ÍNFIMA CUANTÍA	
No. DE ORDEN DE COMPRA: SERVICIO	**IC-INEC-064-2022**
FECHA:	08 de diciembre de 2022
AREA REQUIRENTE:	DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
NÚMERO DE CERTIFICACIÓN PRESUPUESTARIA:	2333
OBJETO DE CONTRATACIÓN:	El Contratista se obliga con el Instituto Nacional de Estadística y Censos a proveer las LICENCIAS ANTIVIRUS NECESARIO PARA EL DESARROLLO DE LAS ACTIVIDADES DEL INSTITUTO NACIONAL DE ESTADÍSTICA Y CENSOS requeridos a entera satisfacción del Instituto Nacional de Estadística y Censos, conforme el siguiente detalle: **METODOLOGÍA DE TRABAJO** Al día siguiente de la suscripción de la orden, el proveedor se pondrá en contacto con al administrador de la orden para coordinar el cronograma de trabajo a efectuarse, en el que se considere lo siguiente: • El proveedor deberá realizar la implementación y Soporte (incluye la consola) del antivirus en los equipos del INEC y la consola en su infraestructura de nube, la información proporcionará el área de Gestión de Seguridad Informática, Interoperabilidad y Riesgos quien será responsable de la administración de la misma. • El proveedor realizará la implementación del antivirus en el edificio de Planta central y Ed. Benalcázar Mil en 5 días calendario, con su personal técnico, (mínimo 5 técnicos capacitados), en mínimo 800 equipos definidos por el INEC. • El proveedor deberá disponer de una Mesa de Servicios en el esquema 24X7X365 (24 horas al día los 7 días de la semana y los 365 días del año). La mesa de servicios asignara de manera inmediata un número de ticket para seguimiento y control de incidentes. • El proveedor deberá incluir en su oferta 10 horas de soporte técnico presencial en el esquema 7X24X365 sin costo adicional para la institución, el tiempo de vigencia del soporte técnico, será igual a la del licenciamiento del antivirus. • Una vez suscrita la orden de servicio, el proveedor deberá presentar inmediatamente un documento con los Acuerdos de Niveles de Servicio (SLA) de atención, los cuales deberán cumplir con los siguientes requerimientos mínimos: o Nivel 1: 2 horas de atención y 4 horas de respuesta o Nivel 2: 2 horas de atención y 8 horas de respuesta o Nivel 3: 2 horas de atención y hasta 5 días calendario para la solución definitiva. • En el caso de existir por parte del fabricante actualizaciones y/o liberaciones de nuevas versiones de la consola, agente, y/o producto del antivirus durante el tiempo de vigencia del licenciamiento, el proveedor deberá informar inmediatamente al administrador de la orden de servicio para planificar y realizar la actualización integral a la nueva versión de los componentes antes

mencionados, sin que esto implique un costo adicional a la institución.
• El proveedor realizará la actualización en un lapso de tiempo no mayor a 5 días calendario a partir de que el fabricante libero la última versión, la cual no tendrá ningún costo adicional para la institución.
• El proveedor deberá realizar una transferencia de conocimientos para 4 funcionarios de DITIC, referente a la operación y administración de la consola del antivirus ofertado, así como a temas relacionados con seguridad informática. La planificación de los temas de seguridad informática y fechas de transferencia de conocimientos, se acordarán conjuntamente entre el proveedor y el Administrador de la orden de servicio, 3 días posteriores a la suscripción de la orden de servicio mediante un acta de acuerdo.
• El proveedor deberá emitir un certificado de asistencia de transferencia de conocimientos para cada funcionario.
• El proveedor deberá presentar un certificado, donde se comprometa a realizar sin costo adicional para la institución; una (1) visita técnica durante el periodo de vigencia del antivirus ofertado (el mismo que tendrá una vigencia de 12 meses una vez activado el servicio), para realizar la revisión técnica de la consola de administración de antivirus, con la finalidad de determinar el correcto funcionamiento del sistema de antivirus tanto de estaciones de trabajo y servidores.
• El proveedor deberá emitir en formato físico o digital manuales técnicos en idioma español, referente a la actualización, instalación, configuración y operación de la solución en la consola de administración, estaciones de trabajo y servidores de la institución.

INFORMACIÓN QUE DISPONE LA ENTIDAD

El INEC cuenta con 1000 licencias de antivirus con vigencia de un año y un parque informático de alrededor de 1200 equipos distribuidos entre computadores de escritorio, computadores portátiles y servidores a nivel nacional.

SERVICIO ESPERADO
Se requiere el siguiente servicio de acuerdo con las especificaciones técnicas detalladas a continuación:

Ítem	Descripción
1	Implementación y Soporte de 1300 licencias para protección de estaciones de trabajo y Servidores, por un año.
2	Soporte técnico ilimitado durante la vigencia de la orden
3	Transferencia de conocimientos - in situ

DETALLES DE LAS CARACTERISTICAS DEL ANTIVIRUS	
Administración Centralizada de la solución	La solución debe disponer una consola de administración unificada que se administre en la nube **(Consola WEB)** con capacidad de administrar un número ilimitado de equipos.

		La solución debe proporcionar un único punto para la implementación, aplicación y administración de las políticas de seguridad para el número de puntos finales solicitados por la institución, siendo estos de cualquier tipo y en cualquier ubicación. La solución debe aportar múltiples capas de seguridad para puntos finales, incluyendo servidores de correo de Microsoft Exchange, asegurando protección antimalware con monitorización del comportamiento, protección contra amenazas de día cero, control de aplicaciones y entorno de pruebas, cortafuego, control de dispositivos, control de contenidos, antiphishing y antispam. La solución debe brindar soporte para múltiples plataformas sin importar el número de portátiles, equipos de escritorio y servidores Windows, Linux y Mac OS X, contando con las tecnologías antimalware mejor valoradas. Además, para sistemas Windows debe brindar una seguridad aún más avanzada con un cortafuego bidireccional, detección de intrusiones, control y filtrado de acceso Web, protección de datos sensibles, y control de aplicaciones y de dispositivos, la heurística proactiva De La solución debe clasificar los procesos maliciosos según su comportamiento, asegurando la detección de nuevas amenazas en tiempo real. La solución debe brindar seguridad para centros de datos virtualizados, protegiendo tecnología de próxima generación pre-ejecución, que utiliza modelos de Machine Learning especializados, técnicas de análisis del comportamiento entrenados para detectar herramientas de pirateo, exploits y técnicas de ocultación de malware. Bloquea eficazmente los ataques que pasan por alto tanto las defensas tradicionales para endpoints como las denominadas defensas “antivirus de última generación en sistemas Windows y Linux. La solución debe aporta mejoras significativas de rendimiento e impulsar la consolidación del servidor. Las políticas pueden aplicarse a un pool de recursos de VMware vCenter La solución debe incluir un mecanismo automático de detección de redes que le

		permita detectar otros puntos finales en la red de la institución. Los puntos finales detectados deben mostrase como puntos finales no administrados en la Consola de Administración. La solución debe permitir instalar los agentes de seguridad en puntos finales físicos y virtuales ejecutando los paquetes de instalación localmente o ejecutando tareas de instalación remotamente desde la Consola de Administración. Adicional la consola WEB de administración, será capaz de gestionar un enlace web (Link de descarga) el cual podrá ser enviado por mail para realizar la instalación remota de clientes fuera de la red corporativa, el mismo que se auto configurará para enlazarse con la consola web, sin intervención del personal de TI El kit de instalación para puntos finales además debe permitir instalar la protección en los puntos finales sin conexión a Internet o con conexiones lentas. Debe utilizar un solo paquete, tanto para sistemas operativos de 32 bits como de 64 bits: – SO Windows: sistemas de 32 bits y 64 bits – SO Linux: sistemas de 32 bits y 64 bits – Mac OS X: solo sistemas de 64 bits La solución debe garantizar que el agente en los equipos administrados ejecute el análisis en tiempo real incluso cuando no haya conexión, cumpliendo las tareas, políticas y requerimientos configurados previamente aun cuando no haya conexión con la Consola de Administración. El agente de seguridad debe detectar automáticamente la configuración del punto final y adaptará la tecnología de análisis. Debe permitir la visibilidad, administración y consulta de los puntos finales físicos y virtuales, gestionándolos desde la consola de administración. La consola debe permitir la creación ilimitada de grupos o carpetas o subgrupos con el fin de permitir una mejor organización y administración de políticas. La consola deber permitir la asignación de políticas basado en reglas de asignación, ya sea por IP, Usuario, DNS, puerta de enlace o

		Gateway, WINS, DHCP, HOST y tipo de red. **La consola Cloud o web** La solución de seguridad antimalware debe permitir g**estionar en la web a través de una consola alojada en la nube lista y provista en su totalidad por el fabricante** (Cloud) desde un único punto de administración a través de cualquier tipo de dispositivo con acceso internet en cualquier sitios del mundo **sin límite de usuarios**, la consola Web Control Center, facilitara el acceso y la administración de la estrategia general de seguridad, las amenazas a la seguridad global, y el control sobre todos los módulos de seguridad que protegen a los equipos de escritorio virtuales o físicos y a los servidores. El Web Control Center debe ser capaz de abordar las necesidades de incluso las organizaciones más grandes sin la necesidad de utilizar múltiple consola de apoyo. Control Center, una interfaz basada en Web, se debe integrar con los sistemas de monitorización y administración existentes para aplicar fácilmente el sistema de protección a los equipos de escritorio, virtuales y servidores no administrados. Permitir la aplicación y gestión de políticas en los endpoint independientemente de que se encuentren o no en las instalaciones locales. **Soporte para múltiples plataformas,** debe funcionar tanto en equipos Windows como Linux. Permitiendo instalarse todos los componentes deseados simultáneamente con el programa de instalación general o eligiendo los componentes individuales. También debe desplegar el programa como un dispositivo virtual. **Incluir un agente independiente que actúe incluso cuando no hay conexión,** este agente independiente ejecutará todas las tareas, políticas y sucesos directamente en el endpoint, aunque no tenga conexión con la consola. **Una arquitectura de replicador y servidor de comunicación tipo Relay para gestionar la red,** las ubicaciones remotas solo necesitan la implementación de un antivirus con este módulo adicional sin la necesidad

		de instalar una consola de replicación o una consola esclava o un servidor proxy de la consola, el relay recopilará y reenviará los datos agregados al servidor principal. Manejar la comunicación con los agentes, y recopilar y almacenar los datos de las aplicaciones. Ser capaz de manejar decenas de miles de clientes manteniendo su elevada velocidad operativa sin saturar la infraestructura Incluir un **sensor detector de equipos no autorizados,** descubrir todos los equipos de la red que no están protegidos ni administrados y mostrárselos al administrador. El mecanismo automático de detección de red Pensado para detectar los equipos del grupo de trabajo. El mecanismo automático de detección debe utilizar el servicio Microsoft Computer Browser para realizar una detección de red. El servicio Computer Browser es una tecnología de red utilizada por los equipos basados en Windows para mantener listas actualizadas de dominios, grupos de trabajo y los equipos en ellos, y para suministrar estas listas a equipos cliente que lo soliciten. Los equipos detectados en la red por el servicio Computer Browser pueden visualizarse ejecutando el comando de net view en una ventana de símbolo del sistema. Configurar las opciones de notificación siguiendo unos pasos específicos. Ejecutar las políticas directamente en el agente y aplicar políticas específicas para los endpoint incluso cuando no haya conexión con el servidor consola. Otra vez del uso de un usuario con permisos configurado previamente en la política. Recopilar datos necesarios para generar los informes; los registros restantes se deberán almacenar en el cliente para mejorar el rendimiento de la base de datos. Crear múltiples cuentas de usuarios y personalizarlas, los privilegios para cada una se podrán personalizar en forma individual.

		Se podrá usar en muchas ubicaciones distintas y permitir definir políticas corporativas para los administradores locales. El administrador de licencias permitirá el manejo de todas las licencias en forma transparente, desde cualquier punto a través de un navegador Web **sin tener la necesidad de publicar ningún servicio a la Web**. Limpieza de equipos terminales y servidores de código malicioso y programas inseguros no autorizados instalados. La herramienta permitirá realizar acciones en caso de ser necesario. Además de mostrar los informes a través de la consola basada en la Web, se pueden exportar en formato PDF, Excel y guardar en una ubicación predefinida, y enviarse como una notificación por correo electrónico. La solución deberá contar con un módulo de protección que proteja las aplicaciones más comunes como: lectores de PDF, navegadores web, clientes de correo, etc en caso de que se trate de explotar una vulnerabilidad.. Protección contra vulnerabilidades: Mejora la detección de las Vulnerabilidades y Exposiciones Comunes (CVE) en los protocolos más utilizados, como SMB, RPC y RDP. Brinda protección contra las vulnerabilidades para las cuales aún no se publicó o desarrolló la revisión necesaria. Protección ante botnets: Protege ante las infiltraciones por malware de tipo botnet, previniendo el envío de spam y evitando que se lleven a cabo ataques de red desde la endpoint. Desinstalación de soluciones de seguridad: la solución deberá ser capaz de desinstalar la solución que se encuentra instalada actualmente. Deberá contar con la posibilidad de sincronizarse con Active directory en su versión cloud Debe permitir generar grupos de clientes

		dinámicos (paramétricos). La consola de gestión debe mostrar la lista de servidores y estaciones que tienen el antivirus instalado, conteniendo la siguiente información mínima: nombre de la máquina, versión de antivirus, versión del motor, fecha de la vacuna, la última fecha de verificación, política aplacada, ip, sistema operativo y el estado. Se deberá poder visualizar el estado de la red desde paneles portlets o widgets que sean completamente personalizables, tanto en cantidad como en contenido. Dicha información será en tiempo real y se podrá elegir si verla en formato grafico o tabla
	Protección para Plataformas Windows, Linux y Mac	**La solución EndPoint deberá proteger las siguientes plataformas:** **<u>Sistemas operativos de escritorio</u>** ● Windows 11 ● Windows 10 ● Windows 8.1 ● Windows 8 ● Windows 7 ● Windows 7 **<u>Sistemas operativos integrados y de tablets</u>** ● Windows 10 IoT Enterprise ● Windows Embedded 8.1 Industry ● Windows Embedded 8 Standard ● Windows Embedded Standard 7 ● Windows Embedded Compact 7 ● Windows Embedded POSReady 7 ● Windows Embedded Enterprise 7 ● Windows Embedded POSReady 2009 ● Windows Embedded Standard 2009 (1) ● Windows XP Tablet PC Edition(1) **<u>Sistemas operativos de servidor</u>** ● Windows Server 2019 ● Windows Server 2016 ● Windows Server 2016 Core ● Windows Server 2012 R2 ● Windows Server 2012 ● Windows Small Business Server (SBS) 2011 ● Windows Home Server(1)

		SISTEMAS OPERATIVOS LINUX ● Ubuntu 14.04 LTS o superior ● Red Hat Enterprise Linux / CentOS 6.0 o superior ● SUSE Linux Enterprise Server 11 SP4 o superior ● OpenSUSE Leap 42.x ● Fedora 25 o superior(1) ● Debian 8.0 o superior ● Oracle Linux 6.3 o superior ● Amazon Linux AMI 2016.09 o superior **SISTEMAS OPERATIVOS Mac OS X** ● Mac OS X Sierra (10.12.x) ● Mac OS X El Capitan (10.11.x) ● Mac OS X Yosemite (10.10.5) ● Mac OS X Mavericks (10.9.5) ● Mac OS X Mountain Lion (10.8.5) **NAVEGADORES SOPORTADOS** ● Internet Explorer 8+ ● Mozilla Firefox 30+ ● Google Chrome 34+ ● Safari 4+ ● Microsoft Edge 20+ ● Opera 21+ **VIRTUALIZADORES SOPORTADOS** ● VMware vSphere 6.7 actualización 2a, 6.7 actualización 1, 6.7, 6.5, 6.0, 5.5, 5.1, 5.0 con VMware vCenter Server 6.7 actualización 2a, 6.7 actualización 1, 6.7, 6.5, 6.0, 5.5, 5.1, 5.0 ● VMware Horizon/View 7.7, 7.6, 7.5, 7.1, 6.x y 5.x ● VMware Workstation 11.x, 10.x, 9.x, 8.0.6 ● VMware Player 7.x, 6.x, 5.x ● Citrix XenServer 7.x, 6.5, 6.2, 6.0, 5.6 o 5.5 (incluyendo hipervisor Xen) ● Citrix Virtual Apps y Desktops 7 1808, 7 1811, 7 1903, 7 1906 ● Citrix XenApp y XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR ● Citrix VDI-in-a-Box 5.x ● Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2 o Windows Server 2008 R2, 2012, 2012 R2 (incluyendo Hyper-V Hypervisor) ● Red Hat Enterprise Virtualization 3.0 (incluyendo KVM Hypervisor) ● Oracle VM 3.0 ● Oracle VM VirtualBox 5.2, 5.1

	● Nutanix Prism con AOS 5.5, 5.6 (Enterprise Edition) ● Nutanix Prism versión 2018.01.31 (Community Edition)
Protección en tiempo real	El análisis de la solución en tiempo real debe evitar que entren en el sistema nuevas amenazas de malware, La solución debe analizar los archivos locales y de red cuando se acceda a ellos (al abrirlos, moverlos, copiarlos o ejecutarlos), al análisis de los sectores de arranque y al de las aplicaciones potencialmente no deseadas (APND).
Filtrado de correo electrónico malicioso.	El módulo de protección de correo electrónico de la solución debe ofrecer protección multicapa contra las amenazas y phishing mediante una combinación de varios filtros y motores de análisis en la capa de protocolo (POP3 y SMPT) para determinar si los mensajes de correo electrónico son maliciosos.
Filtrado de Navegación	La solución que controla el Tráfico HTTP / FTP del Explorador de Windows debe Permitir o denegar el tráfico HTTP y FTP desde el Explorador de Windows. La solución debe tener la capacidad de crear reglas de cortafuego adicionales para otras aplicaciones instaladas en los puntos finales, esto debe crearlo además de las reglas predeterminadas por defecto.
Remote Troubleshooting	La solución deber permitir recopilar registros básicos y avanzados de forma remota. Con fin de facilitar a el análisis en profundidad del problema y proporcionar una resolución más rápida.
Protección Proactiva	La solución debe poseer tecnología de detección proactiva he innovadora que debe utilizar avanzados métodos heurísticos para que pueda detectar nuevas amenazas potenciales en tiempo real, debe monitorizar continuamente las aplicaciones que se están ejecutando en el punto final en busca de acciones indicativas de malware. Cada una de estas acciones debe puntuarse y calcular una puntuación global para cada proceso.
Consumo de recursos de Memoria del Endpoint	La solución debe utilizar menos de ~220 MB cuando se ejecute un análisis completo
Exclusión de archivos del análisis en tiempo real	La solución deberá contar con la opción para realizar exclusiones de archivos del análisis en tiempo real.

Control de acceso web	La suite de Seguridad deberá contar con un control de acceso web, con categorías para definir qué sitios pueden ser accedidos o no dentro de la red. Limitar el acceso a los sitios Web por categoría y por grupo de usuarios para lograr una eficaz aplicación de las políticas corporativas cuyo objetivo es maximizar el cumplimiento de directivas de seguridad y la productividad de los empleados.
Análisis manual de búsqueda de códigos maliciosos.	La solución deberá contar con la opción de correr un análisis manual de búsqueda de códigos maliciosos. Ofrecer detección avanzada de malware furtivo mediante la exploración minuciosa del contenido de los protocolos seguros HTTPS y POP3, así como de los archivos comprimidos.
ERM (Administración de Riesgos)	El módulo de gestión de riesgos de punto final (ERM) ayudara a identificar y remediar una gran cantidad de riesgos de red y sistemas operativos a nivel de punto final, mostrando el porcentaje de vulnerabilidad en la infraestructura. El puntaje de riesgo de la compañía se calcula teniendo en cuenta una amplia lista de indicadores de riesgos y vulnerabilidades de aplicaciones conocidas, mostrándole su evolución en el tiempo. Desglose de la puntuación y las principales configuraciones incorrectas y los widgets de aplicaciones vulnerables hacen que sea más fácil ver dónde su entorno es más vulnerable a los ataques y qué dispositivos son los más afectados. Este módulo deberá contar con al menos 300 indicadores de gestión de Hardening para la generación del nivel de riesgo
Human Risks Analytics	El módulo de gestión de riesgos debe incluir un analizador de riesgos humanos. El cual debe validar los siguientes aspectos: • Verificar si el usuario ha enviado credenciales a través de conexiones HTTP inseguras desde el último escaneo. • Verificar si el usuario ha navegado o no sitios marcados como phishing o fraude desde el último análisis. • Verificar si el usuario ha estado expuesto a una gran cantidad de amenazas desde el último análisis. • Verificar si el usuario ha estado expuesto a una amenaza de un dispositivo extraíble (por ejemplo, unidad flash, disco duro externo) desde el último escaneo.

		• Verificar si el usuario ha accedido a archivos maliciosos a través de una carpeta compartida de red desde el último análisis. • Verificar si el usuario ha accedido a alguna URL maliciosa desde el último análisis. • Verificar si el usuario no ha cambiado la contraseña de inicio de sesión de la cuenta (local o de dominio) durante más de 30 días. • Verificar si el usuario usa las mismas contraseñas en diferentes sitios externos. • Verificar si el usuario usa las mismas contraseñas compartidas entre sitios web internos y externos. • Verificar si el usuario no ha cambiado la contraseña de inicio de sesión para las cuentas HTTP (internas o externas) durante más de 30 días.
	Defensa de ataques de RED	Tecnología enfocada en detectar técnicas de ataque a la red diseñadas para obtener Acceso a puntos finales específicos como: • Ataques de fuerza bruta • Ataques de red • Ladrones de contraseñas • Ataques Laterales.
	Anti-Exploit Avanazdo	Anti-Exploit proporciona protección en ejecución contra intentos de explotación dirigidos a vulnerabilidades conocidas y desconocidas en aplicaciones de uso común y aplicaciones propias, como el navegador, Microsoft Office o Adobe Reader, así como contra intentos específicos de post-explotación en modo kernel.
	Control de Dispositivos	Control de Dispositivos: permite prevenir las infecciones de fugas y malware datos sensibles a través de dispositivos externos conectados a extremos aplicando bloqueo normas y excepciones a través de la política a una amplia gama de tipos de dispositivos (tales como unidades Flash USB, dispositivos Bluetooth, reproductores de CD/DVD, dispositivos de almacenamiento, etc.). Que los bloqueos a dispositivos puedan realizarse por marca, modelo, número de serie o usuario.
	Cifrado de Disco	La solución debe contar con la opción de adicionar como Add-on la protección de los datos de toda la unidad de disco duro del endpoint mínimo para el 25% de las licencias adquiridas, aprovechando los mecanismos de cifrado proporcionados por Windows (BitLocker) y Mac (FileVault). Se basa en el

	cifrado nativo de los dispositivos para garantizar la total compatibilidad y maximizar el rendimiento, sin la necesidad de instalar un agente adicional, ni un servidor de claves, gestionado todo de la misma consola de administración. Debe poseer opción para establecer reglas para excluir unidades del cifrado.
Administración Integrada De Parches	La solución debe contar con la posibilidad de adicionar como Add-on una herramienta de gestión y administración de parches de sistema operativo y aplicaciones mínimo en el 25 % de las licencias adquiridas, permitiendo mantener actualizada toda su base instalada de Windows: estaciones de trabajo, servidores físicos y virtuales. Disponible en la versión elite de las soluciones ofertadas.
Exclusión de archivos	La solución deberá contar con la opción de realizar exclusiones de archivos del análisis del motor por demanda.
Análisis Programados	La solución y la consola de administración remota deberán permitir realizar análisis programados (en demanda) de los discos duros locales. Esta programación se podrá configurar en forma diaria, semanal, mensual.
Cortafuegos de escritorio	La solución deberá contar con un cortafuego de escritorio (Firewall Personal) que cuenta con un filtrado dinámico de paquetes que provea de monitoreo y filtrado de trafico de Red, y tenga total protección para IPv4 e IPv6 y con la opción de agregar reglas y servicios al cortafuego en forma autónoma y centralizada. Impedir el acceso no autorizado a la red corporativa. Ofrecer una fácil instalación, gran capacidad de personalización de reglas y un modo de aprendizaje inteligente para crear reglas de firewall automáticamente basándose en el tráfico de red observado. Combinar perfiles personalizados de firewall con zonas de redes de confianza. Debe poseer distintos modos del módulo de firewall entre los cuales debe tener uno que permita aprender la conducta del usuario generando las reglas permisivas automáticamente. Debe poseer opción para importar y exportar reglas.

	Esta solución no deberá provocar interrupciones con el Firewall de la Institución.
Actualización a través de repositorios de actualización de la solución de todas las estaciones protegidas	La consola de administración deberá permitir actualizar a través de repositorios de actualización a todas las estaciones protegidas con la posibilidad de tener redundancia de repositorios de actualización en forma automáticas (Fail-over).
La actualización de la base de datos de firmas de códigos maliciosos	Las actualizaciones de las bases de datos de firmas de códigos maliciosos de la solución antivirus deberán ser incrementales, evitando de esta manera la saturación del ancho de banda en su despliegue.
Opción de apagado luego de escaneo.	La herramienta antivirus debe permitir el apagado luego de la exploración o Repetición de las exploraciones programadas activadas por el administrador. Esto con el objetivo de ayudar a extender la vida útil del hardware y ahorrar energía y recursos
Programación y actualizaciones diferidas.	La herramienta antivirus debe contar con una selección opcional para la recepción de actualizaciones provenientes de servidores especiales con 12 horas de retraso para brindar tiempo a los administradores del sistema para evaluar el impacto en su red y asegurar una migración organizada.
Reportes	La consola de administración deberá contar con reportes gerenciales detallados con información de configuraciones, actualizaciones de los productos, alertas, estadísticas, etc., las cuales pueden ser exportadas a archivos csv y/o pdf. Deberá permitir generar reportes gráficos tipo barra, pastel, etc., para una vista rápida de la situación de la solución.
Alerta en consola y notificación vía correo electrónico y SNMP	La solución deberá permitir que las acciones de notificación incluyan correo electrónico, SNMP, y entradas de registro.
Compatibilidad con la estructura organizacional del Directorio Activo	La consola de administración web deberá permitir la detección de clientes no registrados sincronizando la estructura del grupo a través de Active Directory.
Análisis de aplicaciones y	Debe permitir clasificar las aplicaciones en al menos 3 grupos según sus características y

procesos	poder configurar el motor antivirus para que las analice o no. Debe otorgar una puntuación a los procesos en ejecución del sistema para medir su nivel de riesgo
Análisis de procesos	Deberá poseer una herramienta integrada para ver los procesos en ejecución, los servicios, las conexiones establecidas, claves de registro importantes, programas instalados, actualizaciones de sistema operativo instaladas, logs del equipo, drivers instalados, tareas programadas del sistema, archivo hosts, system.ini y win.ini. Análisis de causa raíz de las amenazas detectadas y bloqueadas por nuestras tecnologías preventivas, con opciones complejas de filtrado de incidentes y representación gráfica de incidentes, así como capacidades de aislamiento, lista de bloqueo y conexión remota.
Análisis de archivo comprimidos	La solución ofertada deberá detectar virus en archivos compactados, con profundidad máxima (16), en los siguientes formatos: .zip, .rar, .arj, .cab, .lzh, .tar, .gz, ace, izh, upx y otros
Gestión de Políticas	La consola de administración deberá definir y hacer cumplir consistentemente las políticas a lo largo de la red. El Administrador de Políticas facilitará la importación/exportación, para permitir la aplicación y combinación de las políticas de diversas maneras.
Gestión Multi-plataforma	La consola de administración deberá permitir administrar de forma remota desde una única consola todos los equipos de su red, ejecutando las versiones antivirus en clientes finales y servidores de las diferentes plataformas (Windows, Linux, Mac OS)
Servidor de Aplicaciones en Unidades Anexas	El oferente deberá asignar como mínimo a un técnico que acudirá a las oficinas del contratante para la instalación de la solución. El oferente se comprometerá a dejar listas las consolas de administración de la contratante con el total de usuarios respectivos conectados al servidor.
Actualización de versiones	El oferente será responsable de la actualización de la solución antivirus en los equipos y servidores de la contratante a la última versión estable liberada por el fabricante durante el tiempo que dure el licenciamiento.

PROVEEDOR:	DAMAJU S.A.		
RUC:	1792412137001	**PROFORMA Nro.:**	SIN NÚMERO
TELÉFONO:	099 860 3692	**FECHA:**	28/11/ 2022
DIRECCIÓN:	Av. Isla Seymour N44-160 y Rio Coca	**CONTACTO:**	Christian Escobar
CORREO:	ventas@issolutions.com.ec	**VIGENCIA:**	30 días

ITEM	CPC	DESCRIPCIÓN	UNIDAD DE MEDIDA	CANTIDAD	V. UNITARIO	V. TOTAL
1	512900021	LICENCIAS ANTIVIRUS NECESARIO PARA EL DESARROLLO DE LAS ACTIVIDADES DEL INSTITUTO NACIONAL DE ESTADÍSTICA Y CENSOS	Unidad	1300	$ 4,57	$ 5.941,00
SUBTOTAL						$ 5.941,00
IVA 12%						$ 712,92
TOTAL						$ 6.653,92

Notas:
Lo no contemplado en la presente orden, se estará a las disposiciones de la Ley Orgánica del Sistema Nacional de Contratación Pública, su Reglamento General de aplicación, y demás normativa secundaria emitida para el efecto por parte del SERCOP.

ADMINISTRADOR DE LA ORDEN	La administración de la orden, estará a cargo de Carlos Rivas Director de Tecnologías de la Información y Comunicación, quien velará por el cabal y oportuno cumplimiento de todas y cada una de las obligaciones derivadas de la Orden y verificará que los servicios contratados, cumplan con los términos de referencia establecidos en el objeto contractual. La máxima autoridad o su delegado, podrá cambiar de administrador de la orden, en cualquier momento durante la ejecución del referido instrumento, para lo cual bastará únicamente la notificación al contratista.
FORMA DE PAGO:	El Instituto Nacional de Estadística y Censos, pagará la orden para la LICENCIAS ANTIVIRUS NECESARIO PARA EL DESARROLLO DE LAS ACTIVIDADES DEL INSTITUTO NACIONAL DE ESTADÍSTICA Y CENSOS, una vez que se hayan ejecutado y cumplido con todos los componentes de los servicios, conforme con el siguiente detalle: El Instituto Nacional de Estadística y Censos se compromete a pagar el 100% de la orden a la entrega recepción de las licencias, debidamente instaladas y configuradas, previa suscripción del Acta de Entrega Recepción Definitiva y presentación de la factura correspondiente y a plena satisfacción de la entidad contratante.
PLAZO DE EJECUCIÓN:	El plazo para la prestación de los servicios contratados a entera satisfacción de la contratante es de 5 días calendario a partir del día siguiente a la suscripción de la orden para entregar la licencia, la vigencia de esta será de 365 días calendario desde su activación.
OBLIGACIONES DEL CONTRATISTA:	✓ Suscribir el acta entrega de recepción definitiva. ✓ Todo el servicio debe ser ejecutado a entera satisfacción del INEC. ✓ El cumplimiento de todas y cada uno de los Términos de referencia ✓ Y las demás que estipula la normativa legal vigente.
MULTAS:	Las multas se impondrán por retardo en la ejecución de las obligaciones contractuales, así como por incumplimientos de las demás obligaciones contractuales, las que se determinarán por cada día de retraso; las multas se calcularán sobre el porcentaje de las obligaciones que se

	encuentran pendientes de ejecutarse conforme lo establecido en la orden y serán del 1 por mil. La multa será descontada al momento de efectuarse el pago correspondiente al contratista.
GARANTÍA:	No aplica
LUGAR DE ENTREGA:	El lugar designado para la entrega en el edificio de Planta central y Ed. Benalcázar Mil, según las especificaciones técnicas y/o términos de referencia, que se agregan y forman parte integrante de esta orden. El proveedor deberá realizar la implementación y Soporte (incluye la consola) del antivirus en los equipos del INEC y la consola en su infraestructura de nube, la información proporcionará el área de Gestión de Seguridad Informática, Interoperabilidad y Riesgos quien será responsable de la administración de la misma.
RECEPCIÓN:	La Recepción del servicio, se realizará conforme lo dispuesto en el artículo 321 del Reglamento General a la Ley Orgánica del Sistema Nacional de Contratación Pública.
COMUNICACIONES ENTRE LAS PARTES:	Todas las comunicaciones entre las partes, relativas al objeto de esta contratación, sin excepción, serán formuladas por escrito y en idioma castellano. Las comunicaciones también podrán efectuarse a través de medios electrónicos.
DOCUMENTOS HABILITANTES:	- Término de referencia de la contratante. - La certificación que acredite la existencia de la partida presupuestaria y disponibilidad de recursos, para el cumplimiento de las obligaciones derivadas de la orden. - Proforma.
ACEPTACIÓN:	DAMAJU S.A. con RUC 1792412137001, certifica e informa que el servicio cumplirá con las especificaciones descritas en la proforma aceptada por el Instituto Nacional de Estadística y Censos la misma que forma parte integrante de esta orden y garantiza su calidad. Esta orden es intransferible y obliga únicamente a quien se le otorga; quien asume todas las responsabilidades que pueden sobrevenir, en caso de utilización indebida por parte de otras personas. El Instituto Nacional de Estadística y Censos podrá dar por terminada la orden de conformidad con lo determinado el artículo 92 de la Ley Orgánica del Sistema Nacional de Contratación Pública. Esta Orden no surtirá ningún efecto si la misma no se encuentra firmada por la máxima autoridad o su delegado y si no se cuenta con la certificación presupuestaria sobre la existencia actual y futura de fondos. Las partes libre, voluntaria y expresamente declaran que conocen y aceptan el texto íntegro de lo expuesto en la orden de ínfima cuantía.

BASE LEGAL

El artículo 52.1 de la Ley Orgánica del Sistema Nacional de Contratación Pública –LOSNCP-, prevé:

"Se podrá contratar bajo este sistema en cualquiera de los siguientes casos:

1.- Las contrataciones para la adquisición de bienes o prestación de servicios no normalizados, exceptuando los de consultoría, cuya cuantía sea inferior a multiplicar el coeficiente 0,0000002 del presupuesto inicial del Estado del correspondiente ejercicio económico;

2.- Las contrataciones para la adquisición de bienes o prestación de servicios normalizados, exceptuando los de consultoría, que no consten en el catálogo electrónico y cuya cuantía sea inferior a multiplicar el coeficiente 0,0000002 del presupuesto inicial del Estado del correspondiente ejercicio económico; y,

3.- Las contrataciones de obras que tengan por objeto única y exclusivamente la reparación, refacción, remodelación, adecuación, mantenimiento o mejora de una construcción o infraestructura existente, cuyo presupuesto referencial

sea inferior a multiplicar el coeficiente 0,0000002 del presupuesto inicial del Estado del correspondiente ejercicio económico. Para estos casos, no podrá considerarse en forma individual cada intervención, sino que la cuantía se calculará en función de todas las actividades que deban realizarse en el ejercicio económico sobre la construcción o infraestructura existente. En el caso de que el objeto de la contratación no sea el señalado en este numeral, se aplicará el procedimiento de menor cuantía.

Las contrataciones previstas en este artículo se realizarán de forma directa con un proveedor seleccionado por la entidad contratante, sin que sea necesario que este habilitado en el Registro Único de Proveedores. (…)"

El artículo 71 de la LOSNCP, preceptúa:
"Las multas se impondrán por retardo en la ejecución de las obligaciones contractuales conforme al cronograma valorado, así como por incumplimientos de las demás obligaciones contractuales, las que se determinarán por cada día de retardo; las multas se calcularán sobre el porcentaje de las obligaciones que se encuentran pendientes de ejecutarse conforme lo establecido en el contrato.

En todos los casos, las multas serán impuestas por el administrador del contrato, y el fiscalizador, si lo hubiere, el o los cuales establecerán el incumplimiento, fechas y montos.

Las multas impuestas al contratista pueden ser impugnadas en sede administrativa, a través de los respectivos recursos, o en sede judicial o arbitral."

MÁXIMA AUTORIDAD O SU DELEGADO	CONTRATISTA
Firmado electrónicamente por: MARITZA YOLANDA JUMBO OVIEDO	Firmado electrónicamente por: CHRISTIAN ANDRES ESCOBAR OBANDO
MARITZA YOLANDA JUMBO OVIEDO	CHRISTIAN ANDRES ESCOBAR OBANDO
DIRECTORA ADMINISTRATIVA	**REPRESENTANTE LEGAL DE DAMAJU S.A.**

	Nombre	Sumilla
Elaborado por:	Lizeth Trujillo	LT
Revisado por:	Gonzalo Álvarez	GA