CONTRATO Nº 23/2.022

ADQUISICIÓN DE EQUIPOS INFORMÁTICOS Y SOFTWARE, ADJUDICADO EN EL LLAMADO A CONCURSO DE OFERTAS Nº 04/2.022

Entre el **MINISTERIO DE DEFENSA NACIONAL**, domiciliado en la casa de la Avda. Mcal. López esq. Vicepresidente Sánchez, República del Paraguay, representados para este acto por el Señor Ministro de Defensa Nacional **GRAL EJ (R) BERNARDINO SOTO ESTIGARRIBIA, con Cédula de Identidad Civil N.º 412.151**, denominado en adelante el CONTRATANTE, por una parte, y por la otra, la firma **PASO PARAGUAY S.A.** con RUC N° 80024954-2, domiciliado en la casa de las calles Domingo Portillo 1181 casi Fuerte Borbón, Asunción – República del Paraguay, representada para este acto por la Señora **FABIANA GIMÉNEZ, con Cédula de Identidad Civil Nº 2.977.140**, en calidad de representante legal, denominado en adelante el CONTRATISTA, denominados en conjunto "LAS PARTES", acuerdan celebrar el presente "CONTRATO", el cual estará sujeto a las siguientes cláusulas y condiciones:

1. OBJETO DEL CONTRATO.

El objeto del contrato es: "Adquisición de Equipos Informáticos y Software".

2. DOCUMENTOS INTEGRANTES DEL CONTRATO.

Los documentos contractuales firmados por las partes y que forman parte integral del Contrato son los siguientes:

1. Contrato;
2. El pliego de bases y condiciones y sus adendas o modificaciones;
3. Los datos cargados en el SICP;
4. La oferta del Proveedor;
5. La resolución de adjudicación del Contrato emitida por la contratante y su respectiva notificación;

Los documentos que forman parte del contrato deberán considerarse mutuamente explicativos; en caso de contradicción o discrepancia entre los mismos, la prioridad se dará en el orden enunciado anteriormente.

3. IDENTIFICACIÓN DEL CRÉDITO PRESUPUESTARIO PARA CUBRIR EL COMPROMISO DERIVADO DEL CONTRATO.

El crédito presupuestario para cubrir el compromiso derivado del presente contrato está previsto conforme al Certificado de Disponibilidad Presupuestaria vinculado al Programa Anual de Contrataciones (PAC) con el ID N°: 409.261.

4. PROCEDIMIENTO DE CONTRATACIÓN.

El contrato es el resultado del procedimiento de Concurso de Ofertas N° 04/22 "Adquisición de Equipos Informáticos y Software", convocado por la Dirección de Contratación de Bienes y Servicios. La adjudicación fue realizada por Resolución Administrativa N° 146/2.022.

5. PRECIO UNITARIO Y EL IMPORTE TOTAL A PAGAR POR LOS BIENES.

Ítem	Descripción	Cantidad	Unidad de Medida	Presentación	Marca	Procedencia	Precio Unitario IVA Incluido	Precio Total IVA Incluido
11	Software antivirus para computadora (Conforme a especificaciones técnicas del PBC)	125	Unidad	Unidad	Panda Security	España	179.000	22.375.000
TOTAL IVA INCLUIDO								**22.375.000**

ÍTEM Nº 11.

Características	Descripción
Cantidad	125 unidades
Consola de Administración	Todos los componentes que forman parte de la solución, de seguridad para móviles, servidores y estaciones de trabajo deben ser suministrados por un solo fabricante. No se aceptarán composiciones de productos de diferentes fabricantes
	El oferente deberá actualizar el software a nuevas versiones durante el periodo que dure el mantenimiento del Software (12 meses)
	La administración deberá ser a través de una consola central única, basada en web y en nube, que deberá contener todas las componentes para el monitoreo y control de la protección de los dispositivos
	La consola deberá presentar un Dashboard con el resumen del estado de protección de los ordenadores y usuarios, así como indicar las alertas de eventos de criticidades alta, media e informativa
	Debe poseer un mecanismo de comunicación vía API, para su integración con otras soluciones de seguridad, como por ejemplo SIEM
	La consola debe permitir la división de los ordenadores dentro de la estructura de administración en grupos
	Debe permitir la sincronización con Active Directory (AD) para la gestión de usuarios y grupos integrados en las políticas de protección.
	Debe poseer la posibilidad de aplicar reglas diferenciadas por grupos de usuarios, usuarios individuales, grupos de máquinas y equipos individuales

	La instalación debe poder realizarse a través del cliente descargado de la consola central y también vía correo electrónico de configuración. El instalador debe permitir la distribución del cliente a través de Active Directory (AD) para múltiples máquinas.
	Proporcionar actualizaciones del producto y de las definiciones de virus y protección contra intrusos
	Debe permitir exclusiones de escaneo para un determinado sitio web, archivo o carpeta, aplicación o proceso. Tanto a nivel global, como específico en cada política.
	La consola de administración debe permitir la definición de grupos de usuarios con diferentes niveles de acceso a la configuración, las políticas y los registros
	Actualización incremental, remota y en tiempo real, de las vacunas de los Antivirus y del mecanismo de verificación (Engine) de los clientes
	Permitir la programación de la exploración contra virus con la posibilidad de seleccionar una máquina o grupo de máquinas, con periodicidad definida por el administrador
	Utilizar protocolos seguros estándar HTTPS para la comunicación entre la consola de administración y los clientes administrados.
	Los mensajes generados por el agente deben estar en el idioma español o permitir su edición.
	Permitir la exportación de los informes gerenciales a los formatos CSV y PDF
	Los recursos del informe y el monitoreo deben ser nativos de la propia consola central de administración
	Posibilidad de mostrar información como nombre de la máquina, versión del antivirus, sistema operativo, dirección IP, versión del motor, fecha de la actualización, fecha de la última verificación, eventos recientes y estado
	La comunicación debe permitir QoS para controlar el ancho de banda de red.
	Debe permitir seleccionar un grupo de equipos para aplicar la actualización para controlar el ancho de banda de red. La actualización de la versión debe ser transparente para los usuarios finales.
	La herramienta de administración centralizada debe administrar todos los componentes de la protección para estaciones de trabajo y servidores y debe diseñarse para administrar, supervisar y elaborar informes de endpoint y servidores.
	La Consola de administración debe incluir un panel con un resumen visual en tiempo real para comprobar el estado de seguridad

	Deberá proporcionar filtros pre-construidos que permitan ver y corregir sólo los ordenadores que necesitan atención
	Deberá mostrar los ordenadores administrados de acuerdo con los criterios de categoría (detalles del estado del equipo, detalles sobre la actualización, detalles de avisos y errores, detalles del antivirus, etc.), y ordenar los equipos en consecuencia
	Actualizar de forma automática las directivas de seguridad cuando un equipo se mueve de un grupo a otro
	Grabar un registro de auditoría seguro que supervise la actividad en la consola de administración para el cumplimiento de regulaciones, auditorías de seguridad, análisis y solución de problemas forenses
	Deberá permitir exportar el informe de registros de auditoría en formatos CSV y PDF
	Debe contener varios informes para el análisis y control de los usuarios y endpoints. Los informes se deben dividir, como mínimo, en informes de: eventos, usuarios, control de aplicaciones, periféricos y web, indicando todas las funciones solicitadas para los endpoints
	Permitir la ejecución manual de todos estos informes, así como la programación y envío automático por correo electrónico en los formatos CSV y PDF
	Deberá tener la posibilidad de implementar servidores de caché locales para utilizar de manera eficiente el uso del ancho de banda.
	Deberá tener la posibilidad de instalar un servidor para reenvío de eventos (message relay) en caso de que el agente no pueda comunicarse con la consola en la nube.
	La solución de endpoint, servers, móviles y seguridad perimetral, debe ser administrada desde la misma consola en la nube.
	Debe realizar envío automático de alertas criticas mediante correo electrónico a los administradores
	Debe permitir identificar y proteger desde la misma consola instancias de servidores desplegados en AWS.
	Debe permitir identificar y proteger desde la misma consola instancias de servidores desplegados en Azure.
Capacidad de generación de informes	Detalle de usuarios activos, inactivos o desprotegidos, así como detalles de los mismos
	Detalle de los ordenadores que están activos, inactivos o desprotegidos, así como detalles de las exploraciones y alertas en los ordenadores
	Detalle de los periféricos permitidos o bloqueados, así como detalles de dónde y cuándo se utilizó cada periférico

	Detalle de las principales aplicaciones bloqueadas y los servidores / usuarios que intentaron acceder a ellas
	Detalle de las aplicaciones permitidas que fueron accedidas con mayor frecuencia y los servidores / usuarios que las acceden
	Detalle de los servidores / usuarios que intentaron acceder a aplicaciones bloqueadas con mayor frecuencia y las aplicaciones que ellos intentaron acceder
	Detalle de todas las actividades disparadas por reglas de fuga de información.
Idiomas	Inglés (predeterminado)
	Portugués
	Alemán
	Francés
	Italiano
	Español
	Japonés
	Chino (tradicional y simplificado)
Opciones de corrección de problemas	Proteger el dispositivo con la opción de inicio de una exploración
	Forzar una actualización en ese momento
	Ver los detalles de los eventos ocurridos
	Ejecutar la comprobación completa del sistema
	Forzar el cumplimiento de una nueva política de seguridad
	Mover el equipo a otro grupo
	Borrar el equipo de la lista
Características básicas del agente de protección	El agente antivirus debe proteger computadoras portátiles, escritorios y servidores en tiempo real, bajo demanda o programado para detectar, bloquear y limpiar todos los virus, troyanos, gusanos y spyware. En Windows, el agente también debe detectar PUA, adware y comportamiento sospechoso,
	Además del control de amenazas, el mismo agente (al menos Windows) debe proporcionar control de dispositivos, control de aplicaciones, control web y prevención de fuga de información (DLP).
	Detección del malware en pre-ejecución y comprobar el comportamiento malicioso para detectar malware desconocido
	Debe realizar la verificación de todos los archivos accedidos en tiempo real, incluso durante el proceso de arranque
	Debe realizar la limpieza del sistema automáticamente, eliminando elementos maliciosos detectados y aplicaciones potencialmente indeseables (PUA)

	Debe proteger las funciones críticas en los navegadores de Internet (Safe Browsing)
	Debe permitir la autorización de detecciones maliciosas y excluir de la exploración de directorios y archivos específicos
	Se requiere protección integrada, es decir, en un solo agente, contra amenazas de seguridad, incluyendo virus, spyware, troyanos, gusanos, adware y aplicaciones potencialmente no deseadas (PUA)
	Posee la funcionalidad de protección contra el cambio de la configuración del agente, impidiendo a los usuarios, incluyendo el administrador local, reconfigurar, deshabilitar o desinstalar componentes de la solución de protección
	Debe tener un mecanismo contra la desinstalación del endpoint por el usuario y cada dispositivo deberá tener una contraseña única, no siendo autorizadas soluciones con una contraseña que funcione en todos los dispositivos
	Permitir la utilización de contraseña de protección para posibilitar la reconfiguración local en el cliente o desinstalación de los componentes de protección
	Ser capaz de aplicar un análisis adicional, inspeccionando finamente el comportamiento de los códigos durante la ejecución, para detectar el comportamiento sospechoso de las aplicaciones, tales como desbordamiento de búfer.
	Debe prevenir el ataque de vulnerabilidades de navegador a través de web exploits
	Debe permitir el monitoreo y el control de dispositivos extraíbles en los equipos de los usuarios, como dispositivos USB, periféricos de la propia estación de trabajo y redes inalámbricas, aplicando estas políticas tanto para usuarios como para dispositivo
	El control de dispositivos debe estar al nivel de permiso, sólo lectura o bloqueo
	Los siguientes dispositivos deben ser, como mínimo, administrados: HD (hard disks) externos, pendrives USB, almacenables removibles seguras, CD, DVD, Blu-ray, floppy drives, interfaces de red inalámbrica, módems, bluetooth, infrarrojo, MTP (Media Transfer Protocol) y PTP (Picture Transfer Protocol) como cámaras digitales
	Control de aplicaciones para monitorear e impedir que los usuarios ejecuten o instalen aplicaciones que puedan afectar la productividad o el rendimiento de la red
	Capacidad de reconocer y bloquear automáticamente las aplicaciones en los clientes basándose en la huella digital (hash) del archivo.

	Actualización automática de la lista de aplicaciones que se pueden controlar, permitiendo aplicaciones específicas o las categorías específicas de aplicaciones que pueden ser liberadas o bloqueadas
	Detectar aplicaciones controladas cuando los usuarios acceden, con las opciones de permitir y alertar o bloquear y alertar
	Debe contar con prevención de intrusión en el host (HIPS), que monitoree el código y bloques de código que pueden comportarse de forma maliciosa antes de ser ejecutados
	Control de acceso a sitios web por categoría
	El Control Web debe controlar el acceso a sitios inapropiados, con al menos 14 categorías de sitios inadecuados. También debe permitir la creación de listas blancas y listas negras.
	La aplicación de políticas de control web, debe contar con capacidad de horarios.
	Debe poseer protección de fugas o pérdida de datos sensibles en el mismo agente de protección, considerando su contenido, además de la posibilidad de evaluar la extensión del archivo y múltiples destinos
	Permitir la identificación de información confidencial, como números de pasaporte u otra información personal identificable y / o información confidencial, incluso si los documentos no se han clasificado correctamente, utilizando CCL (Lista de control de contenido)
	Posibilitar el bloqueo, sólo registrar el evento en la Consola de administración, o preguntar al usuario si él o ella realmente quiere transferir el archivo identificado como sensible
	Soportar agregar reglas propias de contenido con un asistente proporcionado para este propósito
	Capacidad de autorizar, bloquear y confirmar el movimiento de información sensible y en todos los casos, grabar la operación realizada con las principales informaciones de la operación
	El Agente para servidores debe contemplar monitoreo de integridad de archivos, al menos en servidores Windows.
Identificadores de listas CCL preconfiguradas	Números de tarjetas de crédito
	Números de cuentas bancarias
	Números de pasaportes
	Direcciones
	Números de teléfono
	Lista de correos electrónicos
Medios para control de datos	Adjunto en el cliente de correo electrónico (al menos Outlook y Outlook Express)

	Adjunto en el navegador (al menos IE, Firefox y Chrome)
	Adjunto en el cliente de mensajería instantánea (al menos Skype)
	Adjunto a dispositivos de almacenamiento (al menos USB, CD / DVD)
Funcionalidad de detección proactiva de reconocimiento de nuevas amenaza	Protección de amenazas de día 0 a través de tecnología de deep learning (signature less).
	Funcionalidad de detección de amenazas desconocidas que están en memoria
	Capacidad de detección, y bloqueo proactivo de keyloggers y otros malwares no conocidos (ataques de día cero) a través del análisis de comportamiento de procesos en memoria
	Capacidad de detección y bloqueo de Trojans y Worms, entre otros malwares, por comportamiento de los procesos en memoria
	No debe requerir descarga de firmas de ningún tipo.
	Capacidad de analizar el comportamiento de nuevos procesos al ser ejecutados, en complemento a la exploración programada.
	Análisis forense de lo sucedido, para entender cuál fue la causa raíz del problema con el detalle de los procesos y sub-procesos ejecutados, la lectura y escritura de archivos y de las claves de registro.
	Bloqueo y protección contra amenazas desconocidas potencialmente sospechosas (PUA).
	Generación de excepciones ante falsos positivos.
Funcionalidad de protección contra ransomware	Disponer de capacidad de protección contra ransomware basada en comportamiento
	Disponer de capacidad de remediación de la acción de encriptación de los ransomware
	Capacidad de detección del cifrado malicioso de forma local o remoto
	Debe poseer protección anti-ransomware para el sector de booteo (master boot record).
	Debe restaurar automáticamente los archivos cifrados por un proceso malicioso de ransomware.
	Debe informar a la consola todo el detalle del incidente – análisis de causa raíz sin la necesidad de instalar otro agente o dispositivo en la red
Protección contra Vulnerabilidades y técnicas de explotación	Debe poseer la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidades conocidas o de día cero
	Mitigación de inyección de códigos en procesos
	Protección contra robo de credenciales
	Protección contra malware escondido en aplicaciones legitimas (code cave)

	Evitar la migración de procesos maliciosos, evitando que un proceso malicioso migre a otro.
	Evitar obtener escalamiento de privilegios
	Modificación de las claves de registro para la ejecución de código arbitrario
	Enforce Data Execution Prevention
Detección y protección de las siguientes técnicas de explotación	Mandatory Address Space Layout Randomization
	Bottom-up ASLR
	Null Page (Null Deference Protection)
	Heap Spray Allocation
	Dynamic Heap Spray
	Stack Pivot
	Stack Exec (MemProt)
	Stack-based ROP Mitigations (Caller)
	Branch-based ROP Mitigations (Hardware Assisted)
	Structured Exception Handler Overwrite (SEHOP)
	Import Address Table Filtering (IAF)
	Load Library
	Reflective DLL Injection
	Shellcode
	VBScript God Mode
	Wow64
	Syscall
	Hollow Process
	DLL Hijacking
	Squiblydoo Applocker Bypass
	APC Protection (Double Pulsar / AtomBombing)
	Process Privilege Escalation
	La solución deberá permitir al administrador aislar de forma manual una máquina de la red para su investigación
	El aislamiento de la red de los equipos también podrá realizarse de manera automática en caso de presencia de actividad sospechosa
	El administrador tendrá la capacidad de realizar búsqueda de amenazas en los equipos de la red al menos por hash, IP o URL.
	La herramienta debe permitir la captura de un snapshot forense
Despliegue Agente	Soportar máquinas con arquitectura de 32 bits y 64 bits
	El cliente para instalación en estaciones de trabajo debe ser compatible con los sistemas operativos Mac OS X 10.10 en adelante.

	El cliente para instalación en estaciones de trabajo debe ser compatible con los sistemas operativos Windows 7 en adelante
	El cliente para instalación en servidores debe ser compatible con los sistemas operativos Windows server 2008 en adelante.
Sistemas Operativos Linux soportados (en tiempo real)	CentOS 6/7
	Debian 9
	Oracle Linux 6/7
	Red Hat Enterprise Linux 6/7
	SUSE 12/15
	Ubuntu 14/16/18
Implementación de la solución	El oferente deberá prever la implementación de la consola y el despliegue de los clientes con las correspondientes políticas a ser consensuadas con la Convocante.
Validez de las Licencias	12 (doce) meses.

El Monto total Adjudicado asciende a la suma total de **Gs. 22.375.000 (guaraníes veinte y dos millones trescientos setenta y cinco mil) IVA incluido.**

El Proveedor se compromete a proveer los Bienes a la Contratante y a subsanar los defectos de éstos de conformidad a las disposiciones del Contrato.

La Contratante se compromete a pagar al Proveedor como contrapartida del suministro de los bienes y servicios y la subsanación de sus defectos, el Precio del Contrato o las sumas que resulten pagaderas de conformidad con lo dispuesto en éstas bases y condiciones.

6. VIGENCIA DEL CONTRATO.

El plazo de vigencia del contrato será: Hasta el cumplimiento total de las obligaciones.

7. PLAZO, LUGAR Y CONDICIONES DE LA PROVISIÓN DE BIENES.

Los bienes deben ser entregados dentro de los plazos establecidos en el Cronograma de Entregas del Pliego de Bases y Condiciones.

8. ADMINISTRACIÓN DEL CONTRATO.

La administración del contrato estará a cargo de: Dirección de Coordinación Administrativa.

9. FORMA Y TÉRMINOS PARA GARANTIZAR EL CUMPLIMIENTO DEL CONTRATO.

La garantía para el fiel cumplimiento del contrato se regirá por lo establecido en las Condiciones Contractuales del presente pliego de bases y condiciones, la cual se presentará a más tardar dentro de los diez (10) días calendarios siguientes a la firma del contrato.

10. MULTAS.

Las multas y otras penalidades que rigen en el presente contrato serán aplicadas conforme con lo establecido en las Condiciones Contractuales del presente pliego. Llegado al monto equivalente a la Garantía de Fiel Cumplimiento de Contrato, la Contratante podrá aplicar el procedimiento de rescisión de contratos de conformidad al Artículo 59 inc. c) de la Ley N° 2.051/2003 "De Contrataciones Públicas", caso contrario deberá seguir aplicando el monto de las multas que correspondan.

La rescisión del contrato o la aplicación de multas por encima del porcentaje de la Garantía de Cumplimiento del Contrato deberá comunicarse a la DNCP a los fines previstos en el artículo 72 de la Ley N° 2051/2003 "De Contrataciones Públicas", modificado por Ley N° 6716/2021.

11. CAUSALES Y PROCEDIMIENTO PARA SUSPENDER, TERMINAR O RESCINDIR.

Las causales y el procedimiento para suspender temporalmente, dar por terminado en forma anticipada o rescindir el contrato, son las establecidas en la Ley N° 2051/2003 y en las condiciones contractuales del presente pliego de bases y condiciones.

12. SOLUCIÓN DE CONTROVERSIAS.

Cualquier diferencia que surja durante la ejecución del contrato se dirimirá conforme a las reglas establecidas en la legislación aplicable y en las condiciones contractuales.

13. ANULACIÓN DE LA ADJUDICACIÓN

Si la Dirección Nacional de Contrataciones Públicas resolviera anular la adjudicación de la Contratación debido a la procedencia de una protesta o investigación instaurada en contra del procedimiento, y si dicha nulidad afectara al contrato ya suscrito entre LAS PARTES, el Contrato o la parte del mismo que sea afectada por la nulidad, quedará automáticamente sin efecto de pleno derecho, a partir de la comunicación oficial realizada por la DNCP, debiendo asumir LAS PARTES las responsabilidades y obligaciones derivadas de lo ejecutado del contrato.

En prueba de conformidad se suscriben 2 (dos) ejemplares de un mismo tenor y a un solo efecto en la Ciudad de Asunción, República del Paraguay, a los 21 días del mes de Octubre de 2.022.

FABIANA GIMÉNEZ
REPRESENTANTE LEGAL
C.I.C. Nº 2.977.140
Contratista
Paso Paraguay S.A.
RUC 80024954-2

MINISTERIO DE DEFENSA NACIONAL
REPÚBLICA DEL PARAGUAY
MINISTRO

GRAL EJ (R) BERNARDINO SOTO ESTIGARRIBIA
MINISTRO
C.I.C. Nº 412.151.
Contratante