SERVICIO DE RENOVACION DE LICENCIA DE SOFTWARE ANTIVIRUS - EP EG 2026 2025

1. ÁREA SOLICITANTE

Gerencia de Informática y Tecnología Electoral (GITE).

2. ANTECEDENTES

RESOLUCIÓN JEFATURAL N° 000072-2025-JN/ONPE publicado el 05 de mayo de 2025 que aprueba el Plan Operativo Institucional 2025, Versión 02", de la Oficina Nacional de Procesos Electorales.

Resolución Jefatural N° 000131-2025-JN/ONPE (11AGO2025), se aprobó los "Lineamientos para la contratación de bienes y servicio requeridos por la ONPE para la realización del proceso electoral Elecciones Generales 2026".

Resolución Jefatural N° 000143-2025-JN/ONPE (09/09/2025) que aprueba la modificación de la Resolución Jefatural N° 000131-2025-JN/ONPE, con la finalidad de incorporar precisiones procedimentales relativas a la invitación de proveedores, las condiciones aplicables a contrataciones con proveedores, los requisitos de documentación obligatoria y las garantías exigibles; así como adecuar la normativa interna a lo dispuesto en la Ley N° 32416 y en la Ley N° 32069, en lo que corresponda. Se precisa que los demás extremos de la Resolución Jefatural N° 000131-2025-JN/ONPE y sus anexos, que no han sido objeto de modificación mediante la presente resolución, conservan plena vigencia.

La contratación del SERVICIO DE RENOVACION DE LICENCIA DE SOFTWARE ANTIVIRUS, permitirá cumplir la Actividad Operativa: ACTIVIDAD OPERATIVA: AOI00047901051: Gestión de la infraestructura tecnológica y base de datos.

3. DESCRIPCIÓN GENERAL DEL REQUERIMIENTO

Se requiere contar con el SERVICIO DE RENOVACION DE LICENCIA DE SOFTWARE ANTIVIRUS - EP EG 2026 2025 con el objetivo de brindar protección y seguridad a los equipos y a la red institucional, resguardándolos ante amenazas informáticas y posibles ataques (malware, ransomware, intrusiones, entre otros). Además, permitirá el control de aplicaciones y de dispositivos externos, entre otras características.

4. FINALIDAD PÚBLICA

La finalidad pública del presente servicio es garantizar la protección de los equipos de cómputo institucional mediante la suscripción de licencias de software antivirus, permitiendo prevenir amenazas informáticas, proteger la integridad de la información y asegurar la continuidad de los servicios ofrecidos por la ONPE a la ciudadanía. Asimismo, contribuye al uso legal y adecuado del software en la entidad.

5. OBJETIVOS DE LA CONTRATACIÓN

- Garantizar la protección eficiente de los equipos de cómputo, previniendo ataques informáticos, y la pérdida o corrupción de información causada por infecciones de software malicioso.
- Ofrecer servicios e información segura y confiable a la ciudadanía.

6. FUENTE DE FINANCIAMIENTO

RECURSOS ORDINARIOS (R.O).

7. DESCRIPCIÓN DEL SERVICIO

ÍTEM	CANTIDAD	UNIDAD DE MEDIDA	DESCRIPCIÓN DEL SERVICIO
01	01	SERVICIO	RENOVACION DE LICENCIA DE SOFTWARE ANTIVIRUS

El servicio consiste en la dotación de quinientas (500) licencias de software antivirus, que deberán contar con resguardo ante amenazas informáticas y posibles ataques (malware, ransomware, intrusiones, entre otros). Además, permitirá el control de aplicaciones y de dispositivos externos.

a) Las suscripciones a licencias de software de antivirus incluidas en la contratación del presente servicio deberán cumplir con las siguientes características:

- La seguridad antimalware deberá estar basada en la nube (cloud) del mismo fabricante, bajo la modalidad de suscripción y con vigencia durante el plazo del servicio contratado.
- La solución deberá ser capaz de detectar tanto malware conocido como amenazas de día cero (zero-day).
- La solución debe ser capaz de remediar la infección de al menos dos maneras: remediación automática y remediación manual.
- La solución propuesta debe garantizar una detección rápida y eficiente de archivos sospechosos, mediante el análisis instantáneo de los mismos en la nube.
- La solución debe tener un resultado igual o superior al 90% de efectividad en Telemetría (Telemetry Coverage) y Visibilidad (Visibility) sobre la última evaluación MITRE ATT&CK (Carbanak+FIN7) del año 2021.

7.1 INSTALACIÓN, PUESTA EN FUNCIONAMIENTO Y DESINSTALACIÓN DEL SOFTWARE

a) Las actividades programadas serán supervisadas por el personal de la ONPE.
b) La solución deberá estar completamente basada en software, sin incluir la adquisición de equipamiento adicional como complemento.
c) La solución deberá permitir realizar el descubrimiento de los equipos de cómputo sin antivirus instalado.
d) La instalación del software de antivirus se realizará a través de la consola principal de administración del antivirus.
e) La desinstalación del antivirus se deberá realizar desde la consola principal de administración del antivirus.
f) El contratista deberá habilitar una (01) consola de administración de antivirus para la gestión de las suscripciones de antivirus para los equipos de cómputo.

7.2 COMPATIBILIDAD

El software de antivirus deberá ser compatible con los siguientes Sistemas Operativos:

a) Microsoft Windows 10
b) Microsoft Windows 11

Opcionalmente podrá tener compatibilidad con las plataformas CentOS 5, CentOS 6, Cloud Linux 5, Cloud Linux 6, SUSE® Enterprise 10, SUSE® Enterprise 11.

7.3 CARACTERÍSTICAS INTERNAS

a) La solución de seguridad para las computadoras de la institución será de tipo integrada, lo que significa que contará con un único agente capaz de proporcionar protección completa contra diversas amenazas, incluyendo virus, spyware, adware y rootkits. Además, ofrecerá detección de comportamientos sospechosos, filtrado de seguridad de URL, protección web contra ataques basados en scripts maliciosos y control de aplicaciones potencialmente peligrosas en todos los protocolos de la red.
b) La solución debe proteger de forma proactiva frente a los ataques conocidos y de día cero frente a vulnerabilidades conocidas.
c) La solución debe examinar todo el tráfico entrante y saliente en busca de desviaciones de protocolo, infracciones de políticas o contenido que haga sospechar de un ataque.
d) La solución debe defender frente a ataques SQL injection, secuencias de sitios cruzados y otras vulnerabilidades de aplicaciones web.
e) La solución deberá incluir la herramienta de cuarentena para el usuario final, que facilite la gestión y autorización del uso de aplicaciones potencialmente no deseadas, permitiendo su control de manera segura y eficiente.
f) La solución de seguridad implementada deberá generar notificaciones sobre eventos relacionados con virus, spyware, adware, troyanos, malware y otras amenazas. Asimismo, deberá monitorear y reportar cualquier archivo creado, accedido o modificado, la detección de aplicaciones no deseadas, intentos de intrusión y cambios en la configuración del cliente de seguridad, enviando toda esta información a la consola de administración del antivirus.
g) La solución deberá realizar el filtrado de URL y la detección de ataques web mediante scripts maliciosos, restringiendo el acceso a sitios no autorizados y mostrando una página de bloqueo en el navegador de internet (IE, Mozilla, Chrome, Opera, entre otros) para notificar al usuario sobre la restricción aplicada.
h) La solución deberá contar con un sistema de control de acceso web a sitios inapropiados. Este sistema permitirá notificar o bloquear el acceso a páginas web según su clasificación por categorías, garantizando una navegación segura y controlada.
i) La solución ofertada debe realizar un análisis profundo y mediante las mismas realizar un reporte de diagnóstico detallado sobre su estructura, incluyendo librerías, aplicaciones instaladas y otros componentes. Además, deberá identificar y reportar cualquier comportamiento sospechoso que pueda ser indicativo de un ataque de malware.
j) La solución deberá contar con protección anti-ransomware proactiva para detectar y bloquear el cifrado en carpetas de red compartidas desde un equipo remoto.
k) La solución deberá emplear IA con *deep learning* para detectar y bloquear ataques en flujo de entrada o salida, previniendo movimientos laterales y/o verticales.
l) Protección de amenazas de día cero a través de tecnología de *deep learning* en el tráfico entrante y/o saliente.
m) La solución deberá contar con tecnologías de detección proactiva de amenazas conocidas y basadas en la nube (cloud) del mismo fabricante.

7.4 PREVENCIÓN DE MALWARE

a) La solución debe proteger sus cargas de trabajo frente a software malintencionado con técnicas avanzadas como machine learning predictivo.
b) La solución debe aislar malware para proteger instancias frente a ataques sofisticados, incluido ransomware.
c) La solución debe detectar actividad sospechosa o cambios no autorizados y brinda la capacidad de poner en cuarentena y recuperarse rápidamente con supervisión del comportamiento.
d) La solución debe proteger de inmediato frente a vulnerabilidades como Shellshock, Heartbleed o WannaCry.
e) La solución debe bloquear malware, incluido ransomware, que trate de evadir la detección.
f) La solución debe detectar y notificar actividades sospechosas o malintencionadas.

7.5 CONTROL DE APLICACIONES

a) La solución debe permitir el control de las aplicaciones por política (grupos de equipos o de forma global).
b) La solución debe restringir el acceso a la red de aplicaciones específicas, para lo cual el administrador podrá definir políticas y reglas con acciones de: permitir, bloquear y finalizar las aplicaciones y procesos. También se debe poder configurar, que una aplicación finalice cuando intente acceder a la red, o tan pronto como se inicie la aplicación.
c) La entidad puede solicitar al fabricante y/o postor la inclusión de nuevos programas y/o aplicaciones en la configuración del producto que considere que deben bloquearse y que se requiera incluir en dicho sistema limitando la ejecución de aplicativos por hash SHA256, nombre de archivo, versión del archivo, nombre del aplicativo, versión del aplicativo, fabricante/desarrollador, categoría (ejemplo, navegadores, gestor de descarga, juegos, aplicación de acceso remoto, etc.), además de tener la capacidad de bloquear la ejecución de un aplicativo que esté en almacenamiento externo.
d) La solución debe tener capacidad de realizar un inventario detallado de las aplicaciones pre-existentes instaladas en los equipos de cómputo de los usuarios finales y sobre la base de dicho inventario, realizar políticas y reglas de control.
e) Los usuarios administradores deben tener la opción de terminar un proceso potencialmente peligroso.
f) Los usuarios administradores deben tener la capacidad de restringir la ejecución de nuevas aplicaciones en los equipos de cómputo, permitiendo únicamente aquellas que hayan sido previamente autorizadas.
g) El sistema de control de aplicaciones debe permitir la afinación de la configuración para agregar programas y/o aplicaciones que causan un impacto negativo en el trabajo de los usuarios, en el uso del ancho de banda en la red y el incumplimiento de políticas de seguridad de la institución.

7.6 CONTROL Y PROTECCIÓN DE DISPOSITIVOS EXTERNOS

a) La solución deberá prevenir el acceso no autorizado a archivos, cambios de privilegios o permisos en los medios extraíbles.
b) La solución deberá permitir o bloquear la entrada y salida en todos los puertos de conexión, incluyendo:

- **Almacenamiento y periféricos:** Dispositivos de almacenamiento, DVD/CD-ROM, módems, impresoras y controladores USB.
- **Dispositivos de captura de imágenes:** Cámaras digitales, webcams, escáneres, dispositivos infrarrojos, lectores de Smart Cards y memorias PCMCIA.
- **Conectividad de red:** Adaptadores de red inalámbricos, Bluetooth y Bluetooth USB.

c) La solución deberá incluir un sistema de control de dispositivos para mitigar riesgos de malware en medios externos, gestionando su habilitación o restricción.
d) El sistema de control deberá estar integrado en el agente antimalware sin necesidad de instalar software adicional en los equipos.
e) Deberá permitir la habilitación temporal de acceso a dispositivos específicos y para usuarios autorizados, sin desactivar la protección.
f) La solución deberá contar con un módulo para aplicar políticas de seguridad en el control de dispositivos, asegurando que cualquier dispositivo de almacenamiento externo tenga solo privilegios de lectura, evitando la ejecución o escritura de aplicaciones maliciosas.
g) La solución deberá permitir la creación de listas blancas basadas en el reconocimiento del ID de hardware de cada dispositivo de almacenamiento, garantizando un control preciso y seguro de los dispositivos permitidos.

7.7 MITIGACIÓN Y CONTINGENCIA DE AMENAZAS DE DÍA CERO

a) La solución debe incluir un módulo para el análisis de vulnerabilidades y la gestión de parches, que permita identificar desde la consola todas las vulnerabilidades asociadas al sistema operativo y a los programas instalados en las computadoras de la institución.
b) El módulo de análisis de vulnerabilidades y gestión de parches debe ser capaz de clasificar los parches necesarios para las estaciones de trabajo, con el fin de resolver las vulnerabilidades de seguridad detectadas. Además, deberá realizar pruebas de aplicabilidad para garantizar que los parches no causen problemas de compatibilidad.

7.8 ACTUALIZACIÓN DEL PRODUCTO Y DE LA BASE DE FIRMAS

a) Debe proporcionar actualizaciones de firmas en tiempo real.
b) Debe gestionar un sistema de distribución de firmas antivirus desde la consola principal hacia las estaciones de trabajo, así como un sistema adicional de consulta de firmas basadas en la reputación de archivos y la reputación web, utilizando tecnología de Cloud Computing.
c) El sistema de firmas antivirus basado en la reputación de archivos debe ser manejado de manera integrada y visualizable desde la misma consola de administración del antivirus.
d) Debe funcionar con una base de firmas de archivos y bloqueo basado en comportamiento.
e) Debe permitir realizar las siguientes acciones sobre antivirus o antispyware: remediación, reparación, cuarentena y eliminación.
f) Debe contar con la capacidad de enviar muestras de archivos sospechosos a la nube del fabricante para detectar amenazas de día cero.
g) La solución debe ser capaz de desplegar los indicadores de compromiso (IoC) a todos los agentes, permitiendo tomar acciones para futuras detecciones.
h) Los indicadores de compromiso deben incluir archivos (Hash MD5 y/o SHA), direcciones IP, dominios y/o URLs.

i) Las actualizaciones del motor de escaneo antivirus en las estaciones de trabajo se deben realizar automáticamente (de forma programada) y manualmente desde la consola de administración del antivirus.
j) Las actualizaciones de nuevas versiones del producto deben realizarse automáticamente y no requieren la desinstalación o reinstalación de componentes previos, siendo actualizaciones incrementales.
k) La actualización del producto debe ser transparente para el usuario.

7.9 PREVENCIÓN CONTRA EXPLOITS

a) Debe proporcionar protección contra ataques basados en exploits que comprometen aplicaciones legítimas como los navegadores y Microsoft Office.
b) Identificar manipulaciones sospechosas de memoria en tiempo de ejecución. Al detectarse, el Anti-Exploit deberá terminar todos los procesos de Exploit, corregir la cadena de ataque completamente y desencadenar un Informe forense.

7.10 APRENDIZAJE DE COMPORTAMIENTOS MALICIOSOS

a) Debe tener un motor de detección de comportamiento malicioso, que detecte y remedie todas las formas de comportamiento malicioso.
b) Cuando se detecte un comportamiento malicioso, se genera un informe forense de todo el ataque. El ataque se puede remediar de forma automática o manual según el informe forense.

7.11 PROTECCIÓN CONTRA MÁQUINAS INFECTADAS DE MALWARE

a) Debe identificar equipos infectados por Bots y bloquear la comunicación del bot hacia sitios de C&C; para asegurar de que no se robe ni se envíe información confidencial fuera de la institución.
b) La solución debe utilizar una base de datos en nube para recibir actualizaciones y consulta la clasificación de IP, URL y recursos DNS no identificados.

7.12 PREVENCIÓN CONTRA RANSOMWARE

a) Debe tener protección contra malware del tipo ransomware que posea detección automática, bloqueo y eliminación de este tipo de amenazas.
b) Debe tener capacidad de monitorear actividad de los archivos y la red, sobre comportamiento sospechosos. Debe detener el ataque inmediatamente cuando detecta que el ransonware modifica los archivos.
c) Debe poseer la capacidad de restaurar archivos que fueron cifrados por el ransomware, como parte de la recuperación automática (remediación).
d) Debe ser posible bloquear tanto ransomware conocido como desconocido.
e) Debe realizar la protección del endpoint que están tanto en línea, como fuera de línea.

7.13 SANDBOXING EMBEBIDO/DISPONIBLE O IA PARA DETONACIONES

a) El Sandbox debe estar disponible de manera embebida en la solución o de acceso sin costo para su uso.
b) De no poseer Sandbox la solución debe poder evaluar los potenciales archivos maliciosos usando IA (machine learning + Deep learning).

c) El SandBoxing debe soportar distintos tipos de archivos, incluyendo como mínimo: Adobe PDF, Microsoft Word, Excel, PowerPoint, Ejecutables (EXE, COM, SCR, Flash SWF, RTF) y Comprimidos (ZIP).
d) Deberá proveer una plataforma en nube del tipo SaaS del propio fabricante, que permita el envío de muestras de archivos para detectar si son maliciosos o no, mediante emulación de malware (sandboxing).
e) La funcionalidad de sandboxing debe permitir el envío de mínimo 50 muestras diarias de archivos.

7.14 ANÁLISIS FORENSE

a) Debe construir automáticamente informes forenses, entregando visibilidad completa del alcance, daño o severidad y vectores del ataque, incluyendo:
   - Actividades sospechosas (conexiones y procesos relacionados al ataque).
   - Actividades de remediación (procesos terminados, archivos en cuarentena o eliminados, archivos restaurados en el caso de Ransomware)
   - Impacto al negocio del incidente, como archivo exfiltrados o cifrados por ransomware.
   - Detalle de la línea de tiempo del Incidente para determinar si es una infección.
b) Debe mostrar un reporte forense detallado, el cual mostrara las tácticas y técnicas de compromiso que fueron ejecutadas por el atacante.
c) Debe mostrar los elementos maliciosos que fueron remediados (cuarentena).
d) Debe indicar el punto de entrada del ataque (ej. Navegador, puerto USB, red interna, etc.)
e) Debe abarcar el arranque del sistema y rastrear los mecanismos de persistencia de malware (ej. Registros, archivos eliminados).

7.15 CAPTURA DE AMENAZAS

Utilizando el mismo agente de protección deberá:

a) Realizar tareas de Threat Hunting sobre todos los equipos donde se encuentre instalado el agente, la cual debe contar con query pre-definidos por el proveedor y además establecer queries personalizados, que permitan realizar el proceso de búsqueda proactiva e iterativa de ataques avanzados, y sobre los cuales debe tener capacidad de acciones de remediación.
b) Las acciones de remediación sobre las amenazas detectadas, puede realizarse de manera masiva o por cada uno de los resultados (amenazas). Estas acciones pueden ser enviar a cuarentena el archivo, terminar un proceso e iniciar un análisis forense en el equipo.
c) Debe contar con capacidades de detección avanzadas, como consultas y automatización, para encontrar actividades maliciosas y extraer pistas necesarias para la captura de amenazas.
d) Los resultados de las queries (consultas) deben mostrarse en una línea de tiempo que permita identificar rápidamente anomalías o picos de ataques, y con información de contexto como clasificación del ataque, familia de malware y técnica de MITRE empleada.
e) La solución debe proporcionar una sólida herramienta de investigación que recopila todos los eventos del endpoint con el agente instalado, incluidos los maliciosos, sospechosos y sin procesar. Estos datos deberán tener una retención predeterminada de 01 a 07 días en la nube del fabricante.

7.16 CONSOLA DE ADMINISTRACIÓN Y EVENTOS

a) La consola de administración deberá estar alojada en nube provista por el fabricante y deberá administrar centralizadamente todos los equipos que cuentan con el producto, a través de Internet.
b) El acceso a consola de administración en nube, debe soportar doble factor de autenticación.
c) Debe permitir la configuración de cada uno de los módulos de seguridad y sus respectivas opciones de manera granular, a través de reglas que deberán estar asociadas a equipos y/o grupos de equipos.
d) Debe contar con un módulo que permita configurar todo lo relacionado al modo de implementación o despliegue de los agentes. Este módulo deberá desplegar distintas versiones del agente, mediante reglas asociadas a equipos y/o grupos de equipos. La adición (instalación) o retiro (desinstalación) de cada uno de los módulos o funcionalidades, se deberá gestionar desde la consola. El despliegue se podrá realizar mediante archivo MSI o paquetes completos preconfigurados.
e) Debe tener capacidad de gestión de equipos finales, integrado con el Directorio Activo existente on-premise, a través de agentes que realicen la función de scanner, para importar todos los equipos y las estructuras organizativas a las que pertenecen.
f) La solución debe ser capaz de crear log de seguridad, de tal forma que se tenga información ante un incidente de seguridad.
g) Debe contar con un módulo que permita ver en forma general cual es el estado de los puntos finales, así como las alertas que están activas.
h) Debe tener un módulo que permita hacer seguimiento de cada módulo de seguridad instalado en los puntos finales, de tal forma que podamos tener información relevante de los usuarios y PC por módulo de seguridad instalado en los agentes.
i) Debe contar con capacidad de establecer roles en la consola de administración por tipos de usuarios: Administrador, Read-Only (Solo lecutura) y HelpDesk o Remote Help (para soporte en tareas de desbloqueo de equipos cifrados).
j) Debe contar con un módulo de reporte, que permita mostrar información de:
   - El estado del despliegue de cada agente.
   - Estado de los módulos de seguridad instalado en los puntos finales.
   - Top de botnets, phishing, malware, host infectados.
k) Debe permitir la gestión y administración impulsada por políticas.
l) Las plantillas de políticas personalizables permiten a los usuarios habilitar y deshabilitar controles de seguridad sobre la marcha basándose en reglas que han asignado.
m) El contratista deberá habilitar una (01) consola de administración de antivirus para la gestión de suscripciones de antivirus para equipos de cómputo.

7.17 ADMINISTRACIÓN DE LICENCIAS

La solución debe permitir el manejo flexible de las licencias, de manera que puedan ser reasignadas en caso se restaure el sistema o el usuario cambie de computadora.

7.18 ALERTAS Y REPORTES

a) La solución debe proporcionar notificación inmediata de sucesos o actividades que puedan requerir atención inmediata.

b) La solución debe brindar informes detallados y auditables que documentan los ataques evitados y el estado de cumplimiento de las políticas.
c) La solución podrá generar reportes gráficos, los cuales deberán ser imprimibles y exportables, mostrando la cobertura de versiones, actualizaciones e infecciones.
d) La solución deberá contar con un sistema de reportes que permita visualizar el estado de protección de la red en tiempo real, mostrando las actividades que están ocurriendo en la red de manera continua.
e) La solución deberá incluir un sistema de reportes que posibilite la programación de la creación y envío de informes en formatos PDF, HTML y XML, a través de correo electrónico, en una fecha y hora predeterminadas.
f) La solución deberá ser capaz de realizar un inventario completo del hardware de todas las computadoras.
g) La solución deberá contar con la capacidad de realizar un inventario de software instalados en todas las computadoras de la institución.

7.19 CONSIDERACIONES GENERALES

Durante el periodo de contratación del servicio, se debe incluir como mínimo lo siguiente:

a) Soporte técnico: Incluye la solución de incidentes que afecten el normal desempeño del software y/o asesoría técnica, disponible las 24 horas del día, los 7 días de la semana, incluidos sábados, domingos y feriados (24x7) durante el plazo del servicio contratado. El servicio se brindará a través de atención telefónica, remota o mediante cualquier otro medio de comunicación disponible.
b) Acceso a parches, actualizaciones y nuevas versiones del software proporcionadas por el fabricante.
c) En caso de las nuevas versiones del software, el contratista será responsable de realizar el despliegue y actualización de los productos solicitados en todas las estaciones de trabajo de la institución.
d) Las actividades o provisiones de equipamiento, componentes, productos, aplicaciones y/o licenciamiento que deba ejecutar el proveedor para la atención y/o subsanación de incidencias y/o requerimientos reportados por la solución ofertada serán cubiertas por el proveedor, sin incurrir en un costo adicional para la entidad.

7.20 NIVELES DE SERVICIO PARA EL SOPORTE TÉCNICO

Para el registro de las solicitudes de soporte técnico se utilizará el correo electrónico, el cual será presentado al inicio del servicio.

Los niveles de servicio (SLA) para la atención de solicitudes de soporte técnico son:

Tiempos de solución:

Niveles de Servicio	Tiempo solución máximo (*)
Alta	04 horas
Media	08 horas
Baja	12 horas

(*) El tiempo de solución se contabiliza a partir de la emisión vía correo electrónico, de la solicitud del soporte técnico por parte de la ONPE, hasta que se solucione el incidente, informado mediante correo electrónico por el contratista.

- **Alta:** Son incidentes que necesita un tratamiento especial por el impacto que representa para la organización; la ausencia de atención inmediata afecta o podría afectar significativamente la operación de algún componente de la infraestructura tecnológica.
- **Media:** Son incidentes con un tiempo de atención intermedio; la ausencia de atención afecta o podría afectar moderadamente a la operación de algún componente de la infraestructura tecnológica.
- **Baja:** Son incidentes con un tiempo de atención menor; la ausencia de atención afecta o podría afectar levemente a la operación de algún componente de la infraestructura tecnológica.

La clasificación de los niveles de servicio lo realizará el personal de la ONPE.

El personal de la ONPE verificará que se haya dado la solución al incidente antes de aceptar el fin del tiempo de solución.

7.21 OTRAS CONSIDERACIONES

a) Las actividades o provisiones de equipamiento, componentes, productos, aplicaciones y/o licenciamiento que deba ejecutar el proveedor para la atención y/o subsanación de incidencias reportados por la solución ofertada serán sin costo alguno para la entidad.

b) Durante los primeros cinco (5) días una vez iniciado el servicio, el contratista debe realizar todas las configuraciones necesarias para el despliegue de los agentes en las estaciones de trabajo final.

c) Los postores deberán sustentar en sus ofertas las características del software antivirus ofrecido mediante hoja de datos o ficha de características o guías de software o especificaciones técnicas del software o documento técnico o manual técnico u otros documentos oficiales del fabricante, con los cuales se sustente el cumplimiento de las características o funcionalidades, en idioma español.

7.22 DOCUMENTO PARA LA SUSCRIPCIÓN DE CONTRATO

Para la firma del contrato, el especialista en la administración del antivirus deberá contar con un curso y/o capacitación en la administración del software antivirus de la marca ofertada, acreditado mediante una certificación o certificado oficial emitido por el fabricante del producto o de la tecnología propuesta.

8. MODALIDAD DE PAGO

El presente procedimiento se rige por el Sistema de A SUMA ALZADA.

9. REQUISITOS QUE DEBERÁ CUMPLIR EL POSTOR

El servicio deberá ser prestado por una persona natural o persona jurídica, el cual debe cumplir con lo siguiente:

- Para la firma del contrato deberá acreditarse como empresa autorizada por el fabricante para la comercialización de los productos ofertados para el presente servicio, esto se acreditará mediante carta emitida por el mismo fabricante.

10. OBLIGACIONES DEL CONTRATISTA

El Contratista es el único responsable ante la Entidad de cumplir con la contratación, no pudiendo transferir esa responsabilidad a otras entidades ni terceros en general.

11. PLAZO DE EJECUCIÓN DEL SERVICIO

El plazo de ejecución del servicio será a partir de la activación de la suscripción de las licencias; hasta el 26 de diciembre de 2025 previa comunicación por parte de la entidad mediante correo electrónico y suscripción del contrato o notificación de la orden de servicio, lo que ocurra primero.

- El contratista deberá realizar el servicio según el siguiente cronograma:

Cuadro de Ejecución del Servicio

Ítem	Descripción de la actividad	PLAZO	
		inicio	Fin
1	Activación inicial de la suscripción de las licencias	Desde el día siguiente de la notificación por parte de la entidad mediante correo electrónico, previa suscripción del contrato o notificación de la orden de servicio, lo que ocurra primero.	Hasta los siete (07) días calendario
2	Plazo de ejecución del servicio	A partir de la activación de la suscripción de las licencias.	Hasta el 26 de diciembre de 2025
3	Inicio del servicio de soporte técnico	A partir de la activación de la suscripción de las licencias.	Hasta el 26 de diciembre de 2025

12. LUGAR DE LA PRESTACIÓN DEL SERVICIO:

El lugar del servicio, será en la sede central de la ONPE, Jr. Washington 1894, Cercado de Lima.

13. ENTREGABLES

Los entregables deberán ser presentados en forma impresa o digital, utilizando formatos compatibles con Microsoft Office y/o PDF:

Entregable	Descripción
Entregable 1	Dentro de los siete (07) días calendario siguientes de la activación de las licencias. a) Documento (carta, constancia o certificado) emitido por el fabricante, el cual acredite el periodo de contratación del software que requiere el servicio a nombre de la ONPE, indicado en el Capítulo denominado PLAZO DE EJECUCION DEL SERVICIO. b) Carta emitida por el Contratista en el cual indique el periodo del servicio de soporte técnico, así como el correo electrónico oficial del contratista, detallado en el numeral 1 del capítulo DESCRIPCIÓN DEL SERVICIO.

Entregable 2	Dentro de los cuarenta (40) días calendarios contados a partir del día siguiente de la activación de las licencias. a) Informe de cumplimiento respecto al servicio contratado incluyendo las atenciones de soporte técnico durante la ejecución del servicio.

El lugar de entrega de dicha documentación será en la mesa de partes presencial de la Sede Central de la ONPE situada en Jr. Washington 1894 - Cercado de Lima, en el horario de lunes a viernes de 8:30 a 16:30 o mediante la mesa de partes virtual externa de la institución a través de la página web de la ONPE (https://www.web.onpe.gob.pe/mpve), con atención a la Subgerencia de Infraestructura y Seguridad Tecnológica de la Gerencia de Informática y Tecnología Electoral.

14. CONFORMIDAD DEL SERVICIO

Será otorgada por la Gerencia de Informática y Tecnología Electoral, previo documento elaborado por la Subgerencia de Infraestructura y Seguridad Tecnológica (SGIST), a través de la verificación del cumplimiento de las condiciones establecidas en los Términos de Referencia en el plazo máximo de siete (07) días calendario de producida la recepción de la prestación parcial efectuada.

15. FORMA DE PAGO

El pago se realizará en dos (02) pagos parciales previa conformidad emitida por la Gerencia de Informática y Tecnología Electoral (GITE), en moneda nacional y a la presentación del comprobante por parte del contratista, de acuerdo a lo siguiente:

Porcentaje de pago	Entregable
1er. Pago: 70%	Entregable 1
2do. Pago: 30%	Entregable 2

El pago se efectuará mediante el respectivo abono en la cuenta bancaria individual del postor ganador, dentro de los diez (10) días hábiles siguientes de otorgada la conformidad, sea a través del Banco de la Nación o de cualquier otra institución bancaria del Sistema Financiero Nacional, para cuyo efecto EL CONTRATISTA comunicará su CODIGO DE CUENTA INTERBANCARIO (CCI), y se debe de contar además con:

- Conformidad por parte del área usuaria
- Comprobante de pago.

Dicha documentación se debe presentar en la mesa de partes virtual externa de la institución a través de la página web de la ONPE (https://www.web.onpe.gob.pe/mpve), o en la oficina de trámite documentario de la Sede Central de la ONPE, situado en Jr. Washington 1894, Cercado de Lima, en el horario de lunes a viernes de 8:30 a 16:30 horas.

16. RESPONSABILIDAD DEL CONTRATISTA

El Contratista es responsable de la calidad ofrecida y de los vicios ocultos de los servicios ofertados hasta la finalización del servicio, contada a partir de la activación de las licencias.

17. PENALIDADES APLICABLES

Penalidad por mora:

En caso de retraso injustificado del contratista en la activación inicial de la suscripción de las licencias y en la ejecución de las prestaciones objeto del contrato, la entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable, de conformidad con el artículo 120 del Reglamento.

La suma de la aplicación de las penalidades por mora y otras penalidades no debe exceder el 10% del monto vigente del contrato o, de ser el caso, del ítem correspondiente.

18. ANTICORRUPCIÓN Y ANTISOBORNO

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

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

Aunado a ello, EL CONTRATISTA se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, y/o cualquier servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.

Adicionalmente, EL CONTRATISTA se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con LA ENTIDAD CONTRATANTE.
Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato.

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

19. INTEGRIDAD

En caso de falsedad de cualquiera de las declaraciones efectuadas por el contratista, la ONPE podrá declarar la nulidad del presente contrato/orden de servicio por infracción del principio de presunción de veracidad, de conformidad a lo establecido en la Ley 32069 Ley General de Contrataciones Públicas.

20. CONFIDENCIALIDAD DE LA INFORMACIÓN

El CONTRATISTA deberá mantener estricta confidencialidad sobre la información a que tendrá acceso durante la ejecución del servicio, no podrá disponer de la misma para fines distintos al desarrollo del servicio. El proveedor y su personal, deben comprometerse a mantener las reservas

del caso y no transmitir los datos e información de ONPE a ninguna persona (natural o jurídica) que no sea debidamente autorizada por la ONPE.

21. REQUISITOS DE CALIFICACIÓN

A. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

El postor debe acreditar un monto facturado acumulado equivalente de S/ 32,000.00 (Treinta y dos mil con 00/100 soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los quince (15) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran servicios similares a los siguientes:

i. Servicio de suscripción de software antivirus.
ii. Licenciamiento o suscripción de software antivirus.
iii. Licenciamiento o suscripción antivirus.
iv. Servicio de Mantenimiento de Solución de Antivirus.
v. Mantenimiento y Soporte de Antivirus.
vi. Servicio de Soporte y Mantenimiento de Herramienta de Antivirus.
vii. Servicio de mantenimiento de licencias antivirus.
viii. Servicio de soporte técnico y licenciamiento del sistema antimalware.
ix. Licenciamiento o suscripción o servicio de soluciones antimalware.
x. Licenciamiento o suscripción o servicio antimalware.
x. Licenciamiento o suscripción o servicio de soluciones de detección de amenazas avanzadas persistentes y de día cero.
xi. Licenciamiento o suscripción o servicio de detección de amenazas avanzadas persistentes y de día cero
xii. Licenciamiento o suscripción o servicio de soluciones de detección ransomware.
xiii. Licenciamiento o suscripción o servicio de detección ransomware.

Acreditación

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 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, correspondientes a un máximo de veinte (20) contrataciones.

En caso el postor sustente su experiencia en la especialidad mediante contrataciones realizadas con privados, para acreditarla debe presentar de forma obligatoria lo indicado en el numeral (ii) del presente párrafo; no es posible que acredite su experiencia únicamente con la presentación de contratos u órdenes de compra con conformidad o constancia de prestación.

B. CAPACIDAD TÉCNICA Y PROFESIONAL

B.1. EXPERIENCIA DEL ESPECIALISTA EN LA ADMINISTRACIÓN DEL ANTIVIRUS

ESPECIALISTA

Requisitos:
El especialista en la administración del antivirus debe acreditar mínimo un (01) año de experiencia en administración del software antivirus propuesto.

Acreditación:
La experiencia del especialista en la administración del antivirus se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del especialista en la administración del antivirus, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.

En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el especialista en la administración del antivirus en meses sin especificar los días se debe considerar el mes completo.

Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.
De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.

B.2. CALIFICACIONES DEL ESPECIALISTA EN LA ADMINISTRACIÓN DEL ANTIVIRUS

B.2.1. FORMACIÓN ACADÉMICA

ESPECIALISTA

Requisitos:
El especialista en la administración del antivirus deberá contar, como mínimo, como Técnico Titulado y/o grado de Bachiller y/o Título Profesional en alguna de las siguientes especialidades:

Sistemas y/o Informática y/o Computación y/o Telecomunicaciones y/o Redes y Comunicaciones y/o Software y/o Cómputo y Telecomunicaciones y/o Sistemas e Informática y/o Ingeniería de Sistemas y/o Ingeniería de Informática y/o Ingeniería de Computación y/o Ingeniería de Telecomunicaciones y/o Ingeniería de Electrónica y/o Ingeniería de Redes y Comunicaciones y/o Ingeniería de Software y/o Ingeniería de Sistemas y Computación y/o Ingeniería de Cómputo y Telecomunicaciones y/o Ingeniería de Sistemas e Informática.

Acreditación:
El Título Profesional o Grado de Bachiller o Título Técnico será verificado por los evaluadores en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior

Universitaria - SUNEDU a través del siguiente link: *https://enlinea.sunedu.gob.pe/* o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: *https://titulosinstitutos.minedu.gob.pe/*, según corresponda.

El postor debe señalar los nombres y apellidos, DNI y profesión del especialista en la administración del antivirus, así como el nombre de la universidad o institución educativa que expidió el grado o título profesional requerido.

En el caso que el Título Profesional o Grado de Bachiller o Título Técnico no se encuentre inscrito en los referidos registros, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.

En caso se acredite estudios en el extranjero del especialista en la administración del antivirus, debe presentarse adicionalmente copia simple del documento de la revalidación o del reconocimiento ante SUNEDU, del grado académico o título profesional otorgados en el extranjero, según corresponda.

Visado digitalmente por
JESUS ALBERTO FELIX ATUNCAR
Subgerente de Infraestructura y Seguridad Tecnológica
SUBGERENCIA DE INFRAESTRUCTURA Y SEGURIDAD TECNOLÓGICA

Visado digitalmente por
ROBERTO CARLOS MONTENEGRO VEGA
Gerente de Informática y Tecnología Electoral
GERENCIA DE INFORMÁTICA Y TECNOLOGÍA ELECTORAL

V(01)