UNIVERSIDAD AUTÓNOMA DE NAYARIT.

ANEXO 01.

LICITACIÓN PUBLICA FEDERAL
LA-918038999-E17-2020

	Descripción de la partida, conforme Anexo 01	Cantidad	Unidad de Medida	Vigencia del Servicio.
1.1	Contratación de enlace de 1000 Mbps (1Gbps) con servicio de internet dedicado en fibra óptica con enlace redundante y seguridad aplicada para la Universidad Autónoma de Nayarit	1	Servicio	Del 1 de enero al 31 de diciembre del 2020.

DESCRIPCIÓN TÉCNICA PARA LA CONTRATACIÓN DE UN ENLACE DE 1000 MBPS (1Gbps Full-Dúplex) DE SERVICIO DE INTERNET DEDICADO EN FIBRA ÓPTICA SIMÉTRICA CON ENLACE REDUNDANTE, SEGURIDAD (Anti DDoS/DoS) Y CONTRATACIÓN DE UN FIREWALL PARA LA UNIVERSIDAD AUTÓNOMA DE NAYARIT.

PARTIDA	DESCRIPCION	UNIDAD	CANTIDAD
Única	**-Enlace de 1000 Mbps (1Gbps) con el servicio de Internet dedicado en fibra óptica con enlace redundante.**	**Servicio mensual**	**12**
	- Servicio de Seguridad Clean Pipes (Anti DDoS/DoS)	**Servicio mensual**	**12**
	- Contratación de un Firewall de Nueva Generación	**Servicio mensual**	**12**

Vigencia: El periodo de Contratación de los servicios será del 01 de enero del 2021 al 31 de diciembre del 2021.

1. **Enlace de 1000 Mbps (1 Gbps) con el servicio de Internet dedicado en fibra óptica con enlace redundante.**

2. **Alcance:** La Universidad Autónoma de Nayarit (UAN) requiere una disponibilidad de ancho de banda dedicado de 1000 Mbps con Internet (disponibilidad para full routing) para atender la operación y funcionamiento de las áreas académicas y administrativas, cuya finalidad es garantizar fluidez del tráfico y consumo del servicio de Internet durante 24 horas al día, los 365 días del año.

3. **Descripción general de los requerimientos:** La Universidad Autónoma de Nayarit requiere contar con un enlace al Centro de Datos de la Universidad ubicado en el SITE de la planta baja del Edificio COMPLEX (Aula 1.11 bis), por medio de un enlace dedicado de fibra óptica de 1000 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 y ambientales, 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 en modalidad Activo-Pasivo.

4. **Requerimientos Específicos de Telecomunicaciones.**

4.1. Requerimientos enlace 1000 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 1000 Mbps en total, simétrico, con redundancia en modalidad activo–pasivo y con diversidad de rutas hacia diferentes centrales o puntos de presencia de acceso del proveedor 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 99.50 % (como mínimo). Con una pérdida de paquetes menor 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 conexión directa al CORE de CUDI para Internet.

4.1.5. El licitante deberá contar con infraestructura de DNS redundante 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 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.

4.1.6. La Universidad Autónoma de Nayarit podrá ampliar o disminuir los anchos de banda contratados inicialmente de acuerdo a las necesidades propias de ella.

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

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

4.1.9. La interfaz para entrega en el equipo de la convocante deberá ser óptica para conexión en puerto SFP

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

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

4.2. Es responsabilidad del concursante adjudicado:

- **a)** Proporcionar la interfaz de entrega requerida para recibir el enlace de 1000 Mbps en el Router Brocade MLXE-4 con puerto SFP de fibra óptica propiedad de la Universidad Autónoma de Nayarit.
- **b)** 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.
- **c)** Proporcionar el servicio DNS secundario en caso de ser requerido por la Universidad Autónoma de Nayarit.
- **d)** Entregar prueba con estándar internacional para verificar la calidad del medio de transmisión entregado.
- **e)** Realizar pruebas de estabilidad del enlace una vez instalados cumpliendo con las necesidades del cliente.
- **f)** Realizar lo conducente de acuerdo a los incisos d y e descritos anteriormente para validar el enlace redundante

4.3. El servicio deberá ser entregado: En las instalaciones de la Universidad Autónoma de Nayarit ubicada en Boulevard Tepic-Xalisco, Ciudad de la Cultura "Amado Nervo" 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 10 peerings Nacionales y/o de Contenido en el territorio Nacional con al menos 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 **5 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 1000 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. Deberá contar con la capacidad de poder acceder a los servicios de monitoreo y operación de los servicios electrónicos por personal autorizado de La Universidad Autónoma de Nayarit de forma remota mediante diversos medios seguros, tales como VPN's en Internet o equivalentes (conexiones vía SSH) que presente reportes relacionados con el servicio de Internet en periodos diarios, semanales y mensuales.

Dichos reportes serán presentados en forma gráfica y deberán contener al menos la siguiente información:

4.3.4.1. Los reportes que se muestren de manera diaria (minuto, hora), semanal, mensual e histórico anual, las 24 horas del día durante la vigencia del contrato.
4.3.4.2. Reporte de utilización del puerto de conectividad a Internet.
4.3.4.3. Capacidad del servicio.
4.3.4.4. Latencia.
4.3.4.5. Bits promedio trasmitidos (TX) / recibidos (RX).
4.3.4.6. Porcentaje de utilización transmitidos / recibidos (opcional).
4.3.4.7. Reportes en formato HTML.
4.3.4.8. Reporte de utilización del enlace de Internet dedicado.
4.3.4.9. Estadísticas que incluyen: utilización del medio de transmisión, Bits entrada/salida, pérdida de paquetes, paquetes descartados, *throughput,* utilización del ancho de banda y errores.

****El proveedor deberá entregar la documentación técnica, diagramas descriptivos de su infraestructura y manifiestos bajo protesta de decir verdad en los que señale cumple con las características señaladas en todo el numeral 4.3.**

4.3.5. Reporte de fallos: Ante un fallo deberá entregarse un reporte con un diagnóstico inicial, adicionalmente de uno detallado a más tardar en tres días naturales o el tiempo empleado en la solución del fallo.

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 soporte para problemas básicos de configuración de los equipos del cliente y aislamiento de fallas para identificación y solución de problemas en el servicio incluyendo los circuitos de acceso dedicado hasta los puntos de demarcación definidos, a través del servicio de soporte a clientes.

5.3 El Proveedor deberá presentar un plan de escalamiento de problemas, especificando los niveles que se aplicarán para cada tipo de problema

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, por lo menos). Las 24 horas del día los 365 días del año.

6 Seguridad del proveedor
6.1. El Proveedor deberá contar con NOC/SOC, 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.

7 Datos Técnicos del Router Brocade MLXE-4 propiedad de la Universidad Autónoma de Nayarit

Router Brocade MLXE-4

8 REPORTE DE FALLAS

Se requiere que el licitante ofrezca un servicio de soporte 24X7 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.

1. En casos de incidentes que sean considerados por la Universidad Autónoma de Nayarit de alto impacto, 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 Servicios Universitarios, con copia para el jefe del Departamento de Telecomunicaciones y Redes, 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 4.3.4 de este apartado.

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 re-abrir los tickets en caso de requerirse, esto por si la falla persiste mientras el proveedor da la solución final.

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.

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 Jefe del Departamento de Telecomunicaciones y Redes de la Universidad Autónoma de Nayarit.

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.

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.

6. El tiempo del inicio del incidente en el servicio se medirá a partir del momento que sea detectado por las herramientas de la Universidad Autónoma de Nayarit antes mencionadas y la penalización por tiempo fuera de servicio será de acuerdo a la que establece la normatividad. No aplica contabilizar la falla a partir de que se generó el reporte por parte de la Universidad Autónoma de Nayarit ante el proveedor.

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 P o r 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 99.50 % mensual, sujeto a penalización convencional por incumplimiento de la misma, con soporte de 24x7x365 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
Porque la disponibilidad al día (24 horas) sea menor del 99.90 % 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	99.49	1 % por día.
99.50	o más	0 %

.

d) Por porcentaje de errores.
Si en la interfaz (puerto) del router se exceda en errores más del 1% del tráfico total cursado por día, independientemente de que se afecte el servicio o no, e independientemente también de que se caiga o no la misma interfaz, se penalizará el día completo donde se dé el evento.

e) Por exceder el tiempo de mantenimiento programados. En caso de que al llevarse a cabo el mantenimiento preventivo se sobrepase la ventana de mantenimiento establecida para tal efecto, se penalizará sobre los servicios afectados, de acuerdo a la falta de disponibilidad del 99.50%.

f) Por falla del sistema de Monitoreo o Visualización de Gráficas. Si el Servicio de Monitoreo indicado en el Apartado Técnico, queda inaccesible para la Universidad Autónoma de Nayarit por más de 15 minutos en un día, se penalizará el 1% conforme a normatividad pero tomando de referencia el 33% del costo total del servicio por cada día de falla hasta su solución.

g) Por anuncios de red no propagados. Los anuncios de red que se soliciten por escrito (a través de un correo del centro de datos de la Universidad Autónoma de Nayarit u oficio), ya sea por un protocolo de enrutamiento dinámico (BGP, BGP+) deberán ser propagados a sus TIER-1's a más tardar en 72 hrs.

Después de haberlo solicitado la Universidad Autónoma de Nayarit. Si esto no se lleva a cabo, el servicio se penalizará por día como no entrega del servicio que se está contratando.

h) Protocolos de ruteo ausentes. En caso de que los anuncios de ruteo de entrada se reduzcan un 20% o los anuncios de ruteo de salida del AS28390, no deberán disminuirse en ningún momento o filtrarse de ninguna forma dentro de la red del proveedor y sus proveedores de Internet (TIER1), se penalizará cada día el servicio de Internet afectado hasta que se restablezcan los mismos IPv4 (o IPv6).

i) Por ausencia en la disponibilidad del servicio de seguridad "Clean Pipe" (Internet seguro). Se requiere que el licitante ofrezca el servicio de seguridad en el enlace con una disponibilidad del 99.50 % mensual, sujeto a penalizaciones por incumplimiento de la misma, con soporte de 24X7X365.

Esta se penalizará en caso de que el licitante ganador no detecte en un período de dos minutos a partir de que se presente cualquiera de los ataques, de entrada o de salida del tráfico, definidos en el Apartado Técnico.

Se penalizará en caso de que el licitante ganador no avise por correo electrónico a noc@uan.edu.mx en un período de dos minutos a partir de que se presente cualquiera de los ataques definidos en el Apartado Técnico.

Se penalizará en caso de que el licitante ganador no mitigue cualquiera de los ataques definidos en el Apartado Técnico en un período máximo de cinco minutos, esto a partir de la solicitud que el NOC-UAN haga a través de un correo electrónico a una cuenta de correo que el licitante ganador defina o una llamada a su servicio de atención a usuarios.

Se penalizará en caso de que el licitante ganador no normalice el servicio en un período máximo de 10 minutos, esto a partir de la solicitud que el NOC-UAN haga a través de un correo electrónico a la cuenta de correo que el licitante ganador defina.

Para las fallas generales del servicio, si el proveedor restablece el servicio en menos de 4 horas, no se penalizarán los primeros dos evento de cada mes, pero a partir del tercero se penalizará el servicio a partir de que no se cumpla la disponibilidad diaria, a partir de 48 horas sin restablecer el servicio se penalizará sobre un porcentaje del 33% del costo total del servicio por cada día de falla hasta su solución.

10 Contratación de un Firewall de Nueva Generación

El licitante deberá considerar un sistema de seguridad perimetral, el cual tendrá como su principal función gestionar y filtrar la totalidad del tráfico entrante y saliente de Internet y de la red Interna de la UAN, a través de este componente se configuran las políticas de operación para establecer los servicios permitidos con base en puertos lógicos y aplicaciones, además se realizará la configuración de las áreas denominadas Zonas Desmilitarizadas (DMZ) para la protección de servicios que requieran publicación a internet por parte de la UAN.

La solución de seguridad perimetral que la UAN requiere debe cumplir con las siguientes características y funcionalidades mínimas:

1.1. Características Generales

- Throughput de por lo menos 36 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 e IPv6, independiente del tamaño del paquete.
- Soporte a por lo menos 8 millones conexiones simultáneas
- Soporte a por lo menos 300 000 nuevas conexiones por segundo
- Throughput de al menos 20 Gbps de VPN IPSec
- Capacidad para soportar 2000 túneles de VPN IPSec site-to-site simultáneos
- Capacidad para soportar 50000 túneles de clientes VPN IPSec simultáneos
- Throughput de al menos 5 Gbps de VPN SSL
- Soportar al menos 10000 clientes de VPN SSL simultáneos
- Tener al menos 8 interfaces GE RJ45
- Tener al menos 8 interfaces GE SFP
- Tener al menos 2 interfaces 10 GE SFP+

- Tener la opción para fuente de poder redundante

1.2. Funcionalidades Generales

a. Deberá ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red.
b. Deberá soportar modo capa - 2 (L2).
c. Deberá soportar modo capa - 3 (L3).
d. Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas.
e. Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo.
f. La configuración de alta disponibilidad deberá sincronizar por lo menos lo siguiente:
    - Sesiones
    - Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red.
    - Las asociaciones de seguridad VPN;
    - Tablas FIB
g. En modo HA (Modo de alta disponibilidad) deberá permitir la supervisión de fallos de enlace.
h. Deberá 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 y estadísticas de uso de las interfaces de red
i. Deberá tener capacidad de integración con Microsoft Active Directory, RADIUS o LDAP para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basados en usuarios y grupos de usuarios;

1.3. Funcionalidades de Firewall

a. Deberá soportar NAT de origen y NAT de destino de forma simultánea.
b. Deberá soportar NAT de origen y NAT de destino en la misma política.
c. Deberá soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico.
d. Deberá ser compatible con NAT64 y NAT46.
e. Deberá implementar el protocolo ECMP.
f. Deberá soportar SD-WAN de forma nativa.
g. Deberá soportar el balanceo de enlace hash por IP de origen.
h. Deberá soportar el balanceo de enlace por hash de IP de origen y destino.
i. Deberá 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.
j. Deberá implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales.
k. Deberá soportar protección contra la suplantación de identidad (anti-spoofing) en las interfaces de red.
l. Para IPv4, soportará enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP).
m. Para IPv6, soportará enrutamiento estático y dinámico (OSPFv3).
n. Deberá contar con políticas de control por puerto y protocolo.
o. Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (con base en las características y comportamiento de las aplicaciones) y categorías de aplicaciones.
p. Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad.
q. Deberá soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.
r. Deberá soportar el protocolo estándar de la industria VXLAN.

1.4. Funcionalidades de VPN

a. Soportar VPN de sitio-a-sitio y cliente-a-sitio.
b. Soportar VPN IPSec.
c. Soportar VPN SSL.

d. La VPN IPSec deberá ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512.
e. La VPN IPSec deberá ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14.
f. La VPN IPSec deberá ser compatible con Internet Key Exchange (IKEv1 y v2).
g. La VPN IPSec deberá ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard).
h. Deberá tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Fortinet, Juniper, Palo Alto Networks, Fortinet, SonicWall; entre otros.
i. Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec.
j. Deberá permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, facilitando el proceso troubleshooting.
k. Deberá permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy.
l. Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL.
m. Soportar autenticación vía AD/LDAP, Secure ID, certificado y base de usuarios local;
n. Deberá permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL.
o. Deberá mantener una conexión segura con el portal durante la sesión.
p. El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.

1.5. Funcionalidades de Control de Aplicaciones

a. Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;
b. Detección de miles de aplicaciones en 18 categorías, incluyendo, pero no limitado a:
   - Peer-to-Peer
   - Redes Sociales
   - Acceso Remoto
   - Actualización de Software
   - Protocolos de Red
   - VoIP
   - Audio
   - Vídeo
   - Proxy
   - Mensajería Instantánea
   - Compartición de Archivos
   - Correo Electrónico
c. 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;
d. 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.
e. Para trafico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante.
f. Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas.
g. Actualización de la base de firmas de la aplicación de forma automática.
h. Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos.
i. 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.
j. El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos.

k. Deberá permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;
l. Deberá permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts y Facebook Chat) permitiendo granularidad de control/reglas para el mismo.
m. Deberá permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitir a Hangouts el chat, pero impedir la llamada de video.
n. Deberá permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, entre otras.) permitiendo granularidad de control/reglas para el mismo.
o. Deberá ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based y Network Protocol).
p. Deberá ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación.
q. Deberá ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación.
r. Deberá ser posible configurar Application Override seleccionando las aplicaciones individualmente.

1.6. Funcionalidades de Filtrado URL

a. Deberá permitir especificar la política de filtrado URL por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora).
b. Deberá 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.
c. Deberá soportar la capacidad de crear políticas basadas en control por URL y categoría de URL.
d. Deberá 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.
e. Deberá tener por lo menos 75 categorías de URL.
f. Deberá tener la funcionalidad de exclusión de URLs por categoría.
g. Permitir página de bloqueo personalizada.
h. 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).

2. SERVICIO DE OPERACIÓN DE LA SEGURIDAD (SOC)

El licitante deberá de proveer el servicio de SOC (Security Operation Center); este servicio deberá proporcionar los elementos necesarios para monitorear y administrar la solución de seguridad perimetral propuesta, así como detectar y alertar de eventos de fallas o incidentes que puedan poner en riesgo la operación y continuidad del servicio de seguridad. Entre las actividades que se requieren de parte del SOC están las siguientes:

- Configuración inicial y puesta a punto del equipo de seguridad perimetral
- Monitoreo de disponibilidad
- Atención y soporte técnico remoto
- Administración y Gestión de cambios
- Reportes del Servicio

El servicio del SOC deberá brindarse en un esquema 7x24x365.

El objetivo del SOC será contar con un área encargada de proporcionar un Soporte de Primer Nivel y sea el primer punto de contacto con la UAN. Se encargará también de atender los requerimientos y escalar con Segundo y Tercer Nivel en caso de ser necesario, realizará el análisis, troubleshooting, ejecución de cambios sobre el equipo y seguimiento de tickets relacionados con la infraestructura de seguridad para evitar fallas o afectaciones en la operación.

El servicio debe incluir:

- Monitoreo de disponibilidad

- Atención y Soporte Remoto 24x7
- Gestión de cambios y configuraciones
- Medio de solicitud vía correo electrónico y telefónica
- Aplicación de Actualizaciones y/o cambio de versiones del SO
- Reporte mensual (predefinido del equipo)

Las funciones que deben contemplarse son las siguientes:

- Monitoreo de la disponibilidad y desempeño
    - El objetivo de este servicio es monitorear de forma proactiva el dispositivo de seguridad, de manera que se puedan detectar oportunamente fallas en el equipo, alertamiento de incidentes relacionados a la disponibilidad del servicio.
    - El servicio debe de proporcionarse en un esquema de 7x24x365.
- Detección y administración de incidentes.
    - El licitante ganador deberá de dar seguimiento a los incidentes detectados y/o reportados por el personal designado de la convocante; el tipo de notificaciones estarán relacionados a los eventos cuando ocurra una falla en el sistema o se detecte una degradación en el servicio, de tal manera que el licitante adjudicado pueda tomar acciones correctivas.
    - El licitante adjudicado deberá de realizar el registro de estos incidentes detectados por la herramienta de monitoreo en una herramienta de administración de incidentes o “Trouble Ticket”, propiedad del licitante adjudicado, donde se dará continuidad hasta su solución, indicando fecha y hora de apertura del caso, tiempo de atención y fecha y hora de cierre del caso.
    - El licitante adjudicado deberá de atender las alertas de seguridad que se generan en función de su criticidad y de acuerdo a los protocolos de actuación pre-establecidos. El objetivo debe ser prevenir, detectar y mitigar cualquier incidente de seguridad.
- Solución de Incidentes de Falla

Una vez detectada una situación de falla, se abrirá un caso o ticket en la herramienta de administración de incidentes y se inicia el proceso de solución de la misma, el cual incluye soporte de primer, segundo y tercer nivel, de la siguiente manera:

- Soporte de primer nivel: se proporcionará de forma remota por los ingenieros del SOC del licitante adjudicado en un esquema de 7x24x365.
- Soporte de segundo nivel: cuando la falla de un equipo no pueda ser resuelta por los ingenieros de soporte de 1er. Nivel, este debe de ser escalada hacia los ingenieros de segundo nivel del licitante adjudicado para atender de forma remota dicho incidente.
- Soporte de tercer nivel: de ser necesario para la solución de la falla, el SOC escalará el problema al fabricante del equipo en cuestión y dará seguimiento hasta su solución.

El licitante adjudicado deberá de proveer a la convocante la matriz de escalamiento a seguir, especificando los métodos de contacto con el SOC. Los diferentes eventos de falla deberán ser catalogados de acuerdo a su nivel de criticidad y atendidos de acuerdo a los niveles de servicio acordado considerando lo siguiente:

Criticidad Descripción

Criticidad	Descripción
Mayor	Cuando el servicio no está disponible.
Alta	Cuando el servicio se encuentra muy degradado
Media	Cuando el servicio está disponible y presenta mensajes de error recurrentemente.
Baja	Cuando el servicio está disponible y presenta mensajes de error eventuales.

UNIVERSIDAD AUTÓNOMA DE NAYARIT.

ANEXO 01.

LICITACIÓN PUBLICA FEDERAL
LA-918038999-E17-2020

PERFIL DEL SOC DEL LICITANTE

1) El SOC del licitante deberá contar con las siguientes certificaciones:
    a) ISO/IEC 27001:2013, el cual debe indicar los sistemas de información que soportan los servicios de soluciones de seguridad; el licitante debe comprobar que tiene al menos 15 procesos certificados.
    b) ISO/IEC 20000-1:2018 el cual debe indicar los sistemas de información que soportan a los servicios de la solución de seguridad.
2) Contar con un equipo de respuesta a incidentes de seguridad informática (CSIRT) con la autorización de usar la marca CERT de Carnegie Mellon University, así mismo, deberá estar avalado por el FIRST el cual se comprobará a través de las páginas de los organismos.
3) El Licitante deberá contar con Certificación de ISO 9001:2015
4) El Licitante deberá contar con Certificación de la Ley Federal de Protección de Datos Personales y normativa aplicable en materia de protección de Datos Personales (LFPDPPP)
5) El licitante deberá contar con un equipo de personas que apoyen para la implementación y ejecución del proyecto, el cual deberá estar formado por los siguientes perfiles:

    a) Administrador de Proyecto
        i. Certificado PMP
        ii. Certificado ITIL Foundation en su última versión

    b) Al menos 2 ingenieros certificados como profesionales en la solución de seguridad perimetral con conocimiento para administrar, monitorear y operar la solución propuesta por el licitante.

Las certificaciones (o equivalentes) deberán de estar vigentes al momento de apertura de propuestas, además el Licitante deberá de presentar una carta en formato libre, firmada por el representante legal y en papel membretado, donde se comprometa a mantener dicha certificación vigente durante la prestación del servicio.

Clausulas acerca de los equipos y servicios licitados:

a) Los equipos una vez terminados el periodo de contratación con el ganador de la licitación pasarán a propiedad de la Universidad Autónoma de Nayarit, en donde se entregará la documentación que lo acredite.

b) Los casos no definidos o que puedan prestarse a ambigüedad serán resueltos en la junta de aclaraciones por el comité tecnico en favor de la Universidad Autónoma de Nayarit

c)El o los licenciamietos que el Firewall requiera para su operación, funcionamiento y desarrollo de las funcionalidades antes mencionadas le correspoderán al licitante ganador

d)Las condiciones de entrega del Firewall será entregado e instalado en sitio y operando al 100% en la red local e Internet de la Universidad Autónoma de Nayarit

e)El licitante ganador proveerá capacitación técnica operativa del Firewall para personal (por lo menos 2) de la Universidad Autónoma de Nayarit en terminos de poder acceder al conocimiento para su operatividad y funcionalidades.