**ANEXO TÉCNICO.**

* 1. **Antecedentes.**

De conformidad con lo dispuesto en el Artículo 9 y 26 quinto párrafo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP), el Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán (INCMNSZ), a través de la Subdirección de Tecnologías de la Información y Comunicaciones (STIC) emite el presente Anexo Técnico para efectos de promover la modernización y desarrollo administrativo, en específico el proteger la información que se genera, almacena y circula dentro de la infraestructura tecnológica de red del Instituto.

Por otro parte, en este anexo técnico se establecen los requisitos y condiciones para todos los participantes del procedimiento de selección del software antivirus que satisfaga la necesidad del Instituto.

* 1. **Situación actual.**

En la actualidad el Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán, gestiona a través de los mecanismos correspondientes la contratación de un servicio que proporcione protección informática a través de un software, que garantice el buen funcionamiento de los equipos de cómputo, estaciones de trabajo, servidores, equipos portátiles y dispositivos móviles, permitiendo el correcto desempeño de los sistemas operativos y sus aplicaciones coexistentes entre sistemas, aplicativos, sistemas web, carpetas de escaneo, bases de datos compartidas, entre otros.

Se sabe que los virus informáticos tienen el propósito de modificar el correcto funcionamiento de los sistemas operativos con el fin de destruir, hurtar o colapsar la memoria y los archivos contenidos en servidores, equipos de cómputo y en general a todo dispositivo que conviva dentro de nuestra infraestructura tecnológica.

Aunado a lo anterior, los ciberataques pueden afectar la privacidad o la integridad de los documentos que se generan en el Instituto.

Para mitigar el riesgo de afectación, se realizó un análisis de las diferentes opciones existentes de antivirus que atiendan los requerimientos del Instituto. Una vez realizado este análisis, se determinó que las firmas de antivirus deben contener como mínimo las siguientes funcionalidades:

*Prevención*

Anticipándose a la infección, no permiten el acceso de ningún tipo de archivos que sea detectado como malicioso.

*Identificación*

Identificar archivos contaminados mediante el proceso de exploración y comparación de una base de datos en lista negra.

*Desinfección o Eliminación*

Neutralizar y/o inutilizar el archivo infectado por virus o en su defecto eliminarlo completamente.

Consola de Administración

* Gestión y administración de estaciones Windows, Mac OS, Linux o teléfonos móviles desde una sola consola.
* Generación de políticas y reglas, monitoreo de las detecciones y configuración remotamente de cualquier equipo de cómputo en nuestra red.
* Actualizar las bases de firmas para todos los equipos y ejecutar las soluciones de antivirus de forma centralizada y para toda la red, sin importar la cantidad de equipos que la conforman o la distribución de la misma.
  1. **Objeto del servicio.**

Contar con un servicio de arrendamiento de licencia de uso de software antivirus 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.

* 1. **Alcance del servicio.**

El servicio de arrendamiento de licencia de uso de software Antivirus tendrá como alcance la protección para 2200 equipos informáticos, con una vigencia del servicio del 01 de septiembre de 2023 al 31 de diciembre de 2024, 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.

* 1. **Descripción del servicio de arrendamiento de licencia de uso y requerimientos.**

**5.1 Requerimientos.**

**5.1.1 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 acabo 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 2200 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 cuenta con una certificación vigente en “ISO 9001 en calidad del servicio”.
* 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.

**5.1.2 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 local.
  + 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.

**5.2 Fases.**

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

**5.2.1 Fase de inicio.**

El proveedor deberá elaborar la planeación, instalación y puesta en operación del software propuesto como Antivirus en 2200 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.

**5.2.1.1 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.

5.2.1.2 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 2200 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

**5.2.1.3 Implementación de la Mesa de Ayuda.**

El Proveedor deberá poner a disposición del Instituto una Mesa de ayuda dentro de los 5 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.

**5.2.1.4 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:

|  |  |  |  |
| --- | --- | --- | --- |
| **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.

**5.2.1.5 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.

**5.2.1.6 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.
* Copia simple del certificado ISO 9001 del proveedor seleccionado.
* Documento del certificado de vigencia de la licencia de uso.

**5.2.2 Fase de operación y soporte.**

El proveedor deberá considerar que en esta fase se deben realizar de manera mandataria 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.

**5.2.2.1 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.

**5.2.3 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.
  1. **Normas y estándares.**

El proveedor deberá estar certificado ISO 9001 para la Gestión de la Calidad y presentar copia simple de dicha certificación.

El personal que instalará el software deberá estar certificado por el fabricante en el manejo (Instalación o configuración) del antivirus propuesto y deberá estar vigente.

* 1. **Plazos y condiciones.**
* El costo total de la licencia de uso se pagará en una sola exhibición al finalizar las actividades de la fase de inicio y de manera posterior al Vo.Bo. de los entregables definidos para esta fase.
* Las actividades de todas las fases definidas en este documento, deberán ser llevadas a cabo por personal certificado por el fabricante en el manejo (Instalación o configuración) del antivirus propuesto y dicha certificación deberá estar vigente.
* El servicio de arrendamiento de licencia de uso de software Antivirus deberá contemplar una vigencia del 01 de septiembre de 2023 al 31 de diciembre de 2024.
* Para la aceptación de la licencia de uso y el trámite de pago correspondiente, el proveedor tendrá que entregar al Administrador de la licencia de uso, la información requerida en los puntos anteriores, con excepción de los reportes mensuales.

* 1. **Lugar de instalación.**

El servicio de arrendamiento de licencia de uso de software Antivirus deberá contemplar la instalación en 2200 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.

* 1. **Entregables.**

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

|  |  |
| --- | --- |
| **Entregable** | **Tiempo de Entrega** |
|
| Minuta y Plan de Trabajo. | La reunión de inicio deberá celebrarse dentro de los primeros 5 días hábiles después del inicio de la vigencia del contrato, la minuta y el Plan de Trabajo deberán entregarse 3 días 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 5 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 la licencia 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. |

Nota: Los reportes mensuales se deberán entregar conforme el punto **5.2.2 “Fase de operación y soporte”**.

* 1. **Vigencia de la contratación.**

**La vigencia del** **servicio de arrendamiento de licencia de uso del software Antivirus será del 01 de septiembre de 2023 al 31 de diciembre de 2024.**

* 1. **Lugar de entrega.**

La entrega e instalación del software motivo de este servicio, será en el Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán, sita en Av. Vasco de Quiroga No. 15, Colonia Belisario Domínguez Sección XVI, CP 14080, Alcaldía Tlalpan de la Ciudad de México.

* 1. **El administrador del servicio.**

Las áreas responsables de verificar el cumplimiento del servicio de arrendamiento de licencia de uso de software Antivirus son:

Subdirección de Tecnologías de la Información y Comunicaciones: Administrador del Contrato.

Jefatura del Departamento de Redes e Infraestructura: Operador del servicio.