio mensual	12
	Servicio de Seguridad Clean Pipes (Anti DDoS/DoS).	Servicio mensual	12
	Licenciamiento de un Firewall Fortinet Modelo Fortigate 600E.	Servicio mensual	12

Vigencia: El periodo de Contratación de los servicios será del 01 de enero al 31 de diciembre de 2027 para el Internet y Servicio de Seguridad Clean Pipes, así como la Contratación del Licenciamiento para Firewall Fortinet 600E.

1. Enlace de 4000 Mbps (4 Gbps) con el servicio de Internet dedicado en fibra óptica con enlace redundante de 1000 Mbps (1 Gbps) en modalidad Activo-Pasivo.

2. Alcance: La Universidad Autónoma de Nayarit (UAN) requiere una disponibilidad de ancho de banda dedicado de 4000 Mbps con Internet para atender la operación y funcionamiento de las áreas académicas y administrativas, así como un enlace redundante en caso de caída del enlace principal de 1000Mbps de Internet, cuya finalidad es garantizar fluidez del tráfico y consumo del servicio de Internet durante 24 horas al día, los 365 días del año.

   Es del conocimiento de la Universidad Autónoma de Nayarit (UAN) que, en caso de falla del enlace principal de 4000 Mbps solicitado, en donde entre como activo el enlace redundante de 1000 Mbps, éste último cuente con un ancho de banda menor que el principal, por lo que existirá una sobresuscripción del enlace hasta que se restablezca el enlace principal, y por ende el enlace redundante vuelva a quedar en estado pasivo (standby).

3. Descripción general de los requerimientos: La Universidad Autónoma de Nayarit requiere contar con un enlace al Centro de Datos (SITE) de la Universidad Autónoma de Nayarit ubicado en la planta baja del Edificio COMPLEX (Aula 1.11 BIS), por medio de un enlace dedicado de fibra óptica de 4000 Mbps, de forma tal que deberá cubrir todos los requerimientos establecidos en las bases de la licitación y las especificaciones técnicas descritas.

El Centro de Datos (SITE) de la Universidad Autónoma de Nayarit ya cuenta con acondicionamientos físicos, eléctricos, ambientales y una sola ruta de entrada que será compartida por ambos enlaces, por lo que el dimensionamiento de los circuitos se realizó para que cuente con capacidad suficiente para satisfacer las demandas de los equipos de infraestructura de cómputo para lo existente.

El licitante deberá entregar el medio de comunicación digital dedicado a través de fibra óptica con redundancia de 1000 Mbps en modalidad Activo - Pasivo.

4. Requerimientos Específicos de Telecomunicaciones.

4.1. Requerimientos enlace 4000 Mbps:
El concursante adjudicado, será el encargado de proveer la conectividad hacia Internet a través de un enlace dedicado con un ancho de banda de 4000 Mbps en total, simétrico, con redundancia de 1000 Mbps en modalidad activo – pasivo, el cual deberá de proveerse a La Universidad Autónoma de Nayarit con las siguientes características:

4.1.1 Redundancia en el Backbone del proveedor que garantice el servicio requerido. El nivel de servicio requerido para este servicio deberá ser de 99.80 % (como mínimo). Con una pérdida de paquetes menor o igual al 1% mensual y una latencia máxima de 45 milisegundos al ruteador de frontera.

4.1.2. Soporte de protocolo IPv4 e IPv6.

4.1.3. Soporte de protocolo de enrutamiento BGP o rutas estáticas en los puntos de acceso.

4.1.4. El licitante deberá contar con infraestructura de DNS secundario de apoyo de resolución con el fin de poder ofrecer el servicio de resolución secundaria e inversa de nombres de los dominios propiedad de la Universidad, y de cuando éste último así lo requiera. El servicio de 4000 Mbps (4 Gbps) debe ser escalable, es decir, debe tener la flexibilidad, eficiencia y transparencia suficiente para que en el momento que sea necesario, se puedan ampliar los anchos de banda considerando el costo adicional al ser implementado, previa cotización y aceptación de la Universidad Autónoma de Nayarit, sin afectar la operación de los demás sitios.

4.1.5. La Universidad Autónoma de Nayarit podrá solicitar dentro del periodo de contratación más servicios de tipo dedicado de acuerdo a las necesidades de la institución.

4.1.6. El licitante ganador deberá entregar el medio de comunicación digital dedicado a través de fibra óptica con redundancia.

4.1.7. La interfaz para entrega en el equipo de la Convocante deberá ser óptica con velocidad 10GE del tipo SR.

4.1.8. El licitante ganador deberá proporcionar el servicio de “Clean Pipes” o similar (Internet seguro), para los enlaces de Internet activo y respaldo.

4.1.9. La Universidad Autónoma de Nayarit no aceptará propuestas que involucren la entrega de los servicios por medios aéreos como cobre, Microondas y/o Satelital en ambos enlaces, tanto el primario como el redundante.

4.1.10. El licitante ganador, deberá de proveer de su router para entregar una sola fibra de conexión a la Universidad.

4.2. Es responsabilidad del concursante adjudicado:

a) El concursante adjudicado será el encargado del mantenimiento preventivo y correctivo de sus equipos y partes, cableados y demás dispositivos que se utilicen para brindar el servicio requerido, hasta el punto de demarcación.

b) Proporcionar el servicio DNS secundario de apoyo de resolución en caso de ser requerido por la Universidad Autónoma de Nayarit.

c) Entregar prueba con estándar internacional para verificar la calidad del medio de transmisión entregado

mediante prueba RFC 2544 para el enlace principal activo.

d) Realizar pruebas de estabilidad del enlace una vez instalados cumpliendo con las necesidades del cliente.

4.3. El servicio deberá ser entregado: En las instalaciones del Edificio Complex, Aula 1.11 BIS de la Universidad Autónoma de Nayarit ubicada en Boulevard Tepic- Xalisco, Ciudad de la Cultura S/N C.P. 63000 y el proveedor de servicios deberá contar con lo siguiente:

4.3.1. Cobertura a nivel nacional mediante infraestructura robusta con esquemas de alta disponibilidad y redundancia automática entre sus puntos de presencia.

4.3.2. Contar con acuerdos de intercambio de redes (conocido como peering agreements) con proveedores de servicios de Internet nacionales y/o extranjeros vigentes, la conexión con al menos 12 peerings nacionales y/o de contenido en el territorio nacional, con al menos 1,100 GB de conexión con dichos peerings.

4.3.3. Contar con acceso a la red dorsal (backbone) de Internet por medio de enlaces de alta capacidad con conexión de al menos 9 proveedores diferentes (ISP's) para asegurar redundancia de rutas, el prestador de servicios deberá manifestar que cuenta con al menos cinco enlaces directos al backbone de Internet en los Estados Unidos con ubicación geográfica distinta cada uno y que al menos la suma de ellos tenga una capacidad de 19,000 Gbps de ancho de banda. Esto lo acreditará mediante un diagrama a bloques de las conexiones, en el que se indican las ciudades en donde se realiza la interconexión.

4.3.4. El licitante deberá garantizar la conexión a los servicios TIER-1 teniendo al menos 6 salidas hacia la red Dorsal de Internet en EEUU con un ancho de banda mínimo de 6,480 Gbps, al menos 4 de estas salidas deberán estar en ciudades diferentes con la finalidad de garantizar el servicio en caso de falla en alguno de los nodos de salida.

4.3.5. Conexión dedicada con las redes de Internet más importantes de EE.UU. y lo servidores más consultados, entre ellos: Microsoft con al menos 900 Gbps, Google con al menos 3,500 Gbps, Oracle con al menos 400 Gbps.

4.3.6. El Licitante deberá contar con infraestructura propia de backbone y la conexión al backbone de Internet en Estados Unidos de América, y no deberá depender de la conexión a otros proveedores de acceso a Internet nacionales para ofrecer el servicio de acceso a Internet.

4.3.7. El licitante deberá entregar por escrito los proveedores con los que está haciendo peering como parte de la evaluación técnica, el tráfico nacional deberá estar optimizado con acuerdos de "peering" con al menos 12 diferentes proveedores, los cuales deben de estar conectados por lo menos a 2 nodos "CORE" del carrier, mismos que deben de encontrarse en diferentes zonas geográficas, las capacidades de las conexiones de "peering" deben ser de al menos 1000 Gbps con cada uno de ellos, con el fin de que el tráfico nacional no tenga que ser intercambiado en Estados Unidos de America. Se solicita que se ilustre por medio de un diagrama las interconexiones de "peering" mencionadas.

4.3.8. Deberá contar con la capacidad de poder acceder a los servicios de monitoreo y operación de los servicios electrónicos. Deberá proporcionar un servicio de monitoreo y soporte las 24 horas del día los 365 días del año sobre el acceso a internet contratado. Se deberá proporcionar al menos un acceso a una herramienta de monitoreo vía WEB con la finalidad de que La Universidad Autónoma de Nayarit pueda realizar monitoreos de forma remota y mediante internet.

4.4. Requerimientos del Servicio de Seguridad (Anti DDoS/DoS):

Proporcionar mecanismos de protección a ataques de denegación de servicios, de conformidad con la siguiente: información:

4.4.1. Detectar, gestionar y mitigar ataques de denegación de servicios (DoS) volumétrico y denegación de servicios distribuido (DDoS) en tiempo real.

4.4.2. Administrar la infraestructura relacionada con la solución, permitiendo determinar en forma automática el comportamiento anómalo del servicio. La infraestructura que compone la solución deberá residir en los equipos e instalaciones del proveedor.

4.4.3. Llevar a cabo un análisis de flujo de tráfico buscando patrones anormales que indiquen la presencia de un ataque de dos tipos DoS/DDoS, el cual podría ser generado por medio de los siguientes protocolos o comportamientos:

- Paquetes IP fragmentados.
- Paquetes IP NULL.
- Paquetes con origen de una IP privada.
- TCP flood.
- TCP Null.
- TCP RST.
- ACK Flood.
- SYN Flood.
- ICMP Flood.
- Hogging CPU.
- Charge.
- FIN Flood.
- DNS Malformend.
- DNS Flood.
- HTTP Flood.
- UDP Flood.
- PPS Flood.
- Zombie.
- Land Attack.
- Slowloris Attack.
- Sockstress Attack.
- NTP Reflection Attack.

4.4.4. Integrar una solución de mitigación de ataques DoS/DDoS que realice inspección del tráfico de acceso a Internet, que permita reducir de manera rápida e inteligente las amenazas a la seguridad y contra cualquier situación desconocida que trate de agotar el ancho de banda o los recursos de la red. La solución debe realizar el análisis del flujo de tráfico buscando patrones de tráfico anormales que indiquen la presencia de un ataque tipo DoS/DDoS generando por medio de la actividad de gusano o de atacantes de tipo botnet.

4.4.5. Detectar y gestionar cualquier condición anómala, el tráfico dañino debe ser filtrado y descartado, dejando pasar sólo el tráfico legítimo hacia la red de La Universidad Autónoma de Nayarit para ser entregado a su destino final.

4.4.6. Para la solución de mitigación de ataques DoS/DDoS no se considera equipo colocado en las instalaciones de La Universidad Autónoma de Nayarit, ni a través de infraestructura subcontratada o de un tercero; dicha solución debe estar implementada y operando en el "backbone" del proveedor.

4.4.7. La solución de mitigación de ataques DoS/DDoS debe basarse en "hardware" de propósito específico comercial especializado para la mitigación de Ataques DoS/DDoS. Dicha infraestructura debe contar con sus licencias de operación y soporte durante la vigencia del contrato. No se aceptan soluciones basadas en "open source" o sistemas de código abierto, "freeware", "shareware" o cualquier otra forma de "software" no comercial. De igual manera, no se aceptan soluciones basadas en hardware tipo IPS y/o "Firewall" por no ser hardware especializado en la Mitigación de Ataques DoS/DDoS.

5. Condiciones del servicio de soporte técnico:

5.1 Proporcionar servicio de soporte técnico con personal calificado, por medio de teléfono o en sitio, las 24 horas del día, los 365 días del año.

5.2 El servicio de soporte técnico deberá incluir detección y solución de fallas en el servicio de Internet del presente concurso, incluyendo los circuitos de acceso dedicado hasta los puntos de demarcación definidos, a través del servicio de soporte a clientes. En caso de ser necesario, el licitante deberá de realizar altas, bajas y cambios en el equipo de su propiedad.

5.3 El Proveedor deberá presentar una tabla de escalamiento de problemas, especificando la información del personal responsable para la solución de la falla, con su nombre, puesto, correo electrónico y numero de teléfono.

5.4 Cuando suceda una falla en el servicio, el escalamiento al primer nivel no deberá exceder de 2 horas.

5.5 El proveedor debe de asegurar un monitoreo constante del enlace solicitado para que, en caso de falla, se notifique de inmediato al personal de Telecomunicaciones de la Universidad Autónoma de Nayarit.

5.6 Proporcionar un usuario y una clave de acceso en una página en Internet para que la Universidad Autónoma de Nayarit, pueda ver el desempeño y monitoreo del enlace instalado por el proveedor (utilización de ancho de banda por minutos, hora, día, semana y mes). Las 24 horas del día los 365 días del año.

6 Seguridad del proveedor:

6.1. El Proveedor deberá contar con NOC/SOC para los servicios de Internet y Clean Pipes, el cual debe de incluir las siguientes gestiones:

- Gestión de Incidentes.
- Gestión de Problemas.
- Gestión de Cambios.
- Gestión de Riesgo.
- Gestión de la Capacidad.
- Gestión de la Continuidad y Disponibilidad.

6.2. El licitante deberá tener la capacidad y tecnología para apoyar a la Universidad Autónoma de Nayarit a contener ataques de denegación de servicios que pudieran presentarse y minimizar el daño, asegurando la continuidad de los servicios. Para comprobar su cumplimiento de la capacidad solicitada, el SOC del licitante deberá mostrar en su propuesta que cuenta con un equipo de respuesta a incidentes.

Adicionalmente deberá de demostrar que cuenta con el personal especializado con las competencias y conocimientos necesarios para poder gestionar y afrontar los diversos tipos de ataques que pudieran presentarse, teniendo la capacidad de análisis profundo y contextualizado directamente en las soluciones de seguridad que conforman la Universidad Autónoma de Nayarit, con el objetivo de poder indicar las mejores acciones de contención ante un incidente de seguridad crítico.

A continuación, se describen las características mínimas que deberá cumplir el Centro de Operaciones de Seguridad del proveedor:

- Ubicación física. - El SOC del proveedor deberá estar ubicado y operar al 100% en la República Mexicana.
- Operación de la gestión de la seguridad bajo el esquema 7x24x365 días.
- El servicio proporcionado por el SOC debe estar basado en estándares y mejores prácticas tales como ITIL.
- El Centro de Operación de Seguridad, deberá contar con un Sistema de Service Desk alineado a estándares como ITIL que almacene todos los tickets generados.
- El proveedor deberá contar con al menos 10 años de experiencia en proyectos de administración de seguridad a través de su Centro de Operación de Seguridad (SOC), integrar a su propuesta técnica carta

bajo protesta de decir verdad, firmada por el representante legal donde lo confirme.

- El Centro de Operaciones de Seguridad del proveedor, deberá contar con al menos 5 procesos de operación del SOC certificados en ISO/IEC 27001: 2022 o superior con una maduración (antigüedad) de al menos cinco años, integrando copia de dicho certificado en su propuesta técnica para lo cual deberá presentar con su propuesta, copia simple de dichos certificados o en su caso carta del organismo correspondiente indicando que el certificado está en proceso de emisión.
- El Centro de Operaciones de Seguridad, deberá contar con la certificación ISO 20000-1:2011 para al menos un servicio de seguridad de la información integrando copia de dicho certificado en su propuesta técnica para lo cual deberá presentar con su propuesta, copia simple de dichos certificados o en su caso carta del organismo correspondiente indicando que el certificado está en proceso de emisión.
- El Centro de Operaciones de Seguridad deberá formar parte de FIRST (Forum of Incident Response and Security Teams), Foro Internacional de equipos de seguridad y respuesta a incidentes.
- El Centro de Operaciones de Seguridad deberá contar con acuerdos de colaboración con CTA Cyber Threat Alliance una de las principales instituciones de investigación en el mundo.

7 Firewall Fortinet Modelo Fortigate 600E con interfaz óptica de velocidad 10GE del tipo SR propiedad de la Universidad Autónoma de Nayarit., para conectarse con el CPE del Licitante.

8 REPORTE DE FALLAS

Se requiere que el licitante ofrezca un servicio de soporte 7X24 durante todo el tiempo del contrato, y deberá proporcionar, un día antes de iniciar el servicio, el procedimiento de levantamiento, seguimiento y escalamiento de reportes, anexando un número único y exclusivo para que la Universidad Autónoma de Nayarit pueda reportar los incidentes, así como los celulares, y cuentas de correo electrónico de las personas involucradas, estos procedimientos deben considerar lo solicitado en la presente licitación en cuanto a tiempos de entrega, servicio y penalizaciones. El procedimiento solo será entregado por el proveedor adjudicado.

8.1 En casos de incidentes que sean considerados por la Universidad Autónoma de Nayarit de alto impacto (falla de mas de 2 horas atribuible a la licitante), y a solicitud expresa de la Universidad Autónoma de Nayarit, el proveedor deberá entregar por escrito un informe detallado del incidente donde describan las actividades para el diagnóstico, seguimiento y solución del incidente incluyendo los tiempos y horarios de cada una de esas actividades. Este informe deberá ser dirigido a la Dirección de Infraestructura y Servicios Tecnológicos, con copia para el responsable del Departamento de Telecomunicaciones y Ciberseguridad, deberá de entregarse a más tardar en 3 días hábiles a partir de la solicitud del mismo, a través de correo electrónico y mediante oficio, adicional e independientemente del resumen mensual de los reportes señalados en el punto 8.3 y 8.4 de este apartado.

8.2 En la fecha de inicio del servicio el licitante ganador deberá contar con un sistema de reportes en donde se identifiquen claramente cuando menos los datos abajo listados, así como proporcionar un número de reporte único por incidente reportado:

1. Fecha de reporte.
2. Hora de apertura del reporte.
3. Problema reportado.
4. Hora de inicio del problema.
5. Nombre del cliente.
6. Nombre de la persona que reporta.
7. Teléfono de la persona que reporta.
8. Número del reporte.
9. Persona que recibe el reporte.
10. Personal a quien se le asigna el reporte.
11. Fecha y hora de asignación.
12. Causa y solución del problema.
13. Fecha y hora de solución del problema.

14. Persona que autoriza el cierre por parte del centro de datos de la Universidad Autónoma de Nayarit del reporte al regularizarse el servicio.
15. El sistema de reporte deberá tener la posibilidad de abrir un registro de problema en caso de que el problema persista de acuerdo con las buenas prácticas de ITIL.

El proveedor deberá entregar un ejemplo de estos reportes o tickets, obtenido de su sistema de atención a usuarios o de operación para que la Universidad Autónoma de Nayarit los pueda cotejar con las bases de la presente licitación. Estos reportes pueden ser solicitados por la Universidad Autónoma de Nayarit cuando así se requieran, y deberán ser entregados vía correo electrónico a las direcciones que se le indiquen.

8.3 El proveedor deberá entregar mensualmente, un resumen de los reportes generados indicando la fecha, número de reporte y tiempo de solución. Este documento deberá estar firmado por el representante que designe el proveedor y el responsable del área de Telecomunicaciones y Ciberseguridad de la Universidad Autónoma de Nayarit.

8.4 En caso de que no haya existido incidente alguno en el servicio, el proveedor deberá entregar un reporte en donde especifique que el servicio se ha mantenido en funcionamiento de acuerdo a lo expuesto en las presentes bases. Este documento deberá ser enviado vía correo electrónico a la cuenta por designar.

8.5 La Universidad Autónoma de Nayarit supervisará la operación del servicio y el comportamiento del enlace contratado a través del sistema de monitoreo (propiedad de la Universidad Autónoma de Nayarit), mediante una plataforma basada en WEB con alarmas de SNMP (Simple Network Management Protocol). Con la cual en el momento que requiera la Universidad Autónoma de Nayarit puede cotejar con el sistema que el proveedor debe proporcionar.

8.6 El tiempo de inicio del incidente en el servicio se medirá a partir del momento en que quede registrado en la herramienta de incidentes del proveedor. La penalización por tiempo fuera de servicio será una vez que se determine que la falla es imputable al proveedor y que se incumple con el SLA comprometido.

8.7 En caso de interrupción o incidente en el servicio objeto de esta contratación, mismo que se debe restablecer en un plazo no mayor a 4 horas.

9 PENALIZACIONES

Las penalizaciones serán abonadas a la Universidad Autónoma de Nayarit a través de una nota de crédito a los CFDI mensuales aplicable al mes posterior a excepción del último mes que será abonado al mes en curso.

Para este servicio contratado se aplicarán penas convencionales del 1 % (uno por ciento) por día sobre el monto total del contrato o conforme se especifique en cada inciso:

a) Por retraso en la entrega y puesta en marcha del enlace, por cada día de atraso en la entrega y puesta en marcha del servicio, se aplicará la pena convencional por día de retraso. Por cada día de retraso al entregar parcialmente algún componente o activo del servicio que se solicite en las presentes bases. Para el retraso en la operación del router server, enrutamiento, acceso al software de visualización de utilización de ancho de banda, se aplicará la penalización sobre el 33% del monto total del contrato del servicio. Esta penalización es aplicable incluso por cada día que pase después de los 4 días previos a la entrega del servicio y que opere al 100%.

b) Por día de falla de servicio, se requiere que el licitante ofrezca los servicios con una disponibilidad al menos de 99.80 % mensual, sujeto a penalización convencional por incumplimiento de la misma, con soporte de 24x7x365 días a la vigencia del contrato, es necesario que el licitante proporcione procedimientos para reportes y escalamientos, anexando datos de contacto de soporte de su NOC.

c) Por disponibilidad del servicio, misma que la disponibilidad mensual sea menor del 99.80 %

de acuerdo a lo siguiente:

DISPONIBILIDAD DEL ENLACE MENSUAL EN %		PENALIZACIÓN SOBRE EL MONTO TOTAL DEL CONTRATO DE SERVICIO POR NO CUMPLIR LA DISPONIBILIDAD MENSUAL.
DE	HASTA	PORCENTAJE
0	99.79	1 % por día.
99.80	o más	0 %