TERMINOS DE REFERENCIA

Denominación de la Contratación	Servicio de Internet Dedicado para las oficinas del PMSAJ
Área Usuaria / Entidad beneficiaria	Unidad de Administración y Finanzas
Meta Presupuestal	0004
Código Único de Inversiones/ Componente del PI	2413068 2.1-Gestión del Programa
Actividad del POI	AOI00143700009

1. FINALIDAD PÚBLICA

La contratación del servicio tiene como finalidad principal, el proveer de acceso al servicio de internet la cual permite mantener interconexión de los aplicativos financieros, descarga y subida de información a través de portales web de las entidades públicas, como así de mantener actualizadas los diferentes aplicativos informáticos instalados en las estaciones de cómputo, servidores como sistema operativo, herramientas de ofimática, antivirus, etc. que son empleados en el desarrollo de las actividades administrativas del Programa de Inversión Mejoramiento de los Servicios de Justicia No Penales a través de la implementación del Expediente Judicial Electrónico (EJE), con código único N 2413068, permitiendo cumplir con los objetivos del programa en los plazos previstos.

2. OBJETO DEL SERVICIO

El servicio de Internet dedicado permitirá publicar, intercambiar información y gestionar adecuadamente los servicios tecnológicos en el cumplimiento de las funciones del Programa "Mejoramiento de los servicios de Justicia No Penales a través de la Implementación del Expediente Judicial Electrónico (EJE) código único N° 2413068; asimismo permitirá la comunicación e intercambio con las instituciones participantes.

3. ALCANCE Y DESCRIPCION DEL SERVICIO

3.1 CARACTERISTICAS TECNICAS MINIMAS DE OPERACION DEL SERVICIO

DESCRIPCIÓN	CARACTERÍSTICA
Velocidad Mínima del Enlace (Ancho de Banda) Nacional e Internacional	400 Mbps (Upstream / Dowstream, Garantizado) - Simétrico
Overbooking	1:1
Herramienta de monitoreo	Vía Web.
Disponibilidad Mínima del Servicio	99.5%
Disponibilidad de Atención de Soporte Técnico	24 x 7 x 365
La Red del Proveedor debe tener la capacidad de soportar	Voz, Datos y Video
Medio físico de backbone del proveedor	Fibra Óptica.
Direcciones IP Publicas	Pool de 4 IPs - Soporte de IPv4 e IPv6.

Firmado digitalmente por: CHAVEZ FERRER DERTEANO Victor Enrique FAU 20546677444 soft
Motivo: Soy el autor del documento
Fecha: 29/12/2025 11:15:40-0500

Firmado digitalmente por: CARDENAS RODRIGUEZ RUDI RONALD FIR 41682277 hard
Motivo: Doy V° B°
Fecha: 29/12/2025 10:27:49-0500

3.2 CARACTERISTICAS DEL SERVICIO DE INTERNET CON ANCHO DE BANDA DEDICADO

3.2.1 CARACTERISTICAS DEL SERVICIO

- La última milla debe ser fibra óptica, la cual debe ser protegida adecuadamente para que no sea de fácil acceso. La fibra podrá ser subterránea.
- El proveedor deberá brindar un servicio de acceso permanente bajo la modalidad de 24x7x365, durante la vigencia del contrato, además de garantizar la disponibilidad y la eficiencia del servicio con un mínimo de 99.50%.
- El proveedor deberá brindar una herramienta de monitoreo del consumo vía web, la cual muestre la información en línea del consumo del ancho de banda real del enlace.
- La infraestructura y equipos del proveedor deberán soportar cualquier requerimiento de ampliación del ancho de banda de hasta el 50% de la capacidad contratada.
- El proveedor deberá encargarse de la instalación y conexión de la fibra óptica, incluyendo los permisos municipales, canalizaciones, obras civiles y demás actividades que sean necesarias. Los gastos que demanden las mismas, no implicarán, en ningún caso, reconocimiento de gastos y deberán ser previstos por el proveedor.
- Durante la prestación del servicio, la entidad podrá solicitar el incremento del ancho de banda hasta un máximo del 50% por 5 días, sin que esto genere un costo adicional para la entidad. Cabe resaltar que el requerimiento para el incremento del ancho de banda deberá ser solicitado mediante un correo por parte del encargado de la Oficina de informática de la entidad con dos (02) días hábiles de anticipación.

3.2.2 REQUISITOS DEL SERVICIO

- El servicio de internet solicitado debe ser de una velocidad no menor a 400 Mbps, con una compresión (overbooking) 1:1, garantizado desde el nodo principal de la entidad hasta el nodo internacional más cercano del proveedor.
- El proveedor deberá proveer un pool de cuatro (04) direcciones IPs públicas para uso de la entidad, esta cantidad deberá ser considerada en la propuesta siguiendo las normas de LACNIC.
- El proveedor deberá ofrecer un servicio de DDoS desde su red; es decir analizará el doble del tráfico contratado y deberá estar protegido contra ataques de este tipo.
- El proveedor deberá instalar un enlace dedicado simétrico para conexión a la Internet, con un ancho de banda de 400 Mbps, un Overbooking 1:1, 99.5 % de disponibilidad desde la puerta de enlace de la entidad hasta la salida internacional por cada año de servicio, no se deberá aplicar compresión de datos alguna a ningún nivel durante el tramo mencionado, utilizará como medio físico de transporte Fibra Óptica desde el POP (Ubicada en la red del proveedor) hasta la Sede Central de la entidad; se deberá adjuntar un plano donde se detalle la ruta física de este enlace.

3.2.3 EQUIPOS DE COMUNICACIÓN Y DATOS

- El proveedor debe instalar los equipos necesarios que formen parte de su propuesta técnica a fin de poner en operación el enlace y servicio solicitado. La

entidad será responsable de proporcionar: Energía estabilizada, tomacorriente, espacio en rack o gabinete y del cableado LAN dentro de la sala de servidores. La configuración de los equipos será realizada por el proveedor durante la vigencia del contrato. La entidad garantizara puertos de red RJ45 (01 como mínimo) en sus SWITCH de conectividad.

- Los equipos serán de última generación para el enlace.
- Los protocolos de comunicaciones base deberán ser el conjunto de protocolos TCP/IP (HTTP, HTTPS, SMTP, POP3, FTP, SSH, RTP, etc.)
- El enrutador a instalarse en el nodo de la entidad, deberá de disponer como mínimo cuatro (04) puertos LAN que soporten tecnología Ethernet 10/100/1000 Mbps y un puerto WAN que soporte como mínimo 400 Mbps, con el protocolo de conexión que disponga el proveedor (MLS, ATM o FAST ETHERNET), así como también deberá soportar redes privadas virtuales (VPN).
- El proveedor deberá mantener un servicio de resolución de nombres DNS de forma replicada y descentralizada.
- Todos los equipos y accesorios que sean utilizados en la infraestructura de comunicaciones deberán ser nuevos. Además, estos deberán estar debidamente etiquetados para facilitar una mejor identificación de las conexiones.
- Todos los equipos, materiales y accesorios a ser instalados en los nodos para la provisión del servicio serán provistos por el proveedor sin un costo adicional

3.2.4 INFRAESTRUCTURA DEL PROVEEDOR

- Deberá ser de fibra óptica con topología redundante (anillada a nivel físico y no colapsado). Será de fibra óptica a nivel metropolitano como a nivel internacional.

3.2.5 SERVICIO DE SEGURIDAD PERIMETRAL

- El proveedor debe gestionar el servicio de seguridad y realizar el monitoreo constante para la detección oportuna de amenazas o de tráfico malicioso.
- El proveedor debe alertar oportunamente la detección de amenazas o tráfico malicioso y tomar acción para mitigar la amenaza.
- El proveedor debe incluir el hardware, software, suscripciones y licenciamiento necesario ya sea en las instalaciones de la entidad o en la nube del proveedor para la correcta operación del servicio requerido, por el periodo contratado. Todo componente de la infraestructura a utilizar en la entidad (hardware, software, suscripciones y licenciamiento) debe ser nuevo y de última generación.
- La solución debe soportar la cantidad de 100 usuarios.
- El dimensionamiento del servicio debe garantizar una utilización de recursos de la solución no mayor al 60% (CPU, memoria RAM).
- El servicio debe permitir la configuración, integración y funcionamiento con protocolo IPv4 e IPv6.

Características a tomar en cuenta:

CARACTERISTICAS	REQUERIMIENTO MINIMO
Firewall	- Debe permitir el análisis de las conexiones entrantes/salientes de la red de la entidad. - Debe permitir la configuración de reglas por direcciones IP origen (o rangos de direcciones IP origen), direcciones IP destino (o rangos de direcciones IP destino), puertos, protocolos y servicios.

	- Debe permitir acciones de aceptación y rechazo de conexiones. - Debe soportar reglas para tráfico multicast que permita la configuración de reglas por direcciones IP multicast origen y/o direcciones IP multicast destino. - Debe permitir el bloqueo de tráfico por país(es). - Debe permitir la visualización de los países de origen y destino en los logs de eventos. - Debe permitir la configuración de reglas con vigencia en base al tiempo o fechas (día, mes y año). - Debe permitir la configuración de NAT, estático y dinámico. - Debe permitir el control de políticas de aplicaciones y reconocimiento de aplicaciones. - Debe permitir inspección de SSL. - Debe permitir la configuración, integración y funcionamiento con protocolo IPv4 e IPv6. - Debe permitir la gestión mediante interfaz web (GUI), para centralizar la administración y monitoreo. - El proveedor debe realizar la implementación de la solución de acuerdo a las buenas prácticas de seguridad, para filtro de tráfico malicioso, en coordinación con el personal de la entidad
Control de Aplicaciones	- Debe permitir la liberación y bloqueo de aplicaciones comerciales (YouTube, redes sociales, páginas multimedia, audio y video, ocio, streaming, etc.), aplicaciones internas (remote desktop, ftp, http, https, sftp, ssh, smtp, vpn, etc.). - Detección y reconocimiento de tráfico relacionado a P2P (Peer-to-Peer), redes sociales, acceso remoto (RDP), VPN (Cisco, citrix, etc.) transferencia de archivos mediante FTP, SFTP, update de software, protocoles de red, VoIP, audio, video, proxy, mensajería instantánea, compartición de archivos, correo electrónico, bittorrent, Gnutella, Skype, Facebook, Linkedin, Twitter, Citrix, logmein, teamviewer, VNC, Gmail, YouTube, http-proxy, http–tunel, facebook Chat, gmail chat, whatsapp, 4shared, dropbox, google drive, OneDrive, DB2, MySQL, Oracle, Active Directory, Ldap, Radius, ,iTunes, Dhcp, Ftp, Sftp, DNS, wins, MS-RPC, Ntp, snmp, RPC over Http, GotoMeeting, Webex, Evernote, Google - docs , entre otros. - Debe permitir la detección de amenazas desconocidas (wannaCry, ransomware, entre otros ataques dirigidos). - Inspección del payload del paquete de datos. - Visualización y control de aplicaciones y los ataques que utilizan tácticas evasivas **(opcional).** - Debe permitir la agrupación de aplicaciones. - Permitir políticas de calidad de servicio mediante traffic shapping y/o QoS. **(opcional).** - Las políticas se deben aplicar por dirección IP, grupos de usuarios, aplicaciones, etc.

	- Actualización automática de base de datos de firmas de aplicaciones. - Debe poseer protección contra vulnerabilidades (IPS), antivirus, antispyware (protección contra bots). - Debe permitir la creación de políticas basadas en el tiempo. - Debe permitir la configuración, integración y funcionamiento con protocolo IPv4 e IPv6. - Debe permitir la gestión mediante interfaz web (GUI), para centralizar la administración y monitoreo.
Prevención de amenazas	- La solución deberá proteger contra malware desconocido, para un máximo de 400 archivos por día entre 100 usuarios. (emulación sandbox en la nube del proveedor de Internet) - Protección mediante antivirus, contra malware, spyware y virus. Debe permitir el análisis, detección y contención de archivos maliciosos en tiempo real, al menos los siguientes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, SFTP, FTP, entre otros. - Sincronización automática de las firmas de IPS. - Sincronización automática de las firmas de antivirus. - Las firmas de IPS y antivirus deben quedar activadas y en funcionamiento. - Permitir excepciones por dirección IP de origen y destino. - Protección contra ataques synflood, ICMPflood, UDPflood. - Debe soportar: análisis de patrones de estado de conexiones, análisis de decodificación de protocolo, análisis para detección de anomalías de protocolo, análisis heurístico, IP Desfragmentación, re-ensamblado de paquetes de TCP y bloqueo de paquetes malformados. - Debe poseer base de datos de firmas para la mitigación de ataques DoS. - Debe permitir la actualización automática del motor de antivirus (firmas, definiciones, etc.) y de firmas de IPS. - Debe permitir la captura de paquetes (PCAP) para análisis de tráfico. - El sandboxing debe de soportar las siguientes maquinas Windows 7, Windows 8.1, Windows 10, Windows 11, macOS**(opcional).**, and Android. - Permitir la configuración de políticas basadas en tiempo, horario o periodo (día, mes, año, día de la semana y hora). - Debe permitir la configuración, integración y funcionamiento con protocolo IPv4 e IPv6. - Debe permitir la gestión mediante interfaz web (GUI), para centralizar la administración y monitoreo.
Filtro de contenido web	- Creación de políticas por usuario, por grupos de usuario, dirección IP, redes, subredes y URL, que permita identificar el acceso a URLs de los usuarios.

	- Debe permitir la integración con servicio de Directorio Activo o LDAP de la Entidad - Permitir el bloqueo de acceso a páginas web o sitios web. - Debe bloquear el acceso a sitios o páginas web, como resultado de búsquedas (google, bing, yahoo, etc.) - Debe contar con al menos 50 categorías de sitios para filtrado de URL. - Debe permitir la creación de listas blancas y listas negras de URL personalizadas en coordinación con el NOC del proveedor. - Debe permitir el filtrado de contenido de Youtube mediante perfiles. - Debe soportar la funcionalidad de "Safe search", que permita el filtrado de resultados considerados no apropiados en los buscadores. Soporte al menos para google, bing y yahoo. - Protección de acceso contra páginas de riesgo alto. - Filtro de contenido en tiempo real, basado en categorías, que permita agregar páginas o sitios web no autorizados. - Debe permitir la actualización automática de su base de datos de filtrado. - Permitir la personalización de la página de bloqueo, en coordinación con la Entidad en coordinación con el NOC del proveedor. - Debe permitir la configuración, integración y funcionamiento con protocolo IPv4 e IPv6. - Debe permitir la gestión mediante interfaz web (GUI), para centralizar la administración y monitoreo.
Conectividad VPN	- Soporte para VPN SSL o VPN IPsec (conexiones site to site). - Soporte de algoritmos 3DES y AES, MD5, SHA. - Debe permitir la integración con servicio de Directorio Activo o LDAP. - Debe permitir la conexión mediante un agente instalado en el equipo de conexión (PC, Laptop) o por medio de interfaz web. El agente de VPN SSL debe ser compatible al menos con: Windows 7, Windows 8, Windows 8,1, Windows 10, Windows 11, Mac OS, Apple iOS y Android. - El proveedor debe incluir todas las licencias asociadas a este servicio y brindar las licencias para la conexión de los usuarios de la entidad. - Debe permitir la configuración, integración y funcionamiento con protocolo IPv4 e IPv6. - El servicio deberá permitir la conexión, como mínimo, de 200 conexiones remotas; dichas conexiones remotas deberán poder conectarse a una red que determine la entidad. - Debe permitir la gestión mediante interfaz web (GUI), para centralizar la administración y monitoreo.

Servicio de mitigación de ataques anti DDOS	- El proveedor debe ofrecer un servicio de mitigación de ataques DDoS ubicado en su backbone o nube. - El servicio de mitigación externo debe ser provisto por un Proveedor de Servicios (ISP). La mitigación en la nube se realiza cuando el enlace de conexión a Internet sea saturado por un ataque DDoS volumétrico. - La capacidad de mitigación de al menos 5Gbps. - El servicio o el equipamiento no debe mantener el estado de las conexiones y debe ser dedicado a esta función para proporcionar disponibilidad de servicios IP. - El servicio debe ser capaz de informar la cantidad de tráfico malicioso bloqueado en bps y pps por el proveedor externo durante una mitigación activa en la nube. - Debe reportar el estado de conexión de señalización del servicio en la nube con los sistemas del ISP, mostrando el estado de la conexión, errores de conexión, entre otros **(Opcional)** - Debe permitir reportar la cantidad de tiempo que una mitigación lleva ejecutándose. - Debe incluir la entrega de credenciales para la visualización en línea de la herramienta de reportes. - Debe incluir la gestión y administración de las funcionalidades de seguridad desde su centro de operaciones de seguridad, para realización de las siguientes labores mínimas: Configuración de mejoras, nuevos usuarios, reglas de acceso y políticas de seguridad, mitigación de ataques en tiempo real, entre otros. - Debe permitir la configuración, integración y funcionamiento con protocolo IPv4 e IPv6. - Debe permitir la gestión mediante interfaz web (GUI), para centralizar la administración y monitoreo.
GESTION DEL SERVICIO	
Administración	- La solución debe permitir la administración de la solución mediante interfaz web, para centralizar la administración de reglas y políticas. - Soportar acceso mediante ssh, cliente web (https) o interfaz gráfica GUI. - Debe permitir la creación de usuarios con permisos basados en roles, para el acceso a la interfaz de administración. - Debe permitir la integración con Active Directory o LDAP o RADIUS. - Debe permitir la creación de reglas por horario definido o periodo de tiempo. - Debe permitir realizar respaldo de las configuraciones por parte del proveedor. - Debe permitir la generación de logs de auditoria detallando configuración realizada, el usuario, fecha y hora de la actividad realizada. - Debe permitir notificaciones de alertas vía correo electrónico, snmp y/o syslog.

	- Debe brindar usuario y contraseña al personal de la entidad, para la visualización en línea de la herramienta de reportes y monitoreo. - Debe permitir el acceso a los reportes, a cualquier hora del día, durante la vigencia del servicio. - El proveedor debe administrar las funcionalidades de seguridad del servicio y la realización de las siguientes labores como mínimo: • Configuración de mejoras de seguridad, nuevos usuarios, reglas de acceso y políticas de seguridad. • Mitigación de ataques en tiempo real. - Respaldo de las configuraciones por parte del proveedor.
Monitoreo	- La interfaz gráfica debe mostrar estadísticas del tráfico del equipamiento de seguridad. - Visualización de principales aplicaciones por riesgo, principales ataques detectados. - Visualizar los usuarios conectados a la interfaz de gestión, conexiones simultáneas, el estado de las interfaces, rendimiento de CPU. - Generación de reportes, como mínimo: • Tráfico de red, por protocolo, aplicación, usuario, entre otros. • Amenazas detectadas por equipo, numero de amenaza. • Reglas de firewall activas. • Utilización de ancho de banda de entrada y de salida. • Aplicaciones por tasa de transferencia.

3.3 GESTIÓN DEL SERVICIO

- El proveedor del servicio deberá contar con un propio **(no tercerizado)** centro que le permite la gestión, administración (Centro de Operaciones Networking – NOC) y un centro para monitorear y analizar la infraestructura (Centro de Operaciones y Seguridad – SOC) de los servicios contratados por la Entidad.
- El proveedor deberá garantizar un eficiente sistema de gestión de sus redes de comunicación. El centro de gestión deberá estar en capacidad de realizar acciones de controles preventivo, correctivos y pruebas técnicas.
- Durante el periodo de prestación del servicio, se evaluará los tiempos de respuesta y la calidad del servicio, a fin de que la entidad determine las acciones necesarias a tomar si fuera el caso, tales como aplicación de penalidades o término del servicio por incumplimiento de los niveles de servicio estipulados en el contrato.
- El proveedor deberá brindar el soporte bajo la modalidad de 24x7x365 durante la vigencia del servicio.
- Las interrupciones en el servicio deberán ser notificadas vía escrita y/o por correo electrónico, con una anticipación de por lo menos dos (02) días hábiles. En el caso de la notificación vía correo electrónico, esta deberá ser remitida al correo que la entidad designe.

Características Complementarias:
El servicio proveerá a la entidad una herramienta de monitoreo de administración y supervisión en línea (WEB) del enlace y el uso del ancho de banda, la cual permita lo siguiente:

a. Un acceso por autenticación del usuario.
b. La herramienta de monitoreo debe permitir realizar el reporte de estadísticas de uso, que contemple el volumen de tráfico mensual, semanal y anual.

3.4 SOPORTE

Se proveerá soporte para incidentes vía una plataforma de soporte Web y por teléfono 24x7 (24 horas durante los 7 días de la semana), por el periodo de **trescientos sesenta y cinco (365) días calendario**, debiendo generar un ticket de atención. Este servicio será provisto durante el plazo de vigencia del servicio con los niveles de atención SLA siguiente:

PRIORIDAD	DESCRIPCIÓN	TIEMPO MÁXIMO DE RESPUESTA
Urgente	Se tiene una indisponibilidad total de los servicios, no hay accesos, hay un impacto grave en las actividades de la ENTIDAD.	Máximo 1 hora contabilizadas una vez generado el ticket de atención para la primera respuesta.
Alta	Mal funcionamiento de partes u opciones de los servicios que impactan sobre actividades importantes para LA ENTIDAD.	Máximo 1 horas contabilizadas una vez generado el ticket de atención para la primera respuesta.
Media	Mal funcionamiento de partes y opciones que impacta sobre actividades no críticas, no existe una alternativa de solución.	Máximo 2 horas contabilizadas una vez generado el ticket de atención para la primera respuesta.
Baja	Casos que impactan sobre actividades no críticas, existe una alternativa de solución.	Máximo 3 horas contabilizadas una vez generado el ticket de atención para la primera respuesta.

4. REQUISITOS DEL PROVEEDOR

- Persona Jurídica.
- Contar con Registro Nacional de Proveedores (RNP) de servicios vigente.
- Contar con Registro Único del Contribuyente (RUC) Activo y Habido
- No estar impedido de contratar con el Estado.
- Ser miembro activo del NAP (Network Access Point) Perú.
- Poseer conexión activa y directa al NAP con infraestructura propia (no rentada a terceros).
- Soporte Técnico vía correo electrónico y teléfono las 24 horas, los 7 días de la semana.

El proveedor debe acreditar un monto facturado acumulado equivalente a S/ 30,000 soles por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los cinco (05) años anteriores a la fecha de la presentación de su cotización,

ofertas que se computa desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran servicios similares a los siguientes: **SERVICIO DE INTERNET DEDICADO MEDIANTE FIBRA OPTICA**

- **Acreditación:**

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 constancia de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago.

5. REQUISITOS PARA PERFECCIONAR CONTRATO

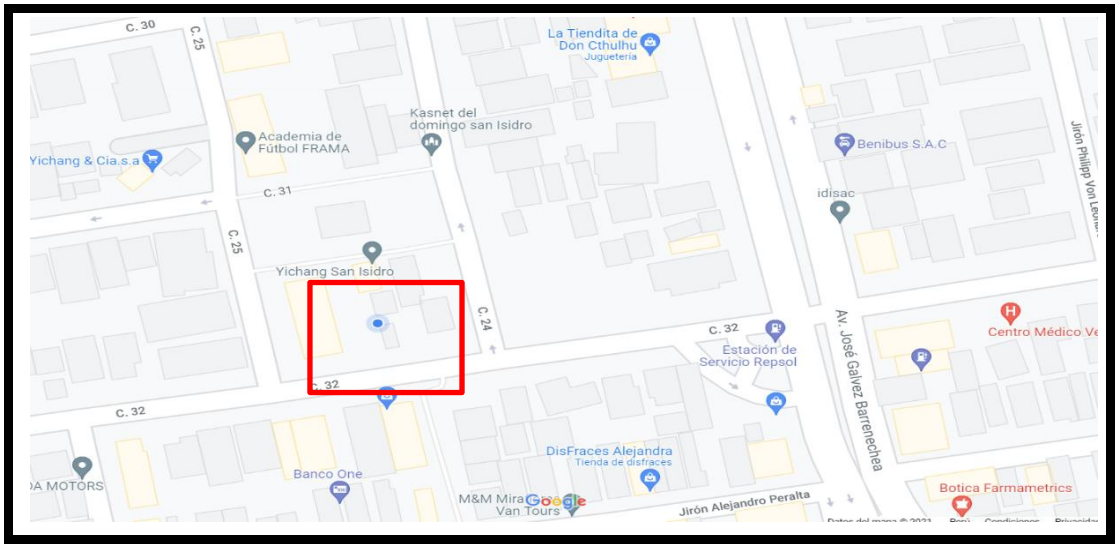
PERSONAL NATURAL	PERSONA JURIDICA
Copia de DNI	Copia de DNI del representante legal
	Copia de la vigencia del poder del representante legal que acredite que cuenta con facultades para perfeccionar el contrato

6. MEDIDAS DE CONTROL DURANTE LA EJECUCION CONTRACTUAL

Area(s) que supervisan y coordinará el CONTRATISTA: Personal de Soporte Tecnico en Sistemas Informáticos o quien haga sus veces – Unidad de Administración y Finanzas.

7. LUGAR, PLAZO DE EJECUCION E IMPLEMENTACION DEL SERVICIO

El servicio será instalado en Jr. Roberto Ramírez del Villar (ex calle 32) Urb. Corpac - San Isidro – Lima.
Se adjunta ubicación del lugar donde se prestará el servicio de Internet Dedicado.



Plazo de ejecución: Será de **trescientos sesenta y cinco (365) días** calendario. El inicio del servicio se contabilizará de forma inmediata al día siguiente del vencimiento del contrato anterior, previa suscripción del contrato actual, asegurando así la continuidad operativa del sistema de correo corporativo.

Implementación del Servicio: El servicio deberá ser implementado en un plazo no mayor a 15 días calendario, mismos que serán contabilizados a partir del día siguiente de la suscripción o emisión de la orden de servicio. Sin perjuicio que el plazo para la activación del servicio se realice el 01 de enero del 2026 a fin de garantizar la operatividad de la entidad y dar continuar al servicio actual finalizado.

8. CONFORMIDAD DEL SERVICIO

Será emitida por la Jefatura de la Unidad de Administración, previo Informe del personal de Soporte Tecnico en Sistemas Informáticos o quien haga sus veces quién verificará la calidad, alcances y cumplimiento de las condiciones solicitadas en los términos de referencia según el Artículo 144º del RLGCP, en la cual indica que la conformidad se emite en un plazo máximo de siete (07) días de producida la recepción del entregable.

9. FORMA DE PAGO

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad realizará el pago de la contraprestación pactada a favor del contratista de forma mensual (12 pagos) hasta la culminación del servicio.

Para ello, el contratista deberá presentar a través de mesa de partes del PROGRAMA "MEJORAMIENTO DE LOS SERVICIOS DE JUSTICIA NO PENALES A TRAVÉS DE LA IMPLEMENTACIÓN DEL EXPEDIENTE JUDICIAL ELECTRÓNICO (EJE), en el horario de lunes a viernes de 08:30 am a 4:30 pm o de manera virtual:

- Carta de presentación, señalando los documentos que adjunta.
- Informe Técnico y/o Entregable mensual, según corresponda.
- Comprobante de pago **(Factura Electrónica).**
- Carta de autorización de depósito en cuenta (CCI), de corresponder.

Cuando los documentos cuenten con firma manuscrita y sean escaneados para enviarse por mesa de partes virtual, se admitirá su presentación al correo electrónico **mesadepartes@ejenopenal.pe** o al siguiente link https://ejenopenal.pe/fmpv/;

No se aceptará firma pegada en la presentación de los documentos.
El pago se realizará con abono en la cuenta "Código de Cuenta Interbancaria" (CCI) del contratista, como máximo, hasta los diez (10) días calendario posteriores a la emisión de la conformidad del servicio respectiva y presentación del comprobante de pago.

10. CONFIDENCIALIDAD:

Toda la información y/o documentación generada como parte del servicio será de propiedad exclusiva del programa, no pudiendo EL CONTRATISTA utilizarla fuera del presente servicio. El CONTRATISTA no podrá comunicar a ninguna persona u otra entidad ajena al presente contrato, la información no publicada o de carácter reservado

o confidencial a la que haya tenido conocimiento con motivo de la ejecución de sus obligaciones emanadas del presente contrato, salvo que la Entidad que corresponda lo hubiera autorizado expresamente para hacerlo.

11. PENALIDADES APLICABLES

11.1. NIVELES DE ACUERDO DE SERVICIO – SLA

La disponibilidad mensual mínima requerida es de **99.50%** para el servicio. La ENTIDAD calculará la disponibilidad, en forma mensual y de la siguiente forma:

$$\text{Disponibilidad} = \frac{\mathbf{TT - TE}}{\mathbf{TT}} \times 100\%$$

Donde:

TT = Cantidad de minutos del mes, brindadas por el proveedor del servicio Internet.
TE = Total de minutos sin servicio en el mes.

Ejemplo:
Si el servicio tuviera 3 caídas en 1 mes de 1 hora de duración cada caída por causas atribuibles al proveedor, la disponibilidad será:

TT = 60x24x30 (en 1 mes con 30 días calendario) = 43200 minutos
TE = 03 horas = 180 minutos

$$\text{Disponibilidad} = \frac{43200 - 180}{43200} \times 100 = \mathbf{99.58\%}$$

El incumplimiento en la atención de reporte de averías de servicio, no deberá superar los 30 minutos al momento de generar el ticket de atención por parte del proveedor, vía los medios indicados en el numeral 3.4. El cálculo se realizará de la siguiente forma:

$$\mathbf{TRE} = TR - 30min$$

TRE es el Tiempo de Respuesta Excedido.
TR es el tiempo de respuesta del proveedor expresado en minutos (min)

11.2. PENALIDADES POR INCUMPLIMIENTO EN DISPONIBILIDAD DEL SERVICIO

Las penalidades indican el porcentaje (%) deducible del pago mensual del servicio, de acuerdo a lo establecido en los niveles de atención SLA, numeral 3.4.1 y 3.4.2 los cuales se aplicarán de acuerdo a la siguiente tabla.

Por incumplimiento de disponibilidad de servicio (imputables al Contratista)	
Criterio: Disponibilidad Mensual del servicio	**% Deducible del recurrente mensual**
Mayor o igual a 99.50%	0%
Entre 99.49 y 99.45% inclusive	2%

Entre 99.44 y 99.40 % inclusive	3%
Entre 99.39 y 99.35 % inclusive	5%
Entre 99.34 y 99.30 % inclusive	7%
Menor o igual a 99.29 %	10%

Por incumplimiento en la atención de averías (Tiempo de atención para brindar una respuesta e iniciar el soporte ante cualquier llamada de reporte de avería)	
Criterio: Incumplimiento en la atención	**% Deducible del recurrente mensual**
Que no exceda el periodo de 30 minutos	0%
Desde 31 minutos hasta 40 minutos adicionales	3%
Desde 41 minutos hasta 50 minutos adicionales	5%
Más de 50 minutos adicionales	10%

11.3. PENALIDAD POR MORA

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto de la contratación, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso. La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente fórmula:

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

Donde F tiene los siguientes valores:
Para bienes y servicios: F = 0.40

Tanto el monto como el plazo se refieren, según corresponda, al monto vigente de la contratación o ítem que debió ejecutarse o, en caso que estos involucraran obligaciones de ejecución periódica o entregas parciales, a la prestación individual que fuera materia de retraso.
Asimismo, son aplicables las disposiciones correspondientes a las penalidades establecidas en los Artículos 119° y 120° del Reglamento de la Ley General de Contrataciones Públicas N° 32069, aprobado con Decreto Supremo N° 009-2025-EF.

A efectos de computar los días de atraso para la aplicación de la penalidad, cuando el plazo con el que cuenta el contratista para ejecutar la prestación a favor de la Entidad vence en día inhábil, debe tomarse en cuenta el primer día hábil siguiente, aplicándose la penalidad correspondiente desde el día posterior a éste, de conformidad con los términos contractuales

OTRAS PENALIDADES

SUPUESTOS DE APLICACIÓN DE PENALIDAD "POR TIEMPO DE RESPUESTA EXCEDIDO"	FORMA DE CÁLCULO	PROCEDIMIENTO

Cuando el tiempo de respuesta (TR) 0 generación de ticket de atención por parte del contratista, excede los 30 minutos.	TRE = TR - 30 TRE es el Tiempo de Respuesta Excedido. TR es el tiempo de respuesta del proveedor	En el caso que el TRE sea mayor a 1, se aplicará una penalidad del 1% deducible del pago mensual del servicio. La aplicación de esta penalidad será determinada y comunicada por LA ENTIDAD mediante acta de conformidad.
SUPUESTOS DE APLICACIÓN DE PENALIDAD "POR NIVEL DE DISPONIBILIDAD DEL SERVICIO"	**FORMA DE CÁLCULO**	**PROCEDIMIENTO**
Cuando la sumatoria de los incidentes ocurridos durante el mes (cuya responsabilidad sea atribuida al contratista), origen un nivel de disponibilidad mensual menor a 99.90%	Disponibilidad es: **(1-(TSS/TTM)) x 100** Donde: TSS es el tiempo total sin servicio en el mes, expresado en minutos. TTM es el tiempo total del mes expresado en minutos	En el caso que el nivel de disponibilidad alcanzado en el mes sea menor al establecido (SLA= 99.90%), se aplicará la penalidad de acuerdo a la fórmula de cálculo indicada y solo se aplicará la penalidad según el nivel al que corresponda de acuerdo a la siguiente tabla:

NIVEL DE DISPONIBILIDAD MENSUAL IMCUMPLIDA	PENALIDAD %
De 99.80% a 99.89%	2%
De 99.70% a 99.79%	3%
De 99.60% a 99.69%	5%
De 99.50% a 99.59%	7%
Menor a 99.50%	9%

La penalidad será aplicada al pago mensual
del servicio.
Ejemplo:
Si en un determinado mes, se obtiene un nivel de disponibilidad mensual del servicio de 99.50%, se aplicará una penalidad de 7%, la misma que será deducible del Pago Mensual del Servicio.

		La aplicación de esta penalidad será determinada y comunicada por LA ENTIDAD mediante acta de conformidad.

12. RESOLUCIÓN DE CONTRATO POR INCUMPLIMIENTO

En el caso de la resolución por incumplimiento del contratista, la entidad contratante debe haber otorgado previamente un plazo de subsanación, salvo que el incumplimiento no pueda ser revertido.
El contrato menor podrá ser resuelto por el incumplimiento de alguna de las cláusulas de Anticorrupción y Antisoborno, Confidencialidad y/o Propiedad Intelectual, sin que sea necesario que medie requerimiento previo.
En caso se llegue a acumular el monto máximo de penalidad por mora u otras penalidades, según sea el caso, la Entidad podrá resolver el contrato menor sin apercibimiento previo.
La comunicación de resolución será con carta simple, notificada al correo electrónico consignado en la oferta, la cual se entenderá recibida con la sola comunicación, sin que sea necesario acuse de recibo; salvo que, entre en vigencia la PLADICOP, en cuyo caso, las notificaciones se realizarán por dicho medio, teniendo los mismos efectos que la notificación física.
Es causal de resolución de contrato la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público. Asimismo, caso se incumpla con los impedimentos señalados en el artículo 5 de dicha ley se aplicará la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad.
Cualquiera de las partes puede resolver, total o parcialmente, el contrato en los siguientes supuestos:
a) Caso fortuito o fuerza mayor que imposibilite la continuación del contrato.
b) Incumplimiento de obligaciones contractuales, por causa atribuible a la parte que incumple.
c) Hecho sobreviniente al perfeccionamiento del contrato, de supuesto distinto al caso fortuito o fuerza mayor, no imputable a ninguna de las partes, que imposibilite la continuación del contrato.
d) Por incumplimiento de la cláusula anticorrupción
e) Por la presentación de documentación falsa o inexacta durante la ejecución contractual.
f) Configuración de la condición de terminación anticipada establecida en el contrato, de acuerdo con los supuestos que se establezcan en el reglamento para su aplicación

Asimismo, es aplicable las disposiciones correspondientes Procedimiento de resolución de contrato descrito en el artículo 122° del Reglamento de la Ley General de Contrataciones Públicas.

13. SOLUCIÓN DE CONTROVERSIAS

Las controversias surgidas durante la ejecución contractual se resuelven mediante conciliación.
Las controversias se resuelven mediante la aplicación de la Constitución Política del Perú, La Ley 32069, Ley General de Contrataciones Púbicas y su Reglamento; así como de las normas de derecho público y las de derecho privado. Se mantiene

obligatoriamente este orden de preferencia en la aplicación del derecho. Esta disposición es de orden público.
El inicio del procedimiento de solución de controversias no suspende o paraliza las obligaciones contractuales de las partes, salvo que la entidad contratante o el órgano jurisdiccional competente disponga lo contrario.
Asimismo, es aplicable las disposiciones correspondientes a las garantías contenidas en los artículos 76, 77, 81, 82, 83 y 84 de La Ley 32069, Ley General de Contrataciones Púbicas y los artículos que correspondan en el Reglamento

14. **RESPONSABILIDAD POR VICIOS OCULTOS**

El proveedor es responsable por la calidad ofrecida y por los servicios ocultos del bien ofertado por un plazo no mayor de un (01) año contado a partir de la conformidad otorgada por la entidad

15. GESTIÓN DE RIESGOS:

Debido a las condiciones del servicio y cuantía a contratar, en el marco de lo establecido en el numeral 42.1 del Reglamento de la Ley 32069, no corresponde efectuar la segmentación para la clasificación de la contratación; en ese sentido, no corresponde determinar el proceso de gestión de riesgos para la presente contratación.

16. ANTICORRUPCIÓN Y ANTISOBORNO

El CONTRATISTA declara y garantiza no haber, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas a las que se refiere el Artículo 30° de la Ley N° 32069, Ley de Contrataciones del Estado, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato.
Asimismo, el CONTRATISTA se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a las que se refiere el Artículo 30° de la Ley N° 32069, Ley de Contrataciones del Estado.
Además, EL CONTRATISTA se compromete a: (i) comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y (ii) adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas, conforme a lo previsto por la Directiva sobre la atención de denuncias por presuntos actos de corrupción y solicitudes de medidas de protección al denunciante en la Unidad Ejecutora 003: Programa Modernización del Sistema de Administración de Justicia - EJE NO PENAL
EL CONTRATISTA se compromete a no colocar a los funcionarios públicos y/u otros contratistas con los que debe interactuar en situaciones reñidas con la ética, en tal sentido reconoce y acepta la prohibición de ofrecerles cualquier tipo de obsequios, donación, beneficio y/o gratificación, ya sea de bienes o servicios, cualquiera sea la finalidad con la que se haga.
EL CONTRATISTA se compromete a cumplir la política antisoborno del programa, aprobada y regulada mediante Resolución de Dirección Ejecutiva N° 13-2025-PMSAJ-EJENOPENAL la cual se encuentra disponible en el siguiente enlace:

https://www.gob.pe/institucion/pmsaj/normaslegales/6648170-13-2025-pmsaj-ejenopenal.

17. CLÁUSULA DE CUMPLIMIENTO

En el marco de lo establecido en el Artículo 8° de la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal, son causales de resolución de contrato la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público. Asimismo, en caso se incumpla con los impedimentos señalados en el artículo 5 de dicha ley se aplicará la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad.

18. INTEGRIDAD EN LA ADMINISTRACIÓN PÚBLICA

En el marco de lo dispuesto en el Numeral 2.1 del Artículo 2° de la Ley N° 31227, Ley que transfiere a la Contraloría General de la República la competencia para recibir y ejercer el control, fiscalización y sanción respecto a la declaración jurada de intereses de autoridades, servidores y candidatos a cargos públicos, corresponde que los sujetos obligados señalados en el Artículo 3° dicha Ley, independientemente de su régimen laboral o contractual, presenten su declaración jurada de intereses (en adelante, la DJI) a través del sistema de la Contraloría General de la República.
En relación a ello, corresponde tener presente que de conformidad con lo dispuesto en el Numeral 2.2 del Artículo 2° de la Ley, la DJI es un documento de carácter público cuya presentación constituye requisito indispensable para el ejercicio del cargo o función pública y demás situaciones que regula la Ley en comentario.

Asimismo, de conformidad con lo dispuesto en el Artículo 5° de la citada Ley el incumplimiento de la presentación de la DJI (inicio, periódica o cese) o la presentación tardía, incompleta o falsa dará lugar a la respectiva sanción administrativa a cargo de la Contraloría General de la República