15740024

MiBus

TRANSPORTE MASIVO DE PANAMA S.A.
R.U.C. 1818454-1-708570 D.V 80

No. de la Orden de Compra: **26499**

Orden de Compra

Proveedor: INNOVA DIGITAL SOLUTIONS, S.A. **Monto:** 37,529.06 USD

Fecha de la Orden de Compra: **29 de octubre de 2024**

Detalle de Compra: **LICENCIAS DE ANTIVIRUS TMPSA Resolución No. 299-2024-DNMySC de 15 de marzo de 2024.**

DATOS DEL PROVEEDOR

Proveedor:	INNOVA DIGITAL SOLUTIONS, S.A.	**R.U.C.**	155626945-2-2016
Dirección:	BELLA VISTA,OBARRIO,CALLE 50 Y 56	**D.V.:**	75
Representante Legal:	HUGO ADRIAN, JUNCO	**Teléfono:**	3099920

DATOS DE LA ENTREGA

Unidad Solicitante	Dirección de Tecnología	**Términos de pago:**	Crédito
A la atención de:	ANGEL MINA	**Moneda:**	USD
Plazo de Entrega:	10 días hábiles	**Tipo de entrega:**	TOTAL

Lugar de entrega: Patio Ojo de Agua
Via Transismica, Los AndesNo. 2
Ciudad de Panama, San Miguelito

Dirección para facturación: Transporte Masivo de Panama SA
Avenida Domingo Diaz, Centro Comercial Los Pueblos
Ciudad de Panama, Panama

Monto en letras: TREINTA Y SIETE MIL QUINIENTOS VEINTI NUEVE DOLARES CON 06/100

Renglón de OC	No. Parte	Descripción	SC	Partida Presupuestal	Cantidad	Unidad de Compra	Costo Unitario	Costo de Línea	Impuesto	Total
1	9084	Servicios tecnológicos	11889	281020710201165	525	UNIDAD	58.42	30,670.50	0.00	30,670.50
2	9084	Servicios tecnologicos	11889	281020710201165	24	MES	0.00	0.00	0.00	0.00
3	9627	Otros cargos por servicios tecnológicos	11889	281020710201165	525	UNIDAD	5.36	2,814.00	0.00	2,814.00
4	9627	Otros cargos por servicios tecnológicos	11889	281020710201165	104	UNIDAD	38.89	4,044.56	0.00	4,044.56
5	9084	Servicios tecnologicos	11889	281020710201165	4	UNIDAD	0.00	0.00	0.00	0.00
6	9084	Servicios tecnologicos	11889	281020710201165	4	UNIDAD	0.00	0.00	0.00	0.00
7	9084	Servicios tecnologicos	11889	281020710201165	2	UNIDAD	0.00	0.00	0.00	0.00
8	9084	Servicios tecnologicos	11889	281020710201165	1	UNIDAD	0.00	0.00	0.00	0.00
9	9084	Servicios tecnologicos	11889	281020710201165	1	UNIDAD	0.00	0.00	0.00	0.00
								Subtotal de Orden de Compra		**37,529.06**
								ITBMS (7%)		**0.00**
								Costo Total de Orden de Compra (moneda)		**37,529.06 USD**

DETALLE DE PARTIDAS PRESUPUESTALES

Partida Presupuestal	Monto
281020710201165	37,529.06

MiBus

TRANSPORTE MASIVO DE PANAMA S.A.
R.U.C. 1818454-1-708570 D.V 80

No. de la Orden de Compra: **26499**

Orden de Compra

Proveedor: INNOVA DIGITAL SOLUTIONS, S.A. **Monto:** 37,529.06 USD

Renglón de OC	No. Parte	Observaciones detalladas
1	9084	NUEVA LICENCIAS PARAA LA SOLUCION INTEGRAL DE ANTIVIRUS POR UNA VIGENCIA DE 24 MESES 1. La solución corporativa de Antivirus ofertada debe poder utilizarse en la nube. El mantenimiento y garantía del uso de consola en la nube debe estar cubierta por la marca propuesta. 2. La consola administrativa tiene que ser administrada a través de una interfaz web y ser capaz de permitir acceso a la plataforma de antivirus por lo mínimo desde los siguientes navegadores: a. Microsoft Edge. b. Mozilla Firefox c. Google Chrome. Safari. 3. La consola de administración tiene que tener la capacidad de la creación de perfiles de acceso a la misma y así poder asignar distintos permisos y roles según las necesidades de los administradores de la solución. 4. La consola de administración debe permitir al administrador la instalación local de los agentes de antivirus, así como el despliegue de forma remota desde la propia consola en los equipos finales utilizando un solo instalador. 5. El instalador generado por la consola o de los repositorios debe ser menor de 200 MB lo que permitirá un despliegue con menor uso de recursos. 6. En la consola de administración o centro de control debe mostrar un informe general de seguridad el cual, dé una vista general de detecciones sin resolver de los últimos 7 días anteriores, que incluye la gravedad, el método de detección, el estado de resolución. 7. La consola de administración o centro de control debe ser personalizable para crear una visión general de equipos, grupos, políticas, usuarios o demás datos recogidos por la consola. 8. La consola de administración o centro de control debe tener capacidad para visualizar las detecciones con tecnología Drill Down. 9. La consola de administración o centro de control debe proveer informes de: a. Detecciones gestionadas por el sandbox o caja de arena en la nube. b. Visión general del estado de salud de los clientes. c. Informe de detecciones del firewall de los equipos. d. Las detecciones del antivirus de los endpoints de los últimos 7 a 30 días. 10. Actualizaciones automáticas, compactas e incrementales que eviten la generación de archivos de gran tamaño, evitando de esta manera que pueda impactar de una manera negativa a los recursos de ancho de banda de la red. 11. SandBox en la nube automatizado, y con módulos configurables en cuanto al nivel de desinfección. 12. La consola de administración o centro de control debe poder ejecutar tareas: 13. Diagnósticos a. Aislar equipo de la red b. Actualización de módulos c. Reversión de actualizaciones de módulos d. Exploración bajo demanda e. Activación del producto f. Enviar el archivo al sandbox g. Instalación de software h. Desinstalación de software i. Solicitud de registro de SysInspector en Windows j. Acciones Anti-Theft para móviles 14. Debe poder administrar políticas de seguridad (Crear, asignar, modificar, renombrar y eliminar) desde el centro de control, políticas que especifican las opciones de seguridad que se aplican a los elementos del inventario de red (equipos, máquinas virtuales). 15. Debe tener la capacidad de creación de políticas de gestión de equipos para la aplicación de un equipo individual o grupos, con las siguientes características: a. Políticas predefinidas que permitan la fácil implementación por parte del usuario. b. Las políticas deben poder activarse / desactivarse mediante indicadores (No aplicar / Aplicar / Forzar). c. Política de control de dispositivos (USB, Disco externos, CD/DVDs, puertos LPT, etc). d. Políticas de control web por categorías o por enlaces. e. Políticas de control contra ataques de fuerza bruta y conexiones de Escritorio Remoto. f. Capacidad de importar / exportar políticas a la consola web desde otra consola similar. 16. Debe permitir crear y visualizar informes centralizados sobre el estado de seguridad de los objetos de red administrados. Los informes deben permitir acceder a los datos y filtrarlos desde la base de datos desde categorías. a. Poseer informes predeterminados. b. Capacidad de modificar informes a través de plantillas predefinidas. c. Capacidad de creación de categorías de informes. d. Capacidad de duplicar informes basados en un informe seleccionado. e. Capacidad de descarga de informes en formato .pdf y .csv. f. Poseer gestión de permisos de usuarios para los informes (Lectura, Uso, Escritura). g. Debe poseer informes tipo tablas y gráficos (barras, puntos, circulares, anillos, líneas, líneas apiladas, barras apiladas). h. Capacidad de ordenar datos en gráficos de tablas mediante ejes "X" y "Y". i. Capacidad de manejo de filtros por elemento de lista o valor. j. Capacidad de programación de informe mediante tareas. k. Generación de inventario de hardware por las siguientes categorías: Chasis, Información de Dispositivo, Pantalla, Adaptador de Pantalla, Dispositivo de Entrada, Almacenamiento en Masa, Adaptador de Red, Impresora, Procesador, RAM y Dispositivo de Sonido. l. Reporte de aplicaciones obsoletas de seguridad.

Contraloría General de la Republic
Dirección Nacional de Fiscalización Gener
VERIFICADO
19 NOV 2024
Ivette D. Blackwood
Fiscalizadora

Orden de Compra

Proveedor: INNOVA DIGITAL SOLUTIONS, S.A. **Monto:** 37,529.06 USD

Renglón de OC	No. Parte	Observaciones detalladas

17. Debe ser compatible con todas las plataformas de hipervisor como mínimo VMWARE y Microsoft Hyper V.
18. Debe soportar los siguientes sistemas operativos en sus últimas versiones: Windows Server 2008 R2 SP1 con KB4474419 y KB4490628 instalado, 2012, 2016, 2019 y 2022 (incluyendo Modo Server core). Windows 7 SP1 con las actualizaciones de Windows más recientes (al menos KB4474419 y KB4490628), 8, 10 y 11 en plataformas de 32 bits y 64 bits. MAC OS X 10.15 y 11 Linux Ubuntu 18.04, 20.04, 22.04 LTS.
19. Debe soportar el funcionamiento de seguridad en el navegador Internet Explorer 8+, Mozilla Firefox 30+, Google Chrome 34+, Safari 4+, Microsoft Edge 20+ y Opera 21+.
20. Debe contar con protección para dispositivos móviles con sistemas operativos Android e IOS.
21. La solución corporativa de antivirus debe proteger aplicaciones de correo y ofimática en la nube de Google Workspace:
a. Business Starter
b. Business Standard
c. Business Plus
d. Enterprise
22. Debe ofrecer protección del sistema de archivos en tiempo real – debe explorar todos los archivos en busca de códigos maliciosos cuando se abren, crean o ejecutan.
23. Debe ofrecer Control del dispositivo: debe proporcionar el control del dispositivo automático (CD/DVD/USB/...). permitir bloquear o ajustar los filtros o permisos extendidos y definir la forma en que el usuario puede acceder y trabajar con un dispositivo determinado.
24. Debe ofrecer Sistema de prevención de intrusos de Host o Host Intrusion Prevention System (HIPS) – debe monitorear los sucesos que ocurren dentro del sistema operativo y reacciona a ellos según un grupo de reglas personalizado.
25. Debe ofrecer la exploración de memoria avanzada: Trabaja en conjunto con el Bloqueador de exploits para fortalecer la protección contra el malware diseñado para evadir la detección por los productos antimalware con el uso de ofuscación o cifrado.
26. Debe tener exploración personalizada de objetos, medios extraíbles, unidades locales, unidades de red, memoria operativa y registros del sistema.
27. Debe ofrecer bloqueador de exploits: está diseñado para fortalecer diferentes tipos de aplicaciones comúnmente explotadas como los navegadores web, los lectores de PDF, los clientes de correo electrónico y los componentes de MS Office. El bloqueador de exploits está habilitado en forma predeterminada.
28. Debe ofrecer protección contra Ransomware es otra capa de protección que funciona como parte de la función HIPS.
29. Debe ofrecer Control web – debe bloquear las páginas Web que puedan contener material potencialmente ofensivo. Además, los administradores del sistema pueden especificar preferencias de acceso para 27 o más categorías de sitios Web predefinidos.
30. Debe ofrecer Protección del acceso a la Web – todo el tráfico que pase a través de HTTP o HTTPS se explora en busca de software malicioso.
31. Debe ofrecer Protección del cliente de correo electrónico – monitorea las comunicaciones recibidas a través de los protocolos POP3 e IMAP.
32. Debe ofrecer Protección antispam – debe explorar en busca de correo electrónico no solicitado o spam.
33. Debe ofrecer Protección Anti-Phishing – debe proteger de sitios web ilegítimos disfrazados de legítimos que intentan obtener contraseñas, datos bancarios y demás información confidencial.
34. Debe ofrecer protección en tiempo real.
35. Debe ofrecer Protección contra Malware – debe proteger de códigos maliciosos que pueden agregarse al principio o al final de archivos existentes en su ordenador, la detección debe ser de aprendizaje automático.
36. Debe ofrecer Protección contra Aplicaciones potencialmente no deseadas – debe proteger de Grayware o Aplicación Potencialmente no Deseada (PUA) Obtenga más información sobre estos tipos de aplicaciones en el Glosario.
37. Debe ofrecer Protección contra Aplicación potencialmente no segura – debe proteger de software comercial y legítimo que puede utilizarse inadecuadamente para fines maliciosos.
38. Debe ofrecer Protección contra Aplicaciones sospechosas - debe poder analizar programas comprimidos con empaquetadores o protectores.
39. Debe tener Caché local compartido – debe tener la capacidad de compartir el caché con otros equipos para mejorar el rendimiento en entornos como máquinas virtuales.
40. Debe ofrecer Protección de Sandbox en la nube.
41. Debe contar con una protección de análisis en la nube como capa extra de seguridad en caso de que el objeto sea de día cero, amenazas persistentes o de dudosa reputación deberá enviar este de manera automática.
42. Las muestras deberán poder ser enviadas de manera automática o manual mediante el módulo de envió desde el endpoint.
43. Las muestras deben poder ser enviadas mediante discriminación tipos de archivos.
44. Deberá poder realizar excepciones según tipo de archivo.
45. Debe contar con Detección y Respuesta Extendida XDR. La herramienta de detección y respuesta debe tener la capacidad de ejecutar acciones de remediación como:
a. Block executables – Bloqueo de ejecutables.
b. Kill processes – detener procesos.
c. Isolate endpoints from the network – aislar puntos finales de la red.
d. Terminal remote Shell – capa de terminal remota.
46. Debe contar Gestión de Vulnerabilidades y parchado: debe proporcionar una descripción general de las vulnerabilidades detectadas en los equipos, para proporcionar información instantánea de cualquier software instalado vulnerable, la misma debe mostrar información sobre la aplicación como: nombre, versión, proveedor, CVE, nombre del

Contraloría General de la R
Dirección Nacional de Fiscalizac
21 NOV 2024
Ivette D. de Blackw
Fiscalizadora

MiBus

TRANSPORTE MASIVO DE PANAMA S.A.
R.U.C. 1818454-1-708570 D.V 80

No. de la Orden de Compra: **26499**

Orden de Compra

Proveedor: INNOVA DIGITAL SOLUTIONS, S.A. **Monto:** 37,529.06 USD

Renglón de OC	No. Parte	Observaciones detalladas
		equipo y categoría de la vulnerabilidad. 46. La gestión de parches debe enumerar todos los parches disponibles que corrigen las vulnerabilidades detectadas y debe facilitar el proceso de corrección a través de actualizaciones de software automatizadas. 47. Los móviles deben poder ser administrados desde la misma consola que los PC y servidores, donde deben poder contar con las siguientes características: a. Antivirus b. Antirrobo c. Anti-Phishing d. Integración con Consola MDM e. Filtro de Llamadas f. Bloqueo de Aplicaciones g. Filtro Web h. Geolocalización i. Protección de SIM j. Control de Dispositivos Bluethoot, USB, Firewire para prevenir robo de datos. 48. Debe ofrecer Cifrado de Discos completos en S.O. Windows 10 y 11, MacOS 10.14, 10.15 y 11. a. Capacidad de cifrar discos de arranque o todos los discos. b. Soporte para uso de módulo de plataforma segura TPM o el soporte para unidades con autocifrado OPAL. c. Poseer políticas de contraseña con opción de Minúsculas / Mayúsculas / Números / símbolos / longitud. d. Políticas de contraseñas erradas en cuanto a mínimos y máximos de intentos. e. Capacidad de instalación remota desde la consola de administración f. Debe tener ejecución de tareas de Invalidación de contraseña remotamente y restablecimiento de acceso. g. Capacidad de generación de contraseña de recuperación para el usuario desde la consola. h. Bloqueo de acceso remoto. i. Generación de llave USB de recuperación. j. Eliminación de contraseña remoto. 49. El fabricante debe contar con oficina oficial en Panamá y brindar soporte local a nivel nacional y a nivel regional Latinoamérica. 50. El fabricante debe contar con un servicio de laboratorio de investigación regional para proporcionar de forma rápida actualizaciones de bases de firmas de virus sobre amenazas enfocadas en regiones específicas. 51. El fabricante debe ofrecer los servicios de consultoría antes y después de la implementación. 52. El fabricante debe contar con una plataforma de certificación orientada a clientes y que permita la realización de cursos sobre la solución adquirida. 53. El fabricante debe realizar la respectiva transferencia de conocimientos al personal técnico de la entidad sobre la implementación y puesta en marcha de la solución adquirida, además debe poder apoyar a la organización en la divulgación de buenas prácticas de seguridad por medio de charlas en sitio, webinarios, e información de interés. 54. El fabricante debe realizar la respectiva actualización a la última versión de la solución e instalación necesaria en todas las capas de seguridad que incluye la herramienta en los endpoints solicitados. 55. El fabricante debe brindar un servicio de acompañamiento / revisión de consola de 52 horas al año (1 hora a la semana) con personal técnico situado en Panamá. 56. El proponente debe contar con personal certificado en la última versión de la plataforma adquirida. 57. El proponente debe presentar carta del fabricante avalando que actualmente es partner certificado (bronce en adelante) en todos los productos ofrecidos a la entidad. Marca: Eset Modelo: Eset Casa productora: Eset País de origen: Eslovaquia
2	9084	Mobile Security POR 24 MESES
3	9627	Implementación total
4	9627	Console Manager/ x Horas
5	9084	Preventive Monitoring Standard
6	9084	Forensic incident analysis
7	9084	Charla de concientización presencial
8	9084	Technical Training Protect
9	9084	Technical Training Protect

VERIFICADO
Contraloría General de la República
Dirección Nacional de Fiscalización General
21 NOV 2024
Ivette D. Blackwood
Fiscalizadora

Otras observaciones: SE REQUIERE LICENCIAS DE ANTIVIRUS PARA TMPSA POR UNA VIGENCIA DE 24 MESES (CONTADOS DESDE EL 9 DE DICIEMBRE DE 2024 HASTA 9 DE DICIEMBRE DE 2026)

MiBus

TRANSPORTE MASIVO DE PANAMA S.A.
R.U.C. 1818454-1-708570 D.V 80

No. de la Orden de Compra: **26499**

Orden de Compra

Proveedor: INNOVA DIGITAL SOLUTIONS, S.A. **Monto:** 37,529.06 USD

Cláusula anticorrupción EL CONTRATISTA garantiza, se compromete y declara que ni él ni a través de interpuesta persona ha incurrido ni incurrirá, directa o indirectamente, en ninguna de las siguientes conductas:
1. Pagar, dar, entregar, recibir, prometer, o acordar una dádiva, donación, coima, soborno, regalos, aportes o comisiones ilegales, bienes u otros objetos de valor, bajo cualquier modalidad.
2. No haber pagado directa o indirectamente sumas o cantidades ilícitas, como premios o incentivos, en moneda local o extranjera en la República de Panamá o en cualquier otro lugar en que dicha conducta se relacione con el contrato en violación de las leyes anticorrupción de la República de Panamá o de cualquiera otra jurisdicción en el extranjero, a servidores públicos, partidos políticos o sus directivos, candidatos políticos o a terceros que puedan influir en la ejecución o supervisión del contrato.
En caso de que **EL CONTRATISTA** incurra en cualquiera de las conductas establecidas en esta cláusula dará lugar Cláusula anticorrupción EL CONTRATISTA garantiza, se compromete y declara que ni él ni a través de interpuesta persona ha incurrido ni incurrirá, directa o indirectamente, en ninguna de las siguientes conductas:

Penalidad

La multa que se impondrá será cuatro por ciento (4%), del valor equivalente a la porción dejada de entregar o ejecutar por el contratista, dividido entre treinta (30), por cada día calendario de atraso.
El valor total de la multa no será en ningún caso superior al veinte por ciento (20%) del valor del contrato y deberá ingresar al Tesoro Nacional.

Fundamento Legal:

Según Reglamento Especial de Contratación, aprobado por la Contraloría General de la República mediante Resolución Número 299-2024-DNMySC de 15 de marzo de 2024. Anexo 1, Grupo A. Insumos. A.12 Software / Sistema Operativo para computadoras / Servidores.

Gerencia de Compras	Dirección de Administración	Presidente Junta Directiva Representante Legal
Fecha: 01/11/24	Fecha:	Fecha: 18-11-24
Tesorería	**Almacén**	**Departamento de Presupuesto**
	MiBus	CRISTABELLA COMBE V. Analista de Presupuesto
Fecha:	Fecha:	Fecha: 1/11/2024 T-46698
Entregado al Proveedor:		**Refrendo de Fiscalización**
Nombre legible		
Fecha:		Fecha: 21/11/24

VB°D°

VERIFICADO
Contraloría General de la República
Dirección Nacional de Fiscalización General
19 NOV 2024
Ivette [illegible] Parkwood
Fiscalizadora