



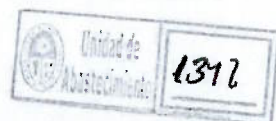
Universidad Nacional de Educación
Enrique Guzmán y Valle
"Alma Máter del Magisterio Nacional"

"Año de la Esperanza y el Fortalecimiento de la Democracia"

OFICINA DE TECNOLOGIAS DE LA INFORMACIÓN
UNIDAD DE SOPORTE TÉCNICO Y REDES



52



1312

FORMATO 02 TÉRMINOS DE REFERENCIA

REQUERIMIENTO DE SERVICIOS PARA PROCEDIMIENTO DE SELECCIÓN

1. DENOMINACIÓN DE LA CONTRATACIÓN

SERVICIO DE INTERNET

2. FINALIDAD PÚBLICA DE LA CONTRATACIÓN

La Universidad Nacional de Educación Enrique Guzmán y Valle requiere contratar un servicio de internet dedicado con seguridad gestionada, con el propósito de garantizar la disponibilidad, estabilidad y seguridad del acceso a internet y de los servicios de red institucional en la sede central y sedes descentralizadas; la implementación de este servicio contribuirá a garantizar la continuidad de las actividades académicas, administrativas, de investigación, innovación y responsabilidad social universitaria, posibilitando el funcionamiento permanente de los sistemas de información, plataformas virtuales de enseñanza, servicios de correo electrónico institucional, aplicaciones en la nube, videoconferencias y demás servicios tecnológicos, así como fortalecer la protección de la infraestructura tecnológica institucional, contribuyendo al cumplimiento de las Condiciones Básicas de Calidad establecidas por la SUNEDU.

3. OBJETIVO DE LA CONTRATACIÓN

Contratar el Servicio de Internet, que comprende la provisión de internet dedicado con seguridad gestionada, para garantizar una conectividad institucional de alta disponibilidad, capacidad, estabilidad, velocidad y seguridad, asegurando la operación continua de la infraestructura tecnológica y la adecuada gestión del tráfico de la red de la Universidad Nacional de Educación Enrique Guzmán y Valle.

El servicio deberá proporcionar enlaces dedicados de alto rendimiento, mecanismos de seguridad perimetral administrada, monitoreo permanente de la conectividad, protección contra amenazas cibernéticas, soporte técnico especializado y atención oportuna de incidencias, garantizando niveles de servicio acordes con las necesidades institucionales.

Asimismo, la contratación tiene como objetivo asegurar el acceso continuo y confiable a los sistemas académicos, administrativos, financieros, de investigación, bibliotecas virtuales, plataformas de educación virtual, servicios en la nube y demás aplicaciones institucionales críticas, fortaleciendo la continuidad operativa, la protección de la información y la calidad de los servicios tecnológicos brindados a la comunidad universitaria.

4. ACTIVIDAD DEL POI

C0136 ATENCIÓN DE USUARIOS

5. CONDICIONES DE CONTRATACIÓN

a. Modalidad de pago

La contratación se rige por la modalidad de **SUMA ALZADA** de conformidad con el artículo 130 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas.



FIRMA
DIGITAL

Firmado digitalmente por:
MORI GARCIA Willy Otmar
FAU 20174950971 hard
Motivo: Soy el autor del
documento
Fecha: 29/09/2026 14:17:11-0500

Av. Enrique Guzmán y Valle 951. La Cantuta - Chosica
Teléfono: 313-3700, anexos 1820
web: www.une.edu.pe Email: sopotecyredes@une.edu.pe



Universidad Nacional de Educación
Enrique Guzmán y Valle
"Alma Máter del Magisterio Nacional"

"Año de la Esperanza y el Fortalecimiento de la Democracia"



51

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
UNIDAD DE SOPORTE TÉCNICO Y REDES

1341
b. Plazo de prestación

Los servicios materia de la presente contratación se prestan en el plazo de 100 días calendarios para la puesta en servicio, contados a partir de la suscripción de contrato para llevar a cabo la implementación del servicio y las gestiones de los servicios municipales.

La prestación del servicio tendrá una duración de treinta y seis (36) meses, contados a partir de la fecha de puesta en operación del servicio, la cual será acreditada mediante la suscripción del Acta de Inicio de Operaciones entre la entidad y el contratista.

El servicio deberá mantenerse disponible y operativo las treinta y seis (36) horas del día, los siete (7) días de la semana, durante todo el periodo de ejecución del contrato, garantizando los niveles de disponibilidad establecidos en el acuerdo de nivel de servicio (SLA).

c. Lugar de la prestación del servicio

El servicio se prestará en las tres (03) sedes de la Universidad Nacional de Educación Enrique Guzmán y Valle (UNE), conforme al siguiente detalle:

- Sede Central: Ubicada en la Av. Enrique Guzmán y Valle N.º 951, La Cantuta, distrito de Lurigancho-Chosica, Lima.
- Sede de la Facultad de Ciencias Empresariales: Ubicada en la Calle Pío Sarobe N.º 200, distrito del Rímac, Lima.
- Sede de la Escuela de Posgrado: Ubicada en la Calle Los Agrícolas N.º 280, urbanización Las Acacias, distrito de La Molina, Lima.

d. Adelantos

No aplica

e. Penalidades

1. Penalidad por mora

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable. La penalidad se aplica automáticamente y se calcula de acuerdo con la siguiente fórmula:

$$\text{Penalidad diaria} = 0.10 \times \text{monto} \\ F \times \text{plazo}$$

Donde F tiene los siguientes valores:

Para bienes y servicios: $F = 0.40$

Para obras:

- a) Para plazos menores o iguales a sesenta días: $F = 0.40$.
- b) Para plazos entre sesenta y uno a ciento veinte días: $F = 0.25$.
- c) Para plazos mayores a ciento veinte días: $F = 0.15$.

Firmado digitalmente por:
MORI GARCIA Willy Othmar
FAU 20174950971 hard
Motivo: Soy el autor del
documento

Fecha: 29/09/2026 14:17:18-0500

Av. Enrique Guzmán y Valle 951, La Cantuta - Chosica
Teléfono: 313-3700, anexos 1820
web: www.une.edu.pe Email: soplectvredes@une.edu.pe





Para consultorías de obras:

- a) Para plazos menores o iguales a sesenta días: $F = 0.40$.
- b) Para plazos mayores a sesenta días: $F = 0.25$.

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobada.

Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando el contratista acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En este último caso, la calificación del retraso como justificado por parte de la entidad contratante no da lugar al pago de gastos generales ni costos directos de ningún tipo.

2. Otras penalidades aplicables

Cuadro N°01: Otras penalidades

Otras penalidades			
N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento
01	Respecto al Soporte: Cuando no se brinde solución a los incidentes o averías en el plazo estipulado.	0.02% de la UIT por cada hora de atraso	Una vez solucionados los incidentes o averías, la Unidad de Soporte Técnico y Redes deberá verificar si fueron atendidos oportunamente. Caso contrario, contabilizará las horas de retraso, notificará al CONTRATISTA y, asimismo, informará a la Unidad de Abastecimiento lo evidenciado para la aplicación de la penalidad, la cual se descontará del pago respectivo y/o se ejecutará la Garantía de Fiel Cumplimiento.
02	Por no cumplir con el plazo de entrega del informe técnico solicitado por la unidad de soporte Técnico y Redes.	0.5% de la UIT por día de incumplimiento de informe solicitado por la unidad de soporte Técnico y Redes.	Cuando el CONTRATISTA no cumpla con la entrega del informe técnico solicitado por la Entidad dentro del plazo máximo de setenta y dos (72) horas, contadas a partir del día siguiente del plazo determinado, la Unidad de Soporte Técnico y Redes contabilizará los días de retraso, notificará al CONTRATISTA y, asimismo, informará a la Unidad de Abastecimiento lo evidenciado para la aplicación de la penalidad correspondiente, la cual se descontará del pago respectivo y/o se ejecutará la Garantía de Fiel Cumplimiento.
03	Por incumplimiento del nivel de disponibilidad del servicio (mínimo 99.5% para la Sede de La Molina y Rímac, pero 98.9% para la sede central), calculado mensualmente	0.02% de UIT por cada hora a partir del incumplimiento del nivel de disponibilidad del servicio.	Para la aplicación de una penalidad, la Unidad de Soporte Técnico y Redes comunicará por escrito al CONTRATISTA, quien tendrá un plazo de dos (2) días calendario para efectuar su descargo. La Unidad de Soporte Técnico y Redes tendrá un plazo de tres (3) días calendario para evaluar dicho descargo. Si el descargo presentado por el CONTRATISTA no es



Universidad Nacional de Educación
Enrique Guzmán y Valle
"Alma Máter del Magisterio Nacional"

"Año de la Esperanza y el Fortalecimiento de la Democracia"



OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
UNIDAD DE SOPORTE TÉCNICO Y REDES

1334

Otras penalidades			
N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento
			aceptado por la Unidad de Soporte Técnico y Redes, se procederá a ejecutar la penalidad correspondiente.

Donde: UIT: Unidad Impositiva Tributaria (UIT).

Nota: Se precisa que, para la aplicación de penalidad, el cálculo se efectuará sobre la base de la UIT vigente a la fecha de haberse producido el incumplimiento.

f. Subcontratación

En base al Artículo 108 (numeral 108.1) del Reglamento de la Ley N° 32069 Ley General de Contrataciones Públicas (D.S. N° 009-2025-EF), indica que se puede subcontratar por un máximo del 40% del monto del contrato vigente de bienes, servicios u obras.

g. Fórmulas de reajustes

No corresponde

h. Garantías

De acuerdo al Artículo 113 Tipos de garantías contractuales, numeral 113.1 (...) El postor ganador entrega a la entidad contratante; como requisito indispensable para perfeccionar el contrato, una garantía de fiel cumplimiento por una suma equivalente al 10 % del monto del contrato original. (...)

De corresponder, se aplicará el artículo 139 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, que indica: (...) no se otorga garantía de fiel cumplimiento del contrato ni garantía de fiel cumplimiento por prestaciones accesorias en los siguientes casos: a. en los contratos de bienes y servicios cuyos montos sean menores o iguales a 50 UIT (...)

i. Solución de controversias contractuales

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación o arbitraje, según el acuerdo de las partes.

Cualquiera de las partes tiene derecho a iniciar el arbitraje a fin de resolver dichas controversias dentro del plazo de caducidad previsto en la Ley N° 32069, Ley General de Contrataciones Públicas, y su Reglamento.

Facultativamente, Cualquiera de las partes tiene el derecho a solicitar una conciliación dentro del plazo de caducidad correspondiente, según lo señalado en el artículo 82 de la Ley N° 32069, Ley General de Contrataciones Públicas, sin perjuicio de recurrir al arbitraje, en caso no se llegue a un acuerdo entre ambas partes o se llegue a un acuerdo parcial. Las controversias sobre nulidad del contrato solo pueden ser sometidas a arbitraje.

El Laudo arbitral emitido es inapelable, definitivo y obligatorio para las partes desde el momento de su notificación, según lo previsto en el numeral 84.9 del artículo 84 de la Ley N° 32069, Ley General de Contrataciones Públicas.

j. Obligaciones del contratista

El contratista deberá elaborar y presentar informes técnicos especializados



Firmado digitalmente por:
MORI GARCIA Willy Otmar
FAU 20174850971 hard
Motivo: Soy el autor del documento

Fecha: 29/09/2026 14:17:33-0500

Av. Enrique Guzmán y Valle 951, La Cantuta - Chosica
Teléfono: 313-3700, anexos 1820
web: www.una.edu.pe Email: soplectvredes@una.edu.pe



**Universidad Nacional de Educación
Enrique Guzmán y Valle**
"Alma Máter del Magisterio Nacional"

"Año de la Esperanza y el Fortalecimiento de la Democracia"

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
UNIDAD DE SOPORTE TÉCNICO Y REDES

vinculados directamente al servicio contratado, cuando estos sean requeridos por la Unidad de Soporte Técnico y Redes. Dichos informes deberán contener el detalle de las actividades ejecutadas, diagnóstico técnico, sustento de las acciones realizadas, resultados obtenidos y recomendaciones, según corresponda, dentro del plazo que establezca el área usuaria.

k. Responsabilidad de por vicios ocultos

La responsabilidad del contratista por vicios ocultos será de tres (03) años, contabilizados a partir del día siguiente de la emisión de la conformidad, del servicio prestado.

i. Confidencialidad

EL CONTRATISTA se obliga a mantener y guardar estricta reserva y absoluta confidencialidad de todos los documentos e información a los que tenga acceso en la ejecución de la prestación. Se entiende que la obligación asumida por EL CONTRATISTA está referida no solo a los documentos e información señalados como "confidenciales" sino a todos los documentos e información que, en ejecución de las actividades señaladas en Los términos de referencia, pueda ser conocida por cualquier medio por EL CONTRATISTA.

j. Propiedad intelectual

La información y material producido bajo los términos de este servicio, tales como escritos, medios magnéticos, digitales, y demás documentos generados por el servicio, pasará a propiedad de la Universidad Nacional de Educación Enrique Guzmán y Valle.

k. Resolución de contrato por incumplimiento

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 68.1 del artículo 68 de la Ley N° 32069, Ley General de Contrataciones Públicas. De encontrarse en alguno de los supuestos de resolución del contrato, LAS PARTES proceden de acuerdo con lo establecido en el artículo 122 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

l. Clausula anticorrupción y antisoborno

EL CONTRATISTA declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a los evaluadores del proceso de contratación o cualquier servidor de la entidad contratante.

Asimismo, EL CONTRATISTA se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente.

Aunado a ello, EL CONTRATISTA se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación¹ y/o cualquier



Universidad Nacional de Educación
Enrique Guzmán y Valle
"Alma Máter del Magisterio Nacional"

"Año de la Esperanza y el Fortalecimiento de la Democracia"



OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
UNIDAD DE SOPORTE TÉCNICO Y REDES

1337

servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.

Adicionalmente, EL CONTRATISTA se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con LA ENTIDAD.

Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato.

Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a LA ENTIDAD CONTRATANTE el derecho de resolver total o parcialmente el contrato². Cuando lo anterior se produzca por parte de un proveedor adjudicatario de los catálogos electrónicos de acuerdo marco, el incumplimiento de la presente cláusula conllevará que sea excluido de los Catálogos Electrónicos de Acuerdo Marco³. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar⁴.

m. Sanciones

El Tribunal de Contrataciones Públicas sanciona a los participantes, postores, proveedores, y subcontratistas, cuando incurran en las infracciones señaladas en el párrafo 87.1 del artículo 87 de la presente ley, sin perjuicio de las responsabilidades civiles o penales a que hubiera lugar.

Las sanciones por imponer pueden ser:

- a) Multa.
- b) Inhabilitación temporal.
- c) Inhabilitación permanente.

La multa o inhabilitación que se impongan no eximen de la obligación de cumplir con los contratos ya perfeccionados a la fecha en que la sanción queda firme.

6. DESCRIPCIÓN DEL SERVICIO A CONTRATAR

Ítem	Cantidad	Descripción del servicio
SERVICIO DE INTERNET	1	Servicio de internet para garantizar conectividad estable, segura y de alta disponibilidad para la red institucional de la Universidad Nacional de Educación Enrique Guzmán y Valle.

6.1. CARACTERÍSTICAS TÉCNICAS MÍNIMAS:

Servicio de Internet dedicado

El servicio de Internet dedicado será simétrico y con un Overbooking 1:1 en el enlace local según el siguiente detalle:

Firmado digitalmente por:
MORI GARCIA Willy Otmar
FAU 20174950971 hard
Motivo: Soy el autor del documento
Fecha: 29/09/2026 14:17:40-0500

Av. Enrique Guzmán y Valle 951. La Cantuta - Chosica
Teléfono: 313-3700, anexos 1820
web: www.une.edu.pe Email: spotecvredes@une.edu.pe





**Universidad Nacional de Educación
Enrique Guzmán y Valle**
"Alma Mater del Magisterio Nacional"

"Año de la Esperanza y el Fortalecimiento de la Democracia"

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
UNIDAD DE SOPORTE TÉCNICO Y REDES

- Cada Sede debe tener la opción de que el servicio debe soportar Dual Stack (soporte simultáneo de IPv4 e IPv6).
- El postor debe entregar adicional por cada sede un bloque de direccionamiento IPv6 público (mínimo un prefijo /48 o /56) por sede, garantizando el enrutamiento y la visibilidad externa bajo este protocolo.
- El servicio prestado muy aparte de brindar el protocolo IPV4 también deberá alinearse a las disposiciones de la Secretaría de Gobierno y Transformación Digital de la PCM respecto a la adopción del protocolo IPv6 y los lineamientos de Seguridad Digital del Estado Peruano.

a. Sede Central

- Conexión a Internet a 4200 Mbps simétrico, dedicado y con ancho de banda 100% garantizado por medio de fibra óptica canalizada y/o subterránea y/o aérea desde el nodo del POSTOR GANADOR hasta los ambientes donde se instalarán los equipos para la prestación del servicio (128 direcciones IPv4 Públicas incluidas la IP del Router, IP de Red e IP de Broadcast).
- Servicio de Internet de 1000 Mbps simétrico, dedicado y con ancho de banda 100% garantizado por medio de fibra óptica para servidores (128 direcciones IP Públicas incluidas la IPv4 del Router, IP de Red e IP de Broadcast).

b. Sede La Molina

- Servicio de Internet de 1000 Mbps simétrico, dedicado y con ancho de banda 100% garantizado punto a punto por medio de fibra óptica canalizada y/o subterránea y/o aérea desde el nodo del POSTOR GANADOR hasta los ambientes donde se instalarán los equipos para la prestación del servicio (64 direcciones IPv4 Públicas incluidas la IP del Router, IP de Red e IP de Broadcast).

c. Sede El Rímac

- Servicio de Internet de 1000 Mbps simétrico, dedicado y con ancho de banda 100% garantizado punto a punto por medio de fibra óptica canalizada y/o subterránea y/o aérea desde el nodo del POSTOR GANADOR hasta los ambientes donde se instalarán los equipos para la prestación del servicio (64 direcciones IPv4 Públicas incluidas la IP del Router, IP de Red e IP de Broadcast).

6.2. CARACTERÍSTICAS TÉCNICAS DEL SERVICIO DE INTERNET

- El acceso a internet deberá estar basado en la implementación de líneas dedicadas y anchos de banda permanentes.
- Enlace a internet dedicado con un ancho de banda según la Tabla 1, simétrico y con un Overbooking 1:1

N°	Sede	Dirección	Ancho de Banda	Medio
1	Central	Av. Enrique Guzmán y Valle N° 951 La Cantuta - Chosica	4200 Mbps	Fibra Óptica

Av. Enrique Guzmán y Valle 951, La Cantuta - Chosica
Teléfono: 313-3700, anexos 1820
web: www.une.edu.pe Email: soplectvredes@une.edu.pe

Firmado digitalmente por:
MORI GARCIA Wily Otmir
FAU 20174950971 hard
Motivo: Soy el autor del documento
Fecha: 29/09/2020 14:17:57-0500

**FIRMA
DIGITAL**



Universidad Nacional de Educación
Enrique Guzmán y Valle
"Alma Máter del Magisterio Nacional"

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
UNIDAD DE SOPORTE TÉCNICO Y REDES

"Año de la Esperanza y el Fortalecimiento de la Democracia"



45

1335

2	Central	Av. Enrique Guzmán y Valle N° 951 La Cantuta - Chosica	1000 Mbps	Fibra Óptica
3	La Molina	Calle Las Agrícolas N° 280 Urb. Las Acacias - La Molina	1000 Mbps	Fibra Óptica
4	Rimac	Jr. Pío Sarobe N° 200 Urb. La Huerta - El Rímac	1000 Mbps	Fibra Óptica

- El Overbooking solicitado de 1:1 corresponde desde la puerta de enlace del router de internet de UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE hasta la puerta de enlace del POSTOR GANADOR conectado directamente al del proveedor de Internet. El overbooking solicitado corresponde desde el router instalado en la Entidad hasta el router de borde del proveedor internacional de internet.
- El medio físico de transporte será 100% fibra óptica en la última milla (desde el Punto de presencia del POSTOR GANADOR hasta las sedes de la UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE).
- Registro del DNS y asignación de las direcciones IP públicas necesarias según la Tabla 2, dentro de las cuales estarán el IP del Router, el IP de la red y el IP del Broadcast, así como el respectivo acceso a Internet y la inscripción de los dominios en los servidores del ISP. Para este fin, el postor deberá registrar los dominios y sub dominios existentes y los nuevos dominios y sub dominios según lo requiera la institución a través de un canal indicado por el proveedor.

N°	Sede	Dirección	Cantidad de IPv4
1	Central	Av. Enrique Guzmán y Valle N° 951 La Cantuta - Chosica	128
2	Central	Av. Enrique Guzmán y Valle N° 951 La Cantuta - Chosica	128
3	La Molina	Calle Las Agrícolas N° 280 Urb. Las Acacias - La Molina	64
4	Rimac	Jr. Pío Sarobe N° 200 Urb. La Huerta - El Rímac	64

- El postor debe incluir en su servicio, una plataforma de autogestión del DNS (Sistema de Nombres de Dominio) que permitirá al usuario autorizado (Con clave de acceso) poder crear, actualizar, modificar y eliminar configuraciones de los registros del DNS. Para ello, se deberá contar como mínimo, con (02) servidores DNS (Principal y redundado) ubicados en Data Center distintos a nivel nacional.
- El postor debe asegurar la comunicación constante durante toda la ejecución del servicio, para ello deberá contar con salidas internacionales de mínimo (03) tres proveedores TIER I, con capacidad mínima de 100 Gbps con cada uno de estos proveedores, para ello el postor deberá presentar, un diagrama de la salida internacional detallando los nombres de los proveedores TIER I, el cual se presentará en la etapa de perfeccionamiento del contrato.
- El POSTOR GANADOR deberá proveer un Router de última generación, nuevo y de primer uso que soporte ampliación de ancho de banda del 30% del ancho.

Firmado digitalmente por:
MORI GARCIA Willy Otmár
FAU 20174050971 hard
Motivo: Soy el autor del
documento
Fecha: 29/09/2026 14:18:05-0500

Av. Enrique Guzmán y Valle 951. La Cantuta - Chosica
Teléfono: 313-3700, anexos 1820
web: www.une.edu.pe Email: sopotecredes@une.edu.pe





- Se precisa que el POSTOR GANADOR deberá garantizar que cuenta con salidas internacionales redundantes, y también deberá asegurar que estas interconexiones tienen independencia de operación y conexión hacia la red de su proveedor internacional. En el cual se presentará con una declaración jurada al inicio del servicio (ejecución del servicio).
- El POSTOR GANADOR deberá considerar el equipamiento necesario hasta el puerto RJ- 45 del switch de la UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE para iniciar el servicio.
- El protocolo de comunicación deberá ser TCP/IP.
- El POSTOR GANADOR deberá tener disponibilidad de protocolo de ruteo IPV4/ IPV6.
- El protocolo de transporte del Backbone del POSTOR GANADOR deberá ser MPLS.
- El POSTOR GANADOR deberá instalar y configurar todos los equipos, dispositivos y/o componentes necesarios para la puesta en funcionamiento y que sean parte del servicio materia de esta licitación sin que esto implique costo adicional para la UNIVERSIDAD NACIONAL DE EDUCACION ENRIQUE GUZMAN Y VALLE. El servicio es considerado llave en mano incluyendo el router terminal.
- Los elementos y/o accesorios que serán proporcionados por la entidad serán los siguientes:
 - Tomacorrientes.
 - Energía estabilizada, UPS.
 - Patch Panel
 - Patch Cords.
 - Puertos disponibles en Switch (donde se conectará el router)
 - Cableado desde el Router hasta el Switch (en caso el Switch no estuviera en el mismo gabinete)
 - Tendido de cableado eléctrico
 - Pozo a tierra con valor menor de 50hm
 - Espacio en Rack o gabinete para instalar los equipos.
- EL POSTOR debe contar con, el medio de acceso de transporte físico de Red (NOC - Network Operations Center) y el Centro de Operaciones de Seguridad (SOC - Security Operations Center) propio y/o tercerizado.
- EL POSTOR GANADOR deberá poseer un NOC y SOC con soporte técnico 24 horas del día, los 7 días de la semana y los 365 días del año durante todo el plazo del servicio.
- Se precisa que el POSTOR GANADOR deberá contar con un NOC y SOC, ubicados en Lima, Perú.
- El POSTOR GANADOR deberá asegurar que el servicio de Internet será brindado las veinticuatro (24) horas del día, los siete (7) días de la semana y los trescientos sesenta y cinco (365) días del año, con una disponibilidad del servicio al (mínimo 99.5% para la Sede del La Molina y Rímac, pero 98.9% para la sede central) mensual.
- El servicio será acceso total a Internet y no deberá contener filtros de ninguna clase, restricción de protocolo, puertos o aplicativos con lo cual se deberá asegurar el



1333

funcionamiento de cualquier tipo de aplicación que se ejecute sobre el protocolo TCP/IP.

- El POSTOR GANADOR deberá proporcionar una herramienta vía web que permita monitorear y supervisar en línea el enlace y consumo de ancho de banda para lo cual entregará un usuario y su clave de acceso respectivo. Así mismo deberá proveer reportes de tráfico diario, semanal y mensual, en línea almacenando una bitácora de las últimas 4 semanas, para fines comparativos.
- El POSTOR GANADOR deberá poseer servidores DNS redundantes y distribuidos geográficamente en locales distintos. Deberá demostrar mediante un diagrama de red (de cualquier nivel) que posee servidores DNS distribuidos en dichos locales, el cual se presentará en la etapa de perfeccionamiento del contrato
- La administración y configuración de los equipos para la prestación del servicio, será responsabilidad exclusiva del POSTOR GANADOR.
- Si para la instalación del servicio de Internet es necesario realizar obras civiles, trámites de permisos municipales y otros necesarios, los costos serán asumidos por el POSTOR GANADOR.
- El postor deberá garantizar el profesionalismo, responsabilidad y conocimientos técnicos de su personal en los Centros de Llamadas de Reportes de Fallas, Centros de Gestión y personal de Reparación de Averías. Así mismo deberá contar con el equipamiento necesario para solucionar los problemas técnicos que se presenten. Para lo cual deberá adjuntar los medios y canales de comunicación para su atención, el cual se presentará en la etapa de perfeccionamiento del contrato.
- La UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE constatará la información presentada por el postor con visitas a los Centros de Gestión de considerarlo necesario.
- El postor deberá pertenecer a la Asociación NAP (Network Access Point) Perú, y presentar la constancia que lo acredite como tal. Se deberá presentar una constancia en la cual se avale lo indicado en la etapa de perfeccionamiento de contrato.

6.3. SERVICIO DE DATOS

El Postor debe brindar el servicio de transmisión de datos entre las sedes de la UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE hacia la sede principal, detalladas a continuación:

Nº	Sede	Dirección	Ancho de Banda	Medio
1	Central	Av. Enrique Guzmán y Valle 951 La Cantuta - Chosica	2000 Mbps	Fibra Óptica
2	La Molina	Calle Las Agrícolas N° 280 Urb. Las Acacias - La Molina	1000 Mbps	Fibra Óptica
3	Rímac	Jr. Pío Sarobe N°200 Urb. La Huerta - El Rímac	1000 Mbps	Fibra Óptica

- El servicio debe garantizar una transmisión segura, íntegra y confiable de la voz, video y datos desde las sedes remotas hacia la Sede Principal, considerando como



factor crítico en el transporte de la información, una trayectoria privada separada de la red pública de Internet (VPN).

- El POSTOR GANADOR deberá proveer un Router de última generación y de una marca de prestigio mundial, que soporte ampliación de ancho de banda, puertos Ethernet.
- El medio de acceso de transporte físico de última milla del POSTOR GANADOR deberá ser 100% Fibra Óptica, el mismo que será canalizado y/o subterráneo y/o aérea; desde el nodo del POSTOR GANADOR hasta los ambientes donde se instalarán los equipos para la prestación del servicio.

6.4. SEGURIDAD GESTIONADA

- El equipamiento propuesto por el postor (Router y Firewall gestionado) debe soportar nativamente el protocolo IPV4 y IPV6 (Static routing, BGP para IPV6, filtrado de paquetes IPV6) sin degradación del rendimiento.
- El servicio de seguridad gestionada debe incluir obligatoriamente: Firewall de próxima Generación (NGFW), Sistema de Prevención de Intrusiones (IPS), Filtrado de Contenido Web, y Reportabilidad mensual de incidentes de seguridad.
- El POSTOR deberá incluir una solución de gestión centralizada de seguridad de red, mediante FortiManager Cloud que permita:
 - Gestión centralizada para los firewalls que forman parte del proceso.
 - Gestión de firmwares con plantillas y actualizaciones programadas.
 - Configuración de dispositivos con grupos de plantillas.
- Se deberá incluir como parte del servicio, una solución de seguridad lógica que sea gestionada de manera remota por el proveedor a través de equipos appliance a ser instalados en las sedes de la Universidad: Ciudad Universitaria (Principal), Rímac, La Molina. Las características requeridas se muestran en el cuadro adjunto. Se deberá considerar que el equipo principal deberá estar como concentrador de VPN contra todos los equipos de seguridad de las diversas sedes.
- Se deberá incluir como parte del servicio, una solución de seguridad lógica que sea gestionada de manera remota por el proveedor, mediante equipos de seguridad (appliance) a ser instalados en las sedes de la Universidad: Ciudad Universitaria (Principal), Rímac y La Molina. Se deberá considerar que el equipo principal deberá funcionar como concentrador de VPN para establecer conexiones VPN con los equipos de seguridad de las diversas sedes.
- El servicio de seguridad deberá ser gestionado por el SOC (Security Operation Center) del PROVEEDOR.
- Se deberá considerar un equipo en la sede central que cumpla la función de recolección de logs y de reportes de la plataforma de seguridad, el equipo deberá contar con un almacenamiento de al menos 8 TB, asimismo, la plataforma de gestión y recolección de eventos deberá permitir la integración nativa y el reenvío de logs (mediante protocolos estándar como Syslog, CEF o a través de APIs) hacia plataformas de terceros, tales como soluciones EDR/XDR o sistemas SIEM.
- El SOC del postor (propio o tercerizado) que atienda los incidentes y casos reportados, deberá estar en Perú y contar con la Certificación ISO 27001 en los procesos de gestión de incidentes, gestión de cambios y ciberseguridad, así como la Certificación ISO 27035 en los procesos de gestión de incidentes, gestión de





1331

cambios, gestión de ciberseguridad (opcional), operando las 24 horas del día en los 7 días a la semana por 365 días (24x7x365-adjuntar declaración jurada de la disponibilidad del personal, el cual deberá presentar como sustento en la etapa de presentación de la oferta

- El equipo de respuesta a incidentes del postor deberá estar ubicado en Perú para una adecuada gestión, y operando 24x7. El postor deberá sustentar mediante una declaración jurada, el cual deberá presentar como sustento en la etapa de perfeccionamiento del contrato.

Características técnicas de los firewalls de nueva generación:

Los 4 dispositivos propuestos deben ser equipos de propósito específico, nuevos y de primer uso.

a. Capacidades de Networking

- La marca del firewall propuesto debe contar con certificación USGv6- r1 en Firewall.
- Los dispositivos deben estar catalogados como NGFW (Firewall de Nueva Generación). y deberá estar en el Cuadrante Mágico de Gartner como líder en los últimos 3 reportes.
- Los dispositivos de seguridad deben soportar VLAN Tags 802.1q, agregación de links 802.3ad, Policy Based Forwarding (PBF) o Policy Based Routing (PBR), ruteo multicast, jumbo frames, subinterfaces ethernet lógicas, NAT de origen y destino.
- Los appliances deben poder incluir Firewall y VPN, todas en un solo hardware, con la posibilidad de ejecutar todas las funcionalidades al mismo tiempo.
- Los appliances deben ser accesibles a través de SSH y de interface Web usando SSL.
- Los equipos deberán establecer conexión VPN IPSEC con el equipo de la ciudad Universitaria.
- La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado (SSL).
- Los equipos deben analizar contenido cifrado (SSL) para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Antivirus, IPS, DLP y Antispam (antispam opcional).
- Se debe contemplar escenario de alta disponibilidad (HA) para la ciudad Universitaria, trabajando en un esquema de alta redundancia de tipo activo-pasivo o activo-activo con balanceo de carga, con todas las licencias de software habilitadas para no permitir la pérdida de conexiones.
- Soportar enrutamiento estático y dinámico (RIPv2, OSPFv2, OSPFv3 y BGP).
- Deben soportar NAT de origen y NAT de destino de manera simultánea.
- Deben ser compatibles con NAT64 y NAT46.
- Deben ser capaces de operar en los modos:
- .odos Capa 3 (con capacidades completas de ruteo y NAT), Capa2 transparente y Sniffer, de forma simultánea mediante el uso de sus interfaces físicas sin necesidad de hacer uso de contextos o dominios virtuales.
- Reconocer al menos 2000 aplicaciones de diversos tipos, incluyendo, pero no limitado a: peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, video, Proxy, mensajería instantánea, compartición de archivos, correo electrónico.
- La solución debe optimizar y gestionar el tráfico WAN ofreciendo control de rutas basado en Acuerdos de Nivel de Servicio (SLA), e incluir características de resiliencia y mejora en la transmisión como la duplicación de paquetes por múltiples rutas (Multi-path Packet Duplication) y Forward Error Correction (FEC).
- La solución debe contar con servicios de red básicos integrados de forma nativa, actuando como servidor DHCP, servidor NTP, servidor DNS y proxy DNS.



FIRMA
DIGITAL



- La solución debe permitir múltiples modos de interfaz y topologías de despliegue, incluyendo la implementación en línea transparente como cable virtual (Virtual wire de Capa 1), modo TAP para conexión a puertos SPAN, y modos de interfaz operando como sniffer, puertos agregados, loopback y segmentación por VLANs (802.1Q y Trunking).
- La solución debe ser capaz de enviar paquetes de restablecimiento (TCP-RST) incluso si el equipo está desplegado en el modo TAP

b. Capacidades funcionales

- La solución debe operar en los modos de funcionamiento NAT/enrutamiento, transparente (puente) y mixto.
- La solución debe soportar objetos de políticas predefinidos, personalizados, de agregación y de agrupación, permitiendo la creación de políticas de seguridad basadas en aplicaciones, roles y geolocalización, así como programaciones únicas y recurrentes, listas dinámicas externas y políticas completas de DNS.
- La solución debe proveer una vista global de gestión de políticas que incluya inspección de redundancia de reglas de seguridad, grupos de políticas, reversión de configuración (rollback), análisis y limpieza de políticas inválidas, asistente de recomendación basado en servicios o aplicaciones, y soporte para importación y exportación de las mismas.
- La solución debe realizar un diagnóstico previo y posterior a la aplicación de la política pudiendo ser capaz de exportar los resultados del análisis y exportar un script de eliminación para la ejecución a criterio del administrador.
- La solución debe soportar configuraciones NAT (por política y mediante tabla central) y detectar redundancia NAT, cubriendo NAT46, NAT64, NAT444, SNAT, DNAT, PAT, Full Cone NAT (IPv4 e IPv6) y STUN.
- La solución debe Deberá ofrecer soporte de Gateway de Nivel de Aplicación (ALG) y sesiones para MSRPC, PPTP, RAS, RSH, SIP, FTP, TFTP, HTTP, dcerpc, dns-tcp, dns-udp, H.245 0, H.245 1, H.323 y tcp full proxy, así como soporte VoIP para NAT traversal en SIP/H.323/SCCP y RTP pin holing.
- IPv6. La solución debe ser totalmente compatible con el protocolo IPv6, soportando sobre este protocolo la gestión, registro, jumbo frames, Radius, SSO-radius, listas blancas de Active Directory, balanceo de carga de enlaces (LLB), QoS(o equivalente de cada fabricante), VPN SSL, control de acceso, e inspecciones de seguridad nativas sobre este protocolo (identificación de aplicaciones y defensa contra ataques Neighbor Discovery).
- IPv6. La solución debe soportar protocolos de enrutamiento y túneles IPv6, incluyendo enrutamiento estático, enrutamiento por políticas, ISIS, RIPng, OSPFv3, BGP4+, y tecnologías de tunelización como DNS64/NAT64, IPv6 ISATAP, IPv6 GRE, IPv6 sobre IPv4 GRE y 6RD. Debe capaz de desplegar un proxy DNS64 sin equipamiento adicional
- IPv6. La solución debe proveer soporte IPv6 en alta disponibilidad (A-A o A-P) y soportar inspección de tráfico IPv6 ALG (TFTP, FTP, RSH, HTTP, SIP, SQLNETv2, RTSP, MSRPC, SUNRPC).
- LLB. La solución debe realizar balanceo de carga de enlaces (LLB) bidireccional, soportando LLB saliente (con enrutamiento basado en políticas incluyendo ECMP, por tiempo, ponderado y enrutamiento ISP integrado, además de detección activa/pasiva de calidad de enlace en tiempo real y funcionalidades de SD-WAN nativo en el sistema operativo del firewall, con selección de la mejor ruta) y LLB entrante con su propio servidor DNS autoritativo inteligente y detección dinámica.
- LLB. La solución debe gestionar eficientemente las conexiones a través de detección de dirección de seguimiento e inspección del estado del enlace mediante ARP, PING y DNS, ejecutando conmutación automática de enlaces basada en ancho de banda, de ruta según SLA (latencia, fluctuación (pérdida de paquetes, jitter), conectividad y tipo de aplicaciones sin requerir un licenciamiento adicional.





1329

c. Características de SSL (soportando TLS V1.0, V1.2 Y V1.3), permitiendo la identificación de IPS:

- Debe detectar y bloquear ataques de red y de aplicación, protegiendo al menos los siguientes servicios: Email, DNS, FTP, servicios de Windows (Microsoft Networking) y SNMP.
- "El IPS debe contar con funcionalidades explícitas de 'Parcheo Virtual' (Virtual Patching) para la protección de vulnerabilidades a nivel de red y aplicación, con actualizaciones automáticas de firmas".
- Debe detectar y bloquear aplicaciones que realizan control remoto, incluyendo aquellas que son capaces de hacer tunneling en tráfico HTTP.
- El IPS debe poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o espejo.
- El IPS deberá estar integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos.
- La interfaz de administración del detector y preventor de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio.
- Debe actualizar de manera automática las firmas para el sistema de detección de intrusos.

d. Inspección de Contenido SSL:

- La solución debe contar con modo de descarga de proxy SSL(offload), soportar la reutilización de sesiones, permitir conexión segura a servidores AD/LDAP vía cifrado SSL, y aplicar identificación de aplicaciones, IPS, sandbox y antivirus para la capacidad de inspeccionar tráfico descifrado por el proxy.
- La solución debe incluir un mecanismo de defensa inteligente contra DoS/DDoS que establezca líneas base mediante Machine Learning, mitigando ataques volumétricos como Ping of Death, Teardrop, fragmentación IP, opciones IP, ataques Smurf/Fragile, Land, paquetes ICMP grandes y WinNuke.
- La solución debe bloquear inundaciones (Flood attacks) incluyendo ICMP, UDP, SYN, SIP y queries simples/recursivas o respuestas DNS, y proteger contra anomalías de protocolo y secuestro DoH (DNS sobre HTTPS).
- La solución debe defender la red contra falsificación (spoofing) de ARP, ND y direcciones IP, así como contra escaneos de puertos (port scan) y barridos de IP (IP sweep).
- La solución debe identificar y mitigar amenazas a nivel aplicativo, protegiendo contra ataques de fuerza bruta en múltiples servicios (por lo menos VNC, RDP, SSH, LDAP, IMAP, SMB), escaneo de archivos sensibles, detección de shell inverso (reverse shell), contraseñas débiles y detección de aplicaciones HTTP, integrando listas de permitidos para IP de destino y bloqueo de dominios con un clic mediante listas de bloqueo dinámicas.

e. Control de aplicaciones

- La solución debe identificar más de 6,000 aplicaciones filtrables por nombre, categoría, subcategoría, tecnología y nivel de riesgo, detallando para cada una su



Firmado digitalmente por:
MORI GARCIA Willy Otmar
FAU 20174050971 hard
Intitvo: Soy el autor del
documento
Fecha: 29/09/2026 14:18:50-0500



descripción, factores de riesgo, dependencias, puertos típicos utilizados y URLs para referencia adicional.

f. Identificación y control de EndPoints

- La solución debe identificar los endpoints soportando al menos 10 sistemas operativos (incluyendo por lo menos Windows, iOS, Android), registrando su dirección IP, cantidad, horarios de conexión/desconexión y duración en línea, además de permitir consultas detalladas basadas en estos parámetros, el estado y las políticas de control.
- La solución debe identificar la cantidad de endpoints que acceden a través de capa 3, permitiendo el registro, la interferencia y el bloqueo de aquellas direcciones IP que excedan los límites permitidos (overrun IP), además de mostrar una página de redirección personalizada tras aplicar operaciones de interferencia.
- La solución debe identificar a los usuarios y aplicar control de tráfico específico para los servicios de escritorio remoto (Remote Desktop Services) de Windows Server.
- La solución debe gestionar identidades mediante una base de datos local de usuarios y soportar autenticación remota (TACACS+, LDAP, Radius, Active Directory, OAuth2), así como autenticación basada en interfaces, direcciones IP y direcciones MAC.
- La solución debe integrar autenticación de dos factores (2FA) con soporte para integraciones de terceros y contar con un servidor de tokens integrado que admita métodos físicos y mediante SMS.
- La solución debe contar con capacidades avanzadas de inicio de sesión único (SSO) para Windows AD, incluyendo soporte para 802.1X, Proxy SSO, ADSSO sin agente (AD Polling) y sincronización de autenticación basada en monitores SSO, permitiendo también la sincronización continua de grupos de usuarios a través de AD y LDAP.
- La solución debe soportar la autenticación mediante Azure Active Directory (AD) para los accesos a través de SSL VPN, ZTNA y WebAuth.
- La solución debe ofrecer un portal de autenticación web (WebAuth) compatible con IPv6, que incluya capacidades de personalización de la página de acceso y mecanismos de prevención contra ataques de fuerza bruta.
- La solución debe aplicar políticas de acceso y seguridad basadas tanto en usuarios como en dispositivos, y soportar la recepción y aplicación de políticas de seguridad de usuario emitidas por un servidor Radius mediante mensajes CoA (Change of Authorization).

g. Monitoreo reportes y configuración del sistema

- La solución debe proporcionar facilidades de registro integral que incluyan almacenamiento local expandible hasta 6 meses (mediante disco duro SSD), integración con servidores syslog genéricos y plataformas de gestión centralizada o análisis de registros de la misma marca
- La solución debe garantizar la integridad y el ser capaz de analizar contenido cifrado de los registros, soportando una transmisión confiable mediante la opción TCP (RFC 3195).
- La solución debe generar registros de tráfico detallados (cubriendo sesiones reenviadas, sesiones violadas, tráfico local, paquetes inválidos y URLs) con opción a un formato resumido y resolución de nombres de IPs/puertos de servicio, además de registros de eventos exhaustivos (auditorías de actividad del sistema y administración, enrutamiento, red, VPN, autenticaciones de usuarios, solicitudes/bloqueos DNS y eventos Wi-Fi).
- La solución debe soportar la auditoría de la configuración de políticas y generar al menos tres reportes predefinidos (Seguridad, Flujo y Red) así como reportes definidos por el usuario, con capacidad de exportación en PDF, Word y HTML a través de Email y FTP.



Firmado digitalmente por:
MORI GARCIA Wily Otmar
FAU 20174050971 hard
Motivo: Soy el autor del
documento
Fecha: 29/09/2026 14:18:0500



1321

- La solución debe soportar arquitecturas de Alta Disponibilidad (HA) en modos Activo/Activo (con protocolo de redundancia virtual) y Activo/Pasivo, incorporando sincronización de sesiones independiente, interfaces de latido (heartbeat) redundantes, puertos duales de enlace de datos HA y una interfaz de gestión reservada para el clúster.
- La solución debe ejecutar conmutación por error (failover) con conservación de estado en tiempos inferiores a un segundo, incluyendo notificación de fallos y monitoreo de puertos y enlaces locales/remotos, con opciones de despliegue HA que soporten agregación de enlaces, malla completa (full mesh) y dispersión geográfica.
- La solución debe ofrecer múltiples métodos de acceso para administración (HTTP/HTTPS, SSH, Telnet, consola, API Restful, NETCONF y acceso a CLI directo desde la interfaz gráfica Web), soportando autenticación de administradores vía Active Directory y LDAP.
- La solución debe permitir la administración centralizada mediante APIs de servicios web y facilitar la integración de sistemas a través de SNMP o syslog.
- La solución debe facilitar un despliegue rápido (Zero-Touch Provisioning) mediante aprovisionamiento basado en USB, y soportar la ejecución de scripts de configuración locales y remotos.
- La solución debe presentar un panel de control (dashboard) dinámico en tiempo real con widgets de profundización (drill-in), visualizando métricas del sistema (sesiones concurrentes, CPU, memoria, temperatura), análisis de tráfico en tiempo real, estadísticas de calidad de servicio (QoS), monitoreo del estado de los enlaces y estadísticas de eventos de amenazas, aplicaciones y URLs.
- La solución debe soportar la recolección de información de tráfico de red y su reenvío utilizando el protocolo Netflow (v9.0).
- La solución debe permitir la carga (upload) y la simulación por repetición (replay detection) de capturas de paquetes lógicas (archivos pcap) sin necesidad de configurar complejos entornos de prueba externos. Esto con el fin de recrear escenarios intermitentes que no son reproducibles en tiempo real y comprobar el comportamiento del cortafuegos o de un dispositivo interno.

h. Seguridad IOT y protección de archivos

- La solución debe identificar automáticamente dispositivos IoT (tales como cámaras IP y grabadoras de video en red) y soportar la configuración de listas blancas personalizadas para su gestión.
- La solución debe permitir la consulta de los resultados del monitoreo aplicando condiciones de filtrado que incluyan el tipo de dispositivo, la dirección IP, el estado, entre otros parámetros operativos.
- La solución debe controlar la transferencia de archivos evaluando su tipo, tamaño y nombre, mediante la identificación precisa de firmas y sufijos para más de 100 formatos de archivo, aplicando esta capacidad de filtrado e identificación sobre protocolos como HTTP, FTP, SMTP, POP3, SMB y tráfico HTTPS (utilizando un Proxy SSL).
- La solución debe ejecutar un filtrado de contenido analizando el interior de los archivos y detectando palabras clave predefinidas a través de los protocolos HTTP-GET, HTTP-POST, FTP y SMTP.
- La solución debe identificar de forma nativa el uso de aplicaciones de mensajería instantánea (IM) y proveer capacidades para auditar el comportamiento de la red.
- VPN
- La solución debe soportar configuraciones de VPN IPsec guiadas, basadas en rutas o en políticas y a través de puertos personalizados, permitiendo despliegues de puerta a puerta (gateway-to-gateway), malla completa (full mesh), hub-and-spoke, túneles redundantes y terminación VPN en modo transparente, incorporando además soporte para balanceo de carga de enlaces (LLB) y conmutación por error (failover) sobre dichos túneles.





1326

- La solución debe ser compatible con IKEv1 e IKEv2 (RFC 4306) operando como cliente o servidor, soportando modos de protección de identidad principal y agresivo en Fase 1, métodos de autenticación por certificado y clave precompartida (PSK), y opciones flexibles de aceptación de pares (cualquier ID, ID específico o ID en grupo de usuarios dialup).
- La solución debe proveer amplias opciones criptográficas para las propuestas de Fase 1 y Fase 2, incluyendo algoritmos de cifrado (DES, 3DES, AES128, AES192, AES256), autenticación (MD5, SHA1, SHA256, SHA384, SHA512) y múltiples grupos Diffie-Hellman (1, 2, 5, 18, 19, 20, 21 y 24 según la versión de IKE), permitiendo configurar la caducidad de la clave de cifrado y la frecuencia de keep-alive para el cruce NAT (NAT traversal).
- La solución debe incluir funcionalidades avanzadas de túnel IPsec como DHCP sobre IPsec, XAuth (en modo servidor y para usuarios dialup), detección de pares inactivos (DPD estándar y DPD bajo demanda), detección de repetición (replay detection) y keep-alive de clave automática para SA en Fase 2.
- La solución debe proporcionar servicios de VPN SSL con soporte para clientes iOS, Android, Microsoft Windows, MacOS y Linux, incluyendo un módulo de reenvío de puertos (port forwarding) que encripte los datos del cliente hacia el servidor de aplicaciones, y permitir la creación de dominios (realms) que asocien múltiples inicios de sesión personalizados a grupos de usuarios y rutas URL.
- La solución debe aplicar controles de acceso y seguridad perimetral para las sesiones VPN SSL, requiriendo verificación de integridad del host, comprobación del sistema operativo y validación de MAC por portal antes de la conexión, previniendo inicios de sesión concurrentes con el mismo usuario (One time login), limitando la cantidad de usuarios simultáneos en el portal y ejecutando la limpieza de caché antes de finalizar la sesión.
- La solución debe gestionar y permitir la visualización centralizada de todas las conexiones VPN IPsec y SSL, soportando además tecnologías adicionales de tunelización como L2TP (modos cliente y servidor), L2TP sobre IPsec, GRE sobre IPsec, PnPVPN y túneles unicast estáticos VxLAN mediante VTEP.
- ZTNA(
- Se debe incluir licencia ZTNA para por lo menos 8 usuarios con las siguientes características:
- La solución debe proveer acceso a la intranet y a los usuarios finales basándose en el principio de Confianza Cero (Zero-Trust), facilitando una transición fluida desde infraestructuras VPN SSL actuales, operando bajo un entorno de dual stack IPv4/IPv6, y soportando la configuración de múltiples instancias ZTNA de forma simultánea en un único dispositivo.
- La solución debe habilitar la configuración de políticas Zero-Trust basadas en los recursos de las aplicaciones y en etiquetas ZTNA (las cuales deben validar las contraseñas de cuentas y el estado de los terminales), permitiendo el ajuste dinámico de los privilegios de autorización cuando cambie el estado del dispositivo (endpoint).
- La solución debe administrar los recursos de las aplicaciones, permitiendo su configuración y la gestión de permisos a nivel de nombre de dominio, integrando además la capacidad de publicar y mostrar visualmente las aplicaciones autorizadas a los usuarios finales a través de un portal ZTNA.
- La solución debe optimizar y asegurar el flujo de conexión ejecutando la selección automática de la puerta de enlace (gateway) óptima, aplicando soporte para autenticación de paquete único (SPA - Single Packet Authentication), y brindando protección nativa anti-DDoS sobre todo el tráfico ZTNA.
- La solución debe garantizar la compatibilidad con dispositivos finales utilizando sistemas operativos iOS, Android, Microsoft Windows, MacOS y Linux, ofrecer soporte para APIs Restful.

i. CALIDAD DE SERVICIO (QOS)



Firmado digitalmente por:
MORI GARCIA Wily Otmar
FAU 20174050971 hard
Motivo: Soy el autor del
documento
Fecha: 29/09/2026 14:19:14-0500



- La solución debe permitir la asignación de túneles y la configuración de límites de ancho de banda máximo o garantizado (por túnel, dirección IP o usuario) utilizando múltiples criterios de clasificación que incluyan dominios de seguridad, interfaces, direcciones, usuarios o grupos de usuarios, servidores o grupos de servidores, aplicaciones o grupos de aplicaciones, categorías de URL, VLAN y TOS.
- La solución debe gestionar y modelar el tráfico de red soportando los estándares Type of Service (TOS), Differentiated Services (DiffServ) y clases de tráfico, permitiendo distribuir el ancho de banda por esquemas de tiempo, prioridad o mediante un uso compartido equitativo, asignar de forma priorizada el ancho de banda restante y limitar el consumo mediante el retraso temporal del acceso para usuarios o direcciones IP.
- La solución debe controlar los recursos del sistema estableciendo un límite máximo de conexiones concurrentes por dirección IP y facilitar la gestión de cuotas mediante la limpieza (tanto manual como por expiración automática) del tráfico consumido por los usuarios.
- La solución debe contar con por lo menos 8 niveles de túneles jerárquicos de forma que se pueda dividir el ancho de banda de la organización en, áreas y sub-áreas dentro de la institución.

j. **ANTIVIRUS, IPS Y FILTRO DE CONTENIDOS (URL)**

- AV. La solución debe actualizar las firmas de virus mediante métodos manuales o automáticos (push o pull), y permitir la gestión de firmas MD5 posibilitando su adición o eliminación manual en la base de datos local, así como su carga hacia el sandbox en la nube del mismo fabricante.
- AV. La solución debe ejecutar un análisis antivirus basado en flujo sobre los protocolos HTTP, SMTP, POP3, IMAP, FTP y SMB, incluyendo la capacidad técnica para escanear y detectar amenazas dentro de archivos comprimidos.
- IPS. La solución debe detectar anomalías de protocolo y amenazas basadas en tasas de transferencia (rate-based), contando con configuraciones de prevención predefinidas, capacidad o SSH) para crear firmas personalizadas, una enciclopedia de amenazas integrada y soporte para la actualización de firmas de forma manual o automática (push/pull).
- IPS. La solución debe aplicar acciones de mitigación frente a intrusiones (por defecto, monitorear, bloquear o restablecer la conexión apuntando a la IP del atacante, la IP de la víctima o la interfaz entrante, configurando un tiempo de expiración), permitiendo la selección y filtrado de firmas según severidad, objetivo, sistema operativo, aplicación o protocolo, y soportando la excepción de direcciones IP para firmas IPS específicas.
- IPS. La solución debe soportar el funcionamiento en modo sniffer (IDS) e incluir opciones para el registro de paquetes.
- URL. La solución debe realizar una inspección de filtrado web basada en flujo y soportar filtrado web dinámico mediante una base de datos de categorización en tiempo real alojada en la nube (con más de 500 millones de URLs clasificadas en al menos 64 categorías, incluyendo 8 enfocadas en seguridad), permitiendo adicionalmente la configuración de filtrado manual basado en URL, contenido web y cabeceras MIME.
- URL. La solución debe proporcionar controles avanzados que permitan filtrar elementos específicos (Java Applets, ActiveX y cookies), bloquear solicitudes HTTP Post, registrar las palabras clave de búsqueda utilizadas, y gestionar de forma nativa listas de URLs permitidas (allow list) y bloqueadas (block list).
- URL. La solución debe ofrecer flexibilidad administrativa mediante la anulación temporal de perfiles de filtrado para su asignación específica a usuarios, grupos o direcciones IP, permitir la creación de categorías locales y la modificación de su clasificación predeterminada (rating override), e incluir la capacidad de exceptuar del escaneo a las conexiones cifradas correspondientes a ciertas categorías para garantizar la privacidad.



1324

k. CAPACIDADES AVANZADAS DE SEGURIDAD

- Antispam. La solución debe clasificar y prevenir el spam en tiempo real, categorizando los mensajes como spam confirmado, spam sospechoso, correo masivo (bulk spam) y correo masivo válido, garantizando esta protección de forma nativa independientemente del idioma, el formato o el contenido del mensaje.
- Antispam. La solución debe realizar la detección de spam tanto en el tráfico de correo de entrada (inbound) como de salida (outbound) a través de los protocolos SMTP y POP3, soportando la configuración de listas blancas para permitir de forma segura los correos electrónicos provenientes de dominios confiables.
- las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Prevención de Botnet. La solución debe descubrir hosts infectados por botnets en la intranet mediante el monitoreo de conexiones de Comando y Control (C&C), bloqueando amenazas avanzadas como botnets y ransomware, y previniendo el acceso hacia IPs, nombres de dominio y URLs maliciosas a través de la actualización regular de las direcciones de los servidores C&C.
- Prevención de Botnet. La solución debe inspeccionar y detectar el tráfico sobre los protocolos TCP, HTTP y DNS, incluyendo capacidades nativas para la identificación de algoritmos de generación de dominios (DGA) y túneles DNS, e incorporar la funcionalidad de sumidero DNS (DNS.sinkhole).
- Prevención de Botnet. La solución debe permitir la configuración y gestión granular de listas de acceso permitidas (allow list) y listas de bloqueo (block list) utilizando como criterios las direcciones IP, nombres de dominio y URLs.
- Reputación de IP. La solución debe identificar, filtrar y aplicar acciones de respuesta (tales como registrar eventos, descartar paquetes o bloquear la conexión) sobre el tráfico proveniente de direcciones IP riesgosas (incluyendo hosts de botnets, spammers, nodos Tor, hosts vulnerados y orígenes de ataques de fuerza bruta) y garantizar la precisión de esta protección mediante la actualización periódica de su base de datos de firmas de reputación de IP.
- Sandbox. La solución debe interactuar con un entorno de sandbox en la nube del mismo fabricante para la carga y evaluación de archivos maliciosos, proporcionando informes completos de análisis de comportamiento, e incluir la capacidad de operar en un modo de solo detección sin requerir la carga del archivo.
- Sandbox. La solución debe inspeccionar el tráfico a través de los protocolos HTTP/HTTPS, POP3, IMAP, SMTP, FTP y SMB, aplicando controles basados en la dirección de transferencia y el tamaño del archivo para formatos que incluyan PE, ZIP, RAR, Office, PDF, APK, JAR, SWF y Script.
- Sandbox. La solución debe contar con capacidades de bloqueo de amenazas en tiempo real respaldadas por la plataforma de inteligencia de amenazas del fabricante, y permitir la configuración administrativa de listas de URL permitidas (allow list) y bloqueadas (block list).

l. Capacidades adicionales.

- Sistemas virtuales. La solución debe soportar la asignación controlada de los recursos del sistema para cada dominio/sistema virtual implementado incluyendo la asignación de CPUs por cada instancia virtual.
- Sistemas virtuales. La solución debe proporcionar, dentro de los dominios/sistemas virtuales que no son raíz (non-root), funcionalidades completas de seguridad, red y gestión que incluyan firewall, VPN IPsec, VPN SSL, IPS, antivirus (AV), filtrado de URL, evaluación de reputación de IP, calidad de servicio (QoS), así como estadísticas y monitoreo detallado del propio dominio/sistema virtual y de las aplicaciones. Fuga de Información, Antivirus e IPS.

6.5. SERVICIOS DE ANTI-DDOS:



Firmado digitalmente por:
MORI GARCIA Willy Otmar
FAU 20174850971 hard
Motivo: Soy el autor del
documento
Fecha: 29/09/2026 14:19:30-0500



1323

El Contratista debe brindar una solución/plataforma de protección anti-ddos, la cual deba contar como mínimo con las siguientes características/funcionalidades:

- El postor ganador de la buena pro deberá contar con una solución de protección contra ataques DDoS/DoS a través de un entorno en nube perteneciente a su propia red.
- No se aceptarán soluciones en las que la protección DDoS sea una funcionalidad adicional de equipos firewall, NGFW, ADC y/o Routers.
- Mecanismo de Aprendizaje y Creación de Firmas: El sistema debe utilizar un motor de Aprendizaje Automático de Comportamiento (Behavioral Analysis) que genere, de forma autónoma y en tiempo real (menos de 20 segundos), una firma matemática/lógica local específico para cada vector de ataque detectado. No se aceptarán soluciones basadas en "Sugerencias" o "Recomendaciones" de configuración (como el ajuste de umbrales/thresholds) que requieran validación o que solo modifiquen parámetros de filtros existentes. La solución debe crear un objeto de firma nuevo y dinámico.
- La plataforma deberá estar licenciada para soportar ataques de hasta 30Gbps asegurando que la Universidad estará protegida de Ataques de Denegación de Servicio Distribuido.
- La solución deberá tener integrado un módulo de IPS (Sistema de Prevención de Intrusos).
- Soporte TLS 1.2 y 1.3 sin Descifrado: El sistema debe ser capaz de proteger contra ataques de Capa 7 (HTTPS Floods) en tráfico cifrado con protocolos TLS 1.2 y TLS 1.3, realizando el aprendizaje del tráfico legítimo y la mitigación del ataque sin necesidad de poseer las llaves privadas (SSL Keys) y sin realizar descifrado de paquetes. Se prohíbe explícitamente el uso de mecanismos de "Challenge-Response" (como inyección de cookies o redirecciones) que dependan del descifrado del tráfico para identificar bots en TLS 1.3.
- Procesamiento de Tráfico Cifrado (No Proxy): La mitigación del tráfico cifrado debe realizarse de forma stateless (sin estado) o mediante inspección de comportamiento de los parámetros del handshake y telemetría de red. No se aceptarán soluciones basadas en TLS Proxy vía Software o módulos de terminación SSL que actúen como intermediarios, debido a la latencia y los riesgos de seguridad que implica el manejo de llaves criptográficas.
- La solución deberá ser de tipo Stateless.
- La solución deberá soportar un incremento del tráfico originado por ataques de Denegación de Servicios del tipo volumétricos desde hasta un máximo del 100% del ancho de banda contratado.
- La solución deberá proteger frente a ataques de denegación de servicios en una arquitectura "always on", también denominada en línea o siempre activa. No se aceptarán soluciones de mitigación de ataques de denegación de servicios bajo una arquitectura de derivación de tráfico.

Se deberá entregar una carta de fabricante que indique que el postor cuenta con la infraestructura en su red para brindar este servicio; asimismo, la carta debe indicar el cumplimiento de cada característica técnica solicitada.

El Contratista deberá brindar un **reporte mensual de la actividad de seguridad relacionada con los ataques de denegación de servicios (DDoS) detectados y mitigados**. El reporte deberá estar plasmado en un informe, el cual deberá ser entregado dentro de los quince (15) días calendario posteriores al cierre de cada mes.

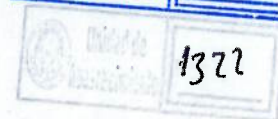
Las características de hardware solicitadas por sede deberán considerar las siguientes capacidades:

a. CIUDAD UNIVERSITARIA (PRINCIPAL):



Firmado digitalmente por:
MORI GARCIA Willy Otmaz
FAU 20174950971 hard
Motivo: Soy el autor del
documento

Fecha: 29/09/2026 14:19:37-0500



Características Firewall:

- Cantidad mínima de equipos: 2

Interfaces GE RJ45	08, debe contar con 2 pares de interfaces bypass (estos pueden ser parte de las 16 interfaces RJ45).
Interfaces 40G QSFP+	02
Interfaces 10G SFP+	16
Módulos adicionales (crecimiento futuro)	Debe contar nativamente o ser capaz de incrementar modularmente 2 puertos 40G QSFP+ o 8 puertos 10G SFP+
Almacenamiento	1.92TB SSD
Tamaño en gabinete	1 RU
Fuentes de Poder AC	02
Firewall Throughput	25 Gbps
NGFW Throughput	20 Gbps usando 64 KB o 30 Gbps usando Enterprise Mix
Threat Protection Throughput	12 Gbps usando 64 KB o 18.5 Gbps usando Enterprise Mix
IPS Throughput	21 Gbps.
IPSec VPN Throughput	18 Gbps.
Sesiones concurrentes	9 millones de conexiones concurrentes (medido con tráfico http) o 14 millones de conexiones concurrentes (medido con tráfico TCP)
Nuevas sesiones por segundo	480,000
Dominios/sistemas virtuales (VSYs)	1

Características mínimas equipos router:

- Cantidad mínima de equipos: 2

Interfaces GE RJ45	08
Interfaces 1G SFP	08
Interfaces 10G SFP+	02 (debe incluirse 2 transceivers SFP+)
Almacenamiento	960GB
Tamaño en gabinete	1 RU
Fuentes de Poder AC	02
Sesiones concurrentes	2.4 millones de conexiones concurrentes (medido con tráfico http) o 5 millones de conexiones concurrentes (medido con tráfico TCP)
Nuevas sesiones por segundo	130,000

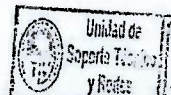
b. SEDE RÍMAC Y SEDE LA MOLINA

Características técnicas mínimas de firewall:

- Cantidad mínima de equipos: 02 (01 equipo por cada sede).



Firmado digitalmente por:
MORI GARCIA Wily Otmaz
FAU 20174950971 hard
Motivo: Soy el autor del
documento
Fecha: 29/09/2028 14:19:45-0500



1321

Interfaces GE RJ45	16, debe contar con 2 pares de interfaces bypass (estos pueden ser parte de las 16 interfaces RJ45).
Interfaces 1G SFP	08
Interfaces 10G SFP+	02
Almacenamiento	1.92TB SSD
Tamaño en gabinete	1 RU
Fuentes de Poder AC	02
Firewall Throughput	20 Gbps
NGFW Throughput	6.5 Gbps
Threat Protection Throughput	3 Gbps
IPS Throughput	11 Gbps.
IPSec VPN Throughput	6 Gbps.
Sesiones concurrentes	4.5 millones de conexiones concurrentes (medido con tráfico http) o 6.5 millones de conexiones concurrentes (medido con tráfico TCP)
Nuevas sesiones por segundo	135,000
Dominios/sistemas virtuales (VSYs)	1

Características mínimas Equipos router:

- Cantidad mínima de equipos: 02 (01 equipo por cada sede).

Interfaces GE RJ45	08
Interfaces 1G SFP	08
Interfaces 10G SFP+	02 (debe incluirse 2 transceivers SFP+)
Almacenamiento	960GB
Tamaño en gabinete	1 RU
Fuentes de Poder AC	02
Sesiones concurrentes	2.4 millones de conexiones concurrentes (medido con tráfico http) o 5 millones de conexiones concurrentes (medido con tráfico TCP)
Nuevas sesiones por segundo	130,000

6.6. SERVICIO DE TELEFONÍA FIJA

- Enlace Sip Trunk configurado con 30 sesiones de comunicación. El que se deberá instalar en Av. Enrique Guzmán y Valle s/n La cantuta – Chosica, Lima. Las líneas IP (Sip Trunk) podrá tener como última milla de conexión a la PBX del cliente, accesos E1 utilizando como medio de comunicación Fibra Óptica canalizada, subterránea o aérea, desde la salida de servicios del proveedor (punto de presencia POP) hasta el extremo del conversor de medios físicos de lugar fijado de cada sede (última milla, red acceso, backbone). La central telefónica de propiedad de la entidad YEASTAR S300 cuenta con las interfaces E1-PRI.
- El proveedor deberá incluir a costo suyo, cualquier equipamiento conversor o solución que se requiera para conectar el sip trunk en interfaz E1, en caso la central sólo tenga estos puertos. La central mencionada en el punto anterior soporta enlace SIP TRUNK
- Se debe garantizar la comunicación SIP del softphone LINKUS para uso externo que utiliza la institución, el alcance del servicio de telefonía fija SIP Trunk se limita a garantizar la interoperabilidad mediante interfaces SIP o E1 con la central telefónica existente, siendo responsabilidad de la Entidad asegurar la compatibilidad, configuración y correcto funcionamiento de la plataforma de comunicaciones Yeastar y del softphone LINKUS, incluyendo los aspectos de firmware, licenciamiento y configuraciones necesarias para su operación.





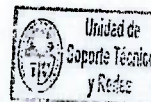
- En la instalación de las fibras ópticas y los equipos correspondientes, el proveedor será responsable de todas las obras civiles, canalizaciones subterráneas, permisos municipales y demás actividades necesarias para una óptima implementación, sin que esto signifique un costo adicional para Universidad Nacional de Educación Enrique Guzmán y Valle.
- El postor se obliga a instalar los equipos modems, routers, multiplexor y/o similares, es decir equipos para la prestación del servicio a través de interfaces E1 o Sip Trunk y siendo responsable de la entrega de las líneas e interconexión con las centrales telefónicas de la Central. La configuración de las centrales telefónicas estará a cargo del personal de Universidad Nacional de Educación Enrique Guzmán y Valle.
- El postor deberá ser responsable del mantenimiento y disponibilidad de los equipos considerados para la prestación del servicio solicitado. En caso ocurra algún desperfecto en su operatividad durante la vigencia del contrato, el postor será responsable de asegurar la continuidad del servicio que este brindando.
- Deberá tener acceso gratuito a los servicios de emergencia.
- Deberá tener las siguientes bolsas mensuales para llamadas a cualquier hora del día:
 - 20,000 minutos a fijos en Lima (incluye las llamadas gratuitas del 0-800)
 - 1000 minutos a fijos en LDN.
 - 1000 minutos a fijos en LDI.
 - 72,000 segundos a celulares locales (cualquiera operador).
- Los minutos que excedan de la bolsa contratada tendrán el mismo costo por minuto de la bolsa y será asumido por la entidad.
- De llamar a destinos no considerados, el costo será asumido por la entidad.
- Servicio de tarificación transparente, es decir se deberá indicar de manera detallada las conexiones o llamadas salientes, así como los minutos reales consumidos en forma mensual, los que deberán llegar mensualmente vía correo electrónico (contrataciones@une.edu.pe con copia a redes@une.edu.pe) y en formato MS Excel. El informe mensual del servicio podrá ser presentado en un plazo máximo de cinco (5) días hábiles, contados a partir del día siguiente del cierre del ciclo de facturación correspondiente.
- El postor deberá entregar un acceso web donde la entidad podrá ver el consumo de llamadas cursadas en forma diaria, para los accesos sip trunk solicitados. En este acceso web se podrá identificar por línea aquellas que han generado llamadas diariamente (sistema de tarificación, consulta y administración).
- El operador no deberá aplicar restricciones de bloqueo para ningún tipo de llamada, sólo lo hará cuando la universidad se lo solicite por escrito a través del área responsable del servicio.
- El servicio debe estar disponible las veinticuatro (24) horas del día, los siete (7) días de la semana los trescientos sesenta y cinco (365) días del año. La disponibilidad del servicio debe ser al 99.5% mensual, caso contrario se ha de considerar como caída del servicio y estará sujeto a las penalidades correspondientes.
- Se tomará en cuenta para la disponibilidad del servicio los requerimientos técnicos mínimos establecidos por el ente regulador y se aplicará las penalidades cuando la caída del servicio sea por causa del operador.
- Una vez reportada una afectación al servicio esta será resuelta en un plazo máximo de 4 horas, debiendo precisarse que de ocurrir una afectación que requiera personal en campo, el tiempo de solución no deberá de exceder de 8 horas; no considerándose como indisponibilidad el tiempo de indisponibilidad causado por situaciones fortuitas o de causa mayor, o aquellas imputables al cliente.
- La entidad se reserva el uso del derecho a la portabilidad numérica en el servicio de telefonía fija.
- Los postores deberán considerar en su propuesta normas y estándares reglamentados por el OSIPTEL y el MTC que aseguren el correcto funcionamiento de todos los enlaces.

6.7. ATENCIÓN DE AVERÍAS

Av. Enrique Guzmán y Valle 951, La Cantuta - Chosica
Teléfono: 313-3700, anexos 1820
web: www.une.edu.pe Email: soplecvtredes@une.edu.pe



Firmado digitalmente por:
MORI GARCIA Willy Otmar
FAU 20174950971 hard
Motivo: Soy el autor del
documento
Fecha: 29/09/2026 14:19:59-0500



1319

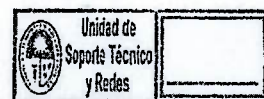
- Se entenderá por avería a una interrupción parcial o total del servicio, así como a un decremento en la calidad de este; puesto que cualquier degradación de servicio afecta el buen funcionamiento del Servicio de Internet.
- Toda actividad o provisión de bienes que tenga que ejecutar el POSTOR GANADOR para subsanar la avería serán sin costo alguno para la UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE, salvo el caso en que la avería sea imputable a la UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE.
- Se entenderá por Tiempo de Atención, al tiempo transcurrido desde que la UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE comunique vía telefónica o genere el ticket de atención hasta que el Postor reciba el detalle de la avería a través de la plataforma de ticket, este tiempo no excederá de 30 minutos. Se entenderá por Tiempo de Subsanación, al tiempo transcurrido que demore el POSTOR GANADOR en solucionar la avería reportada, el tiempo no deberá exceder de 04 horas, pero para el tiempo de subsanación de avería en la sede Chosica será de ocho (08) horas contabilizadas después de la entrega del ticket de atención y/o llamada telefónica.
- La UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE solamente reportará a un único número telefónico el cual será una ventanilla única que atenderá todas las averías del servicio contratado, permitiendo un adecuado control, gestión y seguimiento de la misma. El POSTOR GANADOR deberá contar con un número gratuito para la atención de las llamadas.
- La UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE podrá efectuar llamadas de servicio de lunes a domingo incluyendo feriados desde las 00:00 hasta las 24:00 horas. El POSTOR GANADOR deberá contar con un centro de atención de llamadas de reparación o asistencia técnica instalado de tal manera que le asegure a la UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE que se encuentra en condiciones de cumplir con lo estipulado en las bases.
- El POSTOR GANADOR deberá entregar al área usuaria una relación de contactos responsables para asegurar la continuidad del servicio; donde solamente para los casos donde las averías reportadas vía llamada telefónica o ticket generado no sea atendido y no se tenga respuesta alguna de una posible solución al problema reportado dentro de los SLA, así como para realizar coordinaciones operativas, administrativas y de facturación durante la ejecución del servicio, el cual deberá presentar como sustento en la etapa de ejecución del servicio.
- El Tiempo de disponibilidad del servicio para los servicios instalados en la zona de Lurigancho Chosica será de 98.9%, esto debido a que se encuentra en la zona interurbana y para los servicios instalados en las zonas de la Molina y el Rímac es de 99.5%.

6.8. CALIDAD DEL SERVICIO

- El servicio se contratará bajo la modalidad de atención de 7 x 24.
- EL POSTOR GANADOR deberá garantizar el profesionalismo, responsabilidad y conocimientos técnicos de su personal en los Centros de Llamadas de Reportes de Fallas, Centros de Gestión, y personal de Reparación de Averías. Así mismo deberá contar con el equipamiento necesario para solucionar los problemas técnicos que se presenten, en cada una de las ciudades antes mencionadas.
- Ante los casos de pérdida de servicio por avería de planta externa (fibra óptica), normalmente se ocasionan por factores externos como cortes del cable, incendios, derrumbe de postes el contratista deberá realizar dicha reparación del servicio hasta un máximo de 8 horas adicionales al tiempo de subsanación por pérdida de servicio.

6.9. INSPECCIÓN Y PRUEBAS





1318

- El POSTOR GANADOR y el personal de la UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE, una vez terminada la instalación, realizarán en forma conjunta los procedimientos de inspección y pruebas sobre la infraestructura y equipos instalados, de tal forma que le permita, establecer que el servicio será brindado de conformidad con lo requerido en las bases y en la propuesta del POSTOR GANADOR.
- Las pruebas se realizarán en el lugar de instalación. Los costos que demanden las mismas, no implicarán en ningún caso reconocimiento de gastos por parte de la UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE y serán provistos por el POSTOR GANADOR.
- Cualquier defecto notificado por la UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE al POSTOR GANADOR durante la realización de las pruebas de aceptación, será rectificado por este sin cargo alguno, teniendo como plazo máximo 7 (siete) días calendario a partir de su notificación.
- Una vez realizados los procedimientos de inspección y pruebas a conformidad de UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE, éste levantará y entregará al POSTOR GANADOR el Acta de Inicio de Operaciones mediante un documento formal.
- Las pruebas de inspección y validación se ejecutarán de acuerdo con la arquitectura implementada en cada sede. El alcance, procedimiento y criterios de aceptación de las pruebas serán definidos y aprobados en coordinación entre la Entidad y el contratista durante la etapa de implementación, verificando el cumplimiento de las especificaciones técnicas y el correcto funcionamiento de la solución.

6.9.1. Actividades

El proveedor adjudicado deberá ejecutar, como mínimo, las siguientes actividades durante la prestación del servicio:

a. Implementación de la infraestructura

- Realizar el tendido de fibra óptica desde el punto de presencia del proveedor hasta las sedes de la universidad.
- Instalar routers, equipos de acceso, firewalls y demás dispositivos necesarios para la prestación del servicio.
- Ejecutar las obras civiles, canalizaciones y permisos necesarios para la instalación de la infraestructura.

b. Configuración de los servicios

- Configurar los enlaces de Internet dedicados según los anchos de banda establecidos.
- Configurar el direccionamiento IP público asignado a la institución.
- Configurar los servicios de DNS y registro de dominios y subdominios.
- Implementar la red privada de transmisión de datos entre sedes.

c. Implementación de la seguridad perimetral

- Instalar y configurar los equipos NGFW en las sedes de la Universidad.
- Configurar políticas de seguridad, filtrado de contenido, control de aplicaciones y prevención de intrusiones.
- Implementar túneles VPN entre sedes.
- Configurar alta disponibilidad para los firewalls en la sede principal

d. Implementación del servicio de telefonía

- Instalar y configurar el enlace SIP Trunk.



1317

- Integrar el servicio con la central telefónica Yeastar S300.
- Configurar las sesiones de comunicación y los planes de llamadas.

e. Monitoreo y gestión del servicio

- Monitorear permanentemente el estado de los enlaces y equipos.
- Proporcionar acceso web para monitoreo de tráfico y consumo de ancho de banda.
- Generar reportes periódicos de uso y desempeño del servicio.

f. Atención de incidencias

- Atender reportes de averías las 24 horas del día, los 7 días de la semana.
- Garantizar tiempos de atención y solución establecidos en el contrato.
- Mantener personal técnico especializado para la resolución de incidentes

g. Pruebas y puesta en operación

- Realizar pruebas de funcionamiento y aceptación del servicio junto con el personal de la universidad.
- Subsanan cualquier observación detectada durante las pruebas.
- Suscribir el acta de inicio de operaciones una vez verificado el correcto funcionamiento del servicio.

6.10. SEGUROS

No corresponde

6.11. CAPACITACIÓN

El proveedor adjudicado deberá brindar capacitación al personal designado por la Universidad Nacional de Educación Enrique Guzmán y Valle (UNE), con la finalidad de asegurar el adecuado uso y comprensión del servicio de internet dedicado con seguridad gestionada.

La capacitación deberá contemplar como mínimo los siguientes aspectos:

a) Capacitación en administración del servicio de Internet

- Monitoreo del consumo de ancho de banda.
- Interpretación de reportes de tráfico y disponibilidad del servicio.
- Uso de la plataforma web de monitoreo proporcionada por el proveedor.
- Procedimientos para reporte y escalamiento de incidencias.
- 2 horas de duración como mínimo.

b) Capacitación en administración de la solución de seguridad (Firewall NGFW)

- Acceso a la consola de administración del firewall.
- Creación y modificación de políticas de seguridad.
- Configuración de reglas de firewall.
- Gestión de control de aplicaciones.
- Administración del filtrado web.
- Revisión de registros de eventos (logs).
- Generación de reportes de seguridad.
- Configuración y monitoreo de VPN (Red Privada Virtual).
- SOC (Centro de Operaciones de Seguridad).
- Gestión de incidentes (Atención y respuesta ante incidentes de seguridad).



- Análisis de logs (Revisión de registros de eventos).
- 8 horas de duración como mínimo.

c) Modalidad de la capacitación

- La capacitación podrá realizarse de manera presencial o virtual, según coordinación con la entidad.
- El proveedor deberá proporcionar material de capacitación digital o impreso, incluyendo manuales técnicos y guías de operación.

d) Participantes

- La capacitación estará dirigida a un máximo de 22 profesionales designados por la Unidad de Soporte Técnico y Redes de la Universidad.

e) Constancias

- El proveedor deberá otorgar constancias o certificados de participación a los asistentes que culminen la capacitación.

6.12. SOPORTE TÉCNICO

- El contratista proveedor deberá contar con un centro de soporte técnico o similar, propio o tercerizado, que opere local 24x7 en formato 24x7x365, las 24 horas del día durante los 365 días del año, incluyendo los domingos y feriados. Este centro debe estar en idioma español, permitiendo la apertura de soporte debe contar con personal especializado para la resolución de incidencias mediante llamada telefónica y/o plataforma de averías en los equipos y/o servicios ofrecidos. Para tal fin, se entenderá por avería una interrupción parcial, total y/o degradación del servicio bajo soporte técnico.
- El servicio debe contar con un Centro de Operaciones de Seguridad (SOC) propio y/o tercerizado. Debiendo contar con personal especialista de soporte que estará en el SOC, deberá atender de manera remota y contar con acceso a los equipos de seguridad perimetral para las atenciones a la entidad. y trazabilidad de los casos reportados durante toda la vigencia del servicio.
- Al requerir la entidad, uno o varios cambios en las políticas y/o configuraciones de los equipos de seguridad perimetral, este se reportará al CONTRATISTA por teléfono o correo electrónico o chat. Cabe indicar que el contratista atenderá de manera ilimitada los cambios en las políticas y/o configuraciones, sin restricción de cantidad de solicitudes y sin costos adicionales.
- El ticket será cerrado, cuando se solucione el incidente y se obtenga la correspondiente aprobación por parte del personal de la entidad.
- El soporte proporcionado será por telefónico, remoto y/o on-site, dependiendo de la severidad del caso.
- El SOC del postor (propio o tercerizado) que atienda los incidentes y casos reportados, deberá estar en Perú y contar con la Certificación ISO 27001 en los procesos de gestión de incidentes, gestión de cambios y ciberseguridad y la Certificación ISO 27035 en los procesos de gestión de incidentes, gestión de cambios, gestión de ciberseguridad,



Firmado digitalmente por:
MORI GARCIA Willy Otmar
FAU 20174950971 hard
Motivo: Soy el autor del
documento
Fecha: 29/09/2020 14:20:33-0500



1315 operando las 24 horas del día en los 7 días a la semana por 365 días (24x7x365-adjuntar declaración jurada de la disponibilidad del personal, el cual deberá presentar como sustento en la etapa de presentación de la oferta.

7. GARANTÍA COMERCIAL

El proveedor deberá otorgar una garantía de treinta y seis (36) meses (3 años) a partir de la fecha de conformidad del servicio, la cual deberá cubrir cualquier falla derivada de una ejecución deficiente del servicio de internet dedicado con seguridad gestionada.

8. RECURSOS A SER PROVISTOS POR EL CONTRATISTA

No corresponde

9. MEDIDAS DE CONTROL DURANTE LA EJECUCIÓN CONTRACTUAL

Área encargada de coordinar con el contratista: Unidad de Soporte Técnico y Redes.
Área responsable de las medidas de control: Unidad de Soporte Técnico y Redes.

10. ENTREGABLES

El postor ganador deberá presentar los siguientes documentos, de acuerdo con lo establecido en la siguiente tabla:

Entregable	Tipo	Forma Entrega	Informe Técnico debe incluir lo siguiente	FRECUENCIA		
				P	C	M
Informe de implementación del servicio	Acta	Digital	• Diagrama de la arquitectura de red implementada. • Detalle de los enlaces instalados por sede. • Direccionamiento IP público asignado a la entidad. • Configuración básica de los equipos instalados (routers, firewalls u otros dispositivos). • Registro de dominios y subdominios configurados. • Documentación de la configuración de VPN entre sedes. • Resultados de las pruebas de conectividad y rendimiento realizadas.	X		
Acta de instalación y puesta en operación	Informe	Digital	• Instalación de los enlaces de Internet. • Instalación de los equipos de comunicaciones. • Instalación y configuración de los equipos de seguridad. • Pruebas de conectividad y disponibilidad del servicio. • Acta de Inicio del Servicio (Con firma por parte del proveedor y el área usuaria)	X		



Documentación técnica del servicio	Informe	Digital	• Diagramas de red lógica y física. • Manual de operación básica de la solución implementada, elaborado por el contratista, el cual deberá incluir como mínimo los procedimientos básicos de operación, acceso, monitoreo, respaldo y restauración de la configuración, así como la referencia o enlaces oficiales a la documentación técnica y guías de administración publicadas por el fabricante, correspondientes a la versión de la solución implementada. • Procedimientos de contacto para soporte técnico y escalamiento de incidentes. • Relación del personal de contacto del proveedor.	X		
Informe de capacitación	Acta de Entrega	Digital	• Temario desarrollado. • Lista de participantes. • Constancias de participación emitidas.		X	
Reportes mensuales del servicio	Informe	Digital	• Disponibilidad del servicio de Internet. • Consumo de ancho de banda por enlace. • Incidentes reportados y tiempo de atención. • Estadísticas de tráfico y uso del servicio. Reporte de eventos de seguridad generados por la solución Firewall o por la plataforma de gestión, analítica y reportaría que forme parte de la solución ofertada, incluyendo ataques DDoS detectados y mitigados, siempre que la información provenga de los equipos de seguridad implementados y cumpla con el contenido mínimo requerido por la Entidad.			X
Leyenda						
P	(10) días calendarios posteriores al acta de culminación de la implementación del servicio.					
C	(10) días calendarios posteriores a la realización de la capacitación.					
M	Mensual (15) días calendarios posteriores al cierre del ciclo de facturación					

La documentación requerida deberá remitirse en formato digital (PDF o Excel), podrá ser a través de Mesa de Partes física o virtual (digital) con copia a la Unidad de soporte Técnico y Redes mediante correo electrónico soptecyredes@une.edu.pe.



1314

Mesa de Partes Física:

- Dirección: Av. Enrique Guzmán y Valle N°951, La Cantuta – Chosica.
- Horario de Atención: De lunes a viernes de 8:00 a.m. a 4:00 p.m.

Mesa de Partes Virtual

- Correo Electrónico: tramite@une.edu.pe
- Plataforma Web: <https://apps.une.net.pe/mpvf/vistas/principal3.html>
- Horario de Atención: De lunes a viernes de 9:00 a.m. a 5:00 p.m.

Para los Reportes mensuales del Servicio la disponibilidad mensual será calculada en función del tiempo acumulado de indisponibilidad (caídas o interrupciones del enlace) el cual será registrado durante el período mensual, expresado como porcentaje respecto al tiempo total del mes, considerando únicamente las averías atribuibles al proveedor y excluyendo mantenimientos programados previamente comunicados y eventos no imputables al contratista.

11. CONFORMIDAD DE LA PRESTACIÓN

La conformidad será emitida por el jefe de la Unidad de Soporte técnico y Redes en un plazo máximo de 7 días calendarios, contabilizados desde el día siguiente de la recepción del entregable. Conforme a lo establecido en el artículo 144 del Reglamento de la Ley General de Contrataciones Públicas.

12. FORMA DE PAGO

- La Entidad realizará el pago de la contraprestación pactada a favor del contratista en forma parcial mensualmente por el monto equivalente a 1/36 del valor contratado, para cuyo efecto debe contar con la siguiente documentación:
- La conformidad del Servicio que será otorgada por el jefe de la Unidad de Soporte Técnico y Redes de la UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE.
- Comprobante de pago original (factura).
- El contratista estará facultado para emitir el comprobante de pago (factura) correspondiente dentro de los siete (7) días calendario posteriores a la culminación de cada período mensual de prestación del servicio, siempre que la Unidad de Soporte Técnico y Redes no haya comunicado observaciones relacionadas con el cumplimiento de las obligaciones contractuales y haya emitido la conformidad de la prestación correspondiente.
- La Entidad debe efectuar el pago dentro de los diez (10) días calendario siguientes al otorgamiento de la conformidad respectiva, siempre que se verifiquen las demás condiciones establecidas en el contrato.
- El ciclo de facturación inicia con la suscripción del Acta de Inicio del Servicio (Con firma por parte del proveedor y el área usuaria).
- La documentación para el pago deberá remitirse de manera física o en formato digital (PDF), a través de Mesa de Partes física o virtual (digital) con copia a la Unidad de soporte Técnico y Redes mediante correo electrónico sopotecyredes@une.edu.pe.
- Mesa de Partes Física:
 - Dirección: Av. Enrique Guzmán y Valle N°951, La Cantuta – Chosica.
 - Horario de Atención: De lunes a viernes de 8:00 a.m. a 4:00 p.m.





• Mesa de Partes Virtual

- Correo Electrónico: tramite@une.edu.pe
- Plataforma Web: <https://apps.une.net.pe/mpvf/vistas/principal3.html>
- Horario de Atención: De lunes a viernes de 9:00 a.m. a 5:00 p.m.

Luego de transcurridos 03 meses sin que la entidad haya cancelado la contraprestación mensual correspondiente al servicio prestado por el contratista, el operador de telecomunicaciones podrá suspender el servicio por falta de pago, sin que ello implique la aplicación de penalidades y/o forme parte, en caso de corresponder, del porcentaje de cumplimiento del nivel de servicio requerido.

13. GESTIÓN DE RIESGOS

Se deben identificar los riesgos que esta enfrenta en la contratación, dichas actividades y acciones se realizan sobre la base de la identificación, análisis, valoración, gestión, control y monitoreo de riesgos, que permiten tomar decisiones informadas y aprovechar las oportunidades potenciales derivadas de estos.

A continuación, se presenta un análisis cualitativo y cuantitativo para los riesgos identificados.

Matriz de Riesgos

Riesgo	Probabilidad (P)	Impacto (I)	Nivel de Riesgo (P x I)	Tratamiento
Retraso en la instalación y puesta en funcionamiento de los enlaces de Internet y equipos de seguridad (routers, firewalls) (**)	4 (Alto)	5 (Muy Alto)	20 (Crítico)	Aplicación de penalidades por mora según contrato. Seguimiento del cronograma de implementación, coordinación permanente con el proveedor y supervisión técnica durante la instalación.
Ejecución deficiente del servicio o soporte técnico inadecuado (**)	3 (Medio)	4 (Alto)	12 (Medio)	Supervisión técnica permanente, revisión de reportes de servicio, validación de entregables y aplicación de penalidades en caso de incumplimiento.
Postor no acredita experiencia o capacidad técnica requerida (*)	3 (Medio)	4 (Alto)	12 (Medio)	Supervisión técnica permanente, revisión de reportes de servicio, validación de entregables y aplicación de





1311

Riesgo	Probabilidad (P)	Impacto (I)	Nivel de Riesgo (P x I)	Tratamiento
				penalizaciones en caso de incumplimiento.
Falta de proveedores en la indagación de mercado (*)	2 (Bajo)	4 (Alto)	8 (Bajo)	Revisar las especificaciones técnicas, diversificar las fuentes de búsqueda, comunicación directa con los proveedores, evaluar a los pocos proveedores para determinar la opción viable.
Contratar con proveedores no especializados o dedicados directamente al rubro de la necesidad (**)	4 (Alto)	5 (Muy Alto)	20 (Crítico)	Exigir al proveedor acreditar su experiencia en el rubro.
Incumplimiento de la garantía comercial (***)	4 (Alto)	5 (Muy Alto)	20 (Crítico)	La entidad se reserva el derecho de reclamar por defectos o vicios ocultos durante un plazo de un año a partir de la conformidad.

*Riesgos en el proceso de contratación

**Riesgos en la ejecución de la contratación

- ESCALA A USAR PARA DETERMINAR LA PROBABILIDAD (P) Y EL IMPACTO (I)
 - 1 = Muy Bajo
 - 2 = Bajo
 - 3 = Medio
 - 4 = Alto
 - 5 = Muy alto
- ESCALA A USAR PARA DETERMINAR EL NIVEL DE RIESGO (PxI)
 - 1 al 8 = Bajo
 - 9 al 16 = Medio
 - 17 al 25 = Crítico

14. REQUISITOS DE CALIFICACIÓN

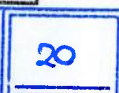
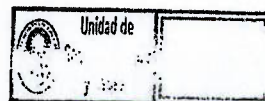
14.1. REQUISITOS DE CALIFICACIÓN OBLIGATORIOS

a. CAPACIDAD LEGAL

Requisitos:



Firmado digitalmente por:
MORI GARCIA Wily Otmar
FAU 20174950971 hard
Motivo: Soy el autor del documento
Fecha: 29/09/2026 14:21:13-0500



El postor deberá estar autorizado por el Ministerio de Transportes y Comunicaciones para la prestación de servicio de Internet de cobertura Nacional.

Acreditación:

Copia de autorización emitida por el MTC y/u Oficio del MTC con las concesiones y autorizaciones vigentes y/o la impresión de la página web del MTC donde se visualice la relación de empresas prestadoras de valor añadido y/o certificado de inscripción en el registro en el registro para servicios de valor añadido para prestar el servicio de internet y/o Conmutación de datos por paquetes (Internet) emitido por el MTC y/o Copia Simple del Registro o Autorización del Ministerio de Transporte y Comunicaciones (MTC) como Empresa Prestadora de Servicios de Valor Añadido en Telecomunicaciones.

b. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Requisitos:

El postor debe acreditar un monto facturado acumulado equivalente a a S/ 1,500,000.00 (UN MILLÓN QUINIENTOS MIL CON 00/100 SOLES), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los quince (15) años anteriores a la fecha de la presentación de ofertas que se computa desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran bienes similares a los siguientes: Servicio de internet dedicado y/o Servicio de Acceso Dedicado a Internet y/o Servicio de Transmisión de Datos y/o Enlaces de Datos y/o Enlace de Comunicación Punto a Punto y/o Servicios de Conectividad Mediante Fibra Óptica y/o Servicio de Acceso a Internet y/o Servicio Integral de Telecomunicaciones, Servicios de seguridad gestionada y/o implementación o gestión de firewall y/o servicio de transmisión de datos y/o Servicio de Transmisión de Voz y Datos y/o Servicio de Acceso Dedicado a Internet Enlace de Comunicación Punto a Punto y/o Servicio de Plan de Datos y/o Servicio de plan de telefonía y datos servicios de seguridad perimetral y/o servicios de redes y comunicaciones y/o servicios de conectividad de red y/o otros servicios relacionados a infraestructura de redes y telecomunicaciones.

Acreditación:

La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de compra, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con constancia de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago⁵, o comprobante de retención electrónico emitido por SUNAT por la retención del IGV, correspondientes a un máximo de veinte contrataciones. En caso el postor sustente su experiencia en la especialidad mediante contrataciones realizadas con privados⁶, para acreditarla debe presentar de forma obligatoria lo indicado en el numeral (ii) del presente párrafo; no es posible que acredite su experiencia únicamente con la presentación de contratos u órdenes de compra con conformidad o constancia de prestación.





1310

14.2. REQUISITOS DE CALIFICACIÓN FACULTATIVOS - CAPACIDAD TÉCNICA Y PROFESIONAL

a. Experiencia del personal clave

- Un (01) Jefe de Proyecto

Requisitos:

Experiencia general:

Deberá acreditar una experiencia mínima de dos (02) años en el sector público y/o privado, desempeñando funciones como jefe y/o gerente y/o supervisor y/o coordinador y/o en cargo similar de nivel de responsabilidad.

Experiencia específica:

Deberá acreditar experiencia en:

- Proyectos de conexión de datos e internet y/o servicios de conmutación de paquetes, y/o servicios de telecomunicaciones.
- Gestión y coordinación de proyectos TI y/o gestión y/o supervisión y/o implementación de proyectos de tecnologías de información.
- Proyectos de telecomunicaciones para los servicios de acceso de Servicios Internet y/o Internet dedicado y/o transmisión de datos empresarial.

- Un (01) Especialista en Redes y Seguridad de la Información

Requisitos:

Deberá acreditar mínimo dos (02) años en el sector público y/o privado, desempeñándose como especialista y/o analista y/o y/o proyectos ingeniero en seguridad informática o seguridad de redes, y/o en cargo similar de nivel de responsabilidad, con experiencia en implementación y/o configuración y/o administración de equipos de seguridad para servicios de acceso a internet y/o internet dedicado y/o conexiones de enlace de datos y/o gestión de soluciones de seguridad informática y redes.

Acreditación:

El postor debe señalar la denominación del puesto, cargo y/o posición, y tiempo de experiencia del personal clave propuesto (años, meses y días) en el Anexo N° 19, adjuntando en su oferta, copia simple de cualquiera de los siguientes documentos: (i) contratos y su respectiva conformidad; (ii) constancias; (iii) certificados; o (iv) cualquier otra documentación que, de manera fehaciente, demuestre la experiencia del personal propuesto.

Asimismo, la acreditación de las capacitaciones y/o certificaciones del personal clave se realizará mediante copia simple de certificados emitidos por la entidad u organización correspondiente. En el caso de la experiencia de Metodologías Ágiles serán validadas en la web o URL de la entidad certificadora.

Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el



día, mes y año de inicio y culminación, el nombre de la entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.

b. Formación académica

- Un (01) Jefe de Proyecto

Requisitos:

Deberá contar con el Título Universitario en Ingeniería de Sistemas y/o Computación y/o Informática y/o Telecomunicaciones y/o Redes y/o Ingeniería de sistemas e informática y/o Ingeniería de software y/o Ingeniería de telecomunicaciones e informática y/o Ingeniería en computación y/o Ingeniería Electrónica.

- Un (01) Especialista en Redes y Seguridad de la Información

Requisitos:

Debe contar con título y/o bachiller Universitario en las carreras de Ingeniería de Sistemas y/o Ingeniería de Sistemas e Informática y/o Ingeniería Informática y de Sistemas y/o Ingeniería de Computación y/o Ingeniería en Ciencias de la Computación y/o Ingeniería en Telecomunicaciones y/o Ingeniería de Telecomunicaciones y Redes y/o Ingeniería de Telecomunicaciones e Informática y/o Ingeniería en Redes y/o Ingeniería de Redes y Comunicaciones y/o Ingeniería de Software o Ingeniería Electrónica o Ingeniería Electrónica y Telecomunicaciones o con mención en Telecomunicaciones.

Acreditación:

El Postor debe contar con título y/o bachiller será verificado por en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: <https://enlinea.sunedu.gob.pe/> o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: <https://titulosinstitutos.minedu.gob.pe/>, según corresponda.

c. Capacitación del Personal Clave

- Un (01) Jefe de Proyecto

Requisitos:

Deberá acreditar contar con las siguientes certificaciones:

- Certificado PMP.
- Capacitación mínima de cuarenta (40) horas en gestión de Servicios ITIL, y/o, certificación ITILv4 mínimo.
- Diploma en Gerencia de Proyectos y Calidad, con un mínimo de 120 horas lectivas de estudio.
- Programa Integral en Ciberseguridad en la Protección de Infraestructura de Red mínimo 120 horas.
- Curso o Capacitación de la Norma ISO 31000:2018 como mínimo 15 horas.

- Un (01) Especialista en redes y Seguridad de la Información

Requisitos:



Firmado digitalmente por:
MORI GARCIA Wily Otmar
FAU 20174950971 hard
Motivo: Soy el autor del documento
Fecha: 29/09/2020 14:21:37-0500

1308



**Universidad Nacional de Educación
Enrique Guzmán y Valle**
"Alma Máter del Magisterio Nacional"

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
UNIDAD DE SOPORTE TÉCNICO Y REDES

"Año de la Esperanza y el Fortalecimiento de la Democracia"

Deberá acreditar Mínimo cincuenta (50) horas lectivas en curso de configuración, implementación y gestión de soluciones de seguridad perimetral y/o Certificación oficial en la marca de los Firewalls (al ser certificación oficial del fabricante no será exigible la acreditación de horas lectivas).