AGENCIA NACIONAL DE EVALUACIÓN Y ACREDITACIÓN DE LA EDUCACIÓN SUPERIOR (ANEAES)

CONTRATO Nº 09/2020

CONTRATACIÓN DIRECTA (CD) Nº 06/2020
"ADQUISICIÓN DE LICENCIAS ANTIVIRUS CORPORATIVOS - ID Nº 382.941" con la empresa ITCS S.A.

Entre la **Agencia Nacional de Evaluación y Acreditación de la Educación Superior (ANEAES)**, domiciliada en Yegros Nº 930 entre Manuel Domínguez y Tte. Fariña, República del Paraguay, representado para este acto por el **Dr. RAÚL AGUILERA MÉNDEZ**, con Cédula de Identidad Civil Nº 893.275, en su carácter de Representante y Presidente del Consejo Directivo de la Agencia de Evaluación y Acreditación de la Educación Superior, según consta en el Acta de sesión del Consejo Directivo Nº 18, de fecha 21 de agosto de 2017, denominada en adelante la **AGENCIA**, por una parte, y, por la otra, la firma **ITCS S.A.** con **RUC Nº 80046953-4**, domiciliada en las calles Marcelino Noutz Nº 861 entre Sargento Gauto y Luis de Granada, de la ciudad de Asunción, República del Paraguay, representado para este acto por el **Sr. CESAR ROMEO ACOSTA FORMOSO**, con Cédula de Identidad Civil Nº 3.298.115, denominada en adelante el **PROVEEDOR**, denominadas en conjunto "LAS PARTES" e, individualmente, "PARTE", acuerdan celebrar el presente contrato de **"ADQUISICIÓN DE LICENCIAS ANTIVIRUS CORPORATIVOS"**, el cual estará sujeto a las siguientes cláusulas y condiciones:

1. OBJETO:
El presente Contrato tiene por objeto la adquisición de licencias antivirus corporativos para la **AGENCIA**, a cargo y riesgo del **PROVEEDOR** de conformidad con las especificaciones técnicas contenidas en la Carta de Invitación respectiva y a las disposiciones de este Contrato; y establecer los demás derechos y obligaciones de **LAS PARTES**.

2. DOCUMENTOS INTEGRANTES DEL CONTRATO:
Los documentos contractuales firmados por las partes y que forman parte integral del Contrato son los siguientes:

a) Contrato;
b) La carta de Invitación y sus Adendas o modificaciones;
c) Los datos cargados en el SICP;
d) La oferta del proveedor;
e) La resolución de adjudicación del contrato emitida por la convocante y su respectiva notificación;

Raúl Aguilera Méndez, Dr.
Presidente del Consejo Directivo ANEAES
Ordenador de Gastos

Cesar Acosta
Director
ITCS S.A.

Yegros N° 930 entre Manuel Domínguez y Tte. Fariña
Asunción - Paraguay
Telefax: +595 21 494-940
E-mail: uoc@aneaes.gov.py

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: las **especificaciones técnicas**.

4. 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° 382.941.**

5. PROCEDIMIENTO DE CONTRATACIÓN:

El presente Contrato es el resultado del procedimiento de **Contratación Directa (CD) N° 06/2020**, convocado por la **Coordinación de Contrataciones de la ANEAES**. La adjudicación fue realizada según **Resolución N° 174/2020** de fecha de 22 de julio de 2020.

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

Actividad: 1

ADQUISICIÓN DE LICENCIAS ANTIVIRUS CORPORATIVOS - CD N° 06/2020 - ID N° 382.941						ITCS S.A.			
Ítem	**Código catálogo**	**Descripción de los bienes**	**Unidad de medida**	**Presentación**	**Cant.**	**Marca**	**Procedencia**	**Precio unitario (IVA incluido)**	**Precio total (IVA incluido)**
1	43233205-001	Licencia antivirus corporativo para estaciones de trabajo.	Unidad	Unidad	60	Sophos	E.E.U.U.	221,250	13,275,000
2	43233205-005	Licencia antivirus corporativo para equipos servidores.	Unidad	Unidad	5	Sophos	E.E.U.U.	433,250	2,166,250
								Precio Total:	**15,441,250**

Raúl Apuliera Méndez, Dr.
Presidente del Consejo Directivo ANEAES
Ordenador de Gastos

Cesar Acosta
Director
ITCS S.A.

Yegros N° 930 entre Manuel Domínguez y Tte. Fariña
Asunción - Paraguay
Telefax: +595 21 494-940
E-mail: uoc@aneaes.gov.py

Actividad: 2

ADQUISICIÓN DE LICENCIAS ANTIVIRUS CORPORATIVOS - CD Nº 06/2020 - ID Nº 382.941						ITCS S.A.			
Ítem	Código catálogo	Descripción de los bienes	Unidad de medida	Presentación	Cant.	Marca	Procedencia	Precio unitario (IVA incluido)	Precio total (IVA incluido)
1	43233205-001	Licencia antivirus corporativo para estaciones de trabajo.	Unidad	Unidad	60	Sophos	E.E.U.U.	221,250	13,275,000
2	43233205-005	Licencia antivirus corporativo para equipos servidores.	Unidad	Unidad	5	Sophos	E.E.U.U.	433,250	2,166,250
								Precio Total:	**15,441,250**

El monto total del presente contrato asciende a la suma de **guaraníes treinta millones ochocientos ochenta y dos mil quinientos.**

El **PROVEEDOR** se compromete a proveer el bien y los servicios a la **AGENCIA** y a subsanar los defectos de éstos de conformidad a las disposiciones del Contrato.

La **AGENCIA** se compromete a pagar al **PROVEEDOR** como contrapartida del servicio y la subsanación de sus defectos, el Precio del Contrato o las sumas que resulten pagaderas de conformidad con lo dispuesto en la Carta de Invitación.

Los pagos serán efectuados a través de la Dirección General de Administración y Finanzas (DGAF) de la **AGENCIA**, de acuerdo al plan de caja asignado por el Ministerio de Hacienda una vez que el proveedor haya presentado la factura por las provisiones efectuadas.

La moneda de pago será en todos los casos y sin excepción alguna en guaraníes a los efectos de este contrato en aplicación del Art. 41 de la Ley Nº 3439/07 "Que modifica la Ley Nº 2051/03 *"De Contrataciones Públicas"* y que establece la carta orgánica de la Dirección Nacional de Contrataciones Públicas", se retendrá el 0,4% sobre el importe de cada factura, deducido los impuestos correspondientes que presente al cobro, el Proveedor. El plazo de pago de factura al proveedor será de 60 días que será computado a partir de la presentación de la factura en la Dirección Administrativa de la Agencia.

7. VIGENCIA DEL CONTRATO:
El plazo de vigencia de este Contrato será desde la suscripción del mismo hasta el cumplimiento total de las obligaciones.

8. PLAZO, LUGAR Y CONDICIONES DE LA PROVISIÓN DE SERVICIOS:
Los bienes deben ser entregados dentro del plazo establecido, según se detalla:

Raúl Aguilera Méndez, Dr.
Presidente del Consejo Directivo ANEAES
Ordenador de Gastos

César Acosta
Director
ITCS S.A.

Yegros N° 930 entre Manuel Domínguez y Tte. Fariña
Asunción - Paraguay
Telefax: +595 21 494-940
E-mail: uoc@aneaes.gov.py

Ítem	Descripción de los bienes	Cantidad	Unidad de medida	Lugar de entrega de los bienes	Fecha(s) final(es) de entrega de los bienes
1	Licencia antivirus corporativo para estaciones de trabajo.	120	Unidad	En oficinas de la ANEAES, sito en las calles Yegros N° 930 entre Manuel Domínguez y Tte. Fariña o donde la Agencia disponga.	Los bienes deben ser entregados dentro de los 10 (diez) días corridos, contados a partir de la recepción de la orden de compra por la empresa adjudicada.
2	Licencia antivirus corporativo para equipos servidores.	10	Unidad		

Así mismo, el documento requerido para acreditar el cumplimiento contractual será: la nota de remisión total.
Frecuencia: única vez.

Planificación de indicadores de cumplimiento:

INDICADOR	TIPO	FECHA DE PRESENTACIÓN PREVISTA
Nota de Remisión / Acta de recepción.	Nota de Remisión / Acta de recepción.	Dentro de los 10 (diez) días corridos, contados a partir de la recepción de la orden de compra por la empresa adjudicada.

De manera a establecer indicadores de cumplimiento, a través del sistema de seguimiento de contratos, la convocante deberá determinar el tipo de documento que acredite el efectivo cumplimiento de la ejecución del contrato, así como planificar la cantidad de indicadores que deberán ser presentados durante la ejecución. Por lo tanto, la convocante en este apartado y de acuerdo al tipo de contratación de que se trate, deberá indicar el documento a ser comunicado a través del módulo de Seguimiento de Contratos y la cantidad de los mismos.

9. ADMINISTRACIÓN DEL CONTRATO:

La administración del contrato estará a cargo del Departamento TIC´s de la ANEAES en coordinación con la Dirección de Administrativa.

10. FORMA Y TÉRMINOS PARA GARANTIZAR EL CUMPLIMIENTO DEL CONTRATO:

La garantía para el fiel cumplimiento del contrato se regirá por lo establecido en la Carta de Invitación, la cual se presentará a más tardar dentro de los 10 (días) calendario siguiente a la firma del contrato.

11. CONSTANCIA DE PRESENTACIÓN DE DECLARACIÓN JURADA:

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

Raúl Aguilera Méndez, Dr.
Presidente del Consejo Directivo ANEAES
Ordenador de Gastos

Cesar Acosta
Director
ITCS S.A.

Yegros N° 930 entre Manuel Domínguez y Tte. Fariña
Asunción - Paraguay
Telefax: +595 21 494-940
E-mail: uoc@aneaes.gov.py

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 la Carta de Invitación y en las Condiciones Generales del Contrato. 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° 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"*.

13. CAUSALES Y PROCEDIMIENTO 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 la Carta de Invitación.

14. SOLUCIÓN DE CONTROVERSIAS:
Cualquier diferencia que surja durante la ejecución de los Contratos se dirimirá conforme las reglas establecidas en la legislación aplicable y en la Carta de Invitación.

15. 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 afectado 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 TESTIMONIO 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 Veintidos días del mes de setiembre del año dos mil veinte.

Sr. CESAR ROMEO ACOSTA FORMOSO
Cédula de Identidad Civil N° 3.298.115
ITCS S.A.

Cesar Acosta
Director
ITCS S.A.

Dr. RAÚL AGUILERA MÉNDEZ
Cédula de Identidad Civil N° 893.275
ANEAES

Raúl Aguilera Méndez, Dr.
Presidente del Consejo
Directivo ANEAES
Ordenador de Gastos

Yegros N° 930 entre Manuel Domínguez y Tte. Fariña
Asunción - Paraguay
Telefax: +595 21 494-940
E-mail: uoc@aneaes.gov.py

Especificaciones Técnicas

SOFTWARE ANTIVIRUS CORPORATIVO PARA ESTACIONES DE TRABAJOS Y EQUIPOS SERVIDORES:

Características	Descripción	Exigencia
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.	Exigido
	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.	Exigido
	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.	Exigido
	Debe poseer un mecanismo de comunicación vía API, para su integración con otras soluciones de seguridad, como por ejemplo SIEM.	Exigido
	La consola debe permitir la división de los ordenadores dentro de la estructura de administración en grupos.	Exigido
	Debe permitir la sincronización con Active Directory (AD) para la gestión de usuarios y grupos integrados en las políticas de protección.	Exigido
	Debe poseer la posibilidad de aplicar reglas diferenciadas por grupos de usuarios, usuarios individuales, grupos de máquinas y equipos individuales.	Exigido
	La instalación debe 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.	Exigido
	Proporcionar actualizaciones del producto y de las definiciones de virus y protección contra intrusos.	Exigido
	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.	Exigido
	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.	Exigido
	Actualización incremental, remota y en tiempo real, de las vacunas de los Antivirus y del mecanismo de verificación (Engine) de los clientes.	Exigido

Raúl Aguilera Méndez, Dr.
Presidente del Consejo Directivo ANEAES
Ordenador de Gastos

Cesar Acosta
Director
UOC S.A.

Tte. Fariña N° 930 entre Manuel Domínguez y Tte. Fariña
Asunción - Paraguay
Telefax: +595 21 494-940
E-mail: uoc@aneaes.gov.py

Características	Descripción	Exigencia
	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.	Exigido
	Utilizar protocolos seguros estándar HTTPS para la comunicación entre la consola de administración y los clientes administrados.	Exigido
	Los mensajes generados por el agente deben estar en el idioma español o permitir su edición.	Exigido
	Permitir la exportación de los informes gerenciales a los formatos CSV y PDF.	Exigido
	Los recursos del informe y el monitoreo deben ser nativos de la propia consola central de administración.	Exigido
	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.	Exigido
	La comunicación debe permitir QoS para controlar el ancho de banda de red.	Exigido
	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.	Exigido
	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.	Exigido
	La Consola de administración debe incluir un panel con un resumen visual en tiempo real para comprobar el estado de seguridad.	Exigido
	Deberá proporcionar filtros pre-construidos que permitan ver y corregir sólo los ordenadores que necesitan atención.	Exigido
	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.	Exigido
	Actualizar de forma automática las directivas de seguridad cuando un equipo se mueve de un grupo a otro.	Exigido
	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.	Exigido

Raúl Aguilera Méndez, Dr.
Presidente del Consejo Directivo ANEAES
Ordenador de Gastos

Cesar Acosta
Director
ITCS S.A.

Yegros N° 930 entre Manuel Domínguez y Tte. Fariña
Asunción - Paraguay
Telefax: +595 21 494-940
E-mail: uoc@aneaes.gov.py

Características	Descripción	Exigencia
	Deberá permitir exportar el informe de registros de auditoría en formatos CSV y PDF.	Exigido
	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.	Exigido
	Permitir la ejecución manual de todos estos informes, así como la programación y envío automático por correo electrónico en los formatos CSV y PDF.	Exigido
	Deberá tener la posibilidad de implementar servidores de caché locales para utilizar de manera eficiente el uso del ancho de banda.	Exigido
	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.	Exigido
	La solución de endpoint, servers, móviles y seguridad perimetral, debe ser administrada desde la misma consola en la nube.	Exigido
	Debe realizar envío automático de alertas críticas mediante correo electrónico a los administradores.	Exigido
	Debe permitir identificar y proteger desde la misma consola instancias de servidores desplegados en AWS.	Exigido
	Debe permitir identificar y proteger desde la misma consola instancias de servidores desplegados en Azure.	Exigido
Capacidad de generación de informes	Detalle de usuarios activos, inactivos o desprotegidos, así como detalles de los mismos.	Exigido
	Detalle de los ordenadores que están activos, inactivos o desprotegidos, así como detalles de las exploraciones y alertas en los ordenadores.	Exigido
	Detalle de los periféricos permitidos o bloqueados, así como detalles de dónde y cuándo se utilizó cada periférico.	Exigido
	Detalle de las principales aplicaciones bloqueadas y los servidores / usuarios que intentaron acceder a ellas.	Exigido
	Detalle de las aplicaciones permitidas que fueron accedidas con mayor frecuencia y los servidores / usuarios que las acceden.	Exigido
	Detalle de los servidores / usuarios que intentaron acceder a aplicaciones bloqueadas con mayor frecuencia y las aplicaciones que ellos intentaron acceder.	Exigido
	Detalle de todas las actividades disparadas por reglas de fuga de información.	Exigido

Raúl Aguilera Méndez, Dr.
Presidente del Consejo Directivo ANEAES
Ordenador de Gasto

Yegros Nº 930 entre Manuel Domínguez y Tte. Fariña
Asunción - Paraguay
Telefax: +595 21 494 940
E-mail: uoc@aneaes.gov.py

Cesar Acosta
Director
ITCS S.A.

Características	Descripción	Exigencia
Idiomas	Inglés.	Exigido
	Español.	Exigido
Opciones de corrección de problemas	Proteger el dispositivo con la opción de inicio de una exploración.	Exigido
	Forzar una actualización en ese momento.	Exigido
	Ver los detalles de los eventos ocurridos.	Exigido
	Ejecutar la comprobación completa del sistema.	Exigido
	Forzar el cumplimiento de una nueva política de seguridad.	Exigido
	Mover el equipo a otro grupo.	Exigido
	Borrar el equipo de la lista.	Exigido
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.	Exigido
	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).	Exigido
	Detección del malware en pre-ejecución y comprobar el comportamiento malicioso para detectar malware desconocido.	Exigido
	Debe realizar la verificación de todos los archivos accedidos en tiempo real, incluso durante el proceso de arranque.	Exigido
	Debe realizar la limpieza del sistema automáticamente, eliminando elementos maliciosos detectados y aplicaciones potencialmente indeseables (PUA).	Exigido
	Debe proteger las funciones críticas en los navegadores de Internet (Safe Browsing).	Exigido
	Debe permitir la autorización de detecciones maliciosas y excluir de la exploración de directorios y archivos específicos.	Exigido
	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).	Exigido
	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.	Exigido

Raúl Aguilera Méndez, Dr.
Presidente del Consejo
Directivo ANEAES
Ordenador de Gastos

César Acosta
Director
ITCS S.A.

Yegros N° 930 entre Manuel Domínguez y Tte. Fariña
Asunción - Paraguay
Telefax: +595 21 494-940
E-mail: uoc@aneaes.gov.py

Características	Descripción	Exigencia
	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.	Exigido
	Permitir la utilización de contraseña de protección para posibilitar la reconfiguración local en el cliente o desinstalación de los componentes de protección.	Exigido
	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.	Exigido
	Debe prevenir el ataque de vulnerabilidades de navegador a través de web exploits.	Exigido
	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.	Exigido
	El control de dispositivos debe estar al nivel de permiso, sólo lectura o bloqueo.	Exigido
	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.	Exigido
	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.	Exigido
	Capacidad de reconocer y bloquear automáticamente las aplicaciones en los clientes basándose en la huella digital (hash) del archivo.	Exigido
	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.	Exigido
	Detectar aplicaciones controladas cuando los usuarios acceden, con las opciones de permitir y alertar o bloquear y alertar.	Exigido
	Debe contar con prevención de intrusión en el host (HIPS), que monitoree el código y bloques de códigos que pueden comportarse de forma maliciosa antes de ser ejecutados.	Exigido
	Control de acceso a sitios web por categoría.	Exigido

Raúl Aguilera Méndez, Dr.
Presidente del Consejo Directivo ANEAES
Ordenador de Gastos

Cesar Acosta
Director
ITCS S.A.

Yegros N° 930 entre Manuel Domínguez y Tte. Fariña
Asunción - Paraguay
Telefax: +595 21 494-940
E-mail: uoc@aneaes.gov.py

Características	Descripción	Exigencia
	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.	Exigido
	La aplicación de políticas de control web, debe contar con capacidad de horarios.	Exigido
	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.	Exigido
	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).	Exigido
	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.	Exigido
	Soportar agregar reglas propias de contenido con un asistente proporcionado para este propósito.	Exigido
	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.	Exigido
	El Agente para servidores debe contemplar monitoreo de integridad de archivos, al menos en servidores Windows.	Exigido
Identificadores de listas CCL preconfiguradas	Números de tarjetas de crédito.	Exigido
	Números de cuentas bancarias.	Exigido
	Números de pasaportes.	Exigido
	Direcciones.	Exigido
	Números de teléfono.	Exigido
	Lista de correos electrónicos.	Exigido
Medios para control de datos	Adjunto en el cliente de correo electrónico.	Exigido
	Adjunto en el navegador.	Exigido
	Adjunto en el cliente de mensajería instantánea.	Exigido
	Adjunto a dispositivos de almacenamiento (al menos USB, CD / DVD).	Exigido
Funcionalidad de detección proactiva de	Protección de amenazas de día 0 a través de tecnología de deep learning (signature less).	Exigido
	Funcionalidad de detección de amenazas desconocidas que están en memoria.	Exigido

Raúl Aguilera Méndez, Dr.
Presidente del Consejo Directivo ANEAES
Ordenador de Gastos

Cesar Acosta
Director
TCS-SA

Yegros N° 930 entre Manuel Domínguez y Tte. Fariña
Asunción - Paraguay
Telefax: +595 21 494-940
E-mail: uoc@aneaes.gov.py

Características	Descripción	Exigencia
reconocimiento de nuevas amenaza	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.	Exigido
	Capacidad de detección y bloqueo de Trojans y Worms, entre otros malwares, por comportamiento de los procesos en memoria.	Exigido
	No debe requerir descarga de firmas de ningún tipo.	Exigido
	Capacidad de analizar el comportamiento de nuevos procesos al ser ejecutados, en complemento a la exploración programada.	Exigido
	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.	Exigido
	Bloqueo y protección contra amenazas desconocidas potencialmente sospechosas (PUA).	Exigido
	Generación de excepciones ante falsos positivos.	Exigido
Funcionalidad de protección contra ransomware	Disponer de capacidad de protección contra ransomware basada en comportamiento.	Exigido
	Disponer de capacidad de remediación de la acción de encriptación de los ransomware.	Exigido
	Capacidad de detección del cifrado malicioso de forma local o remoto.	Exigido
	Debe poseer protección anti-ransomware para el sector de booteo (master boot record).	Exigido
	Debe restaurar automáticamente los archivos cifrados por un proceso malicioso de ransomware.	Exigido
	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.	Exigido
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.	Exigido
	Mitigación de inyección de códigos en procesos.	Exigido
	Protección contra robo de credenciales.	Exigido
	Protección contra malware escondido en aplicaciones legitimas (code cave).	Exigido
	Evitar la migración de procesos maliciosos, evitando que un proceso malicioso migre a otro.	Exigido
	Evitar obtener escalamiento de privilegios.	Exigido
	Modificación de las claves de registro para la ejecución de código arbitrario.	Exigido

Raúl Aguilera Méndez, Dr.
Presidente del Consejo Directivo ANEAES
Ordenador de Gastos

Cesar Acosta
Director
ITCS S.A.

Yegros N° 930 entre Manuel Domínguez y Tte. Fariña
Asunción - Paraguay
Telefax: +595 21 494-940
E-mail: uoc@aneaes.gov.py

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

Raúl Aguilera Méndez, Dr.
Presidente del Consejo Directivo ANEAES
Ordenador de Gastos

César Acosta
Director
ITCS S.A.

Yegros N° 930 entre Manuel Domínguez y Tte. Fariña
Asunción - Paraguay
Telefax: +595 21 494-940
E-mail: uoc@aneaes.gov.py

Características	Descripción	Exigencia
	El cliente para instalación en estaciones de trabajo debe ser compatible con los sistemas operativos Windows 7 en adelante.	Exigido
	El cliente para instalación en servidores debe ser compatible con los sistemas operativos Windows server 2008 en adelante.	Exigido
Sistemas Operativos Linux soportados (en tiempo real)	CentOS 6/7.	Exigido
	Debian 9.	Exigido
	Oracle Linux 6/7.	Exigido
	Red Hat Enterprise Linux 6/7.	Exigido
	SUSE 12/15.	Exigido
	Ubuntu 14/16/18.	Exigido
Autorización	El oferente deberá contar con una autorización del fabricante para presentar la oferta. A su vez, el oferente deberá estar debidamente autorizado por el fabricante para prestar servicio técnico.	Exigido

- **Los equipos objetos de la presente contratación, los potenciales oferentes deberán incluir en su cotización, la Instalación de todos los mismos hasta su puesta en funcionamiento.**

Sr. CESAR ROMEO ACOSTA FORMOSO
Cédula de Identidad Civil N° 3.298.115
ITCS S.A.

Cesar Acosta
Director
ITCS S.A.

Dr. RAÚL AGUILERA MÉNDEZ
Cédula de Identidad Civil N° 893.275
ANEAES

Raúl Aguilera Méndez, Dr.
Presidente del Consejo
Directivo ANEAES
Ordenador de Gastos

Yegros N° 930 entre Manuel Domínguez y Tte. Fariña
Asunción - Paraguay
Telefax: +595 21 494-940
E-mail: uoc@aneaes.gov.py