INSTITUTO NACIONAL DE CIENCIAS MÉDICAS Y NUTRICIÓN SALVADOR ZUBIRÁN

FORMATO DE JUSTIFICACIÓN PARA ADQUISICIONES SIN PROCEDIMIENTO DE LICITACIÓN PÚBLICA ARTÍCULO 55 LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO

Fecha de elaboración: junio 2026

Proyecto: INCMNSZ-2026-E-000512
Nombre del proyecto: ESTRATEGIA INSTITUCIONAL DE CONTRATACIONES DEL INCMNSZ
Nombre del servicio: Servicio de Arrendamiento de Licencia de uso de Software Antivirus

La Subdirección de Tecnologías de la Información y Comunicaciones tiene por objeto el conducir la administración y operación de los servicios de Tecnologías de la Información y de Comunicaciones en el Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán (INCMNSZ) mediante la implementación de estrategias tecnológicas que apoyen la operación de las áreas del Instituto, en este sentido la STIC requiere se lleve a cabo la contratación del "Servicio de Arrendamiento de Licencias de Uso de Software Antivirus"

Lo anterior, con fundamento en el Artículo 55, segundo párrafo de la Ley de Adquisiciones Arrendamientos y Servicios del Sector Publico que a la letra dice:

> *"Si el monto de la operación corresponde a una invitación a cuando menos tres personas, la procedencia de la adjudicación directa sólo podrá ser autorizada por la persona titular de la Unidad de Administración y Finanzas o, en su caso, de la Oficialía Mayor o equivalente".*

Adicionalmente, se atiende lo dispuesto en el primero párrafo del Artículo 8 de la Ley Federal de Austeridad Republicana donde se buscará la máxima economía, eficiencia y funcionalidad, observando los principios de austeridad, ejerciendo estrictamente los recursos públicos en apego a las disposiciones legales aplicables.

Alineación al Plan Anual de Trabajo del Instituto en materia de Tecnologías de la Información y Comunicaciones

El presente proyecto se encuentra alineado con el objetivo estratégico institucional orientado a implementar un modelo innovador de organización y administración que fortalezca las actividades institucionales, mediante la definición e implementación de estrategias que contribuyan a la sustentabilidad institucional.

Asimismo, se vincula con la línea de acción relativa al fortalecimiento de la Subdirección de Tecnologías de la Información y Comunicaciones, la cual tiene como propósito mejorar los sistemas informáticos y de comunicaciones para lograr un intercambio de información eficiente tanto al interior del Instituto como con otras instituciones nacionales y extranjeras.

INSTITUTO NACIONAL DE CIENCIAS MÉDICAS Y NUTRICIÓN SALVADOR ZUBIRÁN

FORMATO DE JUSTIFICACIÓN PARA ADQUISICIONES SIN PROCEDIMIENTO DE LICITACIÓN PÚBLICA ARTÍCULO 55 LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO

Fecha de elaboración: junio 2026

Antecedentes

El Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán contaba con una infraestructura tecnológica compuesta por más de 2,200 equipos de cómputo, servidores y dispositivos de red, esenciales para el desarrollo de sus funciones sustantivas, operativas y administrativas. Esta infraestructura está expuesta de manera constante a riesgos de seguridad informática, tales como virus, malware, ransomware, spyware y otras amenazas cibernéticas, las cuales pueden comprometer la confidencialidad, integridad y disponibilidad de la información institucional.

Con el objetivo de proteger esta infraestructura crítica, en los últimos años el Instituto ha celebrado contratos para el servicio de arrendamiento de licencias de uso de software antivirus con distintas empresas especializadas, garantizando así la protección continua de los equipos institucionales.

Dichos contratos han permitido mantener activos los servicios de prevención, detección y eliminación de amenazas en los equipos de cómputo del Instituto, incluyendo protección durante la navegación por internet y el uso del correo electrónico institucional.

Sin embargo, la creciente sofisticación de los ciberataques y la evolución constante de amenazas digitales hacen necesario continuar con la contratación de un servicio actualizado y robusto. Actualmente, la licencia vigente se encuentra en su etapa final y próximamente dejará de contar con soporte técnico y actualizaciones, lo cual representa una vulnerabilidad crítica para la operación tecnológica del Instituto.

Por tanto, resulta indispensable contratar nuevamente el servicio de arrendamiento de licencias de uso de software antivirus, que incluya:

- Protección en tiempo real contra amenazas conocidas y emergentes.
- Actualizaciones automáticas de bases de datos de firmas de virus.
- Administración centralizada para su despliegue y control.
- Capacidades de análisis proactivo y detección conductual.
- Soporte técnico especializado.

Esta contratación permitirá garantizar la continuidad operativa de los servicios institucionales, reducir riesgos informáticos, proteger la información sensible de pacientes, usuarios y personal, y cumplir con los estándares y lineamientos en materia de seguridad de la información establecidos en el marco jurídico aplicable.

Situación actual

Debido al crecimiento de áreas de atención médica, enseñanza e investigación, actualmente en la lista maestra de empleados del INCMNSZ nos encontramos adscritos 5,284 personas, aunado a lo anterior y debido a la digitalización de diversos procesos se

ha incrementado la necesidad de equipos de computo, por lo anterior, pasamos de 2200 a 2,400 equipos instalados y funcionando.

Con el incremento de estas 200 computadoras se logra el ahorro en tiempo de operación de actividades en diversas áreas, reducción de errores de usuarios y un incremento en la calidad de atención al paciente. Dichos equipos fueron instalados en diversas áreas del Instituto, entre las que destacan:

- Atención Institucional Continua y Urgencias.
- Departamento de Medicamentos.
- Departamento de Trasplantes.
- Medicina Crítica
- Hospitalización
- Departamento de Adquisiciones.
- Departamento de Patología
- Departamento de Enfermería
- Microbiología Clínica
- Laboratorio Central.
- Infectología
- Ingeniería Biomédica.
- Departamento de Conservación y Construcción.
- Departamento de Adquisiciones.
- Coordinación de Contratos.
- Entre otros.

En la actualidad, el Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán no cuenta con un servicio de antivirus que brinde protección centralizada a la infraestructura tecnológica institucional. Esta ausencia de protección especializada expone a los equipos de cómputo, estaciones de trabajo, servidores, equipos portátiles y dispositivos móviles a la posibilidad de infección por virus informáticos y otros tipos de software malicioso.

Esta situación incrementa el riesgo de alteración, robo o pérdida de información contenida en sistemas operativos, aplicaciones, carpetas compartidas, bases de datos y documentos institucionales. Asimismo, la falta de un sistema de protección administrado de forma centralizada dificulta la detección oportuna, la respuesta inmediata y la aplicación de políticas de seguridad uniformes en toda la red del Instituto.

En un entorno donde los ciberataques son cada vez más frecuentes y sofisticados, la carencia de este servicio limita la capacidad de prevención y respuesta, afectando potencialmente la disponibilidad, integridad y confidencialidad de la información crítica para el funcionamiento de las áreas médicas, administrativas y de investigación.

INSTITUTO NACIONAL DE CIENCIAS MÉDICAS Y NUTRICIÓN SALVADOR ZUBIRÁN

FORMATO DE JUSTIFICACIÓN PARA ADQUISICIONES SIN PROCEDIMIENTO DE LICITACIÓN PÚBLICA ARTÍCULO 55 LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO

Fecha de elaboración: junio 2026

Alcance del servicio

El servicio de arrendamiento de licencia de uso de software Antivirus tendrá como alcance la protección para 2400 equipos informáticos, con una vigencia del servicio del 01 de julio de 2026 al 29 de febrero de 2028, lo que permitirá mitigar los riesgos de amenazas por archivos o programas ejecutables dañinos mejor conocidos como software malicioso (malware) entre los que se pueden mencionar: gusanos informáticos, troyanos, spyware y ransomware.

Dicho software de antivirus debe contar con al menos:

- Parcheo Virtual.
- Control de Dispositivos y Aplicaciones
- DPL Avanzado.
- Prevención de intrusos (IDS/IPS).
- Sistemas operativos compatibles (Windows, macOS, Linux)
- Integración SIEM
- Gestión de Parches
- Filtro Web.

Beneficios del servicio.

La contratación del servicio facilitara la:

- Protección de datos
- Continuidad en el Servicio
- Seguridad en línea
- Confianza del paciente

1. Servicio de Arrendamiento de Licencias de Uso de Software Antivirus

El Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán, a través de la Subdirección de Tecnologías de la Información y Comunicaciones (STIC), emite el presente Formato de Justificación para efectos de promover la modernización y desarrollo administrativo, así como, establecer los mismos requisitos y condiciones para todos los participantes del procedimiento de contratación del "Servicio de Arrendamiento de Licencias de Uso de Software Antivirus"

INSTITUTO NACIONAL DE CIENCIAS MÉDICAS Y NUTRICIÓN SALVADOR ZUBIRÁN

FORMATO DE JUSTIFICACIÓN PARA ADQUISICIONES SIN PROCEDIMIENTO DE LICITACIÓN PÚBLICA ARTÍCULO 55 LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO

Fecha de elaboración: junio 2026

Objetivo del servicio

Contar con una plataforma centralizada diseñada para proteger computadoras, servidores y dispositivos móviles frente a amenazas cibernéticas. Que permita a los administradores de la Subdirección de Tecnologías de la Información y Comunicaciones, gestionar la seguridad de toda la red desde una consola, ya sea de forma local o en la nube.

Aunado a los anterior, el servicio de arrendamiento de licencia de uso de software antivirus debe ser una plataforma actualizada para prevenir, detectar y eliminar archivos o programas ejecutables dañinos dentro de los equipos de cómputo del Instituto extendiendo esta protección al correo electrónico y a la navegación por internet de los mismos.

I. 1.1 Descripción del servicio objeto de la contratación.

Contar con un Servicio de Arrendamiento de Licencias de Uso de Software Antivirus de última generación, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información generada en las diferentes áreas del INCMNSZ.

1.1.1 Requerimientos

Requerimientos no funcionales

La empresa proveedora deberá atender los siguientes requerimientos no funcionales:

- Acordar el plan de instalación con el administrador del servicio de arrendamiento de licencia de uso de software Antivirus.
- Llevar a cabo la instalación, configuración y puesta en operación de la consola de administración en el servidor propiedad del INCMNSZ.
- Asegurar la instalación y configuración de la licencia de uso de software antivirus para la protección de 2400 equipos de cómputo conectados a la red del INCMNSZ de acuerdo con el plan elaborado en conjunto con el administrador de la licencia de uso de software Antivirus.
- Configurar las políticas de seguridad correspondientes en la consola de administración remota en conjunto y a solicitud del administrador del servicio de arrendamiento de licencia de uso de software Antivirus.
- El proveedor deberá demostrar mediante copia simple que el personal que instalará el software deberá estar certificado por el fabricante en el manejo (Instalación o configuración) del antivirus propuesto y dicha certificación deberá estar vigente.

INSTITUTO NACIONAL DE CIENCIAS MÉDICAS Y NUTRICIÓN SALVADOR ZUBIRÁN

FORMATO DE JUSTIFICACIÓN PARA ADQUISICIONES SIN PROCEDIMIENTO DE LICITACIÓN PÚBLICA ARTÍCULO 55 LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO

Fecha de elaboración: junio 2026

Requerimientos Técnicos

El software antivirus deberá contar con una solución de administración en seguridad para equipos de cómputo, estaciones de trabajo, servidores, equipos portátiles y dispositivos móviles y deberá cumplir con las siguientes características:

- Deberá proporcionar herramientas de protección antivirus, antispyware, malware y ransomware.
- De igual forma deberá proporcionar un sistema de prevención de intrusiones basado en el host (HIPS).
- Deberá facilitar el control de la navegación web.
- Deberá contar con un módulo corta fuegos locales.
- Incluir un control de dispositivos internos y externos (USB, memorias extraíbles, puertos lógicos, etc.)
- Deberá considerar la protección a diversos sistemas operativos.
- La solución de antivirus deberá presentarse en su versión más reciente.
- El software antivirus deberá contar con una consola de administración con al menos las siguientes características:
- Administración remota.
- Configuración de grupos de equipos cliente.
- Notificaciones de sucesos.
- Ejecución aleatoria de tareas.
- Servidor de actualización local.
- Reversión de la actualización.
- El antivirus deberá soportar instalaciones en Estaciones de trabajo con diversos sistemas operativos como son: Microsoft® Windows® 10, Microsoft® Windows® 8.1, Microsoft® Windows® 8, Microsoft® Windows® 7 SP1 con las actualizaciones de Windows más recientes (al menos KB4474419 y KB4490628). En servidores Microsoft Windows Server 2019 (Server Core y Desktop Experience), Microsoft Windows Server 2016 (Server Core y Desktop Experience), Microsoft Windows Server 2012 R2, Microsoft Windows Server 2012, Microsoft Windows Server 2008 R2 SP1, Microsoft Windows Server 2008 SP2 (x86 y x64), Server Core (Microsoft Windows Server 2008 SP2, 2008 R2 SP1, 2012, 2012 R2). Para Almacenamiento, Pequeños negocios y Servidores MultiPoint: Microsoft Windows Storage Server 2016, Microsoft Windows Storage Server 2012 R2, Microsoft Windows Storage Server 2012, Microsoft Windows Storage Server 2008 R2 Essentials SP1, Microsoft Windows Server 2019 Essentials, Microsoft Windows Server 2016 Essentials, Microsoft Windows Server 2012 R2 Essentials, Microsoft Windows Server 2012 Essentials, Microsoft Windows Server 2012 Foundation, Microsoft Windows Small Business Server 2011 (x64), Microsoft Windows Small Business Server 2008 SP2 (x64), Microsoft Windows MultiPoint Server 2012, Microsoft Windows MultiPoint Server 2011, Microsoft Windows MultiPoint Server 2010. Sistemas operativos host

compatibles con la función Hyper-V Microsoft Windows Server 2019, Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2012, Microsoft Windows Server 2008 R2 SP1: Las máquinas virtuales se podrán explorar solo si están fuera de línea.

- Debe ofrecer seguridad integral protegiendo los sistemas empresariales contra virus, troyanos, gusanos, hackers, virus de red, ataques de amenazas mixtas desde múltiples puntos de entrada y spyware; bloquear archivos con contenido ejecutable malicioso y ejecutables incrustados/comprimidos que usen algoritmos de compresión en tiempo real; eliminar rootkits; poner en cuarentena archivos sospechosos; detectar malware mediante detección por comportamiento y otras técnicas. Identificar la fuente de infección, es decir, de dónde se originó la infección en la red.
- Debe tener la capacidad de respaldar y restaurar datos para que, en caso de un ataque de ransomware, los datos puedan recuperarse fácilmente.
- Debe tener la capacidad de restaurar un archivo desde la cuarentena si se considera que el archivo es seguro.
- Debe proporcionar un mecanismo de prevención de brotes de virus, el cual debe activarse según el umbral de malware detectado.
- Los usuarios comunes no deben poder modificar la configuración del antivirus, excepto aquellos en grupos especiales, según lo considere necesario el administrador.
- Gestores de actualizaciones: Deben tener la capacidad de crear múltiples servidores de actualizaciones para distribuir la carga de actualizaciones en un entorno de red grande y así reducir el ancho de banda consumido durante las actualizaciones de definiciones.
- Debe tener la capacidad de escanear archivos comprimidos, archivados y empaquetados.
- Debe tener la capacidad de escanear unidades USB de almacenamiento plug and play tan pronto como se conecten.
- Debe tener la capacidad de desconectar los endpoints infectados de la red.
- Debe tener la capacidad de excluir tipos/extensiones de archivos y carpetas del escaneo en tiempo real.
- Debe contar con una función para enviar notificaciones por correo electrónico con una lista de los sistemas no protegidos en la red.
- Debe tener la capacidad de especificar el tipo de archivo para realizar copias de seguridad críticas en caso de un ataque de ransomware.

Control de Dispositivos:

- Debe tener la capacidad de permitir, bloquear o permitir solo lectura para diversos dispositivos.
- Debe tener la capacidad de otorgar derechos de acceso para dispositivos de almacenamiento como USB, CD/DVD, lector de tarjetas, disquete, etc.
- Debe tener la capacidad de regular el uso de conexiones Wi-Fi y Bluetooth.

- Debe tener la capacidad de mantener el control sobre interfaces como FireWire, puerto serial, controlador SATA, Thunderbolt, etc.
- Debe tener la capacidad de controlar y regular dispositivos PCMCIA, lectores de tarjetas MTD/SCSI, etc.
- Debe tener la capacidad de controlar y regular el uso de impresoras, escáneres, cámaras web y carpetas compartidas en red.
- Debe tener la capacidad de permitir o bloquear la conexión de dispositivos portátiles con Windows como cámaras digitales, smartphones, etc.
- Debe tener la capacidad de permitir o bloquear la conexión de teléfonos móviles como Android, iPhone, iPad, iPod, Blackberry, etc., a los endpoints.
- Debe tener la capacidad de permitir o bloquear dispositivos Teensy Board.
- Debe tener la capacidad de excluir cualquier dispositivo específico de las políticas de control de dispositivos.
- Debe tener la capacidad de excluir cualquier dispositivo específico basado en el nombre del modelo.
- Debe tener la capacidad de cifrar el contenido de las USB y hacerlo accesible solo en endpoints donde esté instalado el cliente de seguridad.
- Debe tener la capacidad de permitir el acceso temporal a USB a algunos usuarios autorizados mediante OTP (contraseña de un solo uso).
- Debe tener la capacidad de bloquear completamente las interfaces USB para denegar el acceso a todos los dispositivos USB (excepto teclado, ratón y dispositivos de almacenamiento masivo).
- Debe tener la capacidad de soportar dispositivos formateados en NTFS y FAT para autorización.
- Provisión para agregar SSID Wi-Fi en lista blanca en la configuración de control de dispositivos. Los endpoints solo podrán conectarse a SSID Wi-Fi permitidos.
- Debe tener la capacidad de excluir dispositivos USB según su número de serie.
- Debe tener la capacidad de controlar el uso de anclaje USB desde los dispositivos conectados.
- Debe tener la capacidad de escanear y reportar vulnerabilidades presentes en las aplicaciones instaladas.
- Debe proporcionar una vista resumida de las vulnerabilidades según su severidad, es decir: Alta, Media y Baja.
- Debe tener la capacidad de programar escaneos de vulnerabilidades de forma periódica para obtener los reportes más recientes de las vulnerabilidades presentes en la red.

Administración de Parches:

- Debe tener la capacidad de escanear parches faltantes para aplicaciones de Microsoft. Por ejemplo: Windows, Office, Internet Explorer.
- Debe tener la capacidad de escanear parches faltantes para aplicaciones que no son de Microsoft. Ej: Adobe Reader, Adobe Acrobat, Adobe Flash

Player, VLC, Java, Putty, Notepad++, 7-Zip, Mozilla Firefox y Mozilla Thunderbird.

- Debe tener la capacidad de instalar parches del sistema operativo y aplicaciones de Microsoft en endpoints aislados (air-gapped).
- Debe tener la capacidad de generar reportes de parches faltantes por cliente.
- Debe tener la capacidad de generar reportes de parches faltantes por cada actualización específica.
- Debe tener la capacidad de generar reportes de estado como número de parches escaneados, parches descargados, parches instalados y número de instalaciones fallidas por cada endpoint.
- Debe proporcionar una vista resumida de las actualizaciones críticas, moderadas e importantes que faltan en los endpoints.
- Debe tener la capacidad de programar el escaneo e instalación de parches faltantes.

Monitoreo de Actividad de Archivos:

- Debe tener la capacidad de monitorear actividades relacionadas con el manejo de archivos como copiar, eliminar o mover archivos en unidades locales y dispositivos removibles.
- Debe tener la capacidad de monitorear ciertos tipos de archivos.
- Debe tener la capacidad de excluir ciertos archivos, carpetas o rutas de los procedimientos de monitoreo.

Administración de Activos:

- Debe tener la capacidad de recopilar información del sistema y del hardware relacionada con los endpoints remotos.
- Debe tener la capacidad de obtener un reporte resumen de los diversos softwares/actualizaciones instaladas en los endpoints.
- Debe tener la capacidad de rastrear los cambios de software que ocurren en los endpoints, es decir, aplicaciones instaladas/desinstaladas.
- Debe tener la capacidad de rastrear cambios de hardware en los endpoints. Ej.: cambio de RAM, cambio de procesador, etc.
- Debe tener la capacidad de mostrar la clave de licencia completa del sistema operativo Windows.
- Debe tener la capacidad de mostrar la clave de licencia de MS Office (últimos 4 dígitos).
- Debe proporcionar reportes completos de administración de activos con base en los siguientes parámetros: sistema operativo, nombre de la aplicación, fabricante del sistema, RAM física instalada, procesador y hora del último apagado.
- La solución debe tener la capacidad de rastrear cambios de hardware en el sistema con notificación automática al administrador.

- La solución debe tener la capacidad de rastrear cambios de software en el sistema.

IDS/IPS – Prevención de Intrusos:

- Debe tener la capacidad de detectar y prevenir intentos de intrusión tanto a nivel de red como de host en las redes domésticas.
- Debe tener la capacidad de generar reportes sobre posibles violaciones de seguridad, incumplimientos de políticas y flujo de tráfico sospechoso.
- Debe tener la capacidad de prevenir ataques de escaneo de puertos.
- Debe tener la capacidad de prevenir ataques DDoS.

Seguridad y Filtrado Web:

- Debe tener la capacidad de bloquear el acceso de los usuarios a sitios web maliciosos y de phishing desde los endpoints configurados.
- Debe tener la capacidad de bloquear el acceso de los usuarios a sitios web según sus categorías, por ejemplo: redes sociales, noticias, etc.
- Debe tener la capacidad de bloquear dominios completos o sitios web/URLs específicos.
- Debe tener la opción de excluir ciertos sitios web o dominios completos.
- Debe tener la capacidad de bloquear sitios https.
- Debe soportar funciones de banca segura para realizar transacciones bancarias.
- Debe soportar navegación en entorno aislado (sandbox) para una navegación segura y protegida.
- Debe tener la capacidad de programar el horario de acceso a Internet.
- Debe tener la capacidad de excluir ciertas URLs internas del horario de restricción de acceso a Internet.
- Debe tener la capacidad de controlar el comportamiento predeterminado ante sitios web/URLs desconocidos o aún no categorizados.
- Debe tener la capacidad de controlar el acceso a cuentas de Google personales o corporativas.
- Debe tener la capacidad de controlar el acceso a videos de YouTube con base en su categoría, editor, etc.

Control de Aplicaciones:

- Debe poder bloquear aplicaciones según categorías de aplicaciones. Ej.: gestores de descargas, aplicaciones para compartir archivos, juegos, etc.
- Debe tener la capacidad de agregar aplicaciones personalizadas a la lista de aplicaciones bloqueadas.
- Debe tener la capacidad de recopilar la lista de todas las aplicaciones instaladas en la red.

- Debe contar con la opción de bloquear aplicaciones según su nombre.
- Debe tener la capacidad de definir una lista de aplicaciones permitidas desde una imagen dorada (Golden Image) desplegada en los endpoints.
- Debe tener la capacidad de crear una lista blanca (Safelist) de aplicaciones permitidas en los endpoints.
- Debe tener la capacidad de agregar y administrar listas blancas de aplicaciones (Safelists).

Firewall:

- Debe ofrecer la flexibilidad de crear reglas de firewall para filtrar conexiones por dirección IP, número de puerto o protocolo, y luego aplicar dichas reglas a diferentes grupos de usuarios.
- Debe tener la capacidad de examinar y controlar todo el tráfico entrante y saliente según configuraciones definidas para puertos, origen o dirección de destino.
- Debe tener la capacidad de monitorear redes Wi-Fi y enviar alertas cuando un cliente se conecte a una red Wi-Fi no segura.
- Opción para permitir o no permitir aplicaciones.

Protección para correos:

- Debe tener la capacidad de bloquear correos infectados y correos no deseados (spam).
- Debe tener la capacidad de permitir solo a clientes de correo electrónico confiables enviar correos.
- Debe tener la capacidad de escanear correos entrantes cifrados mediante el protocolo SSL/TLS.
- Debe tener la capacidad de bloquear archivos adjuntos en correos entrantes que tengan múltiples extensiones (ej. -doc.exe).
- Debe tener la capacidad de bloquear correos que intenten explotar vulnerabilidades del cliente de correo.
- Debe tener la capacidad de bloquear todos o los archivos adjuntos especificados por el usuario en correos entrantes.
- Debe tener la opción de configurar clientes de correo confiables en el servidor.

Grupos y Políticas

- Debe tener la capacidad de crear múltiples grupos de usuarios según la estructura organizacional.
- Debe tener la capacidad de asignar diferentes configuraciones de políticas a cada grupo.
- Debe tener la capacidad para que los endpoints se sincronicen con el

servidor.
- Debe tener la capacidad de importar la estructura de grupos desde Active Directory.

Despliegue e instalación

- Debe tener la capacidad de desplegar el software cliente utilizando los siguientes mecanismos:
- Empaquetador del cliente (formato de paquete ejecutable y Microsoft Installer (MSI))
- Página web de instalación
- Instalación remota en un solo endpoint o en todo un rango de direcciones IP
- A través de Active Directory y mediante la creación de un objeto de política de grupo.
- La desinstalación del cliente solo debe ser realizada por el administrador.
- Debe tener la capacidad de crear un empaquetador de cliente protegido con contraseña.
- Debe contar con la opción de enviar una notificación por correo electrónico cuando se instale o desinstale un nuevo cliente de seguridad de endpoint.

Despliegue del servidor

- Debe contar con la capacidad de desplegar el Servidor de Seguridad de Endpoint en servidores en la nube basados en plataformas como Microsoft Azure y AWS.
- Debe soportar la instalación del Servidor de Seguridad de Endpoint con direcciones IP dinámicas (DHCP).
- Debe contar con la capacidad de desplegar el Servidor de Seguridad de Endpoint utilizando IP pública o FQDN.
- Debe contar con la capacidad de soportar un despliegue multinivel maestro-esclavo.
- Debe tener la capacidad de desplegar el Servidor de Seguridad de Endpoint en Microsoft Windows (OVA) y sistemas operativos Linux Ubuntu.

Características de Administración

- Debe proporcionar una consola de administración segura basada en GUI o en la web que permita a los administradores acceder a todos los clientes y servidores de la red para su administración.
- Debe tener la flexibilidad de revertir actualizaciones si es necesario, a través de la consola de administración.
- Debe contar con capacidad de administración basada en roles.
- Debe soportar módulos complementarios (plug-ins) diseñados para añadir nuevas funciones de seguridad sin necesidad de volver a implementar toda

la solución, reduciendo así el esfuerzo y tiempo requeridos para desplegar nuevas capacidades de seguridad a los clientes y servidores en la red.
- Debe contar con protección contra manipulación o autodefensa (Self/Tamper Protection) para los archivos y carpetas del software de seguridad de endpoint.
- El Administrador de Grupo debe poder gestionar ciertos grupos y las políticas asociadas a dicho grupo.
- Debe soportar autenticación multifactor para administradores.

Notificaciones, Reportes y Registros

- Debe tener la capacidad de generar reportes tanto gráficos como tabulares.
- Debe tener la capacidad de eliminar automáticamente los reportes antiguos después de un tiempo preconfigurado.
- Debe tener la capacidad de registrar todas las actividades del servidor de administración.
- Debe tener la capacidad de exportar reportes en múltiples formatos como PDF y CSV.
- Debe tener la capacidad de programar la generación y distribución de reportes por correo electrónico.
- Debe tener la capacidad de generar un reporte de integridad del host que muestre los endpoints conformes y no conformes.
- Debe proporcionar notificaciones por correo electrónico para diversos eventos críticos como brotes de virus, incidentes de ransomware, vencimiento de licencias, etc.
- Debe tener la capacidad de integrarse con un Gestor de Eventos e Información de Seguridad (SIEM).

Administración de Clientes Móviles (Laptos o Escritorio fuera de la red Corporativa):

- Debe tener la capacidad de configurar políticas para clientes itinerantes, incluso si están fuera de la red.
- Debe tener la capacidad de obtener el estado y reportes de clientes itinerantes, incluso si están fuera de la red.
- Debe tener la capacidad de instalar/desinstalar clientes de seguridad de endpoint en dispositivos que se encuentren fuera de la red corporativa.

Administración de Actualizaciones:

- Debe tener la capacidad de crear múltiples servidores de actualización para distribuir la carga de actualizaciones en un entorno de red grande y así reducir el ancho de banda consumido durante las actualizaciones de definiciones.
- Debe tener la capacidad de programar la frecuencia con la que se descargan las actualizaciones.

- Debe tener la capacidad de asignar un ancho de banda específico por el usuario al Gestor de Actualizaciones a partir del ancho de banda total disponible.

Características Adicionales:

- Debe tener la capacidad de evitar que un usuario acceda al sistema operativo en modo seguro.
- Debe tener la capacidad de mejorar el rendimiento de los endpoints limpiando archivos basura y eliminando entradas inválidas del registro o disco.
- Debe tener la capacidad de gestionar a la fuerza laboral itinerante cuando se encuentre fuera de la red corporativa.
- La solución debe ofrecer una función de cifrado mediante la gestión centralizada de políticas, claves y opciones de recuperación de BitLocker.

Características Técnicas Adicionales:

- l OEM debe estar certificado con SOC 2 Tipo 2, ISO 20000-1:2018, ISO 27001:2013 e ISO 9001:2015.
- Capacitación técnica directamente por parte del OEM.
- Soporte estándar de implementación directamente por parte del OEM.
- La solución debe contar con su propio motor de escaneo antivirus desarrollado de forma nativa.
- La solución debe contar con certificación AV-Test y certificación OPSWAT para seguridad en endpoints.
- El OEM debe tener más de 25 años de experiencia en detección de antivirus.
- La solución debe contar con más de 8 patentes registradas para protección contra malware y ransomware.

1.1.2 Fases

Se describen a continuación las fases requeridas para la implementación del Servicio de Arrendamiento de Licencia de Uso de Software Antivirus.

Fase de Inicio

El proveedor deberá elaborar la planeación, instalación y puesta en operación del software propuesto como Antivirus en 2400 equipos de cómputo definidos por el Instituto en coordinación con el administrador de contrato.

El proveedor deberá considerar la celebración de una reunión de inicio del contrato, dentro de los 5 primeros días hábiles después del inicio de la vigencia del servicio, en la cual se acordará la elaboración del plan de trabajo y se dará seguimiento a los entregables de la fase de Inicio del Proyecto.

Instalación, configuración y puesta en operación de la Consola de Administración

El proveedor deberá considerar la entrega de un Checklist que compruebe las características solicitadas de la consola de administración del antivirus.

El proveedor deberá considerar, dentro de las actividades en esta fase del contrato, la instalación configuración y puesta en operación de la Consola de Administración del antivirus propuesto.

El proveedor deberá configurar las políticas de seguridad, que, de acuerdo a su análisis y experiencia, sean las más adecuadas para el Instituto y en armonía con la herramienta propuesta, todo esto en la consola de administración del antivirus.

El proveedor deberá asegurarse que las políticas de protección de la herramienta antivirus no impacten en funcionamiento de los equipos de cómputo.

Instalación, configuración y puesta en operación del Antivirus

El proveedor deberá considerar la entrega de un Checklist que compruebe las características solicitadas del antivirus.

El proveedor deberá considerar, dentro de las actividades en esta fase del contrato, la instalación configuración y puesta en operación, en 2400 equipos de cómputo, del antivirus propuesto.

El proveedor deberá generar un reporte de instalación del antivirus que deberá contener al menos los siguientes datos:

- Nombre de usuario
- Departamento
- Edificio/Nivel
- Marca
- Modelo
- No. de inventario o número de serie del equipo.
- Dirección IP
- Firma del usuario

Implementación de la Mesa de Ayuda

El Proveedor deberá poner a disposición del Instituto una Mesa de ayuda dentro de los 10 días hábiles posteriores a la fecha de inicio de vigencia del contrato, para que los administradores o usuarios puedan solicitar asistencia técnica para la resolución de fallas y

orientación de uso del software, para lo cual el Proveedor del servicio deberá proporcionar números convencionales y/o celulares, además de correos electrónicos.

La Mesa de Ayuda deberá considerar la implementación registro y seguimiento de tickets para el soporte técnico vía remota o en sitio en caso de ser necesario incluyendo asesoría y soluciones a conflictos técnicos, las 24 horas, los 7 días de la semana, durante la vigencia del servicio de arrendamiento de licencia de uso de Software Antivirus.

Los medios para el registro de tickets de atenciones y de reportes de incidencias deberán ser vía telefónica o por correo electrónico y el proveedor deberá, en este sentido, proporcionar los nombres de los contactos en orden jerárquico con número de teléfono móvil y correo electrónico.

Niveles de Servicio

El proveedor deberá considerar la entrega, de un documento que contenga el procedimiento de escalamiento de reportes de incidentes, al Administrador del servicio de arrendamiento de licencia de uso de Software Antivirus, considerando la siguiente tabla de niveles de servicio:

Cuadro 1. Niveles de atención

NIVELES DE ATENCIÓN	AREA RESPONSABLE	TIEMPO DE ATENCIÓN	DESCRIPCIÓN
Nivel 1	Ingeniero de Soporte del Proveedor	1hora – 4 horas	El incidente deberá ser resuelto por el Ingeniero de Soporte del Proveedor en conjunto con el Administrador del Servicio durante la primera llamada realizada a la mesa de ayuda sin interrumpirla, además de complementar la atención con el uso de correo electrónico.
Nivel 2	Ingeniero de Soporte del Proveedor	2 horas – 5 horas	El incidente involucra un análisis más detallado en sitio junto con el Administrador del Servicio, deberá considerar las pruebas necesarias a fin de buscar la solución del incidente.
Nivel 3	Fabricante	3 horas – 6 horas	El incidente es escalado con el Fabricante de la Solución por el proveedor del servicio y se informa de su avance al Administrador del Contrato.

De igual forma, el proveedor deberá entregar una carta garantía de cumplimiento de los niveles de servicio especificados en este anexo.

INSTITUTO NACIONAL DE CIENCIAS MÉDICAS Y NUTRICIÓN SALVADOR ZUBIRÁN

FORMATO DE JUSTIFICACIÓN PARA ADQUISICIONES SIN PROCEDIMIENTO DE LICITACIÓN PÚBLICA ARTÍCULO 55 LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO

Fecha de elaboración: junio 2026

Documento de Confidencialidad

El proveedor se obliga a no divulgar la información proporcionada, así como los datos e información obtenidos durante las fases de instalación, operación y soporte y cierre, a través de publicaciones, documentos, medios electrónicos o de cualquier otro medio sin la autorización expresa y por escrito del INCMNSZ, ya que dichos datos e información son propiedad exclusiva de este último. El INCMNSZ, podrá ejercer las acciones penales que se deriven de la violación a este punto en cualquier tiempo, sin perjuicio de las acciones civiles administrativas o de cualquier otra naturaleza a que haya lugar. Para tal efecto, el proveedor deberá considerar la elaboración y la entrega de un documento de confidencialidad que debe ser firmado por su representante legal.

Documentación Adicional

El proveedor deberá considerar la entrega de la siguiente documentación adicional dentro de la fase de Inicio del contrato:

- Listado del personal autorizado y copia simple de certificados emitido por el fabricante de la solución.
- Documento del certificado de vigencia de la licencia de uso.

Fase de Operación y Soporte

El proveedor deberá considerar que en esta fase se deben realizar de manera mandatoria las siguientes actividades:

- Una visita mensual durante la vigencia del contrato, la cual podrá ser coordinada por el proveedor y el administrador del servicio dentro de los últimos 5 días hábiles de cada mes a fin de realizar las siguientes actividades:
  - Verificar el estado de base de firmas de virus en el servidor.
  - Generar un reporte de equipos con amenazas activas.
  - Generar un reporte de equipos clientes actualizados y no actualizados.
  - Realizar las adecuaciones solicitadas por el Administrador del servicio de arrendamiento de licencia de uso de Software Antivirus.
  - Elaborar un reporte de actividades por cada visita programada el cual será entregado al Administrador del servicio de arrendamiento de licencia de uso de Software Antivirus.
  - Realizar y entregar un respaldo de la consola de administración y de las políticas de protección del antivirus.

- El proveedor deberá asegurar que se apliquen todas las actualizaciones de la solución propuesta, así como su respectiva instalación, configuración y

puesta a punto durante la vigencia del contrato; para el caso en el que sea liberada una versión estable del producto antivirus al mercado, el proveedor deberá obligarse a realizar la actualización en el transcurso del mes siguiente a la mencionada liberación.

- Entrega de un reporte de tickets registrados en la Mesa de Ayuda de manera mensual.
- Entrega de un listado de los equipos institucionales licenciados durante el período.

Transferencia de conocimiento

El proveedor deberá incluir dentro de la Fase de Operación y Soporte un evento de transferencia de conocimiento al personal del Departamento de Redes e Infraestructura, misma que debe considerar al menos los siguientes temas:

- Antecedes de la Seguridad de la Información.
- Tipos de amenazas para la información.
- Mejores prácticas internacionales en materia de seguridad de la información.
- Instalación y configuración de consola remota de administración de antivirus.
- Instalación y configuración del software de antivirus en equipos cliente.
- Solución a problemas comunes.

El proveedor deberá considerar la entrega de una lista de asistencia y constancia de la transferencia de conocimientos del personal del Departamento de Redes e Infraestructura.

Fase de Cierre

Esta fase deberá iniciar 30 días hábiles antes de la terminación de la vigencia del contrato de Servicio de Arrendamiento de Licencia de Uso de Software Antivirus, considerando las siguientes actividades:

- El proveedor deberá asegurarse que la versión de Licencia de uso de Software Antivirus instalada en todos los equipos TIC del Instituto sea la última estable lanzada al mercado.
- Deberá asegurarse que durante este período se entregue actualizado el respaldo de la consola de administración y de las políticas de protección del antivirus.
- Deberá integrar un informe final con el estado de la base de firmas de virus en el servidor.
- Deberá integrar un reporte final que considere los equipos con amenazas activas, equipos clientes actualizado y no actualizados.

Entregables

El proveedor deberá considerar la entrega del siguiente grupo de entregables:

INSTITUTO NACIONAL DE CIENCIAS MÉDICAS Y NUTRICIÓN SALVADOR ZUBIRÁN

FORMATO DE JUSTIFICACIÓN PARA ADQUISICIONES SIN PROCEDIMIENTO DE LICITACIÓN PÚBLICA ARTÍCULO 55 LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO

Fecha de elaboración: junio 2026

Cuadro 2. Entregables

Entregable	Tiempo de Entrega
Minuta y Plan de Trabajo.	La reunión de inicio deberá celebrarse dentro de los primeros 10 días hábiles después del inicio de la vigencia del contrato, la minuta y el Plan de Trabajo deberán entregarse 3 días hábiles después de celebrar la reunión.
CheckList de las capacidades de la Consola de Administración.	Durante la reunión de Inicio de Contrato.
Reporte de Instalación de la Consola de Administración.	Dentro de los primeros 10 días hábiles después del inicio de la vigencia del contrato, la memoria técnica de la Instalación deberá entregarse un día hábil posterior a la puesta en operación de la consola de administración.
Reporte de Instalación de la Consola de Administración apartado de Políticas de Seguridad.	Dentro de los primeros 10 días hábiles después del inicio de la vigencia del contrato, la memoria técnica de la Instalación deberá entregarse un día hábil posterior a la puesta en operación de la consola de administración.
Reporte de Instalación del Antivirus.	La instalación, configuración y puesta en operación del Antivirus deberá iniciar 15 días hábiles después del inicio de la vigencia del contrato, el reporte de Instalación del Antivirus deberá entregarse 5 días hábiles después de la terminación de la Instalación del Antivirus.
CheckList de las capacidades de del antivirus.	Durante la reunión de Inicio de Contrato.
Manual de la Mesa de Ayuda.	La implementación de la mesa de ayuda deberá realizarse dentro de los 10 días hábiles después del inicio de la vigencia del contrato, el manual de la mesa de ayuda deberá entregarse durante este mismo período.
Documento de Escalamiento.	Durante la implementación de la mesa de ayuda.
Documento de Garantía de Niveles de Servicio.	Durante la implementación de la mesa de ayuda.
Documento de Confidencialidad.	Durante la reunión de Inicio de Contrato.
Listado del personal autorizado y copia simple de certificados emitido por el fabricante de la solución. Copia simple del certificado ISO 9001 del proveedor seleccionado. Documento del certificado de vigencia de las licencias de uso.	Durante la reunión de Inicio de Contrato.
Reportes Mensuales	Dentro de los primeros 5 días hábiles posteriores al término del mes.
Lista de asistencia y constancia de la transferencia de conocimientos del personal del Departamento de Redes e Infraestructura.	Dentro de los primeros 45 días hábiles después del inicio de la vigencia del contrato.
Reportes de Cierre de Contrato	Dentro de los 30 días hábiles anteriores a la terminación de la vigencia del contrato.

INSTITUTO NACIONAL DE CIENCIAS MÉDICAS Y NUTRICIÓN SALVADOR ZUBIRÁN

FORMATO DE JUSTIFICACIÓN PARA ADQUISICIONES SIN PROCEDIMIENTO DE LICITACIÓN PÚBLICA ARTÍCULO 55 LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO

Fecha de elaboración: junio 2026

2. Plazos y condiciones.

II.

a) La vigencia del 01 de julio de 2026 al 29 de febrero de 2028.

De acuerdo con la experiencia técnica acumulada y la opinión especializada del área responsable, la contratación plurianual con vigencia del 16 de junio de 2026 al 31 de enero de 2028 resulta la alternativa más conveniente para garantizar la continuidad operativa, evitar interrupciones derivadas de procesos de contratación intermedios y optimizar el uso de recursos presupuestales.

En este sentido, con la documentación soporte correspondiente, se acredita el cumplimiento de lo dispuesto en los artículos 35 y 50 de la Ley Federal de Presupuesto y Responsabilidad Hacendaria (LFPRH).

b) El pago se realizará en una sola exhibición al finalizar las actividades de la fase de inicio y de manera posterior al Vo.Bo. de los entregables de la fase de inicio. Esto se hará conforme al Artículo 73 de la LAASSP publicada el 16 de abril de 2025 en DOF, el pago se hará dentro de los 17 días hábiles posteriores a la recepción satisfactoria de la factura previa entrega de los bienes o prestación del servicio y con Vo. Bo. de los entregables, conforme a los procedimientos establecidos por la Subdirección de Recursos Financieros del Instituto, y el Artículo 139 de su Reglamento publicado el 18 de diciembre de 2025, los cuales procederán cuando los avances correspondan a entregables que hayan sido debidamente devengados en términos de las disposiciones presupuestarias aplicables.

c) Para la aceptación de las licencias de uso y el trámite de pago correspondiente, el proveedor tendrá que entregar al Administrador de la Licencias de uso, la información requerida en los puntos anteriores, con excepción de los reportes mensuales.

d) El servicio de arrendamiento de licencia de uso de software Antivirus deberá contemplar la instalación en 2400 equipos de cómputo en el Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán, en Av. Vasco de Quiroga No. 15, Colonia Belisario Domínguez Sección XVI, CP 14080, Alcaldía Tlalpan de la Ciudad de México.

Administrador de las licencias de uso.

El Servidor Público responsable de administrar y verificar el cumplimiento del servicio de arrendamiento de licencias de uso de software Antivirus, será el jefe de Departamento de Redes e Infraestructura del INCMNSZ, a partir de la fecha y en el lugar que a continuación se describe.

INSTITUTO NACIONAL DE CIENCIAS MÉDICAS Y NUTRICIÓN SALVADOR ZUBIRÁN

FORMATO DE JUSTIFICACIÓN PARA ADQUISICIONES SIN PROCEDIMIENTO DE LICITACIÓN PÚBLICA ARTÍCULO 55 LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO

Fecha de elaboración: junio 2026

3. Resultado de la investigación de Mercado.

Para resolver la problemática identificada y las necesidades del INCMNSZ, se plantea contratar el Servicio de Arrendamiento de Licencias de uso de Software Antivirus, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información, en este sentido, se llevó a cabo un estudio de mercado, así como la investigación de contratos vigentes en el portal ComprasMX, que fueran el resultado de una Licitación Pública y que conforme a la normatividad vigente el INCMNSZ se pudiera adherir, lo anterior, con el objeto de optimizar tiempos en el proceso de contratación, sin embargo, no se encontró un servicio que satisfaga los requerimientos del Instituto.

Después de analizar la información resultante de la investigación de mercado, se desprende que la mejor opción es llevar a cabo un proceso de Invitación a cuando menos tres personas, toda vez que los precios resultantes, así como la investigación de las empresas consultadas reúnen las características "precio, calidad y experiencia".

En este contexto, una vez obtenido la validación de la Oficina de Representación del Órgano Interno de Control en el Instituto, así como, de la Agencia de Transformación Digital y Telecomunicaciones desde el ámbito técnico, se solicitará a la Subdirección de Recursos Materiales y Servicios Generales, lleve a cabo el proceso de Invitación a Cuando menos tres Personas para su posterior contratación de acuerdo al Artículo 55 primer párrafo de la LAASSP publicada en el DOF el 16 de abril de 2025, esto con el fin de obtener las mejores condiciones para el INCMNSZ.

Así mismo de conformidad con lo establecido en el Artículo 29 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público se determinó y verifico que se cumple con lo establecido.

Se determinó la existencia de oferta de bienes y servicios en la cantidad, calidad y oportunidad requeridas por las mismas, sin embargo, el darle el seguimiento con un proveedor que conoce a detalle los requerimientos del Instituto garantizara obtener mejores resultados, aunado a la conveniencia económica. Por otro lado, se comprobó que el precio del servicio requerido, al momento de llevar a cabo la investigación tiene un costo aceptable.

La investigación de mercado se utilizó por el Instituto para lo siguiente:

- Acreditar la aceptabilidad del precio conforme al cual se realizará la contratación correspondiente.
- Determinar si existen bienes o servicios alternativos o sustitutos técnicamente razonables;
- Elegir el procedimiento de contratación que podrá llevarse a cabo;

INSTITUTO NACIONAL DE CIENCIAS MÉDICAS Y NUTRICIÓN SALVADOR ZUBIRÁN

FORMATO DE JUSTIFICACIÓN PARA ADQUISICIONES SIN PROCEDIMIENTO DE LICITACIÓN PÚBLICA ARTÍCULO 55 LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO

Fecha de elaboración: junio 2026

Cuadro 3. Resultado de la Investigación de Mercado.

N°	Nombre del proveedor	Nombre de identificación del bien, arrendamiento o servicio. "Servicio de Arrendamiento de Licencia de Uso de Software Antivirus"	Proporciona las condiciones técnicas solicitadas de calidad, cantidad y oportunidad	Vigencia del servicio. 01 de julio de 2026 al 29 de febrero 2028	Requisito de participación	Precio mas IVA
CONSULTA COMPRANET						
1	No se encontró antivirus similar y las condiciones de contrato publicadas, no es posible adherirse conforme a la LAASSP	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA
COTIZACIONES, SOLICITUD POR OFICIO FOCON 04						
1	**MIGUEL EMILIANO BOSQUES ALARCON (20 meses)**	SI	SI	SI	SI	$1,319,280.00
2	**TECNOLOGIA AGIL CODELINK, S.A.S. DE C.V. (20 meses)**	SI	SI	SI	SI	$1,818,960.00
3	**FUSION INTELIGENTE, S.A. DE C.V. (20 meses)**	SI	SI	SI	SI	$1,490,784.00
PRECIO HISTÓRICO						
1	**MIGUEL EMILIANO BOSQUES ALARCON (7.5 meses) INCMNSZ/0706/2/AD/079/25**	SI	SI	SI	SI	$715,000.00

Cuadro 4. Costo mensual por licencia del proveedor mas bajo.

Descripción	Proveedor	Tipo de Antivirus	Vigencia	No de licencias	Costo unitario	Costo mensual	Costo total mas IVA
Servicio de Arrendamineto de Licencia de uso de Software Antivirus	Miguel Emiliano Bosques Alarcón	Seqrite EPP 8.4	20 meses	2400	$ 549.70	$ 27.49	$ 1,319,280

Como resultado de la investigación realizada se identifico que el proveedor Miguel Emiliano Bosques Alarcón presenta una oferta de **$1,530,364.80 con I.V.A. incluido** (Un millón quinientos treinta mil trecientos sesenta y cuatro pesos 80/100 MXN con IVA siendo esta la opción más conveniente para el Instituto. Seguido de la investigación se llevará a cabo un proceso de invitación a cuando menos tres personas a través del portal de ComprasMX, con el fin de atender lo dispuesto en la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y obtener las mejores condiciones técnicas y económicas para el Instituto.

INSTITUTO NACIONAL DE CIENCIAS MÉDICAS Y NUTRICIÓN SALVADOR ZUBIRÁN

FORMATO DE JUSTIFICACIÓN PARA ADQUISICIONES SIN PROCEDIMIENTO DE LICITACIÓN PÚBLICA ARTÍCULO 55 LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO

Fecha de elaboración: junio 2026

Cuadro 5. Precio histórico mensual.

INCMNSZ/0706/2/AD/079/25							
Descripción	Proveedor	Tipo de Antivirus	Vigencia	No de licencias	Costo unitario	Costo mensual	Costo total mas IVA
Servicio de Arrendamineto de Licencia de uso de Software Antivirus	Miguel Emiliano Bosques Alarcón	Seqrite Endpoint 7.6	7.5 meses	2200	$ 325	$ 43.33	$ 715,000

Cuadro 6. Análisis de monto histórico.

Ejercicio	Costo mensual
2025-2026 contrato. INCMNSZ/0706/2/AD/079/25	**$ 43.33**
2026-2028 (Propuesta de contratación)	**$ 27.49**

Una vez realizado el análisis se observa que no existe un incremento del costo, ya que el costo mensual del servicio presenta una reducción significativa respecto de contratación anterior.

Comparado contra el contrato 2025-2026:

Costo mensual histórico 2025-2026: $ 43.33
Costo mensual 2026-2028: $ 27.49

Representa una disminución aproximada del 36.60 %.

De acuerdo al análisis de los cuadros anteriores podemos definir que, debido al incremento de número de licencias, así como de vigencia del contrato, resulta mayor los beneficios económicos para la contratación y aprovechamiento de vigencia de software.

Por otro lado, derivado del análisis comparativo de la contratación realizada en ejercicios anteriores para servicio equivalente de Servicio de Arrendamineto de Licencia de uso de Software Antivirus, se identificó que la propuesta económica presentada para el periodo comprendido del 01 de julio de 2026 al 29 de febrero de 2028 mantiene condiciones favorables para el Instituto.

Mientras que la contratación formalizada para el periodo 2025-2026 consideró un importe de $ 715,000.00 antes de IVA por una vigencia de 7.5 meses, la contratación propuesta para el periodo 2026-2028 contempla un importe de $1,319,280.00 antes de IVA para una vigencia de 20 meses, observándose una reducción significativa en el costo mensual promedio del servicio.

Asimismo, el análisis efectuado demuestra que el importe ofertado resulta congruente con las condiciones del mercado identificadas mediante la investigación de mercado realizada, localizando proveedores alternativos con capacidad técnica para proporcionar el servicio

objeto de la contratación bajo las condiciones operativas y tecnológicas demandadas por el Instituto.

En consecuencia, se concluye que la propuesta económica presentada resulta razonable, conveniente y financieramente viable para la Institución, al permitir la continuidad operativa bajo condiciones económicas más favorables que las observadas en ejercicios anteriores.

La contratación propuesta resulta económicamente conveniente para el Instituto, toda vez que el costo de los servicios especializados es significativamente menor que el impacto operativo, administrativo y financiero que podría derivarse de no contar con la misma.

Tipo de Antivirus.

Seqrite Endpoint Protection (EPP) 8.4 salió al mercado el 19 de septiembre de 2025, es la actualización del Seqrite Endpoint Security 7.6 (versión contratada en el ejercicio 2025-2026). Seqrite Endpoint Protection (EPP) 8.4 ofrece ventajas significativas, especialmente en detección de amenazas impulsada por IA, automatización de migración y administración centralizada. El nuevo licenciamiento moderniza la seguridad en el INCMNSZ para bloquear ataques modernos y simplifica el trabajo del grupo de ciberceguridad en la STIC. La principales ventajas que ofrece son:

Seguridad Avanzada y Detección.

Inteligencia Artificial y Aprendizaje Automático: utiliza IA para predecir y bloquear *malware* avanzado antes de que infecte los equipos.
Protección contra *Ransomware*: El nuevo sistema analiza el comportamiento del programa. Si un programa actúa como *ransomware*, lo bloquea y respalda la información automáticamente.
File Sandboxing (Aislamiento de archivos): Analiza archivos sospechosos en una zona segura antes de permitir que se ejecuten en la red del INCMNSZ.

Control de Datos y Dispositivos (DLP)

Control a Nivel de Canal: Como administradores podemos decidir qué información sale y por dónde. Por ejemplo, bloqueo el uso de memorias USB, pero permitir el envío de correos, o aplicar marcas de agua digitales a documentos confidenciales para evitar fugas de información.
Parcheo Virtual (*Virtual Patching*): Otorga una capa de defensa temporal cuando los programas de tu empresa tienen errores o vulnerabilidades conocidas, hasta que el fabricante lanza la actualización oficial.

INSTITUTO NACIONAL DE CIENCIAS MÉDICAS Y NUTRICIÓN SALVADOR ZUBIRÁN

FORMATO DE JUSTIFICACIÓN PARA ADQUISICIONES SIN PROCEDIMIENTO DE LICITACIÓN PÚBLICA ARTÍCULO 55 LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO

Fecha de elaboración: junio 2026

Administración y Licenciamiento

Migración Automática: El licenciamiento 8.4 cuenta con una herramienta nativa para transferir todos los equipos, grupos de trabajo y políticas de seguridad de la versión 7.6 a la 8.4 sin perder el control.
Consola Unificada: En lugar de tener varias consolas, la versión 8.4 permite gestionar todo desde un solo tablero centralizado en cualquier ubicación.
Búsqueda en Tiempo Real (*Live Query*): Permite a los administradores consultar el estado de cualquier equipo de la red al instante para saber qué está pasando.

4. Procedimiento de contratación propuesto.

Invitación a Cuando Menos Tres Personas, con fundamento en los Artículos 134 de la Constitución Política de los Estados Unidos Mexicanos; Artículos 33 primer párrafo, 35 fracción II, 55 primer párrafo de Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Considerando que las empresas MIGUEL EMILIANO BOSQUES ALARCON, TECNOLOGIA AGIL CODELINK, S.A.S. DE C.V. y FUSION INTELIGENTE, S.A. DE C.V. cumplieron con los requerimientos técnicos y económicos, además de que cuentan con la capacidad de respuesta inmediata, recursos financieros, y que, conforme a la opinión y juicio de experto de esta área, sus actividades empresariales están relacionadas con la contratación del Servicio de arrendamiento de licencias de uso de software Antivirus, se propone se realice un procedimiento de Invitación a Cuando Menos Tres Personas, a fin de obtener las mejores condiciones técnicas y económicas, así como, atender lo establecido en el PEF 2025.

5. Monto Estimado de la Contratación.

Arrendamiento de licencia de uso de software Antivirus	Subtutotal	IVA	TOTAL
	$1,319,280.00	$211,084.80	$1,530,364.80

Forma de pago propuesta.
El pago se realizará en una sola exhibición al finalizar las actividades de la fase de inicio y de manera posterior al Vo. Bo. de los entregables. Esto se hará conforme al Artículo 73 de la LAASSP publicada el 16 de abril de 2025 en DOF, el pago se hará dentro de los 20 días naturales posteriores a la recepción satisfactoria de la factura previa entrega de los bienes o prestación del servicio y con Vo. Bo. de los entregables, conforme a los procedimientos establecidos por la Subdirección de Recursos Financieros y las POBALINES del Instituto, y el Artículo 139 de su Reglamento publicado el 18 de diciembre de 2025 en Diario Oficial de la Federación, los cuales procederán cuando los avances correspondan a entregables que hayan sido debidamente devengados en términos de las disposiciones presupuestarias aplicables.

INSTITUTO NACIONAL DE CIENCIAS MÉDICAS Y NUTRICIÓN SALVADOR ZUBIRÁN

FORMATO DE JUSTIFICACIÓN PARA ADQUISICIONES SIN PROCEDIMIENTO DE LICITACIÓN PÚBLICA ARTÍCULO 55 LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO

Fecha de elaboración: junio 2026

Partida Presupuestal

32701 patentes, derechos de autor, regalías y otros

6. Personas Propuestas para el procedimiento de invitación a cuando menos tres personas.

Después de llevar a cabo el estudio de mercado, se proponen

- Miguel Emiliano Bosques Alarcón
- Dirección:Tonalá No. 365 2-B. Colonia Roma Sur. C.P. 06760. CDMX
- Tel. 55 92 22 75 60.
- Correo electrónico. Miguel.emiliano@bosques-cia.com
- BOAM7301114K8

- TECNOLOGIA AGIL CODELINK, S.A. DE C.V.
- Dirección: Calle 32 # 31, Col Estado de México, C.P. 57210. Nezahualcóyotl.
- Tel. 55 24 37 88 97.
- Correo electrónico. info@codelink.com.mx
- TAC240318K74

- FUSION INTELIGENTE, S.A. DE C.V.
- Dirección: Bosques de Chiapas #21, Fracc. Sta. Mónica, Tlanepantla, Edo de Mex. C.P. 54050.
- Tel. 55 53 64 59 45.
- Correo electrónico. fusion@fusioninteligente.com
- FIN0402135M1

7. Acreditamiento de los criterios en que se funda la excepción, así como la justificación de las razones para el ejercicio de la opción.

Con Fundamento en el Artículo 53, párrafo segundo, de la LAASSP, así como lo dispuesto en numeral 4.2.3.1.1 del ACUERDO por el que se expide el Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios el Sector Público (MAAGMAASSP) para los siguientes criterios:

INSTITUTO NACIONAL DE CIENCIAS MÉDICAS Y NUTRICIÓN SALVADOR ZUBIRÁN

FORMATO DE JUSTIFICACIÓN PARA ADQUISICIONES SIN PROCEDIMIENTO DE LICITACIÓN PÚBLICA ARTÍCULO 55 LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO

Fecha de elaboración: junio 2026

ECONOMÍA:

Para acreditar el cumplimiento del criterio de economía, se toma como base el Resultado de la Investigación de Mercado realizada para el "Servicio de Arrendamiento de Licencias de Uso de Software Antivirus", el cual sustenta tanto la eficiencia del procedimiento como la conveniencia económica de la contratación.

En primer lugar, se evidencia un ahorro significativo para el Estado derivado del esquema competitivo de contratación, que permitió obtener las mejores condiciones económicas mediante la comparación entre distintos proveedores.

Los beneficios económicos identificados incluyen:

- Reducción de costos directos: El proveedor más económico, Miguel Emiliano Bosques Alarcón, ofrece el servicio por un total de $1,530,364.80 con I.V.A. incluido (Un millón quinientos treinta mil trecientos sesenta y cuatro pesos 80/100 MXN IVA incluido), lo que representa un ahorro de hasta $579,628.80 (Quinientos setenta y nueve mil seiscientos veintiocho pesos 80/100 MXN) respecto a la oferta más alta TECNOLOGIA AGIL CODELINK, S.A. DE C.V..

- Eficiencia operativa: Todos los proveedores propuestos cuentan con personal técnico capacitado en la administración del software antivirus y su consola de gestión, lo que garantiza una implementación eficiente y reduce tiempos de respuesta en soporte técnico.

- Optimización de recursos tecnológicos: El software a adquirir presenta un consumo mínimo de recursos computacionales, por lo que no se requiere realizar ampliaciones de memoria RAM u otras actualizaciones de hardware, lo que evita costos adicionales.

A continuación, se detallan las cotizaciones recibidas:

PROVEEDOR	MIGUEL EMILIANO BOSQUES ALARCÓN	TECNOLOGIA AGIL CODELINK SA DE CV	FUSION INTELIGENTE SA DE CV
COSTO SIN IVA	$ 1,319,280.00	$ 1,818,960.00	$ 1,490,784.00
COSTO CON IVA	$ 1,530,364.80	$ 2,109,993.60	$ 1,729,309.44

INSTITUTO NACIONAL DE CIENCIAS MÉDICAS Y NUTRICIÓN SALVADOR ZUBIRÁN

FORMATO DE JUSTIFICACIÓN PARA ADQUISICIONES SIN PROCEDIMIENTO DE LICITACIÓN PÚBLICA ARTÍCULO 55 LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO

Fecha de elaboración: junio 2026

En conclusión, con base en los elementos anteriores, se considera que la contratación propuesta cumple con el criterio de economía, al representar la mejor relación costo-beneficio disponible en el mercado. **Incluso una disminución en costo con respecto al contrato anterior inmediato, esto deribado al incremento de numero de licencias y tiempo de contratación de un 36.40 %.**

Asimismo, se justifica con lo siguiente:

Componentes de costo en una licitación nacional:

1. **Costos directos del proceso de licitación:**
   - Publicación de bases.
   - Honorarios de asesores técnicos y jurídicos.
   - Revisión y evaluación de ofertas.
   - Comisiones del comité revisor de bases.
   - Costos administrativos (papelería, notificaciones, logística, etc.)
2. **Costos indirectos:**
   - Tiempo del personal interno involucrado.
   - Eventuales impugnaciones o aclaraciones.
   - Posible retraso en la ejecución del contrato (con su impacto económico).
3. **Costo de oportunidad:**
   - Lo que se deja de ganar o se retrasa por no adjudicar directamente.
   - Impacto en la continuidad de servicios o provisión de bienes.

En consecuencia, y conforme al principio de economía previsto en la normatividad aplicable, se concluye que se encuentra plenamente justificada la modalidad de invitación a cuando menos tres como la alternativa más racional, eficiente y oportuna. Esta decisión permite evitar costos innecesarios, garantiza la continuidad operativa del servicio, y asegura el uso responsable y eficaz de los recursos públicos, la realización de un procedimiento de licitación pública, aun teniendo conocimiento previo derivado de la investigación de mercado de la inexistencia de competencia efectiva, implicaría erogaciones administrativas innecesarias y retrasos operativos injustificados, sin obtener beneficios adicionales para el Estado, contraviniendo los principios de racionalidad, economía y eficiencia del gasto público.

EFICACIA:

Con base en los resultados del estudio de mercado, se determina que el proceso de invitación a cuando menos tres personas resulta eficaz para satisfacer oportunamente las

necesidades del INCMNSZ, ya que permite garantizar la protección oportuna y segura de la información contenida en los equipos de cómputo institucionales.

Este esquema de contratación contribuye directamente a mitigar riesgos operativos y preservar la continuidad de las funciones sustantivas y administrativas del Instituto, al asegurar la implementación inmediata de una solución antivirus confiable y profesional.

Adicionalmente, al tratarse de un proceso competitivo, se favorece la obtención de mejores condiciones en términos de calidad, soporte técnico y precio, lo cual fortalece la eficacia institucional al combinar rapidez en la contratación con resultados técnicos satisfactorios.

En resumen, el procedimiento elegido permite atender de forma eficiente y segura las necesidades del Instituto, garantizando tanto la protección de activos informáticos como el cumplimiento de los objetivos operativos en tiempo y forma.

EFICIENCIA:

El procedimiento propuesto para la contratación del Servicio de Arrendamiento de Licencias de Uso de Software Antivirus, garantiza una asignación óptima de los recursos públicos, al permitir que el Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán (INCMNSZ) cumpla con sus objetivos institucionales en tiempo y forma, sin generar demoras operativas ni costos innecesarios.

Este esquema de contratación permite maximizar la relación entre los recursos aplicados y los resultados obtenidos, al asegurar condiciones favorables en términos de disponibilidad inmediata del servicio, calidad técnica, precio competitivo y soporte oportuno.

Asimismo, se evita la realización de procedimientos más extensos o complejos que podrían implicar mayores cargas administrativas, consumo innecesario de tiempo y posibles retrasos en la implementación del software, lo cual impactaría negativamente en la operación del Instituto.

En este sentido, el procedimiento propuesto cumple con el principio de eficiencia al optimizar los recursos institucionales y reducir al mínimo los tiempos y costos asociados a la contratación, favoreciendo la ejecución eficaz de las funciones sustantivas del INCMNSZ.

HONRADEZ:

El procedimiento propuesto se realiza en estricto apego a la LAASSP y su Reglamento, el MAAGMAASSP, las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones, y en la Seguridad de la Información; evitando que, en el procedimiento de contratación, haya actos de corrupción y que los servidores públicos que intervienen, favorezcan a cualesquiera de los invitados.

INSTITUTO NACIONAL DE CIENCIAS MÉDICAS Y NUTRICIÓN SALVADOR ZUBIRÁN

FORMATO DE JUSTIFICACIÓN PARA ADQUISICIONES SIN PROCEDIMIENTO DE LICITACIÓN PÚBLICA ARTÍCULO 55 LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO

Fecha de elaboración: junio 2026

TRANSPARENCIA:

En aras de fomentar la cultura de la transparencia, la rendición de cuentas y la legalidad, como acciones fundamentales en la Administración Pública, y que toda persona tiene derecho al acceso a la información pública, de acuerdo con lo dispuesto en la ley reglamentaria, la STIC pondrá a disposición del INCMNSZ, y del público en general, a través de la Ley Federal de Transparencia y Acceso a la Información Pública, todos los elementos que constituyen la presente justificación para acreditar la transparencia y legalidad de este procedimiento.

Justificación de las razones para el ejercicio de la opción para la contratación.

Conforme al Artículo 55 primer párrafo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Publico que a la letra dice:

> *"Las dependencias y entidades, bajo su responsabilidad, podrán contratar adquisiciones, arrendamientos y servicios, sin sujetarse al procedimiento de licitación pública, a través de los de invitación a cuando menos tres personas o de adjudicación directa, cuando el importe de cada operación no exceda los montos máximos que al efecto se establecerán en el Presupuesto de Egresos de la Federación, siempre que las operaciones no se fraccionen para quedar comprendidas en los supuestos de excepción a la licitación pública a que se refiere este artículo.*

En este contexto y de acuerdo al estudio de mercado, es viable la contratación propuesta, derivado de que no se exceden los montos de actuación establecidas en el Presupuesto de Egresos de la Federación para el Instituto durante el ejercicio 2026.

Así mismo, desde un ámbito técnico, la presente contratación tiene como finalidad la protección de los equipos de cómputo y servidores con los que cuenta actualmente en el INCMNSZ. Este tipo de servicios tiene como objetivo proporcionar la seguridad interna y externa de estos, ayudará a detectar amenazas potenciales antes de que puedan provocar algún tipo de daño y a mantener dentro de la red el flujo de información sin tener problemas de tráfico, demora en el envío y recepción de datos.

La administración y monitoreo se llevará a cabo a través de una consola, con la cual se determinarán problemas de virus en los equipos de cómputo, así como proteger a los usuarios de robo de información sensible, protección en la convivencia de los servicios de red e internet, protección en los servicios correo electrónico Institucional, exploración en estado inactivo y durante la descarga de archivos. Así mismo como beneficio fundamental se evita poner en riesgo la integridad de los servidores principales, los sistemas aplicativos, los equipos de cómputo y la convivencia de estos en la red institucional, además de brindar la máxima protección contra las amenazas informáticas.

INSTITUTO NACIONAL DE CIENCIAS MÉDICAS Y NUTRICIÓN SALVADOR ZUBIRÁN

FORMATO DE JUSTIFICACIÓN PARA ADQUISICIONES SIN PROCEDIMIENTO DE LICITACIÓN PÚBLICA ARTÍCULO 55 LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO

Fecha de elaboración: junio 2026

8. Lugar y fecha de emisión

Ciudad de México, a 12 de junio de 2026

Atentamente

Mtra. Fanny Alvarado Chávez
Subdirectora de Tecnología de la Información y Comunicaciones