



## CONTRATO N° 02/2022

Entre la Dirección Nacional de la Propiedad Intelectual (DINAPI), domiciliada en España N° 323 casi E.E.U.U., en la Ciudad de Asunción, Capital de la República del Paraguay, representada para este acto por su Director Nacional ABG. JOEL TALAVERA, con Cedula de Identidad N° 887.552, denominada en adelante la CONTRATANTE, por una parte, y, por la otra, la firma CORPORATION SEKIURA S.A.C.E.I. con RUC N° 80070889-0, domiciliada en Avda. Boggiani N° 6212 c/ R.I. 5 General Diaz, en la Ciudad de Asunción, Capital de la República del Paraguay, representada para este acto por NELIDA RAFAELA APONTE DE FISCHER con Cedula de Identidad N° 397.359, denominada en adelante el PROVEEDOR, denominadas en conjunto "LAS PARTES" e, individualmente, "PARTE", acuerdan celebrar el presente CONTRATO PARA LA "RENOVACION DE LICENCIAS VARIAS (KASPERSKY, WILDCARD SSL, GSUITE, FORTINET)" con ID N° 406.608, el cual estará sujeto a las siguientes clausulas y condiciones:

### 1. OBJETO.

El presente contrato tiene por objeto regular los derechos y obligaciones de las partes con relación a la contratación de la empresa que resultara adjudicada para la LICITACION POR CONCURSO DE OFERTAS N° 01/2022 PARA LA ADQUISICIÓN DE LICENCIA VARIAS (KASPERSKY, WILDCARD SSL, GSUITE, FORTINET) ID N° 406.608.

### 2. DOCUMENTOS INTEGRANTES DEL CONTRATO.

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

- Contrato;
- El pliego de bases y condiciones y sus adendas o modificaciones;
- Los datos cargados en el SICP;
- La oferta del proveedor;
- 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 diferencia entre los mismos, la prioridad de los mismos será en el orden enunciado anteriormente.

### 3. DOCUMENTOS ADICIONALES DEL CONTRATO.

Los documentos adicionales del contrato son: No aplica

### 4. IDENTIFICACION DEL CREDITO 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° 406.608.

  
  
CORPORATION  
**SEKIURA**  
S.A.C.E.I.  
RUC N° 80070889-0

  
Abg. Joel E. Talavera Z.  
Director Nacional  
Dirección Nacional de Propiedad Intelectual





## 5. PROCEDIMIENTO DE CONTRATACION.

El presente contrato es el resultado del procedimiento de Licitación por Concurso de Ofertas LCO N° 01/2022, convocado por la DIRECCION NACIONAL DE PROPIEDAD INTELECTUAL. La adjudicación fue realizada según Resolución DINAPI N° 100/2022.

## 6. PRECIO UNITARIO Y EL IMPORTE TOTAL A PAGA POR LOS BIENES y/o SERVICIOS.

Ítem	Código	Descripción del Bien	U.M	Cant.	PROCEDENCIA	MARCA	Precio Unitario (IVA incluido)	Precio Total
1	43231512-9992	RENOVACION DE LICENCIAS DE SOFTWARE ANTIVIRUS "KASPERSKY TOTAL SECURITY FOR BUSSINES" POR 2 AÑOS	UNIDAD	250	SUIZA	KASPERSKY	400.000	100.000.000
MONTO TOTAL								GS. 100.000.000

El monto total del presente contrato asciende a la suma de **GUARANIES CIEN MILLONES (GS. 100.000.000)**

## 7. VIGENCIA DEL CONTRATO.

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

## 8. PLAZO, LUGAR Y CONDICIONES DE LA PROVISION DE BIENES.

Los bienes y/o servicios deben ser entregados dentro de los plazos establecidos en el Cronograma de Entregas del Pliego de Bases y condiciones.

## 9. ADMINISTRACION DEL CONTRATO.


La Administración del contrato estará a cargo de: DIRECCION DE INFORMATICA.

## 10. FORMA Y TERMINOS PARA GARANTIZAR EL CUMPLIMIENTO DEL CONTRATO.

La garantía para el fiel cumplimiento del contrato se registrará 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.

## 11. CONSTANCIA DE PRESENTACION DE DECLARACION JURADA

El adjudicado deberá en el plazo de quince (15) días calendario desde la firma del presente contrato, presentar ante el administrador del contrato, la constancia o constancias de presentación de Declaración Jurada de bienes y rentas, activos y pasivos ante la Contraloría General de la Republica, de todos los sujetos obligados en el marco de la Ley N° 6355/19.

  
 **SEKURA**  
S.A.C.E.I.  
RUC N° 80670889-0

Abg. Joel E. Talavera Z.  
Director Nacional  
Dirección Nacional de Propiedad Intelectual  
Página 2 de 11





En el mismo plazo indicado en el párrafo anterior, se deberá remitir a la convocante la actualización de la mencionada declaración jurada, una vez finalizada la ejecución del presente contrato.

## **12. MULTAS.**

Las multas y otras penalidades que rigen en el presente contrato serán aplicadas conforme a lo establecido en las Condiciones Contractuales del presente Pliego. Llegado el 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° 2051/03 "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° 2051/03 "De Contrataciones Públicas", modificado por Ley N° 6716/2021".

## **13. CAUSALES Y PROCEDIMIENTOS PARA SUSPENDER TEMPORALMENTE, DAR POR TERMINADO ANTICIPADAMENTE O RESCINDIR EL CONTRATO.**

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° 2051/03, y en las Condiciones Contractuales del presente Pliego de Bases y Condiciones.


## **14. SOLUCION DE CONTROVERSIAS.**

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

## **15. ANULACION DE ADJUDICACION.**

Si la Dirección Nacional de Contrataciones Públicas resolviera anular la adjudicación de la Contratación debido a la procedencia de una protesta o una investigación 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 afectado por la nulidad quedara 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 dos (2) ejemplares de un mismo tenor y a un solo efecto en la Ciudad de Asunción, República del Paraguay, a los 07 días del mes de abril de 2022.



Nelida Aponte de Fischer  
Representante Legal  
Corporation Sekiura  
S.A.C.E.I.



ABG. Joel Talavera  
Director Nacional  
Dirección Nacional de Propiedad Intelectual





**ANEXO N° 01 AL CONTRATO N° 02/2022**

El Suministro deberá incluir todos aquellos ítems que no hubiesen sido expresamente indicados en la presente sección, pero que pueda inferirse razonablemente que son necesarios para satisfacer el requisito de suministro indicado, por lo tanto, dichos bienes y servicios serán suministrados por el Proveedor como si hubiesen sido expresamente mencionados, salvo disposición contraria en el Contrato.

Los bienes y servicios suministrados deberán ajustarse a las especificaciones técnicas y las normas estipuladas en este apartado. En caso de que no se haga referencia a una norma aplicable, la norma será aquella que resulte equivalente o superior a las normas oficiales de la República del Paraguay. Cualquier cambio de dichos códigos o normas durante la ejecución del contrato se aplicará solamente con la aprobación de la contratante y dicho cambio se registrará de conformidad a la cláusula de adendas y cambios.

El Proveedor tendrá derecho a rehusar responsabilidad por cualquier diseño, dato, plano, especificación u otro documento, o por cualquier modificación proporcionada o diseñada por o en nombre de la Contratante, mediante notificación a la misma de dicho rechazo.

**1. ESPECIFICACIONES TECNICAS**

**Ítem 1 - Kaspersky Total Security for Business**

Ítem	Descripción	Cantidad	U.M
1	Renovación de Antivirus Kaspersky Total Security for Business 2 años. Con instalación, configuración, capacitación y soporte técnico.	250	UNIDAD

Descripción	Requerimientos Mínimos Exigidos
Protección multicapa para estaciones de trabajo	Con tecnologías basadas en el análisis de firmas, la heurística, el análisis de comportamiento y eventualmente servicios de nube. Defensas multicapa para cualquier combinación de estaciones de trabajo Windows, Mac y Linux. Herramientas de Control de aplicaciones, Control de dispositivos y Control web. Protección para servidores de archivos Windows y Linux.
Detección de vulnerabilidades y distribución de parches automáticas	Análisis automático de vulnerabilidades y distribución automática de parches para identificar las vulnerabilidades conocidas de la red y aplicar parches.
Prevención contra la pérdida de datos confidenciales	Cifrado de datos para asegurar archivos, carpetas, discos y dispositivos extraíbles para prevención de la fuga de datos confidenciales. Cifrado de datos de fácil configuración y administración. Opciones de prevención de pérdida de datos basada en contenidos.

*Nélicia R. Spoute de Fischer*





Descripción	Requerimientos Mínimos Exigidos
Protección de dispositivos móviles	Seguridad móvil y capacidades de administración de dispositivos móviles y administración de aplicaciones móviles para protección de los teléfonos inteligentes y tablets, así como los sistemas y datos corporativos a los que tienen acceso. Deben ser compatibles con las plataformas móviles más populares como Android, iOS y Windows Phone, Windows Mobile, BlackBerry, Symbian.
Administración de los recursos de TI	Funciones de administración de sistemas, para reducir la complejidad de administración tanto la seguridad como los sistemas. Automatizar tareas de seguridad y administración, con una única consola de administración. Protección de correo electrónico Análisis de seguridad y filtrado inteligentes de spam para protección del tráfico de correo, bloqueo de más mensajes no deseados evitando al máximo los falsos positivos y reducción del volumen de tráfico en la red corporativa.
Protección del tráfico web	Protección del tráfico de las principales puertas de enlace web con Windows o Linux. Borrando de manera automática programas maliciosos y potencialmente peligrosos del tráfico de datos que ingresa a la red local por medio de protocolos HTTP, HTTPS, FTP, POP3 y SMTP. Con sistema de generación de informes.
Gestión de sistemas y seguridad centralizada	Gestión de sistemas y seguridad centralizada: Consola de administración integrada, para proporcionar control centralizado sobre todas las tecnologías de seguridad de terminales. Actualizaciones por 24 meses. El oferente deberá realizar la actualización de versión en la consola de administración centralizada con todos los módulos solicitados, y despliegue en equipos. Deberá realizar esta actualización y/o revisión del estado de la consola como mínimo una vez por año durante la vigencia del contrato. Y deberá presentar un informe cada año de los trabajos y/o revisiones realizadas. Para lo cual deberá contar como mínimo con personal calificado en la solución ofertada; <ul style="list-style-type: none"><li>Al menos dos profesionales con certificación Kaspersky System Engineer</li><li>Al menos un profesional con certificación Kaspersky Professional: Encryption</li><li>Al menos un profesional con certificación Kaspersky Professional: Systems Management</li><li>Al menos dos profesionales con certificación Kaspersky Endpoint Security Associate</li></ul> A fin de garantizar la correcta implementación y mejores prácticas de seguridad el oferente deberá contar con profesionales certificados en las siguientes áreas como mínimo considerando que la institución tiene estas soluciones implementadas. <ul style="list-style-type: none"><li>Microsoft Certified Solutions Associate Windows Server 2016. Superior o equivalente. Al menos un profesional</li></ul>
Características	Se debe acceder a la consola vía WEB (HTTPS) o MMC; Compatibilidad con Windows FailoverClustering u otra solución de alta disponibilidad Capacidad de eliminar remotamente cualquier solución antivirus (propia o de terceros) que esté presente en las estaciones y servidores, sin la necesidad de la





Descripción	Requerimientos Mínimos Exigidos
	<p>contraseña de remoción del actual antivirus;</p> <p>Capacidad de instalar remotamente la solución de antivirus en las estaciones y servidores Windows, a través de la administración compartida, login script y/o GPO de Active Directory;</p> <p>Capacidad de instalar remotamente la solución de seguridad en smartphones y Android, utilizando estaciones como intermediarias;</p> <p>Capacidad de instalar remotamente la solución de seguridad en smartphones y tablets de sistema iOS;</p> <p>Capacidad de instalar remotamente cualquier app en smartphones y tablets de sistema iOS;</p> <p>Capacidad de gestionar estaciones de trabajo y servidores de archivos (tanto Windows como Linux y Mac) protegidos por la solución antivirus;</p> <p>Capacidad de gestionar smartphones y tablets (tanto Symbian como Windows Mobile, BlackBerry, Android y iOS) protegidos por la solución antivirus;</p> <p>Capacidad de generar paquetes personalizados (autoejecutables) conteniendo la licencia y configuraciones del producto;</p> <p>Capacidad de actualizar los paquetes de instalación con las últimas vacunas, para que cuando el paquete sea utilizado en una instalación ya contenga las últimas vacunas lanzadas;</p> <p>Capacidad de hacer distribución remota de cualquier software, o sea, debe ser capaz de remotamente enviar cualquier software por la estructura de gerenciamento de antivirus para que sea instalado en las máquinas clientes;</p> <p>Capacidad de desinstalar remotamente cualquier software instalado en las máquinas clientes;</p> <p>Capacidad de aplicar actualizaciones de Windows remotamente en las estaciones y servidores;</p> <p>Capacidad de importar la estructura de Active Directory para encontrar máquinas;</p> <p>Capacidad de monitorear diferentes subnets de red con el objetivo de encontrar máquinas nuevas para que sean agregadas a la protección;</p> <p>Capacidad de monitorear grupos de trabajos ya existentes y cualquier grupo de trabajo que sea creado en la red, a fin de encontrar máquinas nuevas para ser agregadas a la protección;</p> <p>Capacidad de, al detectar máquinas nuevas en el Active Directory, subnets o grupos de trabajo, automáticamente importar la máquina a la estructura de protección de la consola y verificar si tiene el antivirus instalado. En caso de no tenerlo, debe instalar el antivirus automáticamente;</p> <p>Capacidad de agrupamiento de máquinas por características comunes entre ellas, por ejemplo: agrupar todas las máquinas que no tengan el antivirus instalado, agrupar todas las máquinas que no recibieron actualización en los últimos 2 días, etc.;</p> <p>Capacidad de definir políticas de configuraciones diferentes por grupos de estaciones, permitiendo que sean creados subgrupos y con función de herencia de políticas entre grupos y subgrupos;</p> <p>Debe proporcionar las siguientes informaciones de las computadoras:</p>





Descripción	Requerimientos Mínimos Exigidos
	<ul style="list-style-type: none"><li>• Si el antivirus está instalado;</li><li>• Si el antivirus ha iniciado;</li><li>• Si el antivirus está actualizado;</li><li>• Minutos/horas desde la última conexión de la máquina con el servidor administrativo;</li><li>• Minutos/horas desde la última actualización de vacunas</li><li>• Fecha y horario de la última verificación ejecutada en la máquina;</li><li>• Versión del antivirus instalado en la máquina;</li><li>• Si es necesario reiniciar la computadora para aplicar cambios;</li><li>• Fecha y horario de cuando la máquina fue encendida;</li><li>• Cantidad de virus encontrados (contador) en la máquina;</li><li>• Nombre de la computadora;</li><li>• Dominio o grupo de trabajo de la computadora;</li><li>• Fecha y horario de la última actualización de vacunas;</li><li>• Sistema operativo con Service Pack;</li><li>• Cantidad de procesadores;</li><li>• Cantidad de memoria RAM;</li><li>• Usuario(s) conectados en ese momento, con información de contacto (si están disponibles en el Active Directory)</li><li>• Dirección IP;</li><li>• Aplicativos instalados, inclusive aplicativos de terceros, con historial de instalación, conteniendo fecha y hora que el software fue instalado o removido.</li><li>• Actualizaciones de Windows Updates instaladas</li><li>• Información completa de hardware conteniendo: procesadores, memoria, adaptadores de video, discos de almacenamiento, adaptadores de audio, adaptadores de red, monitores, drives de CD/DVD</li><li>• Vulnerabilidades de aplicativos instalados en la máquina</li></ul> <p>Debe permitir bloquear las configuraciones del antivirus instalado en las estaciones y servidores de manera que el usuario no consiga modificarlas;</p> <p>Capacidad de reconectar máquinas clientes al servidor administrativo más próximo, basado en reglas de conexión como:</p> <ul style="list-style-type: none"><li>• Cambio de gateway;</li><li>• Cambio de subnet DNS;</li><li>• Cambio de dominio;</li><li>• Cambio de servidor DHCP;</li><li>• Cambio de servidor DNS;</li><li>• Cambio de servidor WINS;</li><li>• Aparición de nueva subnet;</li></ul> <p>Capacidad de configurar políticas móviles para que cuando una computadora cliente esté fuera de la estructura de protección pueda actualizarse vía internet;</p> <p>Capacidad de instalar otros servidores administrativos para balancear la carga y optimizar el tráfico de enlaces entre sitios diferentes;</p> <p>Capacidad de interrelacionar servidores en estructura de jerarquía para obtener informes sobre toda la estructura de antivirus;</p> <p>Capacidad de herencia de tareas y políticas en la estructura jerárquica de servidores administrativos;</p>

*Nelida R. Aponte de Fischer*



*Abg. José E. Talavera Z.*  
Director Nacional  
Dirección Nacional de Propiedad Intelectual





Descripción	Requerimientos Mínimos Exigidos
	<p>Capacidad de elegir cualquier computadora cliente como repositorio de vacunas y de paquetes de instalación, sin que sea necesario la instalación de un servidor administrativo completo, donde otras máquinas clientes se actualizarán y recibirán paquetes de instalación, con el fin de optimizar el tráfico de red;</p> <p>Capacidad de hacer de este repositorio de vacunas un gateway para conexión con el servidor de administración, para que otras máquinas que no logran conectarse directamente al servidor puedan usar este gateway para recibir y enviar informaciones al servidor administrativo.</p> <p>Capacidad de exportar informes para los siguientes tipos de archivos: PDF, HTML y XML.</p> <p>Capacidad de generar traps SNMP para monitoreo de eventos;</p> <p>Capacidad de enviar correos electrónicos para cuentas específicas en caso de algún evento;</p> <p>Debe tener compatibilidad con Microsoft NAP, cuando se instale en Windows 2008 Server;</p> <p>Debe tener compatibilidad con Cisco Network Admission Control (NAC);</p> <p>Debe tener documentación de la estructura del banco de datos para generación de informes a partir de herramientas específicas de consulta (Crystal Reports, por ejemplo).</p> <p>Capacidad de conectar máquinas vía Wake on Lan para realización de tareas (barrido, actualización, instalación, etc.), inclusive de máquinas que estén en subnets diferentes del servidor);</p> <p>Capacidad de habilitar automáticamente una política en caso de que ocurra una epidemia en la red (basado en cantidad de virus encontrados en determinado intervalo de tiempo);</p> <p>Capacidad de realizar actualización incremental de vacunas en las computadoras clientes;</p> <p>Capacidad de reportar vulnerabilidades de software presentes en las computadoras.</p> <p>Capacidad de realizar inventario de hardware de todas las máquinas clientes;</p> <p>Capacidad de realizar inventario de aplicativos de todas las máquinas clientes;</p> <p>Capacidad de diferenciar máquinas virtuales de máquinas físicas;</p>
Cifrado	<p>Características: El acceso al recurso cifrado (archivo, carpeta o disco) debe ser garantizado aún en caso de que el usuario haya olvidado la contraseña, a través de procedimientos de recuperación.</p> <ul style="list-style-type: none"><li>• Utilizar, como mínimo, un algoritmo AES con clave de 256 bits.</li><li>• Capacidad de cifrar completamente el disco duro de la máquina, agregando un ambiente de preboot para autenticación del usuario.</li><li>• Capacidad de utilizar <b>Single Sign-On</b> para la autenticación de preboot.</li><li>• Permitir crear varios usuarios de autenticación preboot.</li><li>• Capacidad de crear un usuario de autenticación preboot común con una contraseña igual para todas las máquinas a partir de la consola de manejo.</li><li>• Capacidad de cifrar drives extraíbles de acuerdo con una regla creada por el administrador, con las opciones:<ul style="list-style-type: none"><li>○ Cifrar solamente los archivos nuevos que sean copiados para el</li></ul></li></ul>





Descripción	Requerimientos Mínimos Exigidos
	<p>disco extraíble, sin modificar los archivos ya existentes.</p> <ul style="list-style-type: none"><li>○ Cifrar todos los archivos individualmente.</li><li>○ Cifrar el dispositivo entero, de manera que no sea posible listar los archivos y carpetas almacenadas.</li><li>○ Cifrar el dispositivo en modo portátil, permitiendo acceder a los archivos en máquinas de terceros a través de una contraseña.</li></ul> <ul style="list-style-type: none"><li>• Capacidad de seleccionar carpetas y archivos (por tipo, o extensión) para ser cifradas automáticamente. En esta modalidad, los archivos deben estar accesibles para todas las máquinas gestionadas por la misma consola de manera transparente para los usuarios.</li><li>• Capacidad de crear reglas de exclusiones para que ciertos archivos o carpetas nunca sean cifrados.</li><li>• Capacidad de seleccionar aplicaciones que pueden o no tener acceso a los archivos cifrados</li></ul>
Gerenciamiento de Sistemas	<p>Capacidad de crear imágenes de sistema operativo remotamente y distribuir esas imágenes para computadoras gestionadas por la solución y para computadoras bare-metal.</p> <p>Capacidad de detectar software de terceros vulnerables, creando así un informe de software vulnerable.</p> <p>Capacidad de corregir las vulnerabilidades de software, haciendo el download centralizado de la corrección o actualización y aplicando esa corrección o actualización en las máquinas gestionadas de manera transparente para los usuarios.</p> <p>Contar con tecnología de Control de Admisión de Red (NAC), con la posibilidad de crear reglas de qué tipos de dispositivos pueden tener accesos a recursos de la red.</p> <p>Capacidad de gestionar licencias de software de terceros.</p> <p>Capacidad de registrar cambios de hardware en las máquinas gestionadas.</p> <p>Capacidad de gestionar un inventario de hardware, con la posibilidad de registro de dispositivos (ej.: router, switch, proyector, accesorio, etc.), informando fecha de compra, lugar donde se encuentra, service tag, número de identificación y otros.</p>
Servidores de gateway	<p>Características:</p> <ul style="list-style-type: none"><li>• Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora.</li><li>• Capacidad de verificar tráfico HTTP 1.0 y 1.1 (RFC 2616), FTP (RFC 959, 2389, Extensiones para FTP) y FTP sobre HTTP;</li><li>• Capacidad de definir listas de tipos de objetos que no serán verificados;</li><li>• Capacidad de definir listas de servidores a los cuales no se les verificará el tráfico;</li><li>• Capacidad de crear grupos de usuarios y aplicar reglas de verificación por grupos;</li><li>• Capacidad de iniciar varias copias del proceso de antivirus;</li><li>• Capacidad de elegir el tamaño reservado en la memoria para almacenamiento de los archivos que serán verificados;</li><li>• Capacidad de elegir el tamaño del buffer del archivo que será verificado;</li><li>• Capacidad de elegir el número máximo de objetos en la fila de verificación;</li><li>• Capacidad de definir el tiempo máximo de verificación de un objeto;</li></ul>

*Nelida R. Aponte de Fischer*





Descripción	Requerimientos Mínimos Exigidos
Servicios que deben ser incluidos	<p>Compatibilidad:</p> <ul style="list-style-type: none"><li>• Windows 10</li><li>• Windows 8.1</li><li>• Windows 8</li><li>• Windows 7 todas las versiones, Service Pack 1 o superior</li></ul>
Adicionales	<ul style="list-style-type: none"><li>• Contar como mínimo con 3 ingenieros certificados con las certificaciones avanzadas del producto</li><li>• contar como mínimo con 2 técnicos con certificaciones de cifrado</li><li>• Contar con por lo menos 2 técnicos con certificaciones en protección de servidores de correo antispam</li><li>• Los técnicos certificados deben ser personales dependientes de la Empresa Oferente, se deben acompañar certificados de inscripción en IPS</li><li>• contar como mínimo con 3 ingenieros con certificaciones ITIL para garantizar la buena asistencia en soporte técnico.</li><li>• contar con al menos 10 contratos o facturas de la provisión del Software ofertado entre los años 2019, 2020 y 2021.</li><li>• Implementación de todos los módulos de la herramienta en todo el parque de equipos.</li><li>• capacitación de la herramienta a todas las personas involucradas en el departamento de tecnología.</li><li>• soporte técnico incluido durante todo el periodo de licenciamiento.</li><li>• cantidad de tickets de soporte ilimitados.</li><li>• El proveedor deberá ser Canal Platinum de la Marca ofertada, para garantizar el buen servicio y respaldo del soporte local, para ello deberá presentar el certificado que los vale.</li><li>• El proveedor deberá tener la Certificación ISO 9001 Sistema de Gestión de Calidad y la Certificación ISO 27001 Sistema de Gestión de Seguridad de la Información para garantizar el buen servicio y respaldo del soporte local.</li><li>• El proveedor deberá presentar con su oferta una Carta de autorización del fabricante expresamente dirigido a la convocante refiriendo el nro. de ID del llamado</li><li>• El proveedor deberá contar con una plataforma y/o sistema de ticket para atención de casos de soporte técnico, a fin de garantizar la respuesta de manera profesional y organizada.</li><li>• El proveedor local deberá contar con una plataforma de autoservicio de preguntas frecuentes, con por lo menos 50 plantillas de respuesta para esos casos, dicha plataforma deberá estar integrada con el sistema del ticket del proveedor</li><li>• La convocante podrá solicitar si cree necesario a los oferentes una demostración del manejo y despliegue de la herramienta</li></ul>

Abg. Joel E. Talavera Z.  
Director Nacional  
Dirección Nacional de Propiedad Intelectual

*Helio R. Aponte de Fischer*  
**SEKURA**  
S.A.C.E.I.  
RUC N° 80070889-0





## 2. PLAN DE ENTREGA DE BIENES

La entrega de los bienes se realizará de acuerdo al plan de entrega y cronograma de cumplimiento, indicado en el presente apartado. Así mismo, de los documentos de embarque y otros que deberá suministrar el proveedor indicado a continuación:

Ítem	Descripción del bien	Cantidad	Unidad de medida	Lugar de entrega de los bienes	Fecha(s) final(es) de entrega de los bienes
1	Renovación de Licencias de Software Antivirus Kaspersky Total Security for Business" POR 2 AÑOS	250	UNIDAD	DINAPI sito en Avda. España 323 casi EEUU	3 (tres) días hábiles a partir de la recepción de la orden de compra/servicio

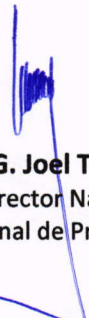
## 3. INDICADORES DE CUMPLIMIENTO

Planificación de indicadores de cumplimiento:

INDICADOR	TIPO	FECHA DE PRESENTACIÓN PREVISTA (se indica la fecha que debe presentar según el PBC)
Nota de Remisión / Acta de recepción 1	Nota de Remisión / Acta de recepción	El plazo de entrega será conforme a la Orden de Compra emitido y entregado al Proveedor

  
**Nelida Aponte de Fischer**  
Representante Legal  
Corporation Sekiura  
S.A.C.E.I.



  
**ABG. Joel Talavera**  
Director Nacional  
Dirección Nacional de Propiedad Intelectual