TÉRMINOS DE REFERENCIA

CONTRATACIÓN DEL SERVICIO DE RENOVACIÓN DE LICENCIAS ANTIVIRUS PARA EL PROGRAMA NACIONAL DE ASISTENCIA SOLIDARIA PENSIÓN 65

1. UNIDAD O AREA QUE REQUIERE EL SERVICIO
Unidad de Tecnologías de la Información.

2. DENOMINACIÓN DE LA CONTRATACIÓN
Servicio de Renovación de licencias antivirus para el Programa Nacional de Asistencia Solidaria Pensión 65.

3. BASE LEGAL
- Ley N° 32069, Ley General de Contrataciones Públicas.
- Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas aprobado mediante Decreto Supremo N° 009-2025-EF.
- Ley N° 32513, Ley de Presupuesto del Sector Público para el Año Fiscal 2026.

4. OBJETO DEL SERVICIO
4.1. Objetivo General:
El objeto del presente es renovar las licencias de antivirus para el Programa Nacional de Asistencia Solidaria Pensión 65, servicio requerido dada la necesidad de este Programa de resguardar y brindar seguridad a la información garantizando las operaciones y las actividades encargadas a la Institución.

4.2. Objetivo Específico:
Renovar cuatrocientas (400) licencias antivirus para los equipos y servidores.

5. ACTIVIDAD DEL POI:
0106536. IMPLEMENTACIÓN DE PLANES, MECANISMOS DE SEGURIDAD Y CONTINGENCIA DE TECNOLOGÍA DE INFORMACIÓN, ADMINISTRACIÓN DE LA RED INFORMÁTICA Y BASE DE DATOS DEL PROGRAMA

6. ANTECEDENTES
Mediante DS N° 081-2011-PCM, de fecha 19 de octubre de 2011, se creó el Programa de Asistencia Solidaria Pensión 65 con la finalidad de otorgar subvenciones económicas a los adultos mayores en condición de extrema pobreza a partir de los 65 años de edad que cumplan con los requisitos establecidos en dicha norma.

El MIDIS, a través del Programa Nacional de Asistencia Solidaria Pensión 65, se ha propuesto conseguir que el Estado y la sociedad prioricen la atención integral de los adultos mayores en vulnerabilidad y lograr con ello la expansión de las iniciativas orientadas a atender y proteger a esta población a fin de que vivan un envejecimiento con dignidad.

Se autorizan Transferencias de Partidas en el Presupuesto del Sector Público para el año fiscal 2026 a favor del Ministerio de Desarrollo e Inclusión Social, cuyo objeto es financiar el incremento de cobertura de las intervenciones orientadas a la protección social correspondiente al Programa Nacional de Asistencia Solidaria – Pensión 65.

7. FINALIDAD PÚBLICA
El Programa Nacional de Asistencia Solidaria Pensión 65, genera padrones para el pago de subvención económica, Por tanto, dada la importancia que tiene esta información para el desarrollo de las actividades del Programa, es necesario la protección de la misma por lo cual se requiere el servicio de renovación de Cuatrocientas (400) licencias antivirus para el Programa Nacional de Asistencia Solidaria Pensión 65, por un periodo de doce (12) meses. La solución deberá ser gestionada desde una consola de administración que permita el monitoreo, llevar un inventario de hardware y software del equipo, administración, análisis de vulnerabilidades de PC's, despliegue de software, protección y eliminación de Virus, Malware, Troyanos, etc.

8. CARACTERÍSTICAS Y DESCRIPCIÓN DEL SERVICIO A REALIZAR:

8.1. Características

El servicio debe contar con lo siguiente:

- La solución (en su última versión) deberá ser compatible con los siguientes sistemas operativos: Microsoft Windows (7 SP1, 8, 8.1, 10, 11) incluyendo versiones Enterprise Multi-session; Windows Server (2012, 2012 R2, 2016, 2019, 2022); entornos macOS; plataformas móviles Android e iOS; así como distribuciones de Linux que incluyan explícitamente RedHat Enterprise Linux, CentOS, Rocky Linux, AlmaLinux, Oracle Linux, Ubuntu LTS, Debian GNU/Linux, SUSE Linux Enterprise Server, openSUSE, Fedora y Amazon Linux en arquitecturas x64 y ARM64.
- Las licencias para renovar deberán contar con las siguientes funcionalidades:
  - Protección asistida en la nube.
  - Firewall
  - Antimalware
  - Ransomware
  - Control de Aplicaciones
  - Lista Blanca de Aplicaciones
  - Control Web
  - Control de Dispositivos
  - Protección de Servidor de Archivos
  - Consola de Administración Centralizada
- La cantidad de licencias de antivirus a renovar son Cuatrocientas (400) para las estaciones de trabajo y dispositivos móviles.
- El servicio deberá incluir la instalación, configuración y puesta en marcha de la consola administrativa a nivel nacional para que puedan sincronizarse todas las estaciones sumado a la capacitación del personal de la Unidad de Tecnologías de la Información.
- Soporte técnico gratuito vía teléfono, correo y asistencia remota on-line en la modalidad de 24x7.
- Soporte de fábrica vía teléfono, chat, foros y apertura de casos por el portal de soporte del fabricante.
- Para el mantenimiento correctivo, se requiere la presencia de un Ingeniero Calificado al presentarse un incidente grave luego de haberse revisado y no solucionado vía remota.
- Deberá realizarse revisiones periódicas remotas con la finalidad de reducir y prevenir futuras incidencias.
- Las licencias tendrán una vigencia de doce (12) meses.
- La solución debe proteger endpoints y servers, sean estos Windows, Linux, macOS, así como también dispositivos móviles iOS y Android.
- La solución debe disponer de una única licencia que debe permitir el uso de la consola nube u on-premise, como así también de todos los endpoints y servers que disponga la organización, independientemente del sistema operativo del dispositivo en cuestión.
- La solución debe permitir la implementación de puntos de distribución en diferentes segmentos de red o ubicaciones geográficas de la organización que permita la distribución de actualizaciones, sondeo de red, instalación remota de aplicaciones, obtención de información sobre equipos de un grupo de administración, y/o difusión de dominio, entre otras.
- La solución debe incluir una infraestructura de servicios en la nube que brinde acceso a la base de conocimientos del fabricante, ofreciendo un recurso en línea que permita conocer la reputación de los archivos, los recursos web y el software, garantizando respuestas más rápidas ante nuevas amenazas, mejorando el rendimiento de algunos componentes de protección y reduciendo el riesgo probable de que se produzcan falsos positivos.
- La solución debe contar con la capacidad de eliminar remotamente cualquier solución antivirus (propia o de terceros) que esté presente en los endpoints y servidores, sin la necesidad de la contraseña de remoción del actual antivirus.
- La solución debe disponer de la capacidad de instalar remotamente la solución de antivirus en los endpoints y servidores Windows, a través de la administración compartida, login script y/o GPO de Active Directory.

- La solución debe contar con la capacidad de generar paquetes personalizados (autoejecutables) conteniendo la licencia y configuraciones del producto.
- La solución debe disponer de la capacidad de importar la estructura de Active Directory para encontrar máquinas.
- La solución debe contar con la capacidad de monitorear diferentes subnets de red con el objetivo de encontrar máquinas nuevas para que sean agregadas a la protección.
- La solución debe disponer de la capacidad de, al detectar máquinas nuevas en el Active Directory, subnets o grupos de trabajo, automáticamente importar la máquina a la estructura de protección de la consola y verificar si tiene el antivirus instalado. En caso de no tenerlo, debe instalar el antivirus automáticamente.

8.2. Características Técnicas Mínimas

8.2.1. Información General

- El fabricante de las soluciones ofertadas debe contar con, al menos, 25 años de presencia en el mercado global.
- El fabricante de las soluciones ofertadas debe contar con un equipo de investigación global y con presencia de por lo menos cinco (5) analistas de investigación de amenazas basados en países de Latinoamérica, dedicados a la investigación y el análisis de amenazas para la región.

8.2.2. Servidor de Administración y Consola Administrativa

- La consola debe ser con infraestructura en la nube o implementado como un servicio SAAS o adicionalmente debe tener la capacidad de implementarse en forma On-premise.
- La consola de administración debe permitir la configuración y administración remota de la solución antivirus instalada en las estaciones de trabajo y servidores.
- Debe permitir la delegación de tareas mediante creación de usuarios con distintos perfiles de administración.
- El servidor de administración remota deberá ser compatible al menos con los siguientes sistemas operativos: Windows Server 2019 o Windows Server 2022.
- El servidor deberá soportar al menos el motor de base de datos: Microsoft SQL Server.
- Se debe proveer una solución tecnológica que incluya una poderosa protección de endpoints basada en IA, controles de seguridad flexibles y características de EDR incorporadas.

8.2.3. Protección para endpoints, consola de administración y reporting

- La solución debe combinar protección basada en firmas, análisis heurístico y de comportamiento, junto con tecnologías asistidas por la nube para proteger los endpoints contra amenazas de malware conocidas, desconocidas y avanzadas.
- La solución debe permitir habilitar la protección con contraseña con el fin de restringir el acceso de los usuarios a la solución en la estación de trabajo según los permisos que se le otorgaron (por ejemplo, permiso para salir de la aplicación).
- La solución debe proporcionar mecanismos de autoprotección con el fin de evitar que otras aplicaciones realicen acciones que puedan interferir con el funcionamiento de la solución propuesta.
- La solución debe permitir realizar un análisis personalizado para cualquiera de los siguientes objetos: Memoria del sistema, Objetos cargados en el inicio del sistema operativo, Copia de seguridad del sistema operativo, Buzón de correo de Microsoft Outlook, Unidades de disco duro, Unidades extraíbles y unidades de red o Cualquier archivo seleccionado.
- La solución debe permitir realizar un análisis en segundo plano de manera que la aplicación no le muestre ninguna notificación al usuario y que tenga menos impacto en los recursos del equipo, para cualquiera de los siguientes objetos: objetos de inicio, el sector de arranque, la memoria del sistema y la partición del sistema.
- La solución debe permitir establecer una programación para el análisis, de manera que se pueda realizar de forma manual o según programación.
- La solución debe permitir analizar archivos compuestos de formatos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos comprimidos.
- La solución debe permitir analizar archivos protegidos con contraseña.

- La solución debe incorporar un componente de protección frente a amenazas web que permita evitar la descarga de archivos maliciosos de Internet y también bloquee sitios web maliciosos y de phishing.
- La solución debe analizar tráfico HTTP, HTTPS y FTP.
- La solución debe bloquear el tráfico HTTP que no cumple con los estándares RFC
- La solución debe incluir un componente de protección frente a amenazas en el correo que permita analizar los archivos adjuntos de mensajes de correo electrónico entrantes y salientes en busca de virus y otras amenazas.
- La solución de protección frente a amenazas en el correo debe ser compatible con POP3, SMTP, IMAP y NNTP.
- La solución de protección frente a amenazas en el correo debe intentar desinfectar un objeto infectado en un mensaje entrante o saliente. Si el objeto no se puede desinfectar, el componente de protección en el correo deberá eliminar el objeto infectado y añadir información sobre la acción realizada al asunto del mensaje, por ejemplo: [Se ha procesado el mensaje] <asunto del mensaje>.
- La solución debe incluir un componente de protección frente a amenazas en la red que monitoree el tráfico de red entrante en busca de actividad característica de los ataques de red.
- La solución debe bloquear la conexión de red con el equipo atacante.
- La solución debe incluir una base de datos que ofrezca descripciones de los tipos de ataques de red actualmente conocidos y los modos para contrarrestarlos.
- La solución debe bloquear el equipo que realiza el ataque y restringir el envío de paquetes de red durante un periodo determinado de al menos una hora.
- La solución debe permitir seleccionar el protocolo y el puerto que se van a usar para la comunicación y permitir actividades de red específicas.
- La solución debe permitir activar y administrar la protección contra los siguientes tipos de ataques a la red, mínimamente: Inundación de red (flooding) ataques de tipo "Port scan", Ataques de spoofing de MAC.
- La solución debe incluir un componente de Firewall de escritorio que bloquee las conexiones no autorizadas al equipo mientras se trabaja en Internet o en la red local.
- El componente de firewall de escritorio debe controlar la actividad de red de las aplicaciones en el equipo.
- El componente de firewall de escritorio debe proporcionar protección del equipo con la ayuda de bases de datos antivirus, el servicio de inteligencia global en la nube y reglas de red predefinidas.
- El componente de firewall de escritorio debe incluir un componente prevención de intrusiones en el host que proporcione acceso controlado de las aplicaciones a los recursos, procesos y datos personales del sistema operativo mediante el uso de derechos de aplicación.
- El componente de firewall de escritorio debe controlar la actividad de la red sobre el protocolo seleccionado: TCP, UDP, ICMP, ICMPv6, IGMP y GRE.
- El componente de firewall de escritorio debe permitir seleccionar los adaptadores de red que pueden enviar o recibir paquetes de red.
- El componente de firewall de escritorio debe permitir restringir el control de los paquetes de red según su período de vida (TTL).
- El componente de firewall de escritorio debe, de forma predeterminada, crear un conjunto de reglas de red para cada grupo de aplicaciones que la solución detecta en el equipo
- La solución debe incluir un componente de prevención de ataques a nivel de USB impide que dispositivos USB infectados que emulan un teclado se conecten al equipo.
- El componente de prevención de ataques a nivel de USB debe permitir que los dispositivos USB que el sistema operativo identifique como teclados y que estén conectados al equipo antes de instalar el componente se consideren autorizados después de la instalación del componente.
- El componente de prevención de ataques a nivel de USB debe bloquear automáticamente el dispositivo USB si el código de autorización se introduce incorrectamente un número de veces especificado.
- El componente de prevención de ataques a nivel de USB debe permitir utilizar un teclado en pantalla para autorizar dispositivos USB que no permitan introducir caracteres aleatorios

(p.ej., escáneres de códigos de barras).

- La solución debe incluir un componente de protección AMSI diseñado para ser compatible con Antimalware Scan Interface de Microsoft.
- El componente de protección AMSI debe permitir configurar el análisis de protección AMSI para archivos compuestos, como archivos de almacenamiento, paquetes de distribución o archivos en formatos de Office.
- La solución debe incluir un componente de prevención de exploits que permita detectar código de software diseñado para aprovechar vulnerabilidades en el equipo y, a través de estas, realizar acciones maliciosas o abusar de los privilegios de administración
- El componente de prevención de exploits debe incluir un mecanismo de protección de la memoria de procesos del sistema, de manera que la solución bloquee los procesos externos que intentan acceder a los procesos del sistema
- La solución debe incluir un componente de prevención de intrusiones en el host que evite que las aplicaciones realicen acciones que puedan resultar peligrosas para el sistema operativo.
- El componente de prevención de intrusiones en el host debe controlar el funcionamiento de las aplicaciones mediante el uso de derechos de las aplicaciones.
- El componente de prevención de intrusiones en el host debe activar la protección del acceso a audio y vídeo, de manera que se evite que los ciberdelincuentes puedan usar programas especiales para intentar obtener acceso a dispositivos que graban audio y vídeo (como micrófonos o cámaras web), controlando cuándo las aplicaciones reciben una transmisión de audio o vídeo y protege los datos contra la interceptación no autorizada.
- La solución debe incluir un componente de motor de reparación que le permita revertir las acciones realizadas por aplicaciones maliciosas en el sistema operativo.
- La solución debe incluir un componente de control web que permita regular el acceso de los usuarios a los recursos web.
- El componente de control web debe permitir supervisar tráfico HTTP y HTTPS.
- La solución debe incluir un componente de control de dispositivos que administre el acceso de los usuarios a dispositivos instalados o conectados al equipo (por ejemplo, discos duros, cámaras o módulos wifi), con el fin de proteger el equipo de infecciones cuando se conectan los dispositivos; y se evitan pérdidas o fugas de datos
- El componente de control de dispositivos debe permitir la creación de reglas de acceso que permitan ajustar la configuración que determina qué usuarios pueden usar dispositivos instalados en un equipo o conectados a él.
- El componente de control de dispositivos debe proporcionar funciones de Anti-Bridging con el fin de impedir establecer conexiones de red simultáneas en un equipo para prevenir la creación de puentes de red.
- La solución debe incluir un componente de control de aplicaciones que permita gestionar el inicio de aplicaciones en los equipos de los usuarios.
- El componente de control de aplicaciones debe permitir crear categorías de aplicaciones que se quieren gestionar.
- El componente de control de aplicaciones debe permitir crear reglas en la directiva para el grupo de administración.
- El componente de control de aplicaciones debe crear una imagen propietaria de los programas que garantizan el funcionamiento normal del sistema operativo.
- El componente de control de aplicaciones debe realizar un inventario de los archivos con los siguientes formatos: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX y SCR, cuando se añade contenido manualmente.
- La solución debe incluir características básicas de Endpoint Detection and Response (EDR).
- La solución debe permitir agregar un Widget de alertas de EDR que muestre información sobre la cantidad de alertas en los dispositivos durante el último mes.
- La solución debe contar con la capacidad de mostrar toda la información disponible sobre la amenaza detectada.
- La solución debe proveer un gráfico de la cadena de desarrollo de amenazas que proporcione información visual sobre los objetos involucrados, como procesos clave en el dispositivo, conexiones de red, bibliotecas y subárboles de registro.

8.3. Instalación

- El contratista deberá instalar y/o actualizar el software sobre los equipos y servidores del Programa Nacional de Asistencia Solidaria Pensión 65.
- Pension 65 brindará el servidor y las facilidades para la instalación y/o actualización del producto.
- La instalación y/o actualización puede hacerse de manera remota.

9. PRESTACIONES ACCESORIAS A LA PRESTACIÓN PRINCIPAL

No aplica

10. REQUISITOS MINIMOS QUE DEBE CUMPLIR EL CONTRATISTA

El postor (postulante) para la ejecución del servicio deberá cumplir obligatoriamente con los siguientes requisitos mínimos:

PERFIL DEL PROVEEDOR:

- Persona Jurídica con registro Unico del Contribuyentes (RUC) Activo y habido, con más de cinco (05) años de operación.
- Empresa dedicada a la venta de soluciones similares al rubro de licenciamiento o instalación de software antivirus.
- El postor deberá acreditar para admisión de la oferta ser representante o distribuidor autorizado de la marca ofertada, adjuntando una carta del fabricante haciendo referencia al proceso.

EXPERIENCIA:

El Postor, mediante i) contratos u órdenes de servicio, 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 mediante cancelación en el mismo comprobante de pago, correspondientes a un máximo de diez (10) contrataciones, deberá acreditar un monto facturado acumulado equivalente a S/ 10,000.00 (Diez mil y 00/100 Soles) por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los tres
(03) 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 licenciamiento o instalación de software antivirus en entidades públicas y/o privadas.

11. SEGUROS

No Aplica

12. PLAZO DE EJECUCIÓN DEL SERVICIO

Se estima que el plazo para la activación de las licencias no deberá exceder a los diez (10) días calendario, contados a partir del día siguiente de la notificación de orden de servicio.

13. LUGAR DE EJECUCIÓN DEL SERVICIO

El servicio será prestado en la sede del Datacenter de PENSION 65: Calle Schell N° 310 Piso 5 – Miraflores - Lima o de manera remota, previa coordinación entre la Unidad de Tecnologías de la Información y el proveedor.

14. PRODUCTO A OBTENER (ENTREGABLE)

- ✓ Informe técnico de la implementación. El mismo deberá incluir la documentación descriptiva de las tareas realizadas, así como los resultados de las pruebas efectuadas durante la renovación de licencias para el PROGRAMA NACIONAL DE ASISTENCIA SOLIDARIA PENSION 65. El informe debe incluir:
  - Procedimiento de escalamiento de fallas, así como datos de los contactos de soporte técnico.
  - Toda bibliografía y/o documentación necesaria para utilizar los elementos que forman parte de la contratación.
  - Cuatrocientas (400) Licencias de equipos y servidores.

El producto será presentado vía Mesa de Partes Digital del Programa Nacional de Asistencia Solidaria PENSIÓN 65 (https://mdp.pension65.gob.pe/mpde/#/SolicitudTramite).

OBLIGATORIO: El entregable deberá contener el informe de actividades con el respectivo sustento, además del comprobante de pago electrónico al crédito con un mínimo de 10 días hábiles de vencimiento, suspensión de 4ta categoría (de corresponder) y la Validez del Comprobante de Pago Electrónico emitido (https://e-consulta.sunat.gob.pe/ol-ti-itconsvalicpe/ConsValiCpe.htm).

15. GARANTÌA DEL SERVICIO

Garantía mínima de 12 meses contados a partir de instalación de las licencias de antivirus en la consola de Administración. Además, supedita el proceso a las normativas de garantías del Artículo 61 de la Ley 32069.

16. VERIFICACION TECNICA DE LAS CONTRATACIONES

El área responsable de la verificación Técnica y la Supervisión de la ejecución de la contratación es la Unidad de Tecnologías de la Información.

17. CONFORMIDAD DEL SERVICIO

La conformidad del bien, estará a cargo del jefe de la Unidad de Tecnologías de la Información con V°B° del Especialista de Infraestructura de Aplicaciones y Base de Datos.

18. FORMA DE PAGO

Pago único posterior a la entrega, instalación, configuración, recepción conforme y presentación del comprobante de pago.

19. PENALIDAD POR MORA, de ser necesario.

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto de la contratación, PENSIÓN 65 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:

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

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.

De conformidad al numeral 119.2 del articulo 119 del Reglamento de la Ley General de

Contrataciones Públicas N° 32069, aprobado con Decreto Supremo N° 009-2025-EF, ***"La suma de la aplicación de las penalidades por mora y de otras penalidades no debe exceder el 10% del monto vigente del contrato o, de ser el caso, del ítem correspondiente."***

20. OTRAS PENALIDADES (De corresponder)

No Aplica.

21. MEDIDAS DE CONTROL DURANTE LA EJECUCIÓN CONTRACTUAL

- Áreas que coordinan con el proveedor: Unidad de Tecnologías de la Información
- Áreas responsables de las medidas de control: Unidad de Tecnologías de la Información
- Áreas que brindarán la conformidad: Unidad de Tecnologías de la Información

22. GESTIÓN DE RIESGOS

LAS PARTES realizan la gestión de riesgos de acuerdo con lo establecido en el presente contrato y los documentos que lo conforman, a fin de tomar decisiones informadas, aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación

23. RESPONSABILIDAD DEL CONTRATISTA POR CALIDAD OFRECIDA Y VICIOS OCULTOS

Condición obligatoria. El contratista es el responsable por la calidad ofrecida y por los vicios ocultos del servicio ofertados por un plazo no menor de un (1) año contado a partir de la conformidad otorgada por el Programa PENSIÓN 65.

24. COMPROMISO ANTICORRUPCIÓN.

El proveedor/contratista acepta expresamente que no llevará a cabo acciones que están prohibidas por las leyes locales u otras leyes anticorrupción. Sin limitar lo anterior, el proveedor/contratista se obliga a no efectuar algún pago, ni ofrecerá o transferirá algo de valor, a un funcionario o servidor público o a cualquier tercero relacionado con el servicio aquí establecido de manera que pudiese violar las leyes locales u otras leyes anticorrupción, sin restricción alguna.

En forma especial, el proveedor/contratista declara con carácter de declaración jurada que no se encuentra inmerso en algún proceso de carácter penal vinculado a presuntos ilícitos penales contra el estado peruano, constituyendo su declaración, la firma del mismo en la Orden de Servicio de la que estos términos de referencia forman parte integrante.

25. COMPROMISO ANTISOBORNO

El proveedor, no debe ofrecer, negociar o efectuar cualquier pago, objeto de valor o cualquier dádiva en general, o cualquier beneficio o incentivo ilegal en relación al contrato, que pueden constituir un incumplimiento a la ley, tales como robo, fraude, cohecho o tráfico de influencias, directa o indirectamente, o a través de socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas, en concordancia a lo establecido en la normativa vigente. Asimismo, el proveedor 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, participantes, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas. De lamisma forma, el proveedor se compromete a comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviere conocimiento; así también, en adoptar medidas técnicas, prácticas, a través de canales dispuestos por el Programa. El proveedor es consciente que, de no cumplir con lo anteriormente expuesto, se someterá a la resolución del servicio o bien contratado y a las acciones civiles y/o penales que el Programa pueda accionar, constituyendo su declaración, la firma de este en la Orden de Servicio de la que estos términos de referencia forman parte integrante.

El contratista declara conocer los compromisos antisoborno del Programa Nacional de Asistencia Solidaría – Pensión 65, el cual se estable en su Política del Sistema de Gestión

Integral que se encuentra disponible en el portal web de PENSION 65: https://cdn.www.gob.pe/uploads/document/file/2107892/2093020-politica-del-sistema-de-gestion-integral%282%29.pdf?v=1737480521

26. MATERIAL DE ORIENTACIÓN PARA DENUNCIAR ACTOS DE CORRUPCIÓN / SOBORNO EN LOS PROCESOS DE CONTRATACION.

En el Programa Nacional de Asistencia Solidaría (PNAS) – Pensión 65, promovemos la ética e integridad de la función pública, por lo que, si conoces de algún acto de corrupción o soborno ejercido por un/a servidor/a del PNAS-Pensión 65, comunícanos tu denuncia ingresando de manera virtual a la Plataforma Digital Única de Denuncias del Ciudadano https://denuncias.servicios.gob.pe/ o para temas de denuncias por soborno a: https://docs.google.com/forms/d/e/1FAIpQLSel3LRxAJegUG4vInZ2dRiCvezEYZr_ceGzlZ_muaOocDU2sg/viewform

También puede visualizar ejemplo y tener una guía para elaborar una denuncia: https://drive.google.com/file/d/1DrvhxU8D38tC40qxGnw41vpoRxg6BPD-/view?usp=sharing

27. CLAUSULA DE CONFIDENCIALIDAD

EL PROVEEDOR, deberá mantener y guardar estricta reserva y absoluta confidencialidad sobre las características, términos y condiciones del contrato de servicio, incluyendo información objeto de derecho de autor, patentes , técnicas, modelos, invenciones, know – how, proceso, algoritmos, programas, ejecutables, investigaciones, detalles de diseño, información financiera, lista de clientesinversionistas empleados, relaciones de negocio y contractuales, pronósticos denegocios, planes de mercadeo y cualquier información revelada sobre terceras personas. EL PROVEEDOR se compromete a respetar y aplicar en la ejecución del servicio, las políticas, procedimientos, estándares y controles de seguridad de la información establecidos por EL CONTRATANTE, los mismos que declara conocer yaceptar. EL PROVEEDOR deberá proteger los activos de información del CONTRATANTE, asimismo ELPROVEEDOR deberá respetar las políticas de acceso no autorizado, pérdida, modificación y/o destrucción, falsificación, robo, uso indebido y/o divulgación de los activos de información del CONTRATANTE. EL PROVEEDORse obliga a mantener y a guardar estricta reserva y absoluta confidencialidad por sus miembros autorizados de su equipo de trabajo todos los documentos e información del CONTRATANTE a los que tenga acceso en ejecución del contrato de servicio. Seentiende que la obligación asumida por EL PROVEEDOR está referida no solo a los documentos e información señalados como "confidenciales" sino a todos los documentos e informaciones que en razón del contrato o vinculado con la ejecución del mismo, pueda ser conocida por cualquier medio por EL PROVEEDOR. En consecuencia, EL PROVEEDOR deberá abstenerse de divulgar tales documentos, conversaciones, acuerdos de reuniones y comentarios que como parte de la función son de uso conocimiento, sea en forma directa o indirecta.

De igual manera se compromete a cumplir con: la Política de Gestión Integral en temas relacionados al sistema de gestión de la calidad, gestión antisoborno y gestión de la seguridad de la Información; así como, las demás normas y leyes correspondientes a dichos temas mencionados.

En caso de que incumpliera con cualquiera de las obligaciones estipuladas en el presente acuerdo, el PNAS – Pensión 65, está autorizado a iniciar todas las acciones judiciales o extrajudiciales necesarias para resarcir del perjuicio, y la obligación de confidencialidad perdurará mientas la información conserve las características para considerarse Confidencial.

28. CLÁUSULA DE PROTECCIÓN DE DATOS PERSONALES

El proveedor declara expresamente conocer los alcances de la Ley N° 29733, Ley de Protección de Datos Personales, y su Reglamento aprobado por Decreto Supremo N° 003-2013- JUS, por lo que asume las responsabilidades que puedan corresponderle derivadas de la legislación vigente sobre protección de datos de carácter personal. La información proporcionada por la institución al PROVEEDOR a través de cualquier medio no tiene efectos

legales de cesión de datos. Únicamente, constituye el simple acceso a los mismos como elemento necesario para brindar el servicio materia del presente contrato. El PROVEEDOR se obliga a mantener en estricta reserva y absoluta confidencialidad todos los documentos, base (banco) de datos, que contengan información personal de usuarios, proveedores, y/o empleados de cualquiera de las partes. Esta información no podrá ser utilizada para fines distintos a los necesarios para la prestación del servicio objeto del presente contrato, ni podrá ser entregada o cedida, parcial o totalmente, a terceras personas ajenas a esta relación contractual.

29. DECLARACION JURADA DE INTERES

En el marco de lo establecido en el art. 3 de la Ley N.º 31227 " Ley de 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", y el artículo 8 del Reglamento aprobado por Resolución de Contraloría N.º 158-2021-CG, el contratista, en su calidad de sujeto obligado, debe cumplir bajo responsabilidad con la presentación de la Declaración Jurada de intereses conforme a los plazos y disposiciones contenidas en dichas normas legales.

30. RESOLUCION DE CONTRATO POR INCUMPLIMIENTO

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) Por la acumulación del monto máximo de la penalidad por mora o por el monto máximo para otras penalidades, en la ejecución de la prestación a su cargo
d) 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.
e) Por incumplimiento de la cláusula anticorrupción.
f) Por la presentación de documentación falsa o inexacta durante la ejecución contractual.
g) 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
h) Desaparición de la necesidad, debidamente justificada por el área usuaria.
i) Por mutuo acuerdo entre las partes.

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.

31. CLÁUSULA DE CUMPLIMIENTO

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.

32. SOLUCIÓN DE CONTROVERSIA

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.

33. GASTOS POR DESPLAZAMIENTO (De corresponder)
No Aplica.

Firma del Área Usuaria

pensión65 tranquilidad para más peruanos

Firmado digitalmente por FRITAS YAYA Herbert Hipolito FAU 20547960051 hard
Motivo: Soy el autor del documento
Fecha: 17.07.2026 09:57:10 -05:00