

REQUERIMIENTO

I. TÉRMINOS DE REFERENCIA

1. DENOMINACIÓN DE LA CONTRATACIÓN

Contratación del servicio de acceso a internet para el Ministerio de Economía y Finanzas.

2. ACTIVIDADES DEL POI

Operación, mantenimiento y seguridad de las plataformas e infraestructuras informáticas del Ministerio.

3. FINALIDAD PUBLICA

La contratación del servicio de Internet para el Ministerio permitirá que los diferentes aplicativos informáticos web, así como el correo electrónico puedan operar en forma satisfactoria sin afectar su servicio.

4. OBJETIVOS DE LA CONTRATACIÓN

4.1. Objetivo General

Mantener la disponibilidad de los servicios informáticos que el Ministerio pone a disposición a través de internet, así como el intercambio de información con terceros.

4.2. Objetivo Específico

- Contratar un servicio de acceso a internet principal, por un periodo de 24 meses.
- Contratar un servicio de acceso a internet secundario, por un periodo de 24 meses.
- Contratar un servicio de acceso a internet auxiliar, por un periodo de 24 meses.
- Garantizar la continuidad de servicios (contingencia de operador). Para lo cual cada servicio (principal y secundario), debe ser de diferente ISP.
- Garantizar la alta disponibilidad del servicio de acceso a internet a nivel de ISP considerando un enlace de fibra a cada Datacenter.
- Realizar pruebas de acceso a internet y conectividad a fin de identificar problemas en los servicios que brindar el Ministerio a los usuarios externos.

5. CARACTERÍSTICAS Y CONDICIONES DEL SERVICIO A CONTRATAR

Se requiere contratar el servicio de internet, al que se referirá en adelante como EL SERVICIO:

5.1. DESCRIPCIÓN Y CANTIDAD DEL SERVICIO A CONTRATAR

Se requiere contratar tres (03) servicios de acceso a internet: un enlace principal y uno secundario en donde cada uno de ellos debe ser de diferente Proveedor de Servicios de Internet (ISP - Contratista) a fin de garantizar la continuidad de servicios (contingencia de operador)¹, el servicio de internet de cada uno de estos ISP debe considerar un enlace a cada Datacenter.

Ítem	Denominación del ítem	Ubicación	Overbooking		Capacidad
			Local	Internacional	
1	Servicio de acceso a internet principal	Lampa 255	1:1	1:1	1 Gbps
2	Servicio de acceso a internet secundario	Lampa 255	1:1	1:1	1 Gbps
3	Servicio de acceso a internet auxiliar	Lampa 255	1:1	1:1	20 Mbps

En relación a los Ítems 1 y 2: como parte de la plataforma informática de alta disponibilidad se requiere disponer de enlaces de telecomunicaciones y acceso a Internet redundantes, para lo cual es necesario contratar con el servicio de acceso a Internet de dos operadores ISP (Contratistas) diferentes, en **una arquitectura que garantice la disponibilidad y continuidad**

¹ Es decir, un postor debe postular únicamente de la siguiente manera; solo al ítem 1 o solo al ítem 2 o solo al ítem 3 o al ítem 1 y 3 o al ítem 2 y 3; esto fin de garantizar que se pueda cumplir el principio de contingencia de proveedores.

del servicio para cumplir con los objetivos institucionales (enlace principal y enlace secundario).

De ser necesario para la elaboración de la oferta, los participantes en el procedimiento de selección podrán realizar los estudios de campo y visitas pertinentes a los locales del Ministerio (Datacenter) a fin de que puedan verificar in situ las condiciones de la implementación; deberán solicitar las facilidades de acceso e información adicional a la siguiente dirección de correo: networking@mef.gob.pe.

Un proveedor podrá ser adjudicado al ítem 1 y 3; o al 2 y 3; sin embargo, un mismo proveedor no podrá ser adjudicado a los ítems 1 y 2 simultáneamente, a fin de garantizar la contingencia de proveedor entre los enlaces principal y secundario.

Los servicios de acceso a Internet deben ser implementados en un esquema 7x24x365 durante un periodo de 24 meses con los siguientes ítems:

5.2. ITEM 01: SERVICIO ACCESO A INTERNET- PRINCIPAL

TIPO ENLACE	VELOCIDAD MINIMA ENLACE	OVERBOOKING LOCAL	OVERBOOKING EN LA SALIDA INTERNACIONAL	ORIGEN
Enlace principal	1 Gbps	1.1	1.1	Jr. Lampa N° 255 Cercado de Lima

El enlace (del ISP al Ministerio) será dedicado y de fibra óptica con canalización subterránea hacia la sede Lampa, el cual está destinado al acceso de los usuarios internos y externos del Ministerio desde y hacia Internet. El contratista debe conectar el servicio de acceso a internet principal con fibra óptica con canalización subterránea, independiente (no compartida) y exclusiva para este enlace desde uno de sus nodos, hacia el datacenter de la sede Lampa 255 y otro enlace de fibra óptica con canalización subterránea independiente (no compartida) y exclusiva para este enlace desde un nodo diferente al anterior hacia el datacenter ubicado en Jr. Lampa 274, permitiendo al Ministerio gestionar la contingencia de manera automática. Ambos enlaces siempre deben operar de forma independiente, se especifica que el contratista debe de implementar el tramo de última milla de nodos distintos, totalmente nuevo específicamente para esta contratación, no se aceptarán tendidos de contrataciones previas con el MEF, mediante tendidos independientes de fibra óptica (por la fibra solo debe pasar el servicio de internet solicitado), y que conecte hacia dos nodos independiente del ISP.

El servicio debe contar con una capa de filtro web, filtro de aplicaciones tolerado desde el data center del operador a través de una solución en arquitectura de alta disponibilidad y de uso exclusivo para el Ministerio. El data center debe contar con certificaciones Uptime TIER III (mínimo en diseño) o ANSI/TIA 942 Rated 3. [Se aceptará que el datacenter sea arrendado, el contratista deberá asumir la responsabilidad de garantizar la disponibilidad del servicio.](#)²

El filtro web solicitado deberá contar con las siguientes características:

- a) Capacidad de Prevención de Malware de Dia Cero o no conocido para el servicio de Internet (mediante emulación de malware – SandBox en nube).
- b) Capacidad de Extracción de Malware o extracción del contenido activo riesgoso de los documentos descargado a través del servicio de Internet.
- c) Capacidad de Prevención de Phishing de Dia Cero o phishing no conocido para el servicio de Internet, que no pueda ser identificado mediante técnicas de reputación de URL y/o dominios.

Las características de la solución de filtro web serán acreditadas en el Anexo B - Características de la solución de filtro web, dicho anexo se presentará para la admisión de la oferta y para la firma del contrato, conforme lo siguiente:

² Absolución de consulta N° 66

- (i) Para la admisión de la oferta, se debe describir lo señalado en el Anexo B - Características de la solución de filtro web.
- (ii) Para la forma del contrato, se debe describir lo señalado en el Anexo B - Características de la solución de filtro web y adicionalmente presentar la siguiente documentación: Folletos, brochures, certificados, catálogos, instructivos, hojas de datos y/o manuales técnicos de los equipos descritos en el Anexo B - Características de la solución de filtro web”, dichos documentos se deben presentar en idioma castellano o en su defecto, acompañado de traducción.
Solo se aceptará carta del fabricante o subsidiaria local del fabricante o representante acreditado en el país, cuando se sustente alguna característica solicitada que no se encuentren en los documentos mencionados; asimismo, se precisa que la acreditación debe ser emitida al postor y no a la Entidad.³

Las capacidades del servicio de Internet, relacionado al filtro web y seguridad, deben tener las siguientes características de rendimiento: en NGFW de 17 Gbps y en Prevención de Amenazas (Threat Prevention) de 7 Gbps y 8MM de conexiones concurrentes.

La fibra debe cumplir con:

- Recomendación UIT-T G.652.D,
- IEC 60793-2-50,
- UIT G.652B,
- G.6522D,
- Norma Internacional IEC 60793-2-50 Tipo B.1.3 Especificación de fibra óptica,
- Telcordia GR-20-CORE,
- ANSI / ICEA S-87-640 y
- RUS 7CFR 1755.900.

Los enlaces no serán en ningún tramo de propiedad del contratista que se adjudique al ítem 2.

El contratista deberá contar como mínimo con 2 proveedores TIER 1 y que cuente con las salidas internacionales de al menos uno de 40 Gbps, asimismo la red del contratista deberá estar en capacidad de soportar IP Multicast.

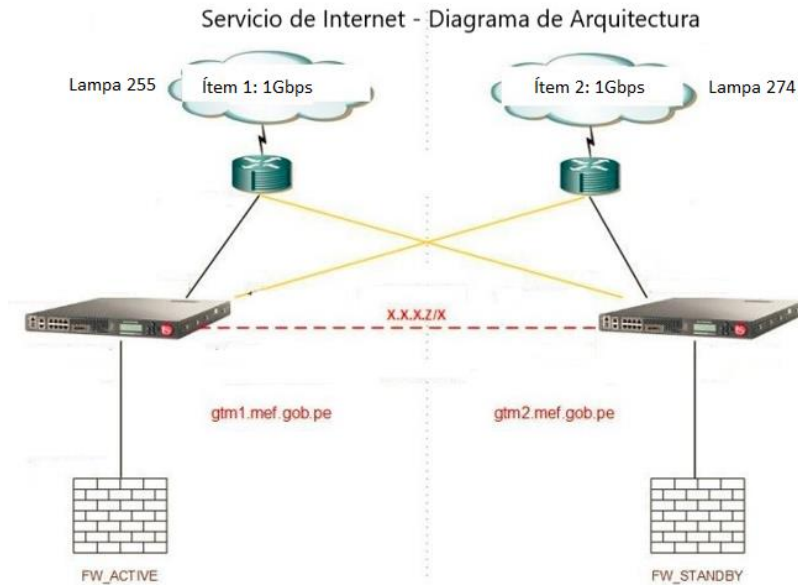
El contratista deberá proveer equipos para balanceos de enlaces, anti DDos, equipos de administración de ancho de banda, entre otros, los cuales deben ser nuevos y de primer uso.

El esquema a implementar debe considerar una alta disponibilidad del servicio y balanceo del tráfico entre: i) el enlace correspondiente al ítem 1 y ii) el enlace secundario correspondiente al ítem 2. Para este efecto, el contratista deberá proporcionar el equipamiento necesario para realizar la configuración, de manera que cualquier interrupción o falla de alguno de los enlaces (tráfico entrante y saliente), este, se dirija hacia el enlace disponible, de forma automática y mantenga así la continuidad del servicio.

La solución debe permitir que El Ministerio decida qué tipo de tráfico entra y sale por cada uno de los centros de datos en forma automática y sin gestión de ningún operador manual.

El Contratista será el encargado de integrar el enlace proveniente del Ítem 2. El Ministerio será el encargado de realizar las coordinaciones con los Contratistas de los enlaces.

³ Absolución de consulta N° 2, 10, 15, 27, 116, 158



A nivel de equipos balanceadores de tráfico de internet, se requiere dos equipos, uno debe ser instalado en el Jr. Lampa 255 y el segundo en el Jr. Lampa 274, ambos equipos deben estar configurados en alta disponibilidad (activo-pasivo).

Con respecto al equipo administrador de ancho de banda no se está solicitando como requerimiento mínimo la configuración de alta disponibilidad.

5.2.1. Servicios Incluidos

5.2.1.1. Servicio de Implementación

Será responsabilidad del contratista la instalación de la solución ofertada en su totalidad, dentro del plazo ofrecido, para lo cual debe proveer todos los bienes y servicios necesarios para su correcta instalación.

El Contratista será responsable de optimizar y configurar adecuadamente cada componente ofertado a satisfacción del Ministerio durante la etapa de instalación. El Contratista adjudicado estará encargado de hacer el levantamiento de información de la red del Ministerio, incluyendo configuraciones, políticas y tablas de ruteo, con la finalidad de que luego de la implementación, no existan problemas de comunicación y seguridad. El Ministerio designará un especialista técnico de contacto, que proporcionará información sobre el equipamiento del Ministerio. El Contratista debe hacer el levantamiento de información de la red del Ministerio, incluyendo configuraciones, políticas y tablas de ruteo.

El acceso a la sede debe ser subterráneo. El acceso a la sede Central del Ministerio debe ser por el Jr. Lampa 255 y Jr. Lampa 274.

En la etapa de activación del servicio el contratista debe realizar una prueba de saturación de ancho de banda, la cual debe quedar a satisfacción del Ministerio.

El contratista que resulte ganador debe cumplir con la implementación del servicio tanto en IP v4 como en IPv6, para lo cual el Ministerio proporcionará el listado de aplicaciones que deben trabajar bajo este requerimiento (el equipamiento debe soportar direccionamiento IPV6 así también, el contratista debe implementar un servicio de migración a IPV6 durante la implementación o posterior a ella).

5.2.1.2. Incluye Capacitación

Se debe considerar capacitación en la administración de los equipos proveídos, con una duración mínimo de 18 horas en temas relacionados a: configuración de protocolos de enrutamiento y análisis de tráfico, que incluya: Configuración de protocolos de enrutamientos básicos, Manejo y análisis de rutas, análisis avanzado de tráfico, balanceo de enlaces y aplicaciones, análisis de políticas de filtrado web y de aplicaciones, para un máximo de 06 personas del Ministerio, pudiendo ser realizada en las instalaciones de El Ministerio, tomando en cuenta que los equipos provistos son:

- Administración de ancho de banda.
- Balanceador de tráfico.
- Router y switches.
- Anti DDos

Dicha capacitación será realizada en el primer mes de la ejecución del servicio el cual será requisito para la emisión de la conformidad del primer pago, una vez finalizado la capacitación se suscribirá un acta de conformidad.

5.2.1.3. Herramienta de Servicio de Monitoreo

El contratista debe suministrar herramientas de monitoreo para la supervisión del funcionamiento de sus enlaces y principales dispositivos de la entidad, crear diagramas topológicos detallados de la Red en tiempo real. Analizador de Tráfico LAN y Sistema para gestión permanente y proactivo de Servicios, tales como:

A.- Monitoreo de Enlaces y Dispositivos Críticos

- a) Suministro del hardware y software requerido para uso exclusivo de la herramienta de monitoreo, incluir todas las licencias requeridas para su óptimo funcionamiento, el cual debe ser instalado en la Sede del cliente.
- b) Suministro e instalación de solución de monitoreo que permita el análisis y captura del flujo de tráfico generado para al menos 200 dispositivos o interfaces WAN o backbone.
- c) Esta solución debe permitir visualizar y analizar la variación de los flujos de tráfico al menos cada 60 segundos e incluir espacio de almacenamiento (storage) suficiente como para almacenar dicha información durante al menos (01) año manteniendo la granularidad de 60 segundos. Esta solución es un entregable del proyecto que será administrada por el Cliente y debe estar preparada para permitir un incremento del 25% de equipos y sin costo para la entidad, debe contar con los siguientes módulos activos, e implementados:
 - o Analizador de tráfico.
 - o Gestor de direcciones IP (al menos 5000 direcciones IP).
 - o Supervisión del Rendimiento de Red.
- d) La solución de monitoreo debe medir como mínimo:
 - o Tráfico de ancho de banda entrante y saliente en periodos: diario, semanal, mensual y anual.
 - o Monitorear la disponibilidad de los enlaces y mediciones críticas de la red, incluida la pérdida de paquetes, errores y descartes.
 - o Monitoreo del Hardware de los diferentes dispositivos de red.
 - o Historial de alarmas con umbrales personalizables.
 - o Consumo por aplicaciones, mínimo requerido: HTTP, HTTPS, SMTP, ICMP Y Netbios.
 - o Consumo según el puerto, protocolo y dirección IP o red.
 - o Soporte de VLAN's, dentro de las cuales se incluirán las de Gestión, Servidores, Voz, Video y Datos.
- e) La solución de monitoreo deberá permitir realizar diagramas topológicos detallados de la red en tiempo real (por lo menos en capa 2).
- f) La solución de monitoreo deberá permitir realizar diseño de Data center y Rack en 3D.
- g) Reportes estadísticos del comportamiento de los enlaces.
- h) La implementación de la solución de monitoreo deberá ser instalada en la sede de Ministerio, para ello se aceptará sea en una versión appliance o virtual, en caso sea virtual, el Ministerio, proveerá la máquina virtual para su implementación y el proveedor deberá incluir el sistema operativo (Windows o Linux), las bases de datos y el licenciamiento necesario de la herramienta.
- i) La solución de monitoreo debe permitir hasta diez (10) usuarios concurrentes.
- j) Generación de alertas mediante Email, SMS, IT Workflow, SNMP Trap Processing y web alarm.

- k) Debe permitir crear vistas en 3D del datacenter y los pisos con racks (frontal y real) y permita el monitoreo de los equipos en tiempo real para identificación de fallas utilizando código de colores, permitiendo la personalización del tamaño del piso. Tamaño del rack (42U, 38U, etc.) y tamaño de los dispositivos (2U, 1U, etc.) y rotación de la vista del mismo
- l) Deberá incluir un módulo de analítica que permita lo siguiente:
 - Información detallada para mejorar la disponibilidad y el rendimiento de la red permitiendo el análisis de los datos y presentar el comportamiento y las tendencias de la red utilizando al menos 100 KPIs.
 - Realizar el seguimiento del inventario y de la utilización de los recursos para optimizar la utilización actual y prever la planificación de la capacidad.
 - Correlacionar las tendencias de las alarmas con la frecuencia de los cortes.
 - La herramienta deberá ser implementada por personal certificado por la marca y deberá incluir una capacitación de al menos 24 horas.

B.- Herramienta Automate Mapping y Troubleshooting

- a) El Contratista debe implementar una solución completa que permita crear diagramas topológicos detallados de la Red en tiempo real, así como guardar el historial de los registros. Debe permitir descubrir como mínimo, los siguientes tipos de equipos (Router, Switches L2, Switches L3, Firewall, Load Balancers, WAN Optimizer, WAPs). La solución debe recopilar la información de los equipos descubiertos por SNMP capturando como mínimo: Dirección IP, Marca, Modelo, MAC y debe tener la opción de poder exportar esta información del inventario de los equipos descubiertos en un archivo MS Excel/CSV. Asimismo, debe disponer la opción de documentar la información recopilada y deberá exportarla en un archivo PDF y/o Word.
- b) La solución debe permitir exportar los mapas/diagramas de red en formato MS Visio, asimismo debe ser capaz de descubrir e identificar como mínimo seis mil (6,000) tipos de dispositivos y al menos 300 diferentes marcas/modelo de equipos en la red. Debe visualizar el Troubleshooting en tiempo real, diagnosticando el diseño y resaltar los errores o problemas en la configuración (BGP, OSPF, RIP Routing).
- c) Capacidad de visualización de la red usando la integración de Google map con el objetivo de tener una visibilidad de la distribución de los dispositivos en todas las sedes.
- d) La solución debe permitir el acceso de múltiples usuarios bajo un esquema cliente servidor, con una simultaneidad de mínimo diez (10) usuarios, con una capacidad de descubrir un mínimo de 200 dispositivos y soportar para 10000 puertos de switches.
- e) La herramienta deberá ser implementada por personal certificado por la marca y deberá incluir una capacitación de al menos 24 horas.
- f) El contratista debe estar a cargo de configurar al 100% todos los módulos propuestos, para ello se coordinará con el personal asignado del contratista para el cumplimiento y soporte en configuración de los equipos del Ministerio, El Ministerio estará a cargo de la ejecución de las configuraciones de sus equipos.

5.2.1.4. Administración del Ancho de Banda

El Contratista debe de incluir en calidad de alquiler dos equipos, del tipo appliance, para la gestión y administración del ancho de banda, un equipo para cada sede (Lampa 255 y Lampa 274), el cual permita visualizar a nivel de aplicación y protocolos el consumo de tráfico y que adicionalmente pueda aplicar políticas de Calidad de Servicio y Priorización de Tráfico bajo el enlace hacia Internet.

Un equipo de Administración de Ancho de Banda debe ser instalado en la sede del Jr. Lampa 255 y el otro en la sede Jr. Lampa 274, desde los cuales se debe administrar los enlaces de internet. La administración de ambos equipos debe ser centralizada cuando los equipos estén en modo cluster.

Cada equipo debe tener las siguientes características mínimas:

- El equipo Administrador de Ancho de Banda deberá ser un appliance en hardware de propósito dedicado. El software en el equipo debe ser integrado directamente por el mismo fabricante ya que no se acepta soluciones de tipo software que depende de sistemas operativos genéricos (Windows o Linux) que deben ser instalados previamente, ya que esto no garantiza el soporte integro de la solución debido a que el sistema operativo seria

independiente a la solución y expuesto a vulnerabilidades, esta capacidad debe ser confirmada directamente por el fabricante.

- Licencia para administración de ancho de banda de acuerdo a lo ofertado. El Contratista debe suministrar licencia para administración de ancho de banda acorde a la configuración oferta.⁴
- Throughput mínimo: 3 Gbps (Full dúplex).
- Deberá soportar una cantidad máxima de usuarios de hasta 100,000. El equipo administrador de ancho de banda propuesto debe estar configurado para soportar hasta 100,000 usuarios totales con una concurrencia de 3000 usuarios concurrentes.
- Capacidad instalada de manejo de 250,000 conexiones o flujos concurrentes.
- Para cada equipo, debe contar con 10 interfaces de red (10/100/1000Base-T) que permitan hacer inspección de 05 líneas físicas de red independientes. **Adicionalmente, deberá contar con 2 interfaces de red de 10 Gbps (fibra multimodo) y para crecimiento futuro debe soportar 2 interfaces de 40 Gbps. Ante una interrupción del servicio del equipamiento administrador de ancho de banda, este debe colocarse en modo bypass⁵.**
- Debe contar con un puerto de Consola y de administración independiente. Asimismo, soportar interfaces de 10Gbps y 40Gbps.
- Debe contar con capacidad de detectar, clasificar y restringir tráfico por direcciones o rangos de direcciones IP (internas), hostname, nombre de usuario, servicio (aplicación), VLAN y ToS (Type of Service). Debe tener conexión con el Active Directory de propiedad del Ministerio la conexión del Active Directory puede ser con agente o sin agente mientras se garantice la identificación del usuario e IP en uso.
- Capacidad de soportar IPv4 e IPv6 así como integración AD en IPv4 e IPv6.
- La solución debe descubrir más de 2000 servicios de aplicaciones en forma automática con la inclusión de: Tráfico de intercambio de información como BitTorrent, eDonkey, Ares, Gnutella, Webhunder, Winny, Freenet incluyendo protocolos P2P Encriptados. Servicios de voz y mensajería como Skype empresarial (Skype for Business) y Skype diferenciando entre voz y video, Google Talk, Google Duo, WhatsApp, Telegram, Snapchat y Google Jibe. Streaming de Audio y Video MPEG, AVI, MP3, Quicktime, Silverlight, YouTube, YouTube Music, Vimeo, Dailymotion, QUIC, Netflix, Disney Plus, Disney Radio, Amazon Prime (diferenciando entre Music y Video), Apple TV, Apple Music, Crackle, HBO Max, Hulu, NBA, NBC, TNT y ESPN. Servicios de conferencias como Zoom, Google Meet, Microsoft Teams, Webex, GoToMeeting, Discord, Facetime, RingCentral y Slack. Aplicaciones empresariales como SAP, Salesforce, Office365, LotusNotes, Microsoft Exchange, Citrix, Amazon Web Services, Windows Azure, Google Docs, Google API, Google Analytics, Adobe Creative Cloud, iCloud, Evernote, Paypal, TeamViewer, AnyDesk y Zendesk. Servicios de actualizaciones propios de fabricantes de dispositivos móviles como Apple, Samsung, Xiaomi, Blackberry y Huawei además de los sistemas operativos como App Store y Google Play.
- La solución debe permitir la creación de aplicaciones personalizadas que permita identificar tráfico propietarios de la entidad, esta capacidad de creación debe incluir al menos los siguientes criterios: Tráfico HTTP por tipo de contenido, tipo de archivo, host/URL o dominio, método (GET, PUT, POST, etc.), navegador web usado. Tráfico SSL por nombre de organización y nombre común. Tráfico Flash por host/dominio. Tráfico Windowsmedia host/dominio. Tráfico RTP de VoIP por Codec. Marcación DSCP. Puerto o rango de puertos TCP y Puerto o rango de puertos UDP.
- La solución debe estar en capacidad de autoevaluar el tráfico a través de un aprendizaje y poder indicar al administrador por medio mensajes a través de la consola o por correo electrónico los cambios importantes a tener en cuenta, como nuevas aplicaciones con alta tendencia de consumo y tráfico que no está siendo atendido por un nivel de política creado.
- La solución debe poder medir por demanda y de forma activa el rendimiento de la red a través de la generación de flujos de tráfico TCP o UDP indicando tamaño del datagrama disponible, paquetes perdidos en la medición y rendimiento de carga útil o "Payload"
- La solución debe permitir acceso directo a la base de datos donde se almacena todos los datos monitoreados y permita interactuar con herramientas de terceros a fin de ampliar las capacidades de analítica, este acceso deber poder ser restringido por dirección IP para la

⁴ Absolución N° 30, 31, 61, 62, 110, 141, 159, 168, 169, 177, 182, 184, 199, 362, 363, 397

⁵ Absolución de consulta N° 297, 298, 299

herramienta con que se realizara la integración y configuración de unas credenciales personalizadas a fin de garantizar la seguridad.

- Debe permitir la generación de políticas de control (restricción o priorización) de ancho de banda para el tráfico entrante y saliente de manera independiente. Debe proporcionar la funcionalidad de cache en capa de aplicación para tráfico HTTP, a través de licenciamiento de software y no agregando componentes de hardware a la solución. La función del cache consiste en reducir el tráfico repetitivo de tipo Web en el enlace gestionado.
- Las políticas o reglas de control de ancho de banda deberán permitir la priorización de tráfico (8 niveles de prioridades), definir un mínimo ancho de banda garantizado y un máximo ancho de banda permitido.
- Deberá poder aplicarse políticas de control de tráfico a través de horarios definidos.
- Número de políticas o reglas soportadas: 2,000 como mínimo.
- Administración centralizada en configuración de modo cluster, gráfica, remota y segura, desde una consola o equipo administrador. Se aceptará que la administración sea a través de una consola externa o integrada en el propio equipamiento siempre y cuando los equipos se encuentren sincronizados entre ellos.
- Respecto a los equipos de administración de ancho de banda, se debe considerar todo hardware, software y licencias necesario para contar con un sistema de administración que permita gestionar y monitorear de manera centralizada los equipos mencionados.
- Debe contar con monitoreo en tiempo real, que permite hacer un análisis de tráfico en profundidad hasta la búsqueda de una estación de trabajo y un servicio específico, para el diagnóstico de problemas y cuellos de botella en la red.
- Debe contar con capacidad de monitoreo de la utilización de ancho de banda y de la cantidad de conexiones activas.
- Debe contar con envío de alarmas por medio de email y snmp.
- Deberá contar con almacenamiento de datos históricos en la misma unidad, para posterior generación de reportes tabulares y gráficos de la utilización del ancho de banda, hasta de un año atrás. Capacidad de almacenamiento de al menos 1.6TB SSD en RAID 1 para garantizar la disponibilidad de la data histórica y fuente redundante.
- Debe contar con capacidad para generación de informes mediante la vista gráfica interactiva, pudiendo exportar los reportes a los siguientes formatos: PDF y CSV. El generador de reportes debe estar integrado al administrador ancho de banda, en una sola unidad.
- Debe poseer sistema by pass interno, el cual debe activarse en forma automática en caso de caída o falla del equipo. Esta configuración by pass también debe poder realizarse en forma manual, en caso el administrador u operador lo disponga.
- Generación de Reportes de Hosts y usuarios más Activos.
- Generación de Reportes de Protocolos más Activos.
- Generación de reportes de popularidad de protocolos.
- Perfiles de Usuarios para acceso a plataforma de Gestión: Administración, Monitoreo. El perfil Operador será opcional.
- Capacidad de Limitar el acceso de Gestión para un grupo específico de direcciones IP, previniendo el acceso no autorizado a la red.

5.2.1.5. Balanceadores de Tráfico de Internet

El Contratista debe de incluir en calidad de alquiler dos equipos (appliance físicos) para el balanceo de tráfico de los enlaces, uno debe instalarse en la sede Central (Lampa 255) y otro en la sede Lampa 274, los cuales deben estar en alta disponibilidad (activo-pasivo). Las características mínimas de cada equipo deberán ser las siguientes:

PARA TRAFICO DE INTERNET	
CARACTERÍSTICA	DETALLE
Cantidad	Dos (02) Equipos.
Arquitectura	Appliance dedicado en formato Rack, configurado en Alta Disponibilidad (Activo – Pasivo).
	Cuenta con sistema operativo especializado para la función.
Descripción	El equipo de Balanceador de Tráfico Internet, proporcionará alta

PARA TRAFICO DE INTERNET	
CARACTERÍSTICA	DETALLE
	disponibilidad en el acceso a la Internet suministrado por el Contratista de servicios de Internet propuesto (Ítem 1) y el servicio de internet correspondiente al Ítem 2. De manera que cuando uno de los enlaces tenga problemas (caída del enlace a Internet), todo el tráfico de Internet de salida y entrada sea re-direccionado a los enlaces que estén disponibles. Este balanceador también podrá definir políticas en capa 7 (modelo OSI) que determinen que enlace se usará para cada aplicación.
Descripción	Para proporcionar esta alta disponibilidad, el balanceador administrará las diferentes direcciones IP proporcionadas por el ISP (Contratista), a través de su propio servicio de DNS interno asociado a algoritmos de resolución de nombres.
Características Básicas	Throughput: 26 Gbps (capa 4 y 7).
	Memoria: 32 Gbytes
	Cada equipo debe cumplir con las siguientes características: <ul style="list-style-type: none"> •La solución debe soportar al menos 32 Millones de conexiones simultáneas en capa 4 •La solución debe soportar al menos 900.000 conexiones por segundo en L4 •La solución debe soportar al menos 2.8 Millones de HTTP Requests por Segundo
	SSD: 240 GBytes. El Contratista de considerar necesario, podrá incluir en su solución, un equipo adicional que tenga la capacidad de almacenar eventos en un storage de 8 TB como mínimo. Se debe considerar un sistema de almacenamiento que soporte los datos históricos para posterior generación de reportes tabulares y gráficos de la utilización del ancho de banda, que se generen por un periodo de tiempo de un año como mínimo. El Contratista será responsable de mantener los equipos debidamente actualizados y con los parches de seguridad aplicados. Debe tener la capacidad de dividirse en 3 o más unidades virtuales que funcionen independientemente.
	Respuestas DNS por segundo o DNS Queries Per Second (QPS) ⁶ : 500 mil Debe funcionar como un servidor DNS autoritativo de alto desempeño, permitiendo manejar un dominio completo o delegación de parte de un dominio. Debe ser autónomo sin necesidad de balancear requerimientos DNS a una granja de servidores DNS. Debe funcionar como un servidor DNS cache autónomo, sin necesidad de balancear requerimientos DNS a una granja de servidores. La solución debe soportar el permitir alta disponibilidad de aplicaciones distribuidas en 2 o más datacenters, sin importar la ubicación geográfica. Debe manejar persistencia a nivel global, manteniendo a los usuarios en un mismo datacenter por el transcurso de su sesión.
	Capacidad de balancear mínimo 4 enlaces de Internet de 1 Gbps cada uno.
	La solución permitirá usar los enlaces de Internet simultáneamente tanto para usuarios internos como externos. Soporte de enlace redundante Activo-Activo o Activo-Pasivo.
	Protocolos de ruteo soportados: OSPF.
	8 puertos 10/100/1000 Base-T RJ45 para cableado en cobre (que permita hacer inspección de 04 líneas físicas de red independientes) o puertos 1 Gigabit Ethernet (fibra óptica mono modo) 6 puertos de 10 SPF+ Gigabit Ethernet (fibra óptica mono modo). Estos datos se presentarán en el “Anexo A” descrito en el punto punto 12. El Contratista debe suministrar todo conector, patch cord, transceiver y todo hardware, licencia y software necesario para garantizar las conexiones.
Monitoreo del Estado de Salud	Chequeo Por: Ping, puerto TCP, UDP, estado del puerto físico, SNMP y HTTP.

⁶ Absolución de consulta N° 345

PARA TRAFICO DE INTERNET	
CARACTERÍSTICA	DETALLE
Algoritmos de Balanceo de Carga	<ul style="list-style-type: none"> • Weighted Round Robin, Global availability, Application availability, Geography, Virtual server capacity, Least connections, Round trip time, Dynamic ratio (opcional), DNS. • Proporcional (característica opcional). • Proporcional dinámico (característica opcional) (dinámico es un algoritmo que el equipo propuesto debe cumplir. Este algoritmo permite monitorear los tiempos de respuesta de cada servidor y en base a ello tomar decisiones dinámicas de carga y balanceo de tráfico).
Balanceo GSLB y LLB	<ul style="list-style-type: none"> • Algoritmos de balanceo de precisión basados en la topología de red, verificando saltos, distribuyendo las solicitudes de resolución de nombres DNS a un servidor virtual en el centro de datos que tenga el menor número de saltos de router desde el LDNS del cliente. • Enlace de mejor rendimiento: Utilizando el tiempo de ida y vuelta y cálculos de calidad del enlace, el balanceador debe comprobar qué conexión proporcionará el mejor servicio para cada usuario, y luego dirigir al usuario a ese enlace. • Control exhaustivo de los enlaces: Con una visión completa de la salud y el rendimiento de los enlaces que pasan por el router, el balanceador debe proporcionar visibilidad del ancho de banda y la capacidad de cualquier enlace. • Debe contar con un servicio de reputación de IP inteligente (hace referencia a una base de datos de direcciones IP de clientes malintencionados que se actualiza periódicamente), que permita bloquear los intentos de conexiones con una intención maliciosa a través de fuentes de datos globales que colaboran para proporcionar inteligencia de amenazas actualizada sobre fuentes hostiles. De esta forma la organización se mantendrá más segura bloqueando IPs con intenciones de conexiones maliciosas. • Alta disponibilidad: el balanceador debe combinar múltiples monitores para determinar con rapidez y precisión la salud y disponibilidad de cada enlace. Si se detecta un problema, el tráfico se puede redirigir a otros disponibles, manteniendo la conectividad de los clientes sin incurrir en tiempo de inactividad. • Persistencia de área: para garantizar que las conexiones de los usuarios persisten a través de aplicaciones y datacenters, el balanceador debe sincronizar los datos, propagar el DNS local y mantener la integridad de la sesión. • Deberá realizar caching de certificados digitales con la capacidad de recuperar fácilmente del caché para que el sistema no tenga que volver a cargarlos cuando los clientes soliciten el servicio (característica opcional). • Equilibrio de carga geográfico: el balanceador debe incluir una base de datos de IP que identifica la ubicación a nivel de continente, país y estado/provincia para conectar a los usuarios con la aplicación o servicio más cercano para obtener el mejor rendimiento. • Supervisión de la infraestructura: el balanceador debe comprobar el estado del flujo de la comunicación de red, eliminando puntos únicos de fallo y dirigiendo el tráfico de aplicaciones lejos de los sitios de bajo rendimiento. • Monitores de salud de aplicaciones: En lugar de depender de una sola comprobación de salud, el balanceador debe contar con múltiples monitores para comprobar el estado de la aplicación en múltiples

PARA TRAFICO DE INTERNET	
CARACTERÍSTICA	DETALLE
	<p>niveles (será realizado a nivel de servidor y no a nivel de código).</p> <ul style="list-style-type: none"> • Debe tener conectores nativos para integrarse con AWS y Oracle Cloud para compartir información de las instancias de AWS y Oracle Cloud recuperando información de las aplicaciones con la finalidad de utilizar esta información y ser parte de los health check para definir la disponibilidad del servicio • Sincronización de configuraciones: sincronizar objetos de configuración de balanceo de enlaces entre clusters. • Monitores DNS: verificar la salud de un servidor al interior del datacenter y tomar decisiones de balanceo, según estén disponibles o no. • Debe permitir examinar los cambios no autorizados de los archivos de un sitio web determinado en un periodo determinado con capacidad de notificar y realizar un rollback o restauración automática del sitio web (esta característica es opcional). • Logging de alta velocidad: gestionar fácilmente el registro de DNS y de aplicaciones de diferentes datacenters para una rápida visibilidad y planificación de la red. • Debe soportar el protocolo DNSSEC. • Informes y análisis avanzados: Módulo de Analytics que proporcione informes y análisis avanzados de DNS de aplicaciones, servidores virtuales, nombres de consulta, IPs de clientes, nombres más solicitados y más para la inteligencia empresarial.
Traducción de Direcciones IP (NAT)	Admite la realización de NAT de las direcciones IP de los hosts internos a múltiples direcciones IP públicas.
	Admite la realización de NAT utilizando una única dirección IP para una serie de hosts internos o usuarios al acceder a la WAN / Internet.
DNS	Permitirá a usuarios externos acceder a recursos internos vía todos los enlaces WAN utilizando URL.
	Soporta operar como un servidor DNS autoritativo de alto desempeño, permitiendo manejar un dominio completo o delegación de parte de un dominio. Debe ser autónomo sin necesidad de balancear requerimientos DNS a una granja de servidores DNS. Debe incluir herramienta de administración grafica para el manejo de zonas DNS.
	Debe funcionar como un servidor DNS cache autónomo, sin necesidad de balancear requerimientos DNS a una granja de servidores.
	Debe permitir realizar balanceo de servidores DNS.
	Debe soportar registros AAAA para IPv6 Debe soportar traducción entre DNS IPv4 y DNS IPv6 La solución debe soportar 500.000 respuestas DNS por segundo o DNS Queries Per Second (QPS) ⁷ .
	Admitir una herramienta de gestión de zona integrada en la interfaz gráfica de usuario que simplifica la gestión de zona DNS y reduce el riesgo de errores de configuración. Proporcionará un entorno seguro para gestionar la infraestructura de DNS. Admitir registros DNS A, AAAA, CNAME, MX, NS, PTR, SOA, SRV y TXT. Capaz de almacenar en caché las respuestas de DNS Capaz de proporcionar flexibilidad al tener monitores deterministas que se comunican con cada nodo para determinar (dependiendo del monitor configurado) su disponibilidad, estado, proximidad o capacidad de respuesta. Capaz de realizar un sondeo inteligente de sus recursos de red para determinar si los recursos están activos o inactivos. Permite especificar qué dispositivo sondea servidores específicos para obtener datos de salud y

⁷ Absolución de consulta N° 345

PARA TRAFICO DE INTERNET	
CARACTERÍSTICA	DETALLE
	rendimiento. Capaz de admitir monitores compuestos. Puede desplegarse como servidor DNS autoritativo en modo screening, o en modo de delegación, que principalmente puede situarse frente a los servidores DNS tradicionales o desplegarse fácilmente y equilibrar la carga de las zonas delegadas por la infraestructura DNS existente.
	La resolución del nombre a IP se hará sobre la base de las decisiones de balanceo de carga (de la salud del router, carga, tipo de tráfico, etc.).
Administración y Monitoreo	Permite la configuración y administración por web (http y https).
	Permite la administración vía línea de comandos usando telnet o ssh y por medio de un cable de consola.
	Debe contar con un sistema de administración centralizado. Respecto a los equipos de balanceo de tráfico de internet, se debe considerar todo hardware, software y licencias necesario para contar con un sistema de administración que permita gestionar y monitorear de manera centralizada los equipos mencionados a través de una consola externa o integrado en los propios equipos propuestos.
	Debe contar con una interfaz de monitoreo de la salud de los enlaces, rendimiento del equipo y estadísticas de tráfico.
Envío de Notificaciones (Logs)	Permitirá envío de logs de eventos a servidores Syslog.
	Permitirá envío de alarmas vía correo electrónico
	Permitirá envío de notificaciones de eventos y alarmas vía SNMP v2, v3.
Fuente de poder	Interna, alimentación a 220V y 60Hz.
Montaje y accesorios	Incluirá todos los componentes necesarios para ser instalado en el Rack (incluir el kit).
	Incluirá todos los componentes de Hardware, software y licencias necesarias para realizar la configuración en Alta Disponibilidad (Tarjetas, Cables, Interfaces y Conectores).

El equipo será entregado en perfectas condiciones para su uso, en donde los rótulos permitan identificar las características y la marca respectiva y si fuera el caso estará impreso en el mismo bien.

El equipo no será reciclado, reensamblado o reacondicionado, tampoco se aceptarán aquellos que tenga la denominación “refurbished”, “remarketing” o su equivalente comercial.

El Contratista deberá proporcionar los enlaces de fibra que incluirán todo lo necesario para que la alta disponibilidad funcione correctamente que interconecten ambos locales (Lampa 255 y Lampa 274), para poder conectar los balanceadores en alta disponibilidad o para conexiones de administración de equipos o enlaces de internet. El Ministerio asignará los switches (marca Aruba) y los puertos que se necesiten para este fin.

El Contratista deberá incluir todos los accesorios necesarios, patch cords, transceivers, switches necesarios para la operatividad y alta disponibilidad de los dispositivos a suministrar. En caso de suministrar switches, estos deberán tener doble fuente de alimentación, deben ser administrables mediante SNMP desde el centro de control del postor y desde el Ministerio.

5.2.1.6. Anti DDOS

5.2.1.6.1. Arquitectura

- Para el ítem 1, deberá considerarse una solución en sitio (aparte de la solución en la nube solicitada también para este ítem), la cual deberá soportar el ancho de banda solicitado para el ítem 1 y para el ítem 2. El contratista adjudicado al ítem 1, deberá realizar las configuraciones y conexiones necesarias a fin de que la solución Anti DDOS (en sitio); solicitada, en modalidad de arrendamiento operativo y en modo aplican, cuente con todo lo necesario para cubrir el enlace del ítem 1 y el enlace del ítem 2.

- El servicio de protección contra ataques de DDoS debe implementar dispositivos dedicados que se instalarán en los dos sites (Lampa 255 y Lampa 274), para tener una solución de alta disponibilidad y deben proteger todas las interfaces de internet (las del ISP 1 y las del ISP2).
- El servicio de protección contra ataques de DDoS debe implementarse con dispositivos de propósito específico dedicado a proteger la disponibilidad del servicio; por lo que no se aceptarán dispositivos que mantengan el estado de la conexión como cortafuegos, sistemas de prevención y sus variantes o combinaciones como UTM, NGFW, NGIPS, Proxis y WAF ya que al conservar el estado de la conexión son susceptibles a ataques de DDoS.
- La solución debe de contar con un mecanismo de bypass (se requiere el bypass sea con los puertos de fibra ya que se requieren interfaces 10GE SFP+), en caso de no contar con bypass en fibra se aceptará el equipo en Alta disponibilidad), en cada interface para garantizar la disponibilidad y continuidad de los servicios, el cual debe de activarse en los siguientes casos:
 - Corte de energía
 - Falla en el hardware
 - Falla Software
- La solución implementada debe proporcionar al menos 4 interfaces de 1 Gbps de cobre para proteger dos segmentos de red en cada uno de los datacenters (sites).
- La solución debe tener una capacidad de inspección de al menos 4 Gbps considerando la sumatoria de tráfico de subida más bajada y debe ser posible ampliar esta capacidad por medio de una licencia de actualización utilizando el mismo dispositivo.
- La solución instalada en sitio deberá soportar un crecimiento de hasta 20Gbps sin necesidad de hacer cambio de hardware. Se requiere de al menos 20Gbps de throughput, es decir 10Gbps de subida y 10Gbps de bajada que es la capacidad de las interfaces 10GE SFP+.
- El sistema no debe de realizar ningún seguimiento a las conexiones, por lo que no deberá de tener un número máximo de conexiones simultáneas.
- Al posicionarse en línea, el sistema deberá de ser completamente transparente. El tráfico debe fluir a través de él y deberá de analizar, detectar y mitigar los ataques antes de que lleguen a su destino.
- El sistema debe ser capaz de soportar un modo inactivo cuando se configura en línea, que permita el ajuste de la configuración de protección sin bloquear el tráfico y proporcione reportes de todo el tráfico que bloquearía si se define como "activo".
- El sistema debe soportar la implementación en modo monitor, en el que no introduce ningún punto adicional de falla a la red por medio de un puerto espejo habilitado en un enrutador ("router"), conmutador ("switch") o un tap de red.
- El sistema debe incluir fuentes de alimentación de energía AC redundantes y debe admitir intercambio caliente ("hot swap") de una fuente de alimentación degradada durante el funcionamiento normal del sistema.
- El sistema debe de soportar interfaces de administración redundantes.
- El sistema debe de permitir el acceso CLI a través de un puerto serial RJ-45.
- El sistema debe soportar el funcionamiento como terminador de túneles GRE (Encapsulación de Enrutamiento Genérico).
- El sistema debe de proporcionar una Interface de Programación de Aplicaciones (API) para poder acceder y ampliar sus funcionalidades.
- El sistema deberá de contar con actualizaciones sobre inteligencia de amenazas, para detectar y detener amenazas emergentes dirigidas hacia la infraestructura y servicios del centro de datos, las cuales deberán de actualizarse de manera automática sin necesidad de actualizar el software.
- El sistema debe de proporcionar un filtro de amenazas salientes para evitar que el tráfico malicioso abandone la red, utilizando la inteligencia de amenazas y sus categorías.
- El sistema debe proporcionar una actualización constante sobre inteligencia de amenazas para las siguientes categorías: Firmas de botnets, comando y control, reputación de DDoS, correo electrónico, por ubicación IP, basadas en su ubicación, de malware, móvil y ataques dirigidos.
- El sistema deberá de poder inspeccionar tráfico SSL a través de un módulo de seguridad basado en hardware embebido dentro del mismo dispositivo
- El sistema debe de realizar una inspección SSL pasiva, por lo que no deberá terminar las sesiones SSL o actuar como proxy.
- La inspección de tráfico SSL deberá de soportar suites de cifrado ECDH (Curvas Elípticas de Diffie Hellman) y uno de los cifrados siguientes: RSA o AES.

- El Hardware ofertado debe ser el de última generación disponible y no debe contar con EoS en el plazo de contrato.

5.2.1.6.2. Administración

- El sistema debe proporcionar documentación en línea en la Interfaz de Usuario (UI) para ayudar a comprender las funciones de cada pantalla.
- La Interfaz de Usuario (UI) del sistema debe permitir múltiples niveles de acceso, como son: de administración completa, de administración limitada para la configuración de mitigaciones y de lectura.
- La interfaz de Usuario (UI) debe incluir un registro de cambios sobre los eventos que ocurren en el sistema, cambios en la configuración, descarga de archivos y para solucionar problemas.
- El sistema debe proporcionar la capacidad para crear y exportar paquetes de diagnóstico que contienen información del estado y configuración a utilizarse para resolver problemas.
- El sistema debe proporcionar la capacidad para administrar sus archivos a través de la Interfaz del Usuario (UI), incluida la carga, descarga y eliminación. Se aceptará opcionalmente la descarga de informes en PDF o CSV.
- El sistema debe proporcionar una interfaz CLI para instalar y actualizar el software, realizar la configuración inicial además de otras funciones avanzadas
- El sistema debe proporcionar notificaciones a través de SYSLOG, SNMP o SMTP.
- El sistema debe admitir su monitoreo a través de SNMP v2 o v3 para obtener el estado del sistema, la configuración o las estadísticas de las interfaces.
- El sistema debe ser capaz de generar los siguientes tipos de alertas: de sistema, de protección, de implementación, de dispositivos bloqueados, ancho de banda y registro de cambios.
- El sistema debe permitir la creación, eliminación y administración de cuentas de usuario a través de la Interfaz de Usuario (UI).
- El sistema deberá permitir el acceso remoto mediante SSH.
- El acceso a la Interfaz de Usuario deberá de ser a través de un protocolo seguro como es HTTPS, con la posibilidad de cambiar el certificado digital por uno propietario.
- Los administradores del sistema deben de poder bloquear una cuenta manualmente y especificar el número de intentos de inicio de sesión que puede hacer un usuario antes de que la cuenta quede bloqueada automáticamente.
- A los usuarios sin privilegios administrativos se le permitirá administrar la configuración de sus propias cuentas y contraseñas, pero no podrá cambiar cuentas de otros usuarios.
- El sistema debe poder realizar una autenticación de contraseña estática por medio de la integración de RADIUS o TACACS +

5.2.1.6.3. Funcionalidades de la Interfaces de usuario

- El sistema debe proporcionar un panel de estado de dispositivo que incluya información sobre las alertas activas, total del tráfico permitido y bloqueado a través de las interfaces, estado de la CPU y memoria de sistema.
- El sistema debe proporcionar estadísticas detalladas para cada protección, mostrando su impacto en el tráfico durante los últimos 5 minutos, 1 hora, 24 horas, 7 días o un rango de tiempo.
- El sistema debe mostrar estadísticas de protección sobre tráfico permitido y bloqueado en bits por segundo (bps) y paquetes por segundo (pps).
- Las estadísticas detalladas y gráficos para cada grupo de protección para servidores genéricos deben incluir información sobre el tráfico total, tráfico por URL, tráfico por dominio, información de ubicación IP, distribución de protocolos, distribución de servicios y estadísticas principales de hosts bloqueados.
- El sistema debe admitir la generación de informes PDF que contiene las estadísticas detalladas y gráficos para cada grupo de protección.
- El sistema debe admitir la generación de reportes por correo electrónico con las estadísticas detalladas y gráficos para cada grupo de protección.

5.2.1.6.4. Funcionalidades de prevención y mitigación

- El sistema debe ser capaz de bloquear paquetes TCP / IP inválidos
- El sistema deberá permitir la configuración de listas de filtros de cabecera L2/L3/L4.

- El sistema debe ser capaz de detectar fuentes que envíen cantidades excesivas de tráfico bajo umbrales configurables, para después colocar esas fuentes en listas de hosts bloqueados temporalmente (bloqueo basado en la tasa de tráfico).
- El sistema debe de ser capaz de descartar paquetes según puertos TCP específicos y payloads que coincidan o no con expresiones regulares configurables.
- El sistema debe de ser capaz de descartar paquetes según puertos UDP específicos y payloads que coincidan o no con expresiones regulares configurables.
- El sistema debe de soportar prevención de inundación suplantada (spoofing) de SYN's TCP que autentifiquen conexiones TCP desde los hosts origen.
- La prevención de inundación suplantada de SYN's TCP debe de ser capaz de especificar los puertos TCP origen a ser ignorados.
- La prevención de inundación suplantada de SYN's TCP deberá de proporcionar mecanismos de autenticación donde el sistema responda con un ACK imitando una conexión existente y semi abierta para las aplicaciones basadas en TCP que son sensitivas a envío de TCP RST.
- La prevención de inundación suplantada de SYN's TCP debe de ser capaz de establecer un umbral para la automatización de este proceso, indicando a cuantos paquetes SYN enviados a cualquier host protegido deberá de realizar la autenticación de TCP.
- El sistema deberá de poder limitar el número de conexiones concurrentes de TCP que provenientes de un solo origen.
- El sistema debe de soportar la supresión de sesiones TCP inactivas si el cliente no envía una cantidad de datos configurable por el usuario dentro de un periodo de tiempo determinado por el usuario.
- El sistema deberá de ser capaz de autenticar solicitudes DNS obligando al origen a que envíen solicitudes a través de TCP y suprimir aquellas que no puedan ser autenticadas dentro de un tiempo específico.
- El sistema debe de soportar el bloqueo de solicitudes DNS malformadas en el puerto 53 que no cumplan con el estándar RFC.
- El sistema debe ser capaz de limitar el número de consultas DNS por segundo a una velocidad configurable por el usuario.
- El sistema debe ser capaz de bloquear el tráfico desde cualquier host que genere más solicitudes DNS fallidas consecutivas del límite configurado y poner al host origen en una lista negra.
- El sistema debe proporcionar la posibilidad de configurar expresiones REGEX para suprimir el tráfico DNS específico con los encabezados que coincidan con las expresiones.
- El sistema deberá de prevenir el bloqueo global de CDN o proxys.
- El sistema debe ser capaz de detectar y eliminar paquetes con formatos incorrectos de HTTP que no se ajusten a los RFC's para los encabezados de solicitud y poner al host origen en una lista negra.
- El sistema debe permitir al usuario configurar el número máximo de solicitudes por segundo y el número máximo de objetos HTTP solicitados por cada host hacia un servicio Web y si la tasa definida es excedida el host deberá de ser bloqueado.
- El sistema debe ser capaz de suprimir paquetes HTTP específicos según los encabezados HTTP coincidentes con expresiones REGEX configurables.
- El sistema debe de proporcionar un mecanismo de protección contra ataques SSL o TLS forzando el uso correcto del protocolo bloqueando solicitudes malformadas.
- El sistema debe de soportar el bloqueo de solicitudes SIP malformadas que no cumplan con el estándar RFC.
- El sistema debe limitar el número de solicitudes SIP que puede enviar un host en un segundo para evitar ataques que podrían irrumpir este servicio.
- El sistema debe de proporcionar la capacidad de limitar la velocidad de reenvío de tráfico que coincide con una expresión específica.
- El sistema debe proporcionar la capacidad para detectar y bloquear las inundaciones de SYN's TCP por encima de la tasa configurada.
- El sistema debe proporcionar la capacidad para detectar y bloquear las inundaciones ICMP por encima de la tasa configurada.
- El sistema debe proporcionar la capacidad para detectar y bloquear las inundaciones UDP por encima de la tasa configurada.
- El sistema debe proporcionar la capacidad de bloquear el tráfico originado por bots según las firmas proporcionadas por el sistema.
- La solución deberá de mitigar ataques de fragmentación.

- El sistema deberá de poder bloquear tráfico Multicast.
- El sistema deberá de poder bloquear tráfico de direcciones privadas.
- El sistema debe proporcionar la capacidad de bloquear el tráfico procedente de fuentes que interrumpen reiteradamente solicitudes HTTP.
- El sistema debe proporcionar la posibilidad de actualizar automáticamente sus firmas de protección de ataques periódicamente a intervalos configurables.
- El sistema deberá de identificar web crawlers y monitorear su uso.
- El sistema debe permitir la configuración de protecciones predefinidas asociadas con servicios específicos, como Web, DNS, VoIP o un servidor genérico.
- El sistema debe de soportar la capacidad de cambiar el Nivel de Protección que se aplica al tráfico, cambiando efectivamente la configuración en uso por el sistema para todas las prevenciones, contando al menos con los niveles de protección: Baja, Media y Alta
- El sistema debe sugerir ciertas configuraciones de protección basadas en el aprendizaje del comportamiento típico de la red.
- El sistema debe de permitir que los parámetros de protección sean cambiados mientras la protección está corriendo.
- El sistema debe de poder bloquear por país de origen.
- El sistema debe poder evitar que el tráfico malicioso salga de la red utilizando un mecanismo de detección y contención a través de categorías de amenazas.
- El sistema debe tener la capacidad de cambiar el nivel de protección a alto de manera automática cuando el tráfico total exceda los umbrales definidos
- El sistema debe soportar la importación de IOC's (Indicadores de compromiso) de fuentes externas en formato STIX and TAXII.
- Los IOC soportados debe incluir, direcciones IP, dominios y Urls.
- El sistema debe soportar hasta 3 Millones de IOC.

5.2.1.7. Apoyo en cambios de configuración del servicio de Mantenimiento

Adicionalmente el Contratista deberá considerar un tiempo de 70 horas anuales (no acumulables) para ser empleadas por el Ministerio para la modificación de la configuración de los equipos balanceadores de tráfico de internet (30 horas), administrador de ancho de banda (20 horas) y equipo Anti-DDoS (20 horas). El personal responsable de realizar las configuraciones deberá contar con certificación oficial de la marca en los productos instalados (la certificación no deberá ser venta y/o preventiva). Estas horas podrán ser solicitadas en cualquier día del mes y en cualquier horario sin restricción alguna. El servicio debe ser presencial, por motivos seguridad y de criticidad que los equipos tendrán en la red del Ministerio.

El acceso para la administración y/o configuración deberá ser desde direcciones IP declaradas por el proveedor, las cuales serán aprobadas por El Ministerio.

5.2.1.8. Gestión de Soporte Técnico

5.2.1.8.1. Soporte Técnico ante fallas de servicio

- Para el caso del ítem 1, el Contratista deberá asignar un ingeniero residente, el cual realizará sus labores en instalaciones del Ministerio en un horario de 8 horas diarias 5 días a la semana. Deberá trabajar a dedicación exclusiva para el Ministerio atendiendo todos los incidentes, averías, reportes, nuevas implementaciones, todo esto sobre la infraestructura provista por el contratista. Deberá contar con, [la certificación oficial del fabricante de Balanceador de tráfico y con la certificación oficial del fabricante del Administrador de ancho de banda propuestos](#)⁸, adicionalmente debe contar con las credenciales de administración a fin de poder realizar configuraciones en todos los equipos provistos por el contratista.
- El contratista deberá indicar el número telefónico, para reportar fallas técnicas (averías) en el servicio, el cual será el único punto de contacto con el operador y niveles de escalamiento, [la que debe ser presentada al inicio de la prestación del servicio](#)⁹.
- El Contratista deberá contar con un centro permanente de operaciones de red (NOC) y un centro de seguridad (SOC), propio para subsanar las fallas técnicas ante cualquier llamada

⁸ Absolución de consulta N° 76

⁹ Absolución de consulta N° 45

de servicio por parte del Ministerio. El Contratista debe contar con un centro permanente de operaciones, con las siguientes características y funciones:

- Monitoreo en modalidad 24x7x365 de la solución oferta. ¹⁰
- El centro debe contar con número de teléfono.
- Debe ser un centro de contacto para recepción de reportes y solución de fallas técnicas.
- Desde dicho centro se debe recepcionar llamadas de servicio del Ministerio, de lunes a domingo de 00 a 24 horas.
- El Ministerio podrá realizar llamadas de servicio de lunes a domingo de 00.00 a 24.00 horas. El Contratista deberá generar tickets de atención por cada incidente reportado.
- El tiempo de reparación de averías del equipamiento a suministrar en el periodo de contrato y que no genere un corte del servicio (Administrador de ancho de banda, balanceador de tráfico de internet y equipo Anti-DDoS), deberá ser como máximo de veinticuatro (24) horas. Contabilizado desde que se crea el reporte de avería. De excederse el tiempo indicado para solucionar un problema, el tiempo de exceso será considerado para el cálculo de penalidades (numeral 16.2). De excederse el tiempo para indicado para solucionar un problema, el contratista podrá instalar un equipo de iguales o similares características. En esta última situación, el tiempo de reposición del equipo no podrá exceder los 60 días calendario.
- El Contratista deberá presentar un informe mensual del servicio de internet, que incluya todas las estadísticas de fallas del periodo, número de ticket, fecha y hora del reporte de falla y fecha y hora de solución de la avería. El informe del servicio de internet será requisito indispensable para otorgar la conformidad mensual del servicio de internet.

5.2.1.8.2. Niveles de Escalamiento:

Nivel de Escalamiento	Descripción	Periodo de atención	Tiempo de respuesta	Tiempo de solución	Modalidad
1	Especialista residente	Lunes a viernes de 9:00 a.m. hasta las 6:00 p.m.	10 minutos	1 hora	Presencial
2	Especialista en NOC/SOC	24x7	30 minutos	2 horas	Remoto
3	Fabricante de la solución	24x7	4 horas	24 horas	Remoto

Cuadro N° 1: Niveles de escalamiento

El Especialista Residente podrá ser reemplazado eventualmente por el Especialista NOC/SOC.

Todos los tiempos indicados como parte del nivel de atención, son contados desde el registro de la solicitud de requerimiento y/o incidente, del Ministerio al Contratista, mediante tickets de atención.

Tiempo de respuesta, se define desde que se reporta el requerimiento y/o incidente del servicio por parte del Ministerio, mediante llamada telefónica o correo electrónico hasta el instante que el personal designado por el proveedor tome contacto con los encargados de la Oficina de Informática del Ministerio.

Tiempo de solución, se define desde que el especialista del proveedor registra el incidente mediante un ticket de atención hasta el instante que el servicio ha retomado a su operación normal.

5.2.1.8.3. Procedimiento de solución de incidentes:

- El contratista deberá asignar un ingeniero residente¹¹, la atención debe ser de forma remota, salvo casos que requiera la presencialidad.
- Al ocurrir una avería o caída del servicio o equipamiento, de severidad media o alta, el NOC/SOC lo alertará de manera automática con su sistema de monitoreo y gestión, y se generará el ticket de manera automática en el ServiceDesk del contratista y que luego será informado al Ministerio.

¹⁰ Absolución de consulta N° 84

¹¹ Absolución N° 079,135.

- Al requerir uno o varios cambios en las políticas y/o configuraciones de los equipos o reportes a demanda, que el Ministerio solicite o desee realizar, será reportado al Ing. Residente por teléfono o correo electrónico. Cabe indicar que los cambios en las políticas, configuraciones o reportes, el Contratista los atenderá de manera ilimitada, sin restricción de cantidad de solicitudes y sin costos adicionales.
- Una vez recibida la notificación, el Ing. residente registrará el requerimiento de servicio y proporcionará al Ministerio un número de ticket de incidente o requerimiento. Dicho ticket servirá para realizar el seguimiento respectivo y escalamiento que fuera necesario.
- El Ing. residente realizará la atención del ticket reportado de manera presencial, dependiendo de la severidad del caso y dentro del horario de oficina lunes a viernes de 9:00am a 6:00pm.
- En caso que el Ing. residente no solucione el incidente tendrá que escalar al nivel 2, donde el Especialista en el NOC/SOC de la solución específica atenderá el incidente presentado.
- De no solucionar la problemática el nivel 2, el incidente se escala al nivel 3 donde el fabricante brinda la solución definitiva.
- El ticket será cerrado, cuando se solucione el incidente o se atienda el requerimiento y se obtenga la correspondiente aprobación por parte del Ministerio.
- El soporte proporcionado por el proveedor será telefónico, remoto y on-site, dependiendo de la severidad del caso.

5.3. ITEM 02: SERVICIO ACCESO A INTERNET- SECUNDARIO

TIPO ENLACE	VELOCIDAD MINIMA ENLACE	OVERBOOKING LOCAL	OVERBOOKING EN LA SALIDA INTERNACIONAL	ORIGEN
Enlace principal	1 Gbps	1.1	1.1	Jr. Lampa N° 255 Cercado de Lima.

El enlace (del ISP al Ministerio) será dedicado y de fibra óptica con canalización subterránea hacia la sede Lampa, el cual está destinado al acceso de los usuarios internos y externos del Ministerio desde y hacia Internet. El contratista debe conectar el servicio de acceso a internet principal con fibra óptica con canalización subterránea, independiente (no compartida) y exclusiva para este enlace desde uno de sus nodos, hacia el datacenter de la sede Lampa 255 y otro enlace de fibra óptica con canalización subterránea independiente (no compartida) y exclusiva para este enlace desde un nodo diferente al anterior hacia el datacenter ubicado en Jr. Lampa 274, lo cual permitirá al Ministerio gestionar la contingencia de manera automática. El enlace solicitado deberá asignar el direccionamiento IP público necesario y deberán realizarse las configuraciones necesarias que permita al Ministerio gestionar la contingencia de manera automática, con el enlace del Item 1. Ambos enlaces siempre deben operar de forma independiente, se especifica que el contratista debe de implementar el tramo de última milla de nodos distintos, totalmente nuevo específicamente para esta contratación, no se aceptarán tendidos de contrataciones previas con el MEF, mediante tendidos independientes de fibra óptica (por la fibra solo debe pasar el servicio de internet solicitado), y que conecte hacia nodos independiente del ISP.

El servicio debe contar con una capa de filtro web, filtro de aplicaciones tolerado desde el data center del operador a través de una solución en arquitectura de alta disponibilidad y de uso exclusivo para el Ministerio, nuevos y de primer uso. El data center debe contar con certificaciones Uptime TIER III (mínimo en diseño) o ANSI/TIA 942 Rated 3, [lo que debe ser presentado para la suscripción de contrato.](#)¹² [Se aceptará que el datacenter sea arrendado, el contratista deberá asumir la responsabilidad de garantizar la disponibilidad del servicio.](#)¹³

[El filtro web solicitado deberá contar con las siguientes características:](#)

- [Capacidad de Prevención de Malware de Dia Cero o no conocido para el servicio de Internet \(mediante emulación de malware – SandBox en nube\).](#)

¹² Absolución de consulta N° 10, 15, 27, 149, 152, 241, 279

¹³ Absolución de consulta N° 81,

- b) Capacidad de Extracción de Malware o extracción del contenido activo riesgoso de los documentos descargado a través del servicio de Internet.
- c) Capacidad de Prevención de Phishing de Día Cero o phishing no conocido para el servicio de Internet, que no pueda ser identificado mediante técnicas de reputación de URL y/o dominios. Las capacidades del servicio de Internet, relacionado al filtro web y seguridad, deben tener las siguientes características de rendimiento: en NGFW de 17 Gbps y en Prevención de Amenazas (Threat Prevention) de 7 Gbps y 8MM de conexiones concurrentes¹⁴.

La fibra debe cumplir con:

- Recomendación UIT-T G.652.D,
- IEC 60793-2-50,
- UIT G.652B,
- G.6522D,
- Norma Internacional IEC 60793-2-50 Tipo B.1.3 Especificación de fibra óptica,
- Telcordia GR-20-CORE,
- ANSI / ICEA S-87-640 y
- RUS 7CFR 1755.900.

¹⁵.

Los enlaces no serán en ningún tramo de propiedad del contratista que se adjudique al ítem 1.

El contratista deberá contar como mínimo con 2 proveedores TIER 1 y que cuente con las salidas internacionales de al menos uno de 40 Gbps, asimismo la red del contratista deberá estar en capacidad de soportar IP Multicast.

El esquema a implementar debe considerar acoplarse al esquema de alta disponibilidad del servicio y balanceo de tráfico del enlace correspondiente al ítem 1, para lo cual El Contratista deberá proporcionar el equipamiento necesario para dicha configuración e integración, de manera que cualquier interrupción o falla hacia alguno de los centros de datos el tráfico entrante y saliente, en forma automática, se dirija hacia el enlace disponible, de manera tal que se mantenga la continuidad del servicio.

El Ministerio será la encargada de realizar las coordinaciones con los Contratistas de los enlaces.

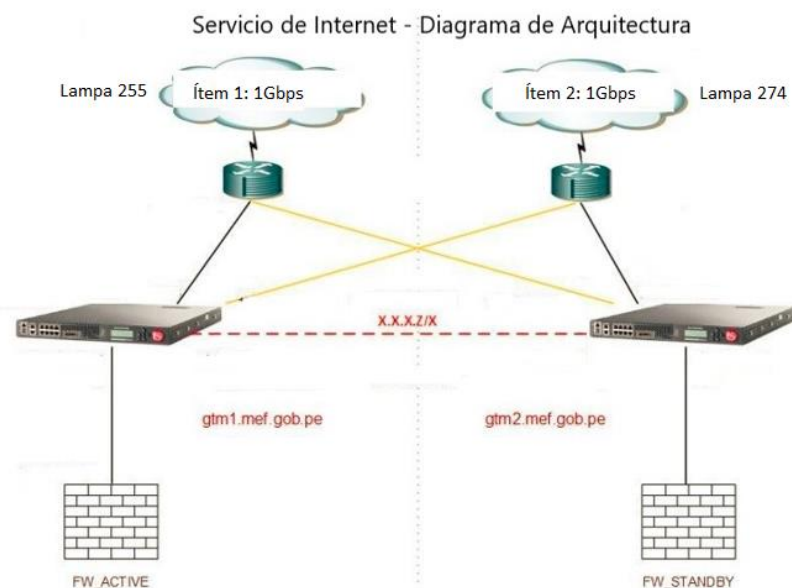


Diagrama 2

5.3.1. Servicios Incluidos

¹⁴ Absolución de consulta N° 390

¹⁵ Absolución de consulta N° 48

5.3.1.1. Servicio de Implementación

Será responsabilidad del Contratista la instalación de la solución ofertada en su totalidad, dentro del plazo ofrecido, para lo cual debe proveer todos los bienes y servicios necesarios para su correcta instalación y acoplamiento a los equipos balanceadores provistos en el Ítem 1.

El Contratista será responsable de optimizar y configurar adecuadamente cada componente ofertado a satisfacción del Ministerio durante la etapa de instalación. El Contratista adjudicado estará encargado de hacer el levantamiento de información de la red del Ministerio, incluyendo configuraciones, políticas y tablas de ruteo, con la finalidad de que luego de la implementación, no existan problemas de comunicación y seguridad. El Ministerio designará un especialista técnico de contacto, que proporcionará información sobre el equipamiento del Ministerio. El Contratista adjudicado debe hacer el levantamiento de información de la red del Ministerio, incluyendo configuraciones, políticas y tablas de ruteo. El Contratista deberá presentar un Plan de Trabajo, en el cual debe contener lo señalado en el numeral 11.1 del presente documento.

El Contratista favorecido con la buena pro deberá presentar un Plan de Trabajo que incluya todos los cambios de configuración necesarios a los equipos propuestos, asimismo, en dicho Plan de Trabajo, se debe indicar que cambios debe realizar el Ministerio a su red, para que el proyecto resulte exitoso. El Plan de Trabajo debe ser entregado como máximo 7 días posteriores a la firma del contrato.

El acceso debe ser subterráneo. El acceso a la sede Central del Ministerio debe ser por el jirón Lampa 255, mientras que el enlace backup por la sede Lampa 274.

En la etapa de activación del servicio el postor debe realizar una prueba de Saturación de ancho de banda, el cual debe quedar a satisfacción del Ministerio.

¹⁶El contratista deberá asignar un ingeniero residente, el cual deberá contar con cursos de capacitación en los equipos a implementar. La atención debe ser de forma remota, salvo casos que requiera la presencialidad. Deberá consignar los datos de contacto en el acta de activación del servicio.

El operador que resulte ganador debe confirmar la operación del servicio tanto en IPv4 como en IPv6.

5.3.1.2. Apoyo en cambios de configuración del servicio de Mantenimiento

Adicionalmente el Contratista deberá considerar un tiempo de 40 horas anuales para ser empleadas por el Ministerio para la modificación de la configuración de los equipos instalados. El personal responsable de realizar las configuraciones deberá contar con certificación oficial de la marca en los productos instalados (la certificación no deberá ser venta y/o preventiva).

El tiempo de 40 horas solicitadas en el párrafo anterior, podrán ser solicitadas en cualquier día del mes y en cualquier horario sin restricción alguna. Adicionalmente, se precisa que el tiempo de 40 horas solicitadas se efectivizarán durante la ejecución del servicio.

5.3.1.3. Gestión de Soporte Técnico

5.3.1.3.1. Soporte Técnico ante fallas de servicio

- Para el caso del ítem 2, el Contratista deberá asignar un ingeniero residente, el cual realizará sus labores de manera remota desde alguna ubicación designada por el contratista.
- El contratista deberá indicar el número telefónico, para reportar fallas técnicas (averías) en el servicio, el cual será el único punto de contacto con el operador y niveles de escalamiento.
- El Contratista deberá contar con un centro permanente de operaciones de red (NOC) y un centro de seguridad (SOC), propio para subsanar las fallas técnicas ante cualquier llamada de servicio por parte del Ministerio. El Contratista debe contar con un centro permanente

¹⁶ Absolución N° 291

de operaciones, con las siguientes características y funciones:

- Monitoreo en modalidad 24x7x365 de la solución oferta¹⁷.
- El centro debe contar con número de teléfono.
- Debe ser un centro de contacto para recepción de reportes y solución de fallas técnicas.
- Desde dicho centro se debe recepcionar llamadas de servicio del Ministerio, de lunes a domingo de 00 a 24 horas.
- El Ministerio podrá realizar llamadas de servicio de lunes a domingo de 00.00 a 24.00 horas. El Contratista deberá generar tickets de atención por cada incidente reportado.
- El tiempo de reparación de averías del equipamiento a suministrar en el periodo de contrato, deberá ser como máximo de veinticuatro (24) horas. Contabilizado desde que se crea el reporte de avería. De excederse el tiempo indicado para solucionar un problema, el tiempo de exceso será considerado para el cálculo de penalidades (numeral 16.2). De excederse el tiempo para indicado para solucionar un problema, el contratista podrá instalar un equipo de iguales o similares características. En esta última situación, el tiempo de reposición del equipo no podrá exceder los 60 días calendario.
- El Contratista deberá presentar un informe mensual del servicio de internet, que incluya todas las estadísticas de fallas del periodo, número de ticket, fecha y hora del reporte de falla y fecha y hora de solución de la avería. El informe del servicio de internet será requisito indispensable para otorgar la conformidad mensual del servicio de internet.
- Las llamadas de servicio podrán efectuar telefónicamente o por correo electrónico (considerándose todas estas formas igualmente validas) a los teléfonos y direcciones electrónicas indicados por el contratista. El Ministerio notificará las averías que se presenten incluyendo información de fecha y hora, descripción del problema y contacto en el Ministerio.

5.3.1.3.2. Niveles de Escalamiento:

Nivel de Escalamiento	Descripción	Periodo de atención	Tiempo de respuesta	Tiempo de solución	Modalidad
1	Ing. Residente	Lunes a viernes de 8:00 a.m. hasta las 6:00 p.m.	10 minutos	2 horas	Remota
2	Especialista 2do Nivel en NOC	24x7	2 horas	4 horas	Remota
3	Gerente del NOC	24x7	4 horas	24 horas	Remota

Cuadro N° 2: Niveles de escalamiento

Se indica que el Especialista Residente y el Especialista NOC/SOC, deberán contar con acceso a los routers y demás herramientas para las atenciones a la entidad.

Todos los tiempos indicados como parte del nivel de atención, son contados desde el registro de la solicitud de requerimiento y/o incidente, del Ministerio al Contratista, mediante tickets de atención.

Tiempo de respuesta, se define desde que se reporta el requerimiento y/o incidente del servicio por parte del Ministerio, mediante llamada telefónica o correo electrónico hasta el instante que el personal designado por el proveedor tome contacto con los encargados del Ministerio.

Tiempo de solución, se define desde que el especialista del proveedor registra el incidente mediante un ticket de atención hasta el instante que el servicio ha retomado a su operación normal.

5.3.1.3.3. Procedimiento de solución de incidentes:

- Al ocurrir una avería o caída del servicio, de severidad media o alta, el NOC alertará de

¹⁷ Absolución N° 84

manera automática con su sistema de monitoreo y gestión, y se generará el ticket de manera automática que luego será informado a la Oficina de Informática.

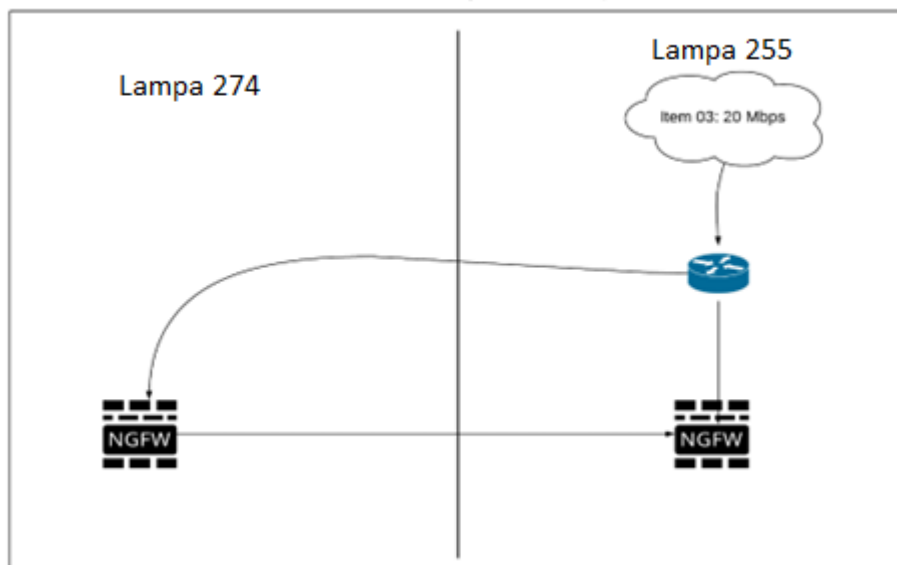
- El Ing. Residente, atenderá de manera personalizada, todos los incidentes y requerimientos remitidos por el Ministerio, deberá contar con los accesos a todos los equipos que forman parte del servicio. El Ing. Residente será asignado al Ministerio, permanecerá durante toda la vigencia del contrato. Se aceptará cambio de Ing. Residente, solo en casos de fuerza mayor, debidamente sustentado y aprobado por el Ministerio. El reemplazante deberá contar con un perfil igual o superior.
- Al requerir uno o varios cambios en las políticas y/o configuraciones de los routers o reportes a demanda, que la entidad solicite o desee realizar, el Ministerio reportará al NOC por teléfono o correo electrónico. Cabe indicar que los cambios en las políticas y/o configuraciones y reportes, el Contratista los atenderá de manera ilimitada, sin restricción de cantidad de solicitudes y sin costos adicionales.
- Una vez recibida la notificación, el Especialista 1er Nivel registrará el requerimiento de servicio y proporcionará al Ministerio un número de ticket de incidente o requerimiento. Dicho ticket servirá para realizar el seguimiento respectivo y escalamiento que fuera necesario.
- En caso que el Especialista 1er Nivel no solucione el incidente tendrá que escalar al nivel 2 y quien atenderá el incidente presentado.
- De no solucionar la problemática el nivel 2, el incidente se escala al nivel 3 donde el Gerente del NOC debe brindar la solución definitiva.
- El ticket será cerrado, cuando se solucione el incidente o se atienda el requerimiento y se obtenga la correspondiente aprobación por parte del Ministerio.
- El soporte proporcionado por el proveedor será telefónico, remoto y on-site, dependiendo de la severidad del caso.

5.4. ITEM 03: SERVICIO ACCESO A INTERNET- AUXILIAR

TIPO ENLACE	VELOCIDAD MINIMA ENLACE	OVERBOOKING LOCAL	OVERBOOKING EN LA SALIDA INTERNACIONAL	ORIGEN
Enlace auxiliar	20 Mbps	1.1	1.1	Jr. Lampa N° 255 Cercado de Lima

El enlace será dedicado y de fibra óptica con canalización subterránea hacia la sede Lampa del Ministerio, destinado a pruebas externas. El contratista debe implementar un enlace de fibra óptica canalización subterránea hacia el centro de cómputo de la sede de Lampa 255 y un enlace de fibra óptica hacia la Sede Lampa 274. El enlace solicitado deberá asignar el direccionamiento IP público necesario y deberán realizarse las configuraciones necesarias que permita al Ministerio gestionar la contingencia de manera automática.

El contratista podrá utilizar el enlace de fibra óptica existente entre Lampa 255 y el Lampa 274 propiedad del Ministerio.



5.4.1. Servicios Incluidos

5.4.1.1. Servicio de Implementación

Será responsabilidad del Contratista la instalación de la solución ofertada en su totalidad, dentro del plazo ofrecido, para lo cual debe proveer todos los bienes y servicios necesarios para su correcta instalación.

El Contratista será responsable de optimizar y configurar adecuadamente cada componente ofertado a satisfacción del Ministerio durante la etapa de instalación. El Contratista adjudicado estará encargado de hacer el levantamiento de información de la red del Ministerio, incluyendo configuraciones, políticas y tablas de ruteo, con la finalidad de que luego de la implementación, no existan problemas de comunicación y seguridad. El Ministerio designará un especialista técnico de contacto, que proporcionará información sobre el equipamiento del Ministerio. El Contratista adjudicado debe hacer el levantamiento de información de la red del Ministerio, incluyendo configuraciones, políticas y tablas de ruteo.

El acceso a la sede Central debe ser subterráneo. El acceso a la sede Central del Ministerio debe ser por el jirón Lampa 255, mientras que al enlace backup será por el Jr. Lampa 274.

En la etapa de activación del servicio el Contratista debe realizar una prueba de Saturación de ancho de banda, el cual debe quedar a satisfacción del Ministerio.

5.4.1.2. Gestión de Soporte Técnico

5.4.1.2.1. Soporte Técnico ante fallas del servicio

- El contratista deberá indicar el número telefónico, para reportar fallas técnicas (averías) en el servicio, el cual será el único punto de contacto con el operador y niveles de escalamiento.
- El Contratista deberá contar con un centro permanente de operaciones para subsanar las fallas técnicas ante cualquier llamada de servicio por parte del Ministerio. El Contratista debe contar con un centro permanente de operaciones, con las siguientes características y funciones:
 - Monitoreo en modalidad 24x7x365 de la solución oferta.
 - El centro debe contar con número de teléfono.
 - Debe ser un centro de contacto para recepción de reportes y solución de fallas técnicas.
 - Desde dicho centro se debe recepcionar llamadas de servicio del Ministerio, de lunes a domingo de 00 a 24 horas.
- El Ministerio podrá realizar llamadas de servicio de lunes a domingo de 00.00 a 24.00 horas. El Contratista deberá generar tickets de atención por cada incidente reportado.

- El tiempo de reparación de averías del equipamiento a suministrar en el periodo de contrato, deberá ser como máximo de veinticuatro (24) horas. Contabilizado desde que se crea el reporte de avería. De excederse el tiempo indicado para solucionar un problema, el tiempo de exceso será considerado para el cálculo de penalidades (numeral 16.2).
- El Contratista deberá presentar un informe mensual del servicio de internet, que incluya lo solicitado en el numeral 11.3 del presente documento. El informe del servicio de internet será requisito indispensable para otorgar la conformidad mensual del servicio de internet.
- Las llamadas de servicio podrán efectuar telefónicamente o por correo electrónico (considerándose todas estas formas igualmente validas) a los teléfonos y direcciones electrónicas indicados por el contratista. El Ministerio notificará las averías que se presenten incluyendo información de fecha y hora, descripción del problema y contacto en el Ministerio.

5.4.1.2.2. Niveles de Escalamiento:

Nivel de Escalamiento	Descripción	Periodo de atención	Tiempo de respuesta	Tiempo de solución	Modalidad
1	Ing. Residente	Lunes a viernes de 8:00 a.m. hasta las 6:00 p.m.	30 minutos	2 horas	Remota
2	Especialista 2do Nivel en NOC	24x7	2 horas	4 horas	Remota
3	Gerente del NOC	24x7	4 horas	24 horas	Remota

Cuadro N° 3: Niveles de escalamiento

Se indica que el Especialista Residente y el Especialista NOC/SOC, deberán contar con acceso a los routers y herramientas para las atenciones a la entidad.

Todos los tiempos indicados como parte del nivel de atención, son contados desde el registro de la solicitud de requerimiento y/o incidente, del Ministerio al Contratista, mediante tickets de atención.

Tiempo de respuesta, se define desde que se reporta el requerimiento y/o incidente del servicio por parte del Ministerio, mediante llamada telefónica o correo electrónico hasta el instante que el personal designado por el contratista tome contacto con los encargados de la Oficina de Informática del Ministerio.

Tiempo de solución, se define desde que el especialista del contratista registra el incidente mediante un ticket de atención hasta el instante que el servicio ha retomado a su operación normal.

5.4.1.2.3. Procedimiento de solución de incidentes:

- Al ocurrir una avería o caída del servicio, de severidad media o alta, el NOC lo alertará de manera automática con su sistema de monitoreo y gestión, y se generará el ticket de manera automática que luego será informado el MEF.
- Al requerir uno o varios cambios en las políticas y/o configuraciones de los routers o reportes a demanda, que la entidad solicite o desee realizar, el Ministerio reportará al NOC por teléfono o correo electrónico. Cabe indicar que los cambios en las políticas y/o configuraciones y reportes, el Contratista los atenderá de manera ilimitada, sin restricción de cantidad de solicitudes y sin costos adicionales.
- Una vez recibida la notificación, el Ing. residente registrará el requerimiento de servicio y proporcionará al Ministerio un número de ticket de incidente o requerimiento. Dicho ticket servirá para realizar el seguimiento respectivo y escalamiento que fuera necesario.
- En caso que el Ing. residente no solucione el incidente tendrá que escalar al nivel 2 y quien atenderá el incidente presentado.
- De no solucionar la problemática el nivel 2, el incidente se escala al nivel 3 donde el Gerente del NOC debe brindar la solución definitiva.

- El ticket será cerrado, cuando se solucione el incidente o se atienda el requerimiento y se obtenga la correspondiente aprobación por parte del Ministerio.
- El soporte proporcionado por el proveedor será telefónico, remoto y on-site, dependiendo de la severidad del caso.
- Deberá consignar los datos de ingeniero residente en el acta de activación del servicio.

5.5. Requerimientos técnicos para todos los ítems

5.5.1. ASPECTOS GENERALES

- Para todos los ítems, la empresa contratista deberá instalar un servicio de Internet y este tendrá presencia en las 2 sedes de Ministerio (Lampa 255 y Lampa 274, ambos con rutas de fibra óptica diferentes) para trabajar en un escenario ACTIVO/PASIVO, manejando el mismo segmento público.
- Para todos los ítems, la empresa contratista deberá instalar un servicio de Internet y este tendrá presencia en las 2 sedes de Ministerio (Lampa 255 y Lampa 274, ambos con rutas de fibra óptica diferentes) para trabajar en un escenario ACTIVO/PASIVO, manejando el mismo segmento público.
- El contratista deberá cumplir con las condiciones, estándares y normas que aseguren el correcto funcionamiento de los enlaces y servicio de accesos a Internet.
- Todos los equipos, materiales y accesorios a ser instalados en las sedes del Ministerio para la provisión del servicio, serán proporcionados por el contratista.
- Los routers para cada enlace serán nuevos, y serán provistos por el contratista, deberán operar de manera independiente para cada uno de los tipos de enlaces ofertados, incluyéndose la operatividad del enlace principal, secundario y auxiliar.
- El contratista debe contar con la infraestructura necesaria para brindar los servicios, tales como enlaces redundantes con capacidad de recuperación ante fallas.
- El contratista debe contar con un cuadro de personal especializado destinado a brindar soporte y asistencia técnica durante el periodo del contrato (asistencia de configuración de equipos de comunicación, definiciones de DNS, etc.). Todas las llamadas que el Ministerio realice deberán tener un trato preferente y prioritario en la atención por parte del personal del contratista para brindar el soporte y asistencia técnica en el menor tiempo posible. El contratista deberá implementar los mecanismos necesarios para atender las llamadas del personal técnico del Ministerio de manera prioritaria.
- Cada uno de los servicios de acceso a internet (principal, secundario y auxiliar) deben operar en modo activo para todos los ítems solicitados.
- Se debe proveer enlaces con protocolos de transporte que garanticen en todo momento el ancho de banda contratado. No se aceptará protocolo Frame Relay u otro, que al compartir el ancho de banda, degraden la performance del enlace.
- El Ministerio puede cambiar la configuración de los enlaces en un esquema multihomed o el sentido del tráfico (ingreso/salida) o la publicación de sus servicios por un enlace en particular, de acuerdo a sus necesidades de operación y bajo el principio técnico de balance global, alta disponibilidad y continuidad de sus operaciones.
- El contratista deberá contar con los mecanismos tecnológicos y de seguridad informática que permitan garantizar la seguridad de sus redes, sistemas de información y el servicio a proveer. Asimismo el contratista debe garantizar la seguridad de sus redes y sistemas de información ante intrusiones de cualquier tipo, para lo cual asumirá la responsabilidad por hechos que afecten la imagen del Ministerio producto de esta intrusión a sus redes, sin perjuicio de las acciones legales a los que el Ministerio pueda tomar en salvaguarda de su imagen Institucional (no necesariamente se hace referencia a la ISO 27001).
- En caso de que existan algún tipo de intrusión y vulneración que no sean imputables al contratista no será de su responsabilidad, por lo que no acarreará penalidad.
- El Contratista deberá garantizar el profesionalismo, responsabilidad y conocimientos técnicos de su personal en los centros de llamadas de reportes de faltas, 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.
- El servicio de internet (**Ítem 1 y 2**) deberá contar con una protección contra todo tipo de ataques de denegación de servicio o DoS (por sus siglas en ingles Denial of Service) y la

denegación de servicio distribuido o DDoS (por sus siglas en inglés Distributed Denial of Service).¹⁸

- ✓ Debe garantizar que este tipo de ataques no sature el enlace contratado ni obstaculice el tráfico legítimo.
 - ✓ Debe ser de tipo stateless.
 - ✓ Debe estar compuesto por componente en nube.
- El componente en nube de AntiDDoS, debe estar ubicado en territorio nacional dentro de la infraestructura del postor, esto con el fin de evitar que el tráfico de la entidad sea analizado fuera del país lo cual podría agregar un riesgo de seguridad, además de latencia a la red. Debe contar mínimamente con vigencia tecnológica y soporte activo de los fabricantes.
 - El Contratista deberá considerar como parte [del primer entregable](#)¹⁹ una topología con los equipos, marca y modelo a considerar. (numeral 11.1).
 - Todos los elementos que forman parte de la solución propuesta para todos los ítems deben ser nuevos y de primer [uso y de uso exclusivo para el Ministerio](#)²⁰.
 - El Ministerio proporcionará los dos puertos necesarios de 10 Gbps (SPF+) en el Firewall.

5.5.2. REQUERIMIENTOS TECNICOS MINIMOS

- Para cada enlace se debe implementar el tramo de última milla hacia cada sede, mediante tendidos independientes de fibra óptica con canalización subterránea y hacia nodos independientes del operador de telecomunicaciones – ISP (Contratista).
- Se debe implementar dos enlaces de fibra de iguales características uno hacia la sede Central (Lampa 255) y el otro enlace alterno hacia la sede Lampa 274.
- Los enlaces de acceso a internet deben operar de forma independiente y en modo activo cada uno.
- El ISP (Contratista) debe de garantizar el acceso de sus usuarios de forma directa a través de su red y con el menor tiempo de respuesta, es decir, no cursando tráfico por otro operador de internet. Para el resto de sus clientes deberá al menos enrutar el tráfico de datos a través del NAP Perú, esto es aplicable a todos los ítems.
- Se debe proveer de una herramienta en línea que permita realizar una gestión de tráfico del enlace. Debe mostrar el consumo de ancho de banda en tiempo real (con un delay máximo de 5 minutos). La herramienta de gestión de tráfico debe permitir como mínimo enviar alarmas y reportes de consumo de ancho de banda, caídas de los enlaces, consumos históricos de hasta los últimos 12 meses, protocolos de comunicaciones mas usados, TCP/IP, HTTP; HTTPS, FTP, SMTP, DNS, etc.
- Registro del DNS y asignación de las direcciones IP necesarias (familia de direcciones), AS como el respectivo acceso a internet e inscripción del dominio en los servidores del ISP público independiente y contar con un mínimo de 128 direcciones IPs (Versión 4), para los servicios de acceso a internet principal y secundario y 8 IPs (Versión 4) para el servicio de internet auxiliar, las cuales incluyen ip de red, ip de broadcast, ip de Gateway predeterminado.
- Acceso a todos los servicios internet, sin filtros ni restricciones para cualquier destino, pudiendose utilizar diferentes aplicaciones.
- Servicio sin restricciones de tráfico o volumen de tráfico de ingreso o salida.
- Garantizar la interoperabilidad con el protocolo de comunicación que el Ministerio emplee en este tipo de conexiones: TCP/IP.
- Contar con un centro de gestión del servicio en forma permanente (7x24), como administración de conectividad punto a punto, monitoreo proactivo.
- Contar con un centro de gestión especializado en seguridad (SOC) propio. Contar con un equipo especializado que brinde un soporte eficaz y oportuno para la atención, detección, tratamiento y resolución de incidentes de seguridad. Permitir la generación de soluciones flexibles a requerimientos del cliente. Soporte y asistencia técnica alineado al Nivel de Acuerdo de Servicio indicado en el numeral 16.2.
- Overbooking mínimo para el tráfico local 1:1

¹⁸ Absolución N° 30, 31, 61, 62, 110, 141, 159, 168, 169, 177, 182, 184, 199, 362, 363, 397

¹⁹ Absolución de consulta N° 51

²⁰ Absolución de consulta N° 115, 238, 327

- Overbooking mínimo para el tráfico internacional 1:1, [hasta el router de borde internacional propiedad del contratista](#)²¹.
- Se debe garantizar que el ancho de banda contratado para los enlaces (principal, secundario y auxiliar) debe ser de uso exclusivo para el Ministerio desde la puerta WAN del router del local del Ministerio hasta el router de borde del ISP (Contratista).
- Routers de Comunicaciones destinados para el servicio: nuevos, con accesorios de fábrica para el rackeo, con capacidad de soportar un crecimiento mínimo del 50 % del ancho de banda solicitado.
- El nivel de disponibilidad del servicio de internet deberá ser como mínimo del 99.70% mensual para cada uno de los servicios de acceso a internet (Ítem 1, Ítem 2 e Ítem 3).

5.5.3. SOPORTE Y ASISTENCIA TECNICA

- Se entenderá por **avería** a una interrupción parcial o total del servicio, así como a un decremento en la calidad del mismo (Calidad del Servicio UPTIME).
- Toda actividad o provisión de bienes que tenga que ejecutar el contratista para subsanar la avería serán sin costo alguno para el Ministerio.
- Se entenderá por Tiempo de Subsanación, al tiempo transcurrido entre la comunicación por parte del Ministerio al contratista, de la existencia de una avería, (llamada de servicio), y la subsanación de la misma a satisfacción.
- El Ministerio podrá efectuar llamadas de servicio **de lunes a domingo incluyendo feriados desde 00:00 a 24:00 horas**. Todas las llamadas que el Ministerio realice deberán tener un trato preferente y prioritario en la atención por parte del personal del contratista para la solución del evento o avería en el menor tiempo posible. El contratista deberá implementar los mecanismos necesarios para atender las llamadas del personal técnico del Ministerio de manera prioritaria.
- El contratista deberá entregar un informe mensual como parte del servicio, el cual será requisito indispensable para otorgar la conformidad mensual del servicio de internet y deberá incluir lo siguiente:
 - Equipo Balanceador, como mínimo: balanceo de aplicaciones, salud de enlaces, estadísticas, desempeño del equipo, entre otros.
 - Equipo Administrador de Ancho de Banda, como mínimo: consumo de aplicaciones de entrada más usadas, consumo de usuarios con más consumo, consumo de direcciones URL, histórico del consumo de tráfico de aplicaciones en la WAN, visibilidad de tráfico por sedes, eficiencia TCP y de aplicaciones, entre otras.
 - Equipo Anti-DDoS, como mínimo: servidores o grupos de protección, tráfico malicioso, bloqueo de hosts maliciosos, lista blanca, histórico de tipos de ataques, histórico de ataques por IP origen, histórico de tráfico por país de origen, histórico de inspección SSL, entre otros,
 - Herramienta de monitoreo: salud de los routers, consumo de los enlaces, aplicaciones que cursan por los enlaces, IPs que más consumen el ancho de banda, conversaciones IPs en los enlaces, entre otras.
- El contratista deberá entregar reportes a demanda en caso se requiera y deberán ser entregados dentro de las 24 horas de solicitado siempre y cuando estas puedan ser obtenidas desde los mismos equipos.
- Deberá entregar una cuenta de modo lectura para el equipo Balanceador, Administrador de Ancho de Banda y Anti-DDoS.
- **Para el mantenimiento correctivo de equipamiento a suministrar y soporte**
El tiempo máximo para solucionar un problema de mantenimiento correctivo del equipamiento a suministrar, que no incluya pérdida de servicio de internet, debe ser de máximo 24 horas contabilizados desde la emisión del ticket de avería emitido por el contratista. De excederse dicho tiempo, las horas de exceso se utilizarán para el cálculo de penalidad, a través del Uptime.

El tiempo máximo para solucionar un problema de soporte de incidentes y averías del servicio a suministrar, debe ser de máximo 02 horas contabilizados desde la emisión del ticket de avería emitido por el contratista.

En el caso del ítem 1, los equipos a suministrar al cual se hace referencia son los siguientes:

²¹ Absolución de consulta N° 95

- Administrador de ancho de banda
- Balanceadores de Tráfico de Internet.
- Equipos de networking que se utilicen (Routers y switches).

En el caso del ítem 2 y 3, los equipos a suministrar al cual se hace referencia son los siguientes:

- Equipos de networking que se utilicen (Routers y switches).

6. CLAUSULAS ESPECIALES

6.1. OTRAS OBLIGACIONES DEL CONTRATISTA

- Suministrar la documentación y bibliografía al Ministerio, del equipamiento a instalar, considerada necesaria para su utilización (instalación, operación, mantenimiento básico etc.) actualizada con la última versión y con la obligación permanente de que durante la vigencia de la garantía de buen funcionamiento de remitir toda modificación. La documentación deberá estar en formato impreso o en DVD / CD ROM, [en el idioma original²²](#), y deberá presentarse por mesa de partes, para la suscripción del contrato. (numeral 12.1)
- El contratista se compromete a laborar, en los horarios que el Ministerio haya establecido como calendario del proyecto y al cumplimiento estricto del plan de gestión del tiempo (cronograma de actividades) fijadas en el plan de trabajo indicado en el numeral 7.2 (asociado a los requerimientos de proyecto) del presente documento.
- El contratista deberá asignar un coordinador de proyecto para la Etapa de Implementación y activación de Servicio
- El contratista deberá asegurar que el personal que asigne al proyecto e interactúe directamente con personal del Ministerio deberá tener una comunicación fluida en lenguaje español. En caso el contratista utilice personal que no hable español fluido deberá incorporar, sin costo alguno para el Ministerio, traductores que permitan una comunicación fluida con el personal del Ministerio.
- El contratista se compromete a cumplir y observar lo establecido en la Ley de Seguridad y Salud en el Trabajo (aprobado mediante Ley N° 29783) y en su Reglamento (aprobado mediante Decreto Supremo N° 005-2012-TR); durante la ejecución de las prestaciones de servicios a su cargo; obligándose a implementar, dotar, proveer y/o suministrar a cada uno de sus trabajadores los implementos de seguridad que corresponda de acuerdo al grado y/o nivel de riesgo que pueda evidenciarse en el desarrollo de las actividades propias de la presente contratación dentro de las instalaciones del Ministerio; así como garantizar la contratación de los respectivos seguros de acuerdo a la normatividad vigente.
- El contratista deberá remitir a la Oficina General de Tecnologías de la Información (OGTI) al momento del inicio de ejecución del contrato, una relación del personal técnico autorizado a realizar labores de mantenimiento y soporte en los locales del Ministerio. Dicha relación deberá ser actualizada cuando se produzcan cambios.

6.2. OTRAS OBLIGACIONES DEL MINISTERIO

- El Ministerio es responsable de las autorizaciones de ingreso, desocupar los espacios, pasillos, etc., donde se realizarán los trabajos de instalación. Cualquier retraso por causas no imputables al Contratista quedara registrado en un Acta de Ocurrencia y/o se comunicará vía correo electrónico.
- El Ministerio proveerá lo siguiente:
 - Toma eléctrica con UPS.
 - Pozo a tierra.
 - Espacio en rack.
 - Cableado estructurado a nivel LAN.
 - Energía estabilizada 220 VAC.
 - Temperatura ambiental en un rango de 15°C a 25°C
 - Humedad relativa en el rango de 45% a 65% sin condensación.

6.3. CONFIDENCIALIDAD

²² Absolución de consulta N° 32, 63, 102, 112, 139, 142, 144, 232

- El contratista se compromete a mantener en reserva y no revelar a tercero alguno sin previa conformidad escrita del Ministerio, toda información que le sea suministrada por este último, excepto en cuanto resultare estrictamente necesario para el cumplimiento del Contrato y que restringirá la revelación de dicha información sólo a sus empleados y subcontratistas, sobre la base de "necesidad de conocer".
- El contratista se compromete (excepto que la ley dispusiera lo contrario o resultare necesario para obtener consejo profesional en relación con este Contrato) a no revelar ni permitir la revelación de cualquier detalle a los medios de prensa o a terceros, a no usar el nombre del Ministerio en cualquier promoción, publicidad o anuncio, sin previa autorización escrita del Ministerio.
- El contratista, o sus empleados, no podrá vulnerar, copiar, almacenar, publicar, o capturar la información del Ministerio que circule por sus Redes bajo ninguna circunstancia (configuraciones, versiones de software, características de la infraestructura, información bases de datos entre otros). La confidencialidad se mantendrá como mínimo el tiempo que ofrecerá el Contratista los servicios, es decir por 730 días calendario.
- Los presentes términos de referencia están regulados por las disposiciones legales en lo referente a los contratos y sujeto a las disposiciones del código penal en lo referente a delitos informáticos. El software o programa producido por el Contratista, así como la documentación generada producto del desarrollo de sus obligaciones, pasará a pertenecer al Ministerio, quien tendrá los derechos exclusivos para utilizar, modificar, publicar o difundir bajo cualquier soporte técnico creado o por crear, el software o programa, así como la información y documentos que se originen de ellos. Este derecho de exclusividad, sin fines de lucro, continuará vigente aún después de concluida la relación contractual de las partes.

6.4. ACTUALIZACION TECNOLOGICA

- En el caso de presentarse una "actualización tecnológica en los bienes o elementos que formen parte de la oferta del Contratista y en cualquier momento anterior a la entrega definitiva de la totalidad de los bienes, el Contratista deberá suministrar tales equipos o elementos actualizados, contando con la autorización previa del Ministerio y sin que esto implique un cargo adicional.
- Se entenderá que ha ocurrido una actualización tecnológica cuando se presenta una nueva versión del mismo producto en el mercado, que reemplaza a éste o un nuevo producto con características técnicas superiores –en la línea de productos ofrecido por el contratista a la generalidad de sus clientes- reemplaza al modelo ofrecido al Ministerio.
- El Contratista podrá, según su conveniencia y sin costos adicionales para el Ministerio, entregar equipos más avanzados o con características superiores a las ofrecidas, siempre y cuando cuente con la aprobación previa del Ministerio.
- En ningún caso el Contratista podrá entregar bienes cuya producción será descontinuada por el fabricante (debe contar con vigencia tecnológica, es decir, no contar con anuncios de EoL por parte del fabricante tales como: End-Of-Life, End-Of-Sale , End-Of-Support, o similares)
- Para efectos prácticos de casos especiales de actualización tecnológica se contrastará y tomará en cuenta la fecha de embarque de los bienes o la fecha de suscripción del contrato, la que se más reciente.

6.5. SEGURIDAD EN EL TRABAJO

- **Equipos de protección personal (EPP)**
El Contratista deberá de proporcionar los correspondientes equipos de protección personal (EPP) a su personal de acuerdo a la especialidad. Se entiende que el uso de dichos equipos es de carácter obligatorio mientras se encuentre laborando en las instalaciones del Ministerio de Economía y Finanzas.
- **Seguridad y Salud en el Trabajo (SST)**
Se pone en conocimiento del Reglamento Interno de Seguridad y Salud en el Trabajo, aprobado por el Comité de Seguridad y Salud en el Trabajo del Ministerio de Economía y Finanzas, Oficializado por Resolución de Secretaría General, publicado en la página Institucional.

El personal propuesto por el Contratista para la ejecución del servicio deberá contar en forma permanente con la indumentaria y equipos de protección personal relacionados con las actividades; y un carné de identificación visible, con fotografía actualizada.

▪ **Seguro Complementario de Trabajo de Riesgo (SCTR)**

Para todo el personal que prestará el servicio dentro de las instalaciones del Ministerio de Economía y Finanzas.

Los trabajadores deberán estar sujetos al Seguro Complementario de Trabajo de Riesgo. Para lo cual el contratista deberá presentar el Seguro Complementario de Trabajo de Riesgo (SCTR) vigente del personal que trabajará en la prestación. El SCTR deberá ser presentado [al día siguiente de la firma del contrato para lo cual la Entidad asignará a un personal de la Oficina de Infraestructura Tecnológica de la OGTI para las coordinaciones](#)²³.

7. NORMAS DEL OBJETO DE LA CONTRATACIÓN

- Ley de Telecomunicaciones, su reglamento y modificaciones.
- Ley N° 29956 de Portabilidad numérica en el servicio público móvil y el servicio de telefonía fija, su Reglamento y modificaciones.
- Código Nacional de Electricidad.
- RM N° 175-2008 MEM / DM, del 11.04.08 Conductores no propagantes de llama, libre de halógenos y ácidos corrosivos, para el cableado dentro de la Entidad.

8. DEL PERSONAL

El contratista deberá asinar un coordinador de proyecto para la Etapa de Implementación y activación de Servicio para cada ítem.

Cantidad	Perfil	Actividades a desarrollar
Coordinador de proyecto (01)	<ul style="list-style-type: none"> • Profesional Universitario titulado en Ingeniería de Sistemas o Ingeniería Electrónica o Ingeniería de Telecomunicaciones o Ingeniería Industrial y/o Ingeniería informática. • Colegiado y habilitado por el colegio de ingenieros del Perú. (deberá ser presentado para el inicio del servicio). • Deberá contar como mínimo tres (03) ²⁴ años de experiencia en gestión de proyectos de implementación o instalación o configuración o mantenimiento o administración de proyectos de internet o enlaces de transmisión de datos. La documentación será proporcionada para la suscripción de contrato. • Cabe señalar que el postor que se adjudique a 2 ítems podrá presentar un solo coordinador de proyecto. 	<ul style="list-style-type: none"> • Gestión del Alcance • Gestión del Tiempo • Gestión de Costos • Gestión de Riesgos • Gestión de Recursos Humanos • Gestión de Comunicaciones • Gestión de Calidad • Gestión de Cambios • Coordinación de la Implementación y activación de Servicio. • Elaboración de entregable 1. • Elaboración de Entregable 2.

Para el caso del Ingeniero Residente: (ítem 1)

Cantidad	Perfil	Actividades a desarrollar
----------	--------	---------------------------

²³ Absolución de consulta N° 56

²⁴ Absolución N° 104,185

Ingeniero Residente (01)	<ul style="list-style-type: none"> Profesional Universitario titulado en Ingeniería de Sistemas o Ingeniería Electrónica o Ingeniería de Telecomunicaciones o Ingeniería Industrial o Redes y Comunicaciones. Contar con la certificación oficial del fabricante de Balanceador de Tráfico y Administrador de Ancho de banda propuestos, o documento emitido por el representante local en el país (Perú) que indique que el personal cuenta con la certificación oficial de Balanceador de Tráfico y Administrador de Ancho de banda²⁵. Deberá contar como mínimo tres (03) años de experiencia en administración en balanceadores y administradores de ancho de banda. 	<ul style="list-style-type: none"> Atención de casos de incidentes, averías y nuevas implementaciones.
--------------------------	--	---

Para el caso del Ingeniero Residente: (Ítem 2 y 3)

Cantidad	Perfil	Actividades a desarrollar
Ingeniero Residente (01)	<ul style="list-style-type: none"> Profesional Universitario titulado en Ingeniería de Sistemas o Ingeniería Electrónica o Ingeniería de Telecomunicaciones o Ingeniería Industrial o Redes y Comunicaciones. Contar con la certificación oficial del fabricante de al menos dos de las soluciones a implementar, o documento emitido por el representante local en el país (Perú) que indique que el personal cuenta con la certificación oficial de al menos dos de las soluciones a implementar²⁶. Contar con capacitaciones en al menos dos de las soluciones a implementar. Deberá contar como mínimo un (01) año de experiencia en administración en routers y/o switches.²⁷ 	<ul style="list-style-type: none"> Atención de casos de incidentes, averías y nuevas implementaciones.

9. PÓLIZAS (Ítems 1 y 2)

Durante la vigencia del contrato, deberá presentar las siguientes pólizas:

- PÓLIZA POR DESHONESTIDAD.** – Por un monto equivalente a US\$ 50,000.00 (Cincuenta Mil y 00/100 Dólares Americanos). Las sumas aseguradas de los convenios de la póliza podrán expresarse en límite agregado anual; sin embargo, estos montos deberán utilizarse para cubrir exclusivamente los siniestros que afecten al MEF. Dicha póliza deberá cubrir la reposición integral de la pérdida de dinero, objetos o bienes por deshonestidad del personal asignado al servicio, tanto de bienes propiedad del Ministerio de Economía y Finanzas, como de terceros que se encuentren en sus instalaciones.
- PÓLIZA DE RESPONSABILIDAD CIVIL,** por un monto equivalente a US\$ 50,000.00 (Cincuenta Mil y 00/100 Dólares Americanos), que comprenda las coberturas de Responsabilidad Civil Extracontractual y Responsabilidad Civil Patronal. La suma asegurada de la póliza podrá expresarse en límite agregado anual; sin embargo, este monto deberá utilizarse para cubrir exclusivamente los siniestros que afecten al MEF. Dicha póliza cubre daños materiales y/o personales incluyendo fallecimientos, de acuerdo a los siguientes casos:
 - De operaciones:** Cubre la responsabilidad civil derivada de incendios y/o explosiones.
 - Patronal:** Cubre la responsabilidad civil de todo el personal destacado para la realización del servicio objeto de la convocatoria.

Nota:

Las pólizas y seguros deberán estar vigentes durante la ejecución del servicio.

²⁵ Absolución N° 05, 06,76

²⁶ Absolución N° 05, 06,76

²⁷ Absolución N° 155

Las pólizas deberán endosar al Ministerio de Economía y Finanzas como asegurado adicional.

- Los deducibles serán a cargo del Contratista.
- El procedimiento por el cual se determinará, en el caso se produjeran pérdidas, daños o perjuicios sobre los bienes de la Entidad, si son atribuibles al contratista por el actuar de su personal, consistirá en la elaboración de un informe por parte de la Oficina de Abastecimiento sobre los hechos ocurridos que generaron el daño o perjuicio, y que deberá incluir el descargo correspondiente por parte del Contratista. Para lo cual, la Oficina de Abastecimiento del Ministerio de Economía y Finanzas, comunicará a más tardar el día siguiente útil de producidos los hechos al Contratista solicitándole su descargo correspondiente, el cual podrá incluir fotos, testimonios u otros que sustente la posición del Contratista. El plazo para remitir el descargo al MEF será a más tardar al día siguiente útil de efectuada la notificación. Lo señalado se realizará sin perjuicio de la denuncia policial que el Ministerio de Economía y Finanzas pueda realizar.

Las pólizas solicitadas se presentarán para la suscripción del contrato.

10. LUGAR Y PLAZO DE EJECUCION DE LA PRESTACION

10.1. Lugar de la Prestación

Ítem 1: Sede Central (Principal) – Jr. Lampa 274 – Cercado de Lima.

Ítem 2: Sede CCM (Secundario) – Jr. Lampa 255 – Cercado de Lima.

Ítem 3: Sede Central (Auxiliar) – Jr. Lampa 274 – Cercado de Lima.

10.2. Plazo de implementación y capacitación

Ítem 1.- El plazo de implementación es de 130 días calendario a partir del día siguiente de la firma de contrato. En un plazo máximo de 10 días calendario de finalizado el plazo de implementación, se firmará un acta de activación del servicio. La fecha de inicio de la prestación, será al día siguiente de la fecha del acta de activación del servicio. En el primer mes de ejecución del servicio se realizará la capacitación del manejo de los equipos.

Ítem 2 y 3.- El plazo de implementación es de 110 días calendario a partir del día siguiente de la firma de contrato. En un plazo máximo de 10 días calendario de finalizado el plazo de implementación, se firmará un acta de activación del servicio. La fecha de inicio de la prestación, será al día siguiente de la fecha del acta de activación del servicio.

10.3. Plazo de ejecución de la prestación (para todos los ítems)

El plazo de ejecución del servicio de internet será por 730 días calendario, contabilizados a partir del día siguiente de la firma del “Acta de Activación del Servicio”²⁸.

11. ENTREGABLES

El contratista deberá presentar los siguientes entregables a través de mesa de partes del Ministerio de Economía y Finanzas.

11.1. Entregable 1 – Plan de trabajo (Para los Ítems 1 y 2)

- El contratista deberá presentar dentro de los 7 días contados a partir del día siguiente de la firma de contrato que incluya:
 - *Plan de gestión del Alcance*
 - *Plan de gestión del Tiempo*
 - *Plan de gestión de Costos*
 - *Plan de gestión de Riesgos*
 - *Plan de gestión de Recursos Humanos*
 - *Plan de gestión de Comunicaciones*
 - *Plan de gestión de Calidad*
 - *Plan de gestión de Cambios*

²⁸ Absolución N° 24

- *Topología con los equipos, marca y modelo a considerar. (numeral 5.5.1).*
- Además el plan debe incluir las etapas de instalación, pruebas, observaciones, levantamiento de observaciones, desarrollo, puesta en producción y capacitación. Asimismo, este plan será aprobado por la Oficina de Infraestructura Tecnológica (OIT) del Ministerio en un plazo máximo de diez (10) días calendarios.
- El Plan de mantenimiento preventivo y correctivo de los enlaces y equipos que componen el servicio deberá describir el procedimiento de mantenimientos, soporte y asistencia técnica, y los cronogramas de mantenimientos de acuerdo a :
 - Mantenimiento correctivo: A demanda
 - Mantenimiento preventivo: Anual
 - Soporte y asistencia técnica: A demanda

11.2. Entregable 2 – Informe de término de implementación

- Como entregable previo al inicio del servicio, el contratista deberá presentar un Informe por el cual comunica la conclusión de la etapa de instalaciones y pruebas, detallando el equipamiento instalado, números de circuitos, ancho de banda, direccionamiento IP WAN/LAN, configuración de calidad de servicio, esquema de conectividad por sede u otras actividades realizadas para brindar el servicio para cada enlace, incluyendo imágenes de cada una de las instalaciones.
- Previo al inicio del servicio el contratista deberá entregar un manual de usuario de la herramienta web que implementará para, la misma que mostrará los enlaces así como la información necesaria para medir los niveles de servicio requeridos. Adicionalmente y mensualmente, presentará la relación y detalle de averías presentadas en el periodo considerando los parámetros definidos en el NIVEL DE ACUERDO DE SERVICIO.
- El presente entregable, será entregado dentro de los cinco días calendario posterior a cumplido el plazo de la implementación del servicio por mesa de partes del Ministerio.

11.3. Entregable mensual (para todos los ítems)

- Contratista entregará un reporte mensual que contenga lo siguiente, el cual servirá para la emisión de conformidad mensual:
 - Consumo de ancho de banda del servicio de internet.
 - Reporte de tickets de solicitud de averías, en el que indicará la solución que se le a dado a cada uno.
 - Disponibilidad del servicio.
- Contratista deberá entregar por mesa de partes del Ministerio, los reportes mensuales dentro de los 5 días calendario posteriores a la culminación del período, el cual será requisito para la emisión de la conformidad mensual.

12. OTROS DOCUMENTOS A PRESENTAR

12.1 DOCUMENTOS PARA LA SUSCRIPCION DE CONTRATO ^{29 30}

- El postor adjudicado, deberá contar con un centro de atención de llamadas de reparación o asistencia técnica instalado de tal manera que le asegure al Ministerio que se encuentra en condiciones de cumplir con lo estipulado en las bases del ítem adjudicado. Para la acreditación de este requisito se deberá presentar declaración jurada, la cual se presentará para la suscripción de contrato.
- El postor adjudicado deberá indicar, mediante declaración jurada, como requisito para la firma del contrato, los números telefónicos, email de contacto para el reporte de averías así como el nombre del personal de contacto del ítem adjudicado y del ingeniero residente y del coordinado de proyecto.
- Procedimiento de “SOPORTE Y ASISTENCIA TÉCNICA” especificado en el numeral 5.5.3.

²⁹ Absolución N° 02,10,15,27: Se precisa que la Opinión N° 049-2022/DTN, señala que podrían presentarse circunstancias en las que cierto tipo de documentación no cumpla con las condiciones necesarias para ser legalizada o apostillada por las autoridades competentes como, por ejemplo: folletos, instructivos, catálogos o similares. Cabe señalar que, el proceso de legalizado o apostillado, se realiza sobre las firmas de los documentos extendidos en el exterior, en ese sentido, los documentos que no contengan firmas, no deberán ser legalizados o apostillados.

³⁰ Absolución N° 29,33,48,248

- El postor adjudicado, deberá presentar descripción detallada de los servicios ofertados y el equipamiento a instalar que evidencien que los mismos cumplen totalmente con lo requerido en los presentes términos de referencia (Anexo A)³¹
Asimismo, deberá presentar la siguiente documentación: Folletos, brochures, certificados, catálogos, instructivos, hojas de datos y/o manuales técnicos de los equipos descritos en el Anexo A “Características de los equipos ofertados”, dichos documentos se deben presentar en idioma castellano o en su defecto, acompañado de traducción.
Solo se aceptará carta del fabricante o subsidiaria local del fabricante o representante acreditado en el país, cuando se sustente alguna característica solicitada que no se encuentren en los documentos mencionados; asimismo, se precisa que la acreditación debe ser emitida al postor y no a la Entidad³².
- Documentos que acrediten el perfil del Personal descrito en el numeral 8 de los términos de referencia³³.
- El postor deberá indicar, mediante declaración jurada, los procedimientos e infraestructura que implementará o tiene implementada para lograr la calidad de servicio solicitado.
- Presentar el Anexo B³⁴ - Características de la solución de filtro web, y adicionalmente presentar la siguiente documentación: Folletos, brochures, certificados, catálogos, instructivos, hojas de datos y/o manuales técnicos de los equipos descritos en el Anexo B - Características de la solución de filtro web”, dichos documentos se deben presentar en idioma castellano o en su defecto, acompañado de traducción.
Solo se aceptará carta del fabricante o subsidiaria local del fabricante o representante acreditado en el país, cuando se sustente alguna característica solicitada que no se encuentren en los documentos mencionados; asimismo, se precisa que la acreditación debe ser emitida al postor y no a la Entidad.
- El postor adjudicado deberá indicar, mediante declaración jurada, que cumple con las características solicitadas en tercer párrafo del numeral 5.2 y 5.3 de los términos de referencia en relación a las características de la fibra óptica solicitada (Para los ítems 1 y 2)³⁵
- Documentación y bibliografía al Ministerio, del equipamiento a instalar, considerada necesaria para su utilización (instalación, operación, mantenimiento básico etc.) actualizada con la última versión y con la obligación permanente de que durante la vigencia de la garantía de buen funcionamiento de remitir toda modificación. La documentación deberá estar en formato impreso o en DVD / CD ROM, en idioma original³⁶.

12.2 DOCUMENTOS PARA EL INICIO DE LA PRESTACIÓN DEL SERVICIO

- Lista del personal que realizará la instalación, nombre completo y DNI.
- Seguro SCRT de todo el personal técnico que realice la instalación.
- El contratista deberá indicar el número telefónico, para reportar fallas técnicas (averías) en el servicio, el cual será el único punto de contacto con el operador y niveles de escalamiento³⁷.

13. OTROS DOCUMENTOS PARA LA ADMISIÓN

- Presentación del Anexo A (Características de los equipos ofertados), según el ítem que ofertará.
- Presentación del Anexo B.³⁸

14. MEDIDAS DE CONTROL

14.1. Área que supervisan:

La Oficina que supervisará el funcionamiento es la Oficina de Infraestructura Tecnológica (OIT).

³¹ Absolución N° 30, 31, 61, 62, 110, 141, 159, 168, 169, 177, 182, 184, 199, 362, 363, 397

³² Absolución N° 30, 31, 61, 62, 159, 168, 169, 177, 182, 184, 199, 362, 363, 397

³³ Absolución N° 34, 143, 161, 162, 163, 239, 266, 322, 323

³⁴ Absolución N° 02,10,15,27

³⁵ Absolución N° 48

³⁶ Absolución N° 32,

³⁷ Absolución N° 45

³⁸ Absolución N° 2, 10, 15, 27, 116, 158, 239, 266, 322, 323, 328, 358, 364, 391, 398

14.2. Área que Coordinará con el proveedor

La Oficina que coordinará con el proveedor será la Oficina de Infraestructura Tecnológica (OIT).

14.3. Área que brindará la Conformidad

La conformidad por el servicio de Implementación será emitida por la Oficina de Infraestructura Tecnológica (OIT) en un plazo máximo de siete (7) días calendario.

La conformidad por el servicio de internet se otorgará en forma mensual durante el periodo del contrato y será emitida por la Oficina de Infraestructura Tecnológica (OIT) en el plazo máximo de siete (7) días calendario de recepcionado el informe mensual.

15. FORMA DE PAGO

El pago se realizará al Código de Cuenta Interbancaria (CCI) del proveedor, en la moneda de Sol, en 24 pagos iguales, de forma mensual, luego de emitida la conformidad del servicio y de acuerdo a lo establecido en el artículo 171° del Reglamento de la Ley de Contrataciones del Estado, según al ítem adjudicado.

Para el primer pago del ítem 1 servicio acceso a internet principal, deberá de adjunta el acta de conformidad de la capacitación realizada.

16. PENALIDADES

16.1. PENALIDAD POR MORA

Ítem 1:

En caso de retraso en culminar la implementación, se aplicará la penalidad por mora indicada en el Reglamento de la Ley de Contrataciones del Estado.

Ítem 2 y 3:

En caso de retraso en culminar la implementación, se aplicará la penalidad por mora indicada en el Reglamento de la Ley de Contrataciones del Estado.

16.2. OTRAS PENALIDADES

De acuerdo con el artículo 163 del Reglamento se pueden establecer penalidades distintas al retraso o mora en la ejecución de la prestación

- **Servicio de internet**

Las penalidades por mora o retrasos durante el período de 730 días calendario del servicio se aplicarán sobre el monto mensual a pagar por cada enlace y de acuerdo a lo indicado en el **NIVEL DE ACUERDO DE SERVICIO siguiente:**

En caso la disponibilidad del servicio de internet (para ambos ítems) sea menor al valor indicado en el numeral 5.5.2., el Ministerio de Economía y Finanzas (Ministerio) se reserva el derecho de aplicar créditos compensatorios según la fórmula y cuadro adjunto.

$$\frac{(\text{Tiempo total} - \text{Tiempo total no disponible})}{\text{Tiempo total}} * 100$$

Cuadro de penalidad aplicable a servicios de acceso a internet:

Nivel de Disponibilidad	Porcentaje de penalidades
$\geq 99.70\%$	Sin penalidad
$< 99.70\%$ y $\geq 99.00\%$	5% del monto mensual del servicio
$< 99.00\%$	10% del monto mensual del servicio

- El servicio mensual se basa en el estimado de 720 horas/meses. La calidad de servicio solicitada es mayor a 99.70% lo que representa 718 horas/mes de disponibilidad mínima del servicio (para cada ítem).

- Se entiende por Tiempo total no disponible, la sumatoria de todos los minutos durante los cuales el Ministerio no tuvo la disponibilidad del servicio, siendo estos minutos acumulables en forma mensual.
- No se contabilizará el tiempo de no disponibilidad de las interrupciones de servicio que pudieran producirse por causas imputables al Ministerio o terceros.

- **Por incumplimientos**

N°	Supuesto de aplicaciones de penalidades	Forma de cálculo	Procedimiento
1	Cuando no se acredite la presencia del coordinador de proyecto, se le aplicará una penalidad que se señala por cada día de ausencia.³⁹	Se aplicará una penalidad de S/. 300.00 por cada día de ausencia del personal.	Según informe de la Oficina de Infraestructura Tecnológica de la Oficina General de Tecnología de la Información.
2	Cuando el Contratista no cumpla con dotar a su personal de los equipos de seguridad personal (EPP), o se registre que algún personal no hace uso de dichos equipos.	Se aplicará una penalidad de S/. 250.00 por día y por persona.	Según informe de la Oficina de Infraestructura Tecnológica de la Oficina General de Tecnología de la Información.
3	Cuando se registre que no se instaló o no se cuenta con las señales de seguridad en la zona de trabajo.	Se aplicará una penalidad de S/. 100.00 por cada hecho registrado.	Según informe de la Oficina de Infraestructura Tecnológica de la Oficina General de Tecnología de la Información.
4	Por dejar y/o almacenar, desechos o materiales en pasadizos y lugares no autorizados por el coordinador del servicio de la Entidad. Por hallazgo	Se aplicará una penalidad S/. 100.00 por hecho registrado.	Según informe de la Oficina de Infraestructura Tecnológica de la Oficina General de Tecnología de la Información.
5	Cuando el personal no porte su carnet de identificación o fotocheck.	S/ 50.00 por día y por persona	Según informe de la Oficina de Infraestructura Tecnológica de la Oficina General de Tecnología de la Información.
6	Demora en la presentación del informe mensual	Se aplicará una penalidad de S/. 100.00 por día	Según informe de la Oficina de Infraestructura Tecnológica de la Oficina General de Tecnología de la Información.
7	No contar con Certificación oficial de la marca, del personal que realiza la implementación	Se aplicará una penalidad S/. 300.00 por persona.	Según informe de la Oficina de Infraestructura Tecnológica de la Oficina General de Tecnología de la Información.
8	Incumplimiento de los Protocolos Sanitarios	5% de una UIT por cada evento identificado.	Según informe de la Oficina de Infraestructura Tecnológica de la Oficina General de Tecnología de la Información.
9	Cuando se presente retraso en la Capacitación	Se aplicará una penalidad S/. 300.00 por día.	Según informe de la Oficina de Infraestructura Tecnológica de la Oficina General de Tecnología de la Información.
10	Cuando se exceda el plazo de 02 horas para solucionar un problema de soporte de incidentes y averías del servicio a suministrar.	Se aplicará una penalidad de 1 % de una UIT por cada hora transcurrida, luego de vencido el plazo de 2 horas.	Según informe de la Oficina de Infraestructura Tecnológica de la Oficina General de Tecnología de la Información.

- **UPTIME**

³⁹ Absolución 55, 324

El UPTIME es un coeficiente que mide el nivel del servicio brindado por el Contratista en un periodo mensual.

Se calculará el UPTIME, en forma mensual de la siguiente forma:

$$\text{UPTIME} = \frac{(\text{THM} - \text{THE}) \times 100}{\text{THM}}$$

Donde:

THM = Cantidad de horas de atención brindadas por el contratista para la provisión del servicio.

THE = Sumatoria de las cantidades de horas de exceso (respecto al tiempo de atención máximo establecido para solucionar el problema, que es de 24 horas) que incurrió el contratista para subsanar las averías.

La penalidad mensual estará en función del UPTIME según la siguiente tabla:

"Tabla de UPTIME"

Rango de UPTIME	Penalidad (1)
>99,90%, <= 99,99%	1,00%
>99,80%, <= 99,90%	1,50%
>99,70%, <= 99,80%	2,00%
>99,60%, <=99,70%	2,50%
>99,50%, <=99,60%	3,00%
>99,40%, <=99,50%	3,50%
>99,30%, <=99,40%	4,00%
>99,20%, <=99,30%	4,50%
>99,10%, <=99,20%	5,00%
>99,00%, <=99,10%	5,50%
Menor o igual a 99,00%	10,00%

Penalidad (1): El porcentaje de penalidad aplicable al contrato.

El Ministerio podrá cobrar una penalidad hasta un monto máximo equivalente al 10% del monto del contrato vigente. Cuando se llegue a cubrir el monto máximo de la penalidad (10%) por mora o de otras penalidades, El Ministerio podrá resolver el contrato por incumplimiento.

17. RESPONSABILIDADES DEL POSTOR

La recepción conforme de EL Ministerio no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos (artículo 146° del Reglamento de la Ley de Contrataciones).

El plazo máximo de responsabilidad del contratista es de un año contado a partir de la conformidad otorgada por EL Ministerio (artículo 40° de la Ley de Contrataciones del Estado).

II. REQUISITOS DE CALIFICACIÓN

A. HABILITACIÓN

Requisito

El contratista deberá presentar copia de la autorización del servicio de valor añadido emitido por el Ministerio de Transporte y Comunicaciones a brindar, dicha autorización deberá de coberturar el servicio de conmutación de datos por paquete (internet) y mensajería interpersonal (correo electrónico).

Acreditación

Copia del documento emitido por la autoridad competente que acredite su autorización al servicio de valor añadido por el Ministerio de Transporte y Comunicaciones para la comercialización del servicio de conmutación de datos por paquete y mensajería interpersonal (correo electrónico).

B. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Requisitos:

Para el ítem 1

El postor deberá acreditar un monto facturado acumulado equivalente a cuatro millones y 00/100 (S/. 4'000,000.00) Soles, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran servicios similares a los siguientes:

- Servicio de internet inalámbrico a través de modem USB.
- Servicio de internet dedicado
- Servicio de internet

- Servicio de transmisión de datos
- Servicio de transmisión de datos a través de fibra oscura.

Para el ítem 2

El postor deberá acreditar un monto facturado acumulado equivalente a un millón y 00/100 (S/. 1'000,000.00) Soles, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de S/ 100,000.00 (Cien mil con 00/100 soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa

Se consideran servicios similares a los siguientes:

- Servicio de internet inalámbrico a través de modem USB.
- Servicio de internet dedicado
- Servicio de internet
- Servicio de transmisión de datos
- Servicio de transmisión de datos a través de fibra oscura.

Para el ítem 3

El postor deberá acreditar un monto facturado acumulado equivalente a cien mil y 00/100 (S/. 100,000.00) Soles, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de S/ 10,000.00 (Diez mil con 00/100 soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa

Se consideran servicios similares a los siguientes:

- Servicio de internet inalámbrico a través de modem USB.
- Servicio de internet dedicado
- Servicio de internet
- Servicio de transmisión de datos
- Servicio de transmisión de datos a través de fibra oscura.

Acreditación para todos los ítems:

La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago⁴⁰, correspondientes a un máximo de veinte (20) contrataciones.

⁴⁰ Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

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

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

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

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

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

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

Si el postor acredita experiencia de una persona absorbida como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo.

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

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

O.G.T.I.

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

(...)

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

ANEXO A
CARACTERÍSTICAS DE LOS EQUIPOS OFERTADOS

Características		Datos del bien propuesto			Pág.	Ítem, numeral, capítulo de la pagina	Indicar texto o párrafo donde se evidencie cumplimiento de la característica solicitada	Fuente (folletos o brochure u hoja de datos o manuales técnicos)
		Marca	Modelo	Número de parte del Fabricante				
	Administrador de Ancho de Banda							
1	El equipo Administrador de Ancho de Banda deberá ser un appliance en hardware de propósito dedicado. El software en el equipo debe ser integrado directamente por el mismo fabricante ya que no se acepta soluciones de tipo software que depende de sistemas operativos genéricos (Windows o Linux) que deben ser instalados previamente, ya que esto no garantiza el soporte integro de la solución debido a que el sistema operativo sería independiente a la solución y expuesto a vulnerabilidades, esta capacidad debe ser confirmada directamente por el fabricante							
2	Debe contar con un puerto de Consola y de administración independiente. Asimismo, soportar interfaces de 10Gbps y 40Gbps							

3	La solución debe estar en capacidad de autoevaluar el tráfico a través de un aprendizaje y poder indicar al administrador por medio mensajes a través de la consola o por correo electrónico los cambios importantes a tener en cuenta, como nuevas aplicaciones con alta tendencia de consumo y tráfico que no está siendo atendido por un nivel de política creado							
4	La solución debe poder medir por demanda y de forma activa el rendimiento de la red a través de la generación de flujos de tráfico TCP o UDP indicando tamaño del datagrama disponible, paquetes perdidos en la medición y rendimiento de carga útil o "Payload"							
5	Debe permitir la generación de políticas de control (restricción o priorización) de ancho de banda para el tráfico entrante y saliente de manera independiente. Debe proporcionar la funcionalidad de cache en capa de aplicación para tráfico HTTP, a través de licenciamiento de software y no agregando componentes de hardware a la solución. La función del cache consiste en reducir el tráfico repetitivo de tipo Web en el enlace gestionado.							

6	Deberá contar con almacenamiento de datos históricos en la misma unidad, para posterior generación de reportes tabulares y gráficos de la utilización del ancho de banda, hasta de un año atrás. Capacidad de almacenamiento de al menos 1.6TB SSD en RAID 1 para garantizar la disponibilidad de la data histórica y fuente redundante.							
	Anti-DDoS							
1	La solución debe de contar con un mecanismo de bypass (se requiere el bypass sea con los puertos de fibra ya que se requieren interfaces 10GE SFP+)							
2	La solución implementada debe proporcionar al menos 4 interfaces de 1 Gbps de cobre							
3	La solución debe tener una capacidad de inspección de al menos 4 Gbps							
4	La solución instalada en sitio deberá soportar un crecimiento de hasta 20Gbps sin necesidad de hacer cambio de hardware							
5	El sistema debe incluir fuentes de alimentación de energía AC redundantes y debe admitir intercambio caliente ("hot swap") de una fuente de alimentación degradada durante el funcionamiento normal del sistema.							

6	El sistema debe de proporcionar un filtro de amenazas salientes para evitar que el tráfico malicioso abandone la red, utilizando la inteligencia de amenazas y sus categorías							
7	El sistema deberá de poder inspeccionar tráfico SSL a través de un módulo de seguridad basado en hardware embebido dentro del mismo dispositivo							
8	El sistema debe proporcionar la capacidad para administrar sus archivos a través de la Interfaz del Usuario (UI), incluida la carga, descarga y eliminación. Se aceptará opcionalmente la descarga de informes en PDF o CSV							
9	El sistema debe admitir su monitoreo a través de SNMP v2 o v3							
10	El acceso a la Interfaz de Usuario deberá de ser a través de un protocolo seguro como es HTTPS							
11	El sistema debe poder realizar una autenticación de contraseña estática por medio de la integración de RADIUS o TACACS +							
12	El sistema debe de soportar prevención de inundación suplantada (spoofing) de SYN's TCP que autentifiquen conexiones TCP desde los hosts origen							
13	El sistema debe de soportar el bloqueo de solicitudes DNS malformadas en el puerto 53 que no cumplan con el estándar RFC.							
14	El sistema deberá de poder bloquear tráfico Multicast							

15	El sistema deberá de identificar web crawlers y monitorear su uso							
	Balanceador de tráfico de Internet							
1	Throughput: 26 Gbps (capa 4 y 7)							
2	SSD: 240 GBytes							
3	Memoria: 32 Gbytes							
4	Cada equipo debe cumplir con las siguientes características:							
4.1	La solución debe soportar al menos 32 Millones de conexiones simultáneas en capa 4							
4.2	La solución debe soportar al menos 900.000 conexiones por segundo en L4							
4.2	La solución debe soportar al menos 2.8 Millones de HTTP Requests por Segundo							
5	Respuestas DNS por segundo o DNS Queries Per Second (QPS) ⁴¹ : 500 mil							
6	8 puertos 10/100/1000 Base-T RJ45 para cableado en cobre (que permita hacer inspección de 04 líneas físicas de red independientes)							
7	6 puertos de 10 SPF+ Gigabit Ethernet							
	Router							
1	Routers de Comunicaciones destinados para el servicio: nuevos, con accesorios de fábrica para el rackeo, con capacidad de soportar un crecimiento mínimo del 50 % del ancho de banda solicitado.							

⁴¹ Absolución de consulta N° 345

	Monitoreo de Enlaces y Dispositivos Críticos							
1	Suministro e instalación de solución de monitoreo que permita el análisis y captura del flujo de tráfico generado para al menos 200 dispositivos o interfaces WAN o backbone							
2	Debe permitir visualizar y analizar la variación de los flujos de tráfico al menos cada 60 segundos e incluir espacio de almacenamiento (storage) suficiente como para almacenar dicha información durante al menos (01) año manteniendo la granularidad de 60 segundos							
3	Debe permitir monitorear la disponibilidad de los enlaces y mediciones críticas de la red, incluida la pérdida de paquetes, errores y descartes.							
4	Debe permitir monitoreo del Hardware de los diferentes dispositivos de red.							
5	La solución de monitoreo deberá permitir realizar diagramas topológicos detallados de la red en tiempo real (por lo menos en capa 2).							
6	Debe permitir hasta diez (10) usuarios concurrentes.							
7	Debe permitir correlacionar las tendencias de las alarmas con la frecuencia de los cortes.							
	Herramienta Automate Mapping y Troubleshooting							
1	Debe permitir crear diagramas topológicos detallados de la Red en tiempo real, así como guardar el historial de los registros.							

2	Debe permitir descubrir como mínimo, los siguientes tipos de equipos (Router, Switches L2, Switches L3, Firewall, Load Balancers, WAN Optimizer, WAPs)							
3	Debe recopilar la información de los equipos descubiertos por SNMP capturando como mínimo: Dirección IP, Marca, Modelo, MAC y debe tener la opción de poder exportar esta información del inventario de los equipos descubiertos en un archivo MS Excel/CSV							
4	Debe permitir exportar los mapas/diagramas de red en formato MS Visio, asimismo debe ser capaz de descubrir e identificar como mínimo seis mil (6,000) tipos de dispositivos y al menos 300 diferentes marcas/modelo de equipos en la red							
5	Debe visualizar el Troubleshooting en tiempo real, diagnosticando el diseño y resaltar los errores o problemas en la configuración (BGP, OSPF, RIP Routing).							

ANEXO B - CARACTERÍSTICAS DE LA SOLUCIÓN DE FILTRO WEB

	Características	Datos del bien propuesto			Pág.	Ítem, numeral, capítulo de la pagina	Indicar texto o párrafo donde se evidencie cumplimiento de la característica solicita.	Fuente (folletos o brochure u hoja de datos o manuales técnicos)
		Marca	Modelo	Número de parte del Fabricante				
1	Filtro web							
2	Capacidad de Prevención de Malware de Día Cero o no conocido para el servicio de Internet (mediante emulación de malware – SandBox en nube).							
3	Capacidad de Extracción de Malware o extracción del contenido activo riesgoso de los documentos descargado a través del servicio de Internet							
4	Capacidad de Prevención de Phishing de Día Cero o phishing no conocido para el servicio de Internet, que no pueda ser identificado mediante técnicas de reputación de URL y/o dominios							