UNIVERSIDAD TÉCNICA NACIONAL
PROVEEDURÍA INSTITUCIONAL
LICITACIÓN ABREVIADA No. 2016LA-000012-UTN
"ADQUISICIÓN DE LICENCIAS"

ESTIMACIÓN PRESUPUESTARIA: ¢81, 890.000,00

Solicitamos nos remitan la oferta original y una copia; de los materiales que se detallan, en un sobre cerrado y presentarla en la oficina de Contratación en el Edificio de la Administración Universitaria ubicada en Villa Bonita de Alajuela. Cualquier consulta o aclaración se debe hacer por escrito al correo jsolis@utn.ac.cr con copia a vcascante@utn.ac.cr

FECHA DE APERTURA: 24 de Agosto de 2016	**HORA:** 10:00 horas

I. OBJETO DEL CONTRATO

La presente licitación radica en abastecer a la UTN de los programas y licencias esenciales para su adecuado funcionamiento.

II. FISCALIZADOR TÉCNICO DE LA CONTRATACIÓN:

Para la ejecución del objeto de contratación, la Universidad Técnica Nacional designa al área de Aprovisionamiento de la Dirección de Gestión de Tecnologías de la información.

III. CONDICIONES TÉCNICAS

Las ofertas deben de entregarse de conformidad con las especificaciones técnicas que se indican en este cartel y las demás condiciones relacionadas con esta compra.

Línea	Unidad de medida	Cantidad	Descripción	Fecha de activación
1	UNI	4	**Licencia Red Hat Enterprise Virtualization for Servers** (1Socket). Standard 1 year, número de contrato 10512477	23/09/2016
2	UNI	2	**Licencia Red Hat Enterprise Linux Server Premium**(1-2 SOCKETS)(Up To I Guest) smart managment 1 year, número de contrato 10283850	23/09/2016
3	UNI	2,000	**Licencia de anti-virus** • Renovación de licencias eset endpoint segurity (antivirus / antispyware /hips / device control / antispam / firewall personal / web control) • Última versión disponible en el mercado	20/10/2016

			• Debe instalarse y configurarse en las computadoras personales como en los servidores • 2 años de licenciamiento • Demás especificaciones **ver anexo N° 1**	
4	UNI	1,210	**Licencia Académica Microsoft - DsktpEdu ALNG LIcSAPk MVL, Part Number 2UJ-00001** • El proveedor debe ser certificado por Microsoft como LSP y Academic Education Reseller para Costa Rica • Licencia por un año	31/10/2016
5	UNI	16	**Licencia Académica Microsoft - WinSvrStd ALNG LicSAPk MVL 2Proc, P73-05897** • El proveedor debe ser certificado por Microsoft como LSP y Academic Education Reseller para Costa Rica • Licencia por un año	31/10/2016
6	UNI	12	**Licencia Académica Microsoft - SQLSvrStdCore ALNG LicSAPk MVL 2Lic CoreLic, 7NQ-00302** • El proveedor debe ser certificado por Microsoft como LSP y Academic Education Reseller para Costa Rica • Licencia por un año	31/10/2016
7	UNI	2	**Licencia Microsoft - VSPremwMSDN ALNG LicSAPk MVL, 9ED-00071** • El proveedor debe ser certificado por Microsoft como LSP y Academic Education Reseller para Costa Rica • Licencia por un año	31/10/2016
8	UNI	27	**Licencia Adobe Creative Cloud para Mac** • Renovación de licencias del Software Adobe Creative Cloud Complete **por dispositivo** y multiplataforma • Sin almacenamiento en la nube • Para uso en el laboratorio de cómputo utilizado por la carrera de tecnología de la imagen. • Licencia por un año	30/11/2016
9	UNI	1	**Licencia Adobe Creative Cloud para Mac** • Renovación de licencias del Software Adobe Creative Cloud Complete **por usuario** y multiplataforma • Para equipos IMac • Licencia en lenguaje español	30/11/2016

			• Licencia por un año	
10	UNI	1	**Licencia de Portal Académico E-Learning de Microsoft** • Esta licencia permite la suscripción al programa de Microsoft IT Academy, que se puede agregar a cualquiera de los contratos de Licenciamiento por Volumen de Microsoft. • Dicho programa está diseñado para que las instituciones, tengan acceso a los últimos recursos de entrenamiento en tecnología, lo que le permitirá al CFPTE ser un Centro de Certificación internacional. • Además incluye: ✓ Materiales de estudio ✓ Definición de Planes de aprendizaje, asignación de códigos de acceso, administración de usuarios y estudiantes ✓ Planes de estudio para profesores ✓ Portal de 2600 cursos de Elearning ✓ Centro de Certificación de Microsoft ✓ 30 Vouchers de Certificación (10 MOS, 10 MTA, 10 MCE) ✓ Material de Mercadeo ✓ Implementación de plataforma de Certiport ✓ Capacitación para administrador de plataforma ✓ Soporte y acompañamiento en el portal Dreamspark ✓ Descarga del software y pedido de licencias ✓ Horas de capacitación en las herramientas para entrenamiento y certificación • Licencia por un año	30/11/2016
11	UNI	8	**Vsphere Standar Académico** • Licencia Academic VMware vSphere 6 Standard for 1 processor • Licencia por un año	08/12/2016
12	UNI	24	**Soporte Vsphere Standar Académico** • Licencia Academic Basic Support/Subscription for VMware	08/12/2016

			vSphere 6 Standard for 1 processor for 1 year • Soporte para 24 licencias de VSPHERE 6 Standar académico: 8 nuevas y 16 existentes • Se debe actualizar las 16 licencias existentes a versión 6 • Referencias VMware Account: 428535389 y 573869698 • Licencia por un año	
13	UNI	1	**Academic VMware v Center Server Standard for vSphere (Per Instance)** • Actualización a la version 6 • Referencias VMware Account: 428535389 • 1 Instancia • Licencia por un año	08/12/2016
14	UNI	1	**Academic Basic Support/Subscription VMware v Center Server Standard for vSphere (Per Instance)** • Actualizar a la versión 6 • Referencias VMware Account: 428535389 • 1 instancia • Licencia por un año	08/12/2016

Nota importante: El proveedor que participe en las siguientes líneas deberá tomar en cuenta los siguientes requisitos de acatamiento obligatorio:

- Líneas 1 y 2 deberán participar en ambas líneas de este cartel.
- Líneas 4, 5, 6 y 7 deberán participar en las cuatro líneas de este cartel.
- Líneas 11, 12, 13 y 14 deberán participar en las cuatro líneas de este cartel.

a) Lo anterior, debido a que estas líneas deben ser adjudicadas al mismo proveedor, por consiguiente en la evaluación de precios se tomará como monto ofertado la suma de los precios totales de las líneas ya mencionadas.

b) Adicionalmente, es de acatamiento obligatorio que el proveedor que se encuentre interesado en participar en las licencias que van a ser renovadas, deberá respetar las fechas establecidas en el capítulo V de este cartel (Columna Fecha de activación), ya que las mismas comienzan a regir a partir de esa fecha y si no se cumple con ese requisito, la Administración no se verá obligada a realizar el pago de las mismas hasta que se ajusten a estas condiciones (fechas programadas).

IV. CONDICIONES INVARIABLES

1. Vigencia de la oferta:

Las ofertas deberán tener una vigencia no menor de 30 días hábiles. En todo caso de ser necesario se aplicará lo establecido en el artículo 67 del Reglamento a la Ley de Contratación Administrativa.

2. Modalidad y Plazo de entrega

2.1. La entrega de licencias se realizará en línea, a excepción de la línea 3 (Anti-virus) la cual deberá instalarse en la administración universitaria en Villa Bonita de Alajuela.

2.2. Para la instalación o entrega de las licencias deberán coordinar con el señor Guillermo Abarca Quesada al correo electrónico: gabarca@utn.ac.cr, Teléfono: 2630-0704.

3. Requisitos de admisibilidad:

Todos los oferentes deberán cumplir con los siguientes requisitos de admisibilidad:

3.1 Ser distribuidor autorizado de la marca de la licencia ofertada; debe presentar carta del fabricante cuya emisión no podrá ser superior a un año.

3.2 Contar con al menos un (1) técnico certificado de la marca ofertada. La certificación del técnico no debe tener más de tres años de obtenida.

4. Monto y plazo de la garantía de participación

4.1 La garantía de participación será de un 1% (uno por ciento) del monto total ofertado, misma que podrá ser rendida mediante las formas establecidas en el artículo 42 del reglamento a la Ley de Contratación Administrativa o bien mediante deposito a la siguiente cuenta bancaria: # 100-01-002-014529-6 del Banco Nacional de Costa Rica.

4.2 Debe indicar en el detalle del depósito "Garantía de Participación de la Licitación Abreviada N°. 2016LA-000012-UTN" y podrá ser otorgada en la misma moneda en la cual se cotizó la oferta. La vigencia no podrá ser inferior a 60 días naturales y comienza a correr a partir del momento en que se efectúe el depósito.

4.3 Los proveedores que demuestren su condición de PYMES, podrán rendir la garantía de participación, según lo dispuesto en la Ley N° 8262 y sus reglamentos, asimismo podrán acogerse a lo dispuesto en el artículo 46 bis del Reglamento de la Ley de Contratación Administrativa.

4.4 Es una obligación del oferente, mantener vigente la garantía de participación, mientras el acto de adjudicación queda en firme.

4.5 Si la garantía de participación es presentada por medio de cheque del Sistema Bancario Nacional, sólo se aceptarán si son certificados o de gerencia.

4.6 Cuando se trate de dinero en efectivo o de títulos valores de inversión endosada a nombre de la Administración, el oferente debe señalar en forma expresa la vigencia de su garantía.

4.7 La Garantía de participación será devuelta a petición de los oferentes no adjudicados, dentro de los 08 días hábiles siguientes a la firmeza del acto de adjudicación. En el caso del adjudicatario, se devolverá una vez rendida a satisfacción la garantía de cumplimiento.

4.8 Cuando la garantía se haya rendido en efectivo, la devolución se realizará mediante depósito en la cuenta bancaria suministrada para tales efectos.

5. Monto y plazo de la garantía de cumplimiento

5.1 La garantía de cumplimiento será de un 5% (Cinco por ciento) del monto total adjudicado con una vigencia de 90 días naturales adicionales, a partir de la fecha probable de aceptación de todos los bienes a satisfacción de la Universidad Técnica Nacional.

5.2 La misma podrá ser rendida de la siguiente manera: depositada a la cuenta # 100-01-002-014529-6 del Banco Nacional de Costa Rica o por medio de las formas establecidas por el artículo 42 del reglamento a la Ley de Contratación Administrativa.

5.3 En caso de que el oferente sea PYMES, podrá acogerse a lo dispuesto en la Ley N° 8262 o por los instrumentos financieros creados al amparo de la Ley N° 8634, siempre y cuando demuestren su condición a la Administración y cumplan con los requisitos que se establecen en sus respectivos Reglamentos.

V. CONDICIONES GENERALES

1. Plazo para adjudicar

La Universidad tomará hasta 30 días hábiles para adjudicar.

2. Forma de Adjudicación

La UTN se reserva el derecho de adjudicar total o parcialmente las ofertas recibidas, o de rechazarlas todas de acuerdo a la conveniencia de sus intereses, o bien declarar desierto el concurso.

3. Forma de pago:

3.1. Se realizará un único pago, el cual se efectuará 30 días naturales siguientes al recibido conforme por parte del usuario final.

3.2. Se efectuará los pagos por medio de transferencia electrónica por lo que deberán adjuntar en la oferta el número de cuenta y la cuenta cliente donde se realizaría el pago.

3.3. La factura deberá presentarse en el tipo de moneda cotizado, cuando se trate de una moneda distinta al colón, el pago se realizará en colones

costarricenses y de acuerdo a lo establecido en el artículo 25 del Reglamento a la Ley de Contratación Administrativa.

4. Garantía y respaldo en el funcionamiento de las licencias:

4.1. La garantía sobre todas las líneas no podrá ser inferior a 12 meses, contados a partir del recibido conforme por parte de la Universidad Técnica Nacional.

4.2. El adjudicatario debe garantizar que las licencias se encuentran en óptimas condiciones de funcionamiento, en caso de detectarse fallas o errores, este deberá verificar y resolver la falla o defecto en el momento que el administrador del contrato lo reporte y el contratista constate la información, lo cual deberá corregirse dentro del plazo máximo de 01 día hábil.

5. Instalación:

Solo aplica para la línea N°3 (Anti-virus), la cual deberá instalarse en forma presencial en la administración universitaria y remotamente en las sedes de la universidad.

6. Presentación de Ofertas

6.1. Las ofertas deben presentarse en original y una copia debidamente firmada por quien tenga capacidad legal para hacerlo y entregarse en sobre cerrado que contenga por fuera el nombre de la institución, código de la licitación abreviada y el nombre de la empresa oferente.

6.2. Adicionalmente se deberán entregar una copia en CD en formato original del cuadro de la oferta detallado en el siguiente punto de este cartel y deberá de incluir dentro del sobre cerrado.

6.3. La oferta debe hacerse en idioma español, sin alteraciones que puedan producir dudas sobre la oferta. Cualquier documentación técnica que acompañe la oferta deberá venir en idioma español.

6.4. Los participantes deberán cumplir con lo que establece la Ley de Contratación Administrativa, el Reglamento General de Contratación Administrativa y otras leyes pertinentes.

6.5. Debe adherir a la oferta un timbre de la Ciudad de las Niñas de ¢20,00 y un timbre de ¢200,00 del Colegio de Profesionales en Ciencias Económicas.

6.6. Las ofertas deben contener la descripción completa de las licencias, indicando marca, modelo y preferiblemente fotografía. Para lo anterior se deberá utilizar el siguiente cuadro:

Línea	Cantidad	Descripción	Marca	Precio Unitario	Precio Total

7. Estructura de la Oferta

La estructura deberá ser preferiblemente la siguiente:

7.1. Portada con un encabezado que haga referencia a la Universidad y número de licitación, debe contener todos los datos de la empresa (medios de contacto, cédula jurídica, etc). Los timbres deben de ir pegados con goma en la portada.

7.2. Incluir índice de contenido; en cuyo caso cada hoja de la oferta debe estar foliada **en la parte inferior**.

7.3. Oferta económica que incluya descripción de los bienes y precios unitarios y totales (por línea), oferta alternativa.

7.4. Indicar la vigencia de la oferta, plazo de entrega, garantía de producto, entre otros.

7.5. Aspectos legales tales como declaraciones juradas, certificación CCSS y FODESAF, personerías, entre otros.

7.6. Cuadro Resumen.

7.7. Cualquier otro documento no mencionado.

8. Evaluación de las Ofertas

Una vez determinado que las ofertas cumplen con los aspectos legales y técnicos y que son admisibles para una eventual adjudicación, se procederá a realizar la calificación de cada oferta, bajo la siguiente metodología de evaluación:

Tabla N° 1

FACTORES DE EVALUACIÓN		
A	Precio	90%
B	Años de experiencia	10%
TOTAL		**100%**

A. <u>Precio (90%)</u>:

Se calificará según la siguiente fórmula:

$$PP = \left(\frac{P_{\min}}{P_{oferta}} \right) * PT$$

Donde:

PP: Puntaje por precio.
P oferta: Precio de la oferta en estudio.
P min: Menor precio ofrecido de cada producto.
PT: Máximo puntaje por precio alcanzable (90%)

B. <u>Experiencia de la empresa (10%)</u>

Se evaluará la experiencia de los oferentes de acuerdo a la siguiente tabla de rangos:

Años de experiencia como distribuidor autorizado	Porcentaje
Mayor o igual a 10 años	10%
Mayor o igual 7 años pero menor a 10 años	7%
Mayor o igual a 5 años pero menor a 7 años	5%
Mayor o igual a 3 años pero menor a 5 años	3%
Menor a 3 años	1%

- Los oferentes deberán aportar carta del fabricante, en la cual deberá contener la cantidad de años que tiene relación laboral como distribuidor autorizado de la marca de licencia cotizada.

- Adicionalmente deberán aportar al menos 5 referencias comerciales que cuenten con producto igual al ofertado, para ello deberán llenar la siguiente tabla de resumen.

Tabla N° 2
Referencias Comerciales

Nombre de la empresa (cliente)	Nombre del contacto	Teléfono y correo electrónico	Nombre de la licencia vendida

8.1. Aspectos generales de la evaluación

8.1.1. **Criterios para el redondeo:** Para los cálculos de puntaje se utilizarán dos decimales

8.1.2. **Criterio de Desempate:** En caso de empate entre dos o más ofertas, se adjudicará a la empresa que demuestre su condición como PYME, de persistir el empate se considerar como segundo factor de desempate la empresa que ofrezca el menor precio, de persistir el empate por tercera vez, la Administración convocará por escrito con tres días de antelación a los representantes de los oferentes que se encuentren en situación de empate, para efectuar una rifa y así seleccionar el adjudicatario, la cual será efectuada en la oficina de Contratación Administrativa usando como criterio la suerte, según lo establecido en el artículo 55 del Reglamento a la Ley de Contratación Administrativa. La no asistencia de

las partes no impedirá la realización de la rifa. De lo actuado se levantará un acta que se incorporará al expediente.

9. Documentación necesaria:

9.1. Certificación sobre la personería jurídica de la sociedad mercantil o copia de la cédula de identidad en caso de persona física.

9.2. Los proveedores interesados en participar que no se encuentren inscritos en el registro de proveedores de la Institución, deben aportar los documentos legales y declaraciones juradas que establece la Ley de Contratación Administrativa y su Reglamento (certificaciones sobre la personería jurídica y propiedad de las acciones, copia certificada de la cédula jurídica, declaración jurada de que no le alcanzan las prohibiciones contenidas en los Artículos 22 y 22 bis incisos a, b, c, d, e y f, No. 24 de la Ley de Contratación Administrativa, y que se encuentra al día en el pago de los impuestos nacionales, según el Artículo 65 inciso a) del Reglamento a la Ley de Contratación Administrativa). La información completa se encuentra disponible en la página Web y específicamente en el módulo de Contratación Administrativa: http://www.utn.ac.cr/.

9.3. Declaración jurada que no le alcanzan, al oferente, las prohibiciones para contratar con la Universidad Técnica Nacional, que se refiere el numeral 22 de la Ley de Contratación Administrativa y en los Artículos 19 y 20 del Reglamento.

9.4. Declaración jurada que el oferente se encuentra al día en el pago de todo tipo de impuestos nacionales de conformidad con lo dispuesto en el art No. 65 a del Reglamento.

9.5. Cualesquiera otros documentos que se considere oportuno acompañar, según la naturaleza del objeto licitado y el tipo de licitación que se haya promovido.

9.6. El oferente debe estar al día con las obligaciones obrero-patronales de la CCSS y FODESAF, o bien deben aportar el arreglo de pago aprobado, vigente al momento de la apertura de las ofertas.

9.7. Declaración jurada que el oferente no está afectado por ninguna causal de prohibición. La oferta deberá ser firmada por el representante legal o su agente debidamente autorizado.

9.8. Toda oferta debe ser cotizada libre de todos los impuestos, salvo que se indique lo contrario. La Universidad Técnica Nacional se encuentra exenta de los mismos, según Artículo No. 13 de la Ley No. 8638, del 14 de mayo de 2008 y publicada el 14 de junio de 2008.

10. Aclaraciones y modificaciones al cartel

10.1. Toda solicitud de aclaración y/o modificaciones al presente cartel, deberá efectuarse por escrito a los siguientes correos electrónicos jsolis@utn.ac.cr con copia a vcascante@utn.ac.cr y lperez@utn.ac.cr

10.2. La Administración se reserva el derecho de realizar las modificaciones o aclaraciones a las condiciones y/o especificaciones del cartel, cuando se consideren necesarias.

10.3. Todas las modificaciones y aclaraciones serán notificadas por medio de correos electrónicos o bien publicados en la página web oficial de la Universidad Técnica Nacional www.utn.a.cr.

11. Regulaciones que deben observarse:

La empresa contratada no podrá ceder o transferir los derechos u obligaciones derivados del contrato, ni los términos y condiciones aplicables.

Los participantes deberán cumplir con lo que establece la Ley de Contratación Administrativa, el Reglamento a la Ley de Contratación Administrativa y otras leyes pertinentes.

12. Incumplimientos para todas las líneas:

En caso de incumplimiento de cualquiera de las cláusulas del cartel, la oferta o del contrato, la Universidad Técnica Nacional se arroga el derecho de rescindir y/o resolver unilateralmente el contrato, sin responsabilidad alguna para la Institución y sin perjuicio de la aplicación de la normativa correspondiente.

13. Derecho de modificación unilateral y contrato adicional

La Administración se reserva el derecho de utilizar la opción de compra de conformidad con lo que establece el artículo 200 y 201 del Reglamento de Contratación Administrativa.

Analista Responsable:	José Roberto Solís Guevara	**Teléfono:**	2401-5200 Ext. 2014
Correo	jsolis@utn.ac.cr		
Firma		**Fax:**	2461-2381

Lic. Miguel González Matamoros
Director, Proveeduría Institucional
27/07/2016

Este cartel se rige bajo la Ley de Contratación Administrativa y su Reglamento, así como la normativa conexa aplicable.

ANEXO N° 1

ESPECIFICACIONES DE LA LÍNEA 3 (ANTI-VIRUS)

RENOVACIÓN DE LICENCIAS ESET ENDPOINT SEGURITY (ANTIVIRUS / ANTISPYWARE /HIPS / DEVICE CONTROL / ANTISPAM / FIREWALL PERSONAL / WEB CONTROL) CON 2 AÑOS DE LICENCIAMIENTO

CLIENTE:

- Incorpore garantía de compatibilidad extendida para sistemas operativos 32bits y 64bits:
  - Microsoft Windows® 10, 8.1, 8, 7, Vista, XP
  - Microsoft Windows Server 2012R2, 2012, 2008R2, 2008, 2003
  - Microsoft Windows Server Core 2012R2, 2012, 2008R2, 2008 Core
  - OS X 10.6 y/o superior
  - RedHat, Debian, Ubuntu, Suse, Fedora & Mandriva asi como la mayoría de distribuciones basadas en gestor de paquetes RPM y DEB
- El licenciamiento otorgado deberá poseer garantía y cobertura sobre los sistemas operativos indicados como requeridos, se acepta un solo y único lote de licenciamiento que involucre a todos los sistemas indicados; puntualmente deberá ocuparse una única clave de activación, llave o similar para todos los productos contratados e indicados como compatiblemente requeridos
- El licenciamiento adquirido en su totalidad deberá poder ser administrado por una única consola de administración, todos los productos adquiridos para los sistemas operativos indicados como compatibles deberán poderse administrar integralmente desde una única consola validada e implementada en la red interna corporativa

ASPECTOS GENERALES:

- Debe incorporar protección en tiempo real contra todo tipo de malware; incluyendo virus, gusanos, troyanos, spyware, phishing, rootkit, adware, riskware, keyloggers y/o otros códigos maliciosos nuevos y desconocidos. Específicamente para dicho fin no deberá depender de que el Sistema Operativo del "Endpoint/Cliente" tenga las actualizaciones y Service Pack al día
- Incorporar protección contra virus boot, virus macros, virus residentes en RAM, virus de acción directa, virus encriptados, virus polimórficos, virus de FAT, etc
- Incorporar motor heurístico proactivo y preciso de tecnología avanzada, dicho motor debe ser propio y no de terceros fabricantes y/o colaboraciones externas ajenas a casa matriz
- Incorporar detección de virus en archivos compactados, sin importar el número de niveles de compresión, en los formatos: .zip, .rar, .arj, .cab, .lzh, .tar, .gz, ace, izh, upx y/o otros
- El producto se debe instalar sin fragmentación para su correcto funcionamiento (múltiples módulos instalados en el computador reflejados en programas instalados "Agregar/Quitar Programas" no serán aceptados, exceptuando únicamente al agente de conexión)

- Deberá permitir importar o exportar configuraciones de clientes de manera fácil, vía archivos xml livianos y transportables
- Incorporar capacidad de poder enviar a los centros de soporte técnico las muestras de virus o códigos maliciosos, con la finalidad de que puedan ser analizados, y clasificados para su contingencia inmediata directamente desde la interfaz gráfica
- Incorporar capacidad de generar casos de soporte vía la interfaz gráfica de la solución
- Incorporar chequeo y control de Actualizaciones para Microsoft Windows, dicho control debe ser capaz de ser configurado para reportar diferentes niveles de actualización o desactivar el informe de las mismas
- Toda configuración a nivel de clientes, deberá poder ser posible realizarse desde consola administrativa y funcionalmente podrá gestionarse integralmente desde una única consola administrativa centralizada. Queda implícitamente descrito todos los productos adquiridos deberán administrarse desde una sola consola de administración, no importando el sistema operativo sobre el cual hayan sido implementados
- Incorporar compatibilidad nativa en su interfaz gráfica con dispositivos que integren tecnología TouchScreen
- Que incorpore cache local de inspección a fin de mejorar el rendimiento en equipos virtualizados, explícitamente la cache de inspección local deberá validar si los ficheros fueron inspeccionados previamente por otro equipo en la red y en todo caso no forzar inspección local si el mismo es sano e inocuo al sistema a fin de acelerar el proceso de inspección. Dicha cache en aceleración de inspección antivirus/antimalware deberá de ser compatible con cualquier plataforma de virtualización, así como funcionalmente hablando no deberá requerir la instalación de ningún plugin o complemento instalado y evidente desde "Control Panel -> Agregar o Quitar programas"
- La solución a contratarse deberá provisionar capacidad para generar CD y/o USB Booteables, los cuales posean capacidad de análisis para la inspección de malware en máquinas que no cuenten con la protección de solución contratada o requieran del uso de los mismos con el fin de eliminar cualquier código malicioso, así mismo dichos medios deben poder ser actualizados vía Internet inmediatamente después del arranque desde los mismos
- La solución a contratarse deberá provisionar capacidad para generar CD y/o USB Booteables, los cuales deberán ofrecer como medio alternativo las siguientes herramientas de diagnóstico y asistencia técnica remota con proveedor o fabricante:
    - Gparted
    - MemTest86+
    - Teamviewer
    - Otras aplicaciones para recibir asistencia remota
- La solución a contratarse deberá cumplir con estándares AMTSO, identificables y validables en cada una de sus pruebas de evidencia técnica; de igual forma fabricante antivirus deberá figurar en el listado de miembros activos de AMTSO
- La solución a contratarse deberá poseer certificaciones CheckMark e ICSA Labs

- Que incorpore protección a nivel Kernel, previniendo la desactivación y/o alteración por un tercero y/o código malicioso
- Incorporar auto-protección del núcleo y componentes de la suite de seguridad a nivel ASLR & DEP, así como funcionalmente no requiera de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas"
- Incorporar protección en tiempo real contra cualquier alteración al estado del kernel antivirus, imposibilitando detenerlo o dejarlo inoperativo para protección del computador donde ha sido implementado
- Que incorpore capacidad de protección por contraseña de acceso al propio motor antivirus, a fin de que no pueda ser alterada configuración de la propia solución y/o alteración al estado de protección del computador
- La instalación de producto podrá realizarse tanto localmente como remotamente desde su consola administrativa; en el término local se entiende se requiere precompilación de un paquete todo-en-uno para la instalación del producto el cual contenga las preconfiguraciones y niveles de seguridad básicos aplicables a la estación de trabajo, así mismo incorpore en un solo paso la unión y sincronización a consola administrativa
- La comunicación entre clientes administrados (endpoints) y servidor de administración deberá realizarse mediante conexión SSL cifrada; dicha conexión deberá ser evidente y descrita en el log de estado del agente de conexión mediante cualquier navegador web para fines de validación o auditoria
- El agente de conexión deberá provisionar log transaccional de referencia, así como en forma simultánea deberá mostrar su estado de conexión y descripción general de sincronizaciones a servidor administrativo; dicho log deberá ser accesible desde cualquier navegador web y en forma dinámica deberá variar en forma automática a fin de evidenciar cualquier problema de comunicación o falla de transferencia y/o comunicación cifrada en la línea del tiempo
- La solución a contratarse requiere soporte técnico directo del fabricante y que este pueda prestarlo localmente en formato 24x7x365; el mismo en sus modalidades deberá garantizarse ya sea en forma presencial, remota, chat en línea, correo electrónico y/o vía telefónica mediante número local; en caso que la empresa adjudicada por alguna razón no pueda proporcionarlo
- Deben incluirse medios de instalación originales provistas por el fabricante, evidenciables mediante certificado de originalidad provisto por el fabricante y entregado con las mismas

HIPS:

- Que incorpore tecnología de control HIPS para estaciones de trabajo y servidores sobre plataforma Microsoft Windows, así como funcionalmente no requiera de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas"
- Incorporar HIPS con capacidades avanzadas de protección y funcionalmente sea capaz de realizar las siguientes acciones básicas pero no limitadas requeridas:
- Que permita bloquear archivos y/o aplicaciones para ejecución

- Permitir ejecutar archivos y/o aplicaciones basados en rutas de acceso y/o ficheros en particular
- Bloquear archivos y/o carpetas contra escritura y/o acceso
- Permitir escritura y/o acceso para archivos y/o carpetas
- Que permita bloquear escritura y/o modificación a llaves del registro de sistema
- Incorporar tecnología avanzada que permita prevenir la explotación de vulnerabilidades en las aplicaciones más comunes; principalmente pero no limitado control de explotación para navegadores web, PDF, clientes de correo electrónico, aplicaciones MS Office & Java
- Que incorpore motor de inspección avanzada en memoria operativa que brinde protección contra el malware moderno que ocupa técnicas de cifrado y/o ofuscación
- Incorporar protección avanzada contra la deshabilitación y/o modificación del propio motor de protección antivirus por parte de terceros y/o algún código malicioso, dicha función deberá reflejarse en el componente HIPS cargado en el sistema

CLUOD PROTECTION:

- Que incorpore tecnología de detección en tiempo real basada en la nube, con el fin de prevenir ataques 0-Day y/o campañas de propagación de malware lanzadas globalmente; dicho alcance deberá garantizarse para correo electrónico así como todo tipo de tráfico de red, tanto para reputación de archivos así como vínculos URL
- Que permita integración de tecnología "Cloud Protection" no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas"
- Incorporar tecnología basada en la nube y en tiempo real, que permita al usuario operador del endpoint verificar la reputación de los procesos activos y de los archivos directamente desde la interfaz del programa o desde el menú contextual
- Incorporar tecnología en la nube para la detección de código nuevo y emergente, posibilitando detección del código malicioso y/o vínculo URL inclusive previo al lanzamiento de firmas antivirus de detección estándar
- Que incorpore tecnología "Antiphishing", de tal forma que prevenga al usuario de los intentos de adquirir contraseñas, datos bancarios y/o otra información sensible por parte de los sitios web falsos, haciéndose pasar por los legítimos; funcionalmente no debe requerir la instalación de módulos adicionales para tales fines así como no deberá reflejarse como componente adicional en "Agregar/Quitar Programas"

ACTUALIZACIONES:

- Las actualizaciones rutinarias de la base de definición de firmas, deberán de ser pequeñas e incrementales; tanto para actualizaciones rutinarias como para repositorios de distribución (mirror). Se consideran como pequeñas e incrementales a las actualizaciones rutinarias menores a 1MB por cada firma de definición

- Funcionalmente una actualización rutinaria, debe ser capaz de actualizar firmas antivirus, módulos y/o componentes del sistema antivirus; no incluyendo pero no limitando la versión de familia del producto contratado y/o futuras versiones del producto adjudicado
- Incorporar capacidad para que un cliente instalado (endpoint) pueda convertirse en repositorio de actualizaciones (mirror), con el fin de poder actualizar otros clientes desde este o poder extraer los archivos de actualización y trasladarlos manualmente a otros clientes "stand-alone"; funcionalmente no debe requerir la instalación de módulos adicionales para tales fines así como no deberá reflejarse como componente adicional en "Agregar/Quitar Programas"
- Deberá poseer factibilidad para actualizar de forma manual todos sus componentes y definiciones de virus, en computadoras sin ningún tipo de conectividad a red; es decir, en status "stand-alone"
- Las actualizaciones de distribución de firmas rutinarias (repositorios de firmas) deberán proveerse a los clientes antivirus internos, mediante servicio HTTP/HTTPS incluido en el propio motor del producto instalado así mismo deberá poder ofrecerse métodos de autenticación básica o vía NTLM a fin de proteger contra el acceso de terceros a firmas antivirus de distribución local; dicha opción deberá integrarse mas no quedar limitada y/o restringida como medio para distribución de firmas mediante motores FTP/Shares de terceros; funcionalmente no debe
- Requerir la instalación de módulos adicionales para tales fines así como no deberá reflejarse como componente adicional en "Agregar/Quitar Programas"
- Las actualizaciones diarias y rutinarias de los componentes del producto se deberán realizar en tiempo real desde Internet o vía LAN Server (Mirror), en forma automática y sin necesidad de intervención del usuario

FILTRADO DE RED Y/O PROTOCOLOS DE COMUNICACIÓN:

- Que incorpore la capacidad de filtrado de protocolos, para todo el tráfico de red; teniendo opción de analizar todo tipo de comunicación saliente/entrante. Funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas"
- Incorporar escaneo y limpieza de paquetes en tráfico HTTP, FTP, SMTP y POP3; tanto en los servidores como en las computadoras personales
- Incorporar filtrado e inspección de protocolos seguros (HTTPS, SMPTS, POP3S, FTPS, entre otros), funcionalmente hablando debe ser capaz de filtrar cualquier comunicación de red segura así como no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control"
- Incorporar capacidad de excluir aplicaciones, direcciones IP y/o rangos de direcciones del filtrado de protocolos e inspección al tráfico de red
- Incorporar capacidad de analizar todo el tráfico de red o bien indicar puertos y/o aplicaciones en particular a inspeccionar a nivel de filtrado de protocolos
- Que incorpore filtrado básico para listas URL y/o IP de acceso; de tal forma que se pueda controlar efectivamente accesos a los listados estáticos

definidos, ya sean sobre comunicación en texto plano (HTTP) o sobre protocolos seguros (HTTPS); funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas"
- Que incorpore plugin para el filtrado, análisis y detección antimalware en los clientes de correo electrónico Microsoft Outlook, Windows Mail & Windows Live Mail; no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control"

FIREWALL E IDS:
- Que incorpore firewall/cortafuegos avanzado de doble vía; capaz de filtrar bidireccionalmente el tráfico de red ya sea este entrante o saliente, funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas"
- El firewall/cortafuegos incorporado deberá ser totalmente administrable desde cliente o desde consola administrativa, así como deberá poseer modo de solución rápida a problemas comunes guiados intuitivamente desde la propia interfaz del producto
- El firewall/Cortafuegos incorporado deberá poseer facilidad para la definición de redes de confianza mediante parámetros de detección que faculten identificar si en realidad dispositivo protegido se encuentra en una red "segura" o bien se requiere un modo superior de protección en una red nueva y desconocida
- Incorporar IDS (Intrusion Detection System) de host para la prevención de acceso no autorizado al computador a nivel de capa de red, funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas"
- Incorporar protección anti "BOTNETS", la cual faculte a la solución bloquear el acceso y comunicación a una red botnet así como alertar al usuario de dicha acción y anomalía detectada; funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas"
- Incorporar Control de Vulnerabilidades a nivel de capa de red, el cual deberá inspeccionar y proteger a los protocolos más ampliamente utilizados SMB, RPC y RDP; evitando con dicho fin la propagación del malware, ataques de red dirigidos y la explotación de vulnerabilidades para las que un parche de seguridad aún no está disponible o ha sido desplegado, funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas"

ANTISPAM:
- Que incorpore solución antispam a nivel endpoint y posea filtrado para protocolo SMTP, POP3 & IMAP en forma transparente e integrada al producto sin requerir instalación de módulos y/o agentes en el computador; no debe
- Requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control"

- Que incorpore plugin para el filtrado, análisis y clasificación antispam en los clientes de correo electrónico Microsoft Outlook, Windows Mail & Windows Live Mail; no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control"
- Proveer la capacidad de generar listas blancas/negras para el filtrado del correo electrónico en la estación de trabajo final y en los clientes de correo electrónico indiciados como compatibles; dicha acción deberá de ser posible realizarse desde el propio producto y/o consola de administración, así como permitirá definir dominios y/o direcciones en cada uno de estos apartados.

FILTRADO WEB:

- Que integre capacidad de Web Filtering basado en categorías, siendo posible definir políticas basadas en grupos de usuario y/o usuarios (tanto a nivel AD como también mediante autenticación local); no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control"
- Incorporar capacidad de Web Filtering mediante grupos de categorías, haciendo factible el agrupamiento de múltiples y diferentes categorías de inspección URL para una misma regla de navegación
- Que permita y/o denegar el acceso URL estáticos mediante reglas configuradas en el Web Filtering
- Que provea la posibilidad de agrupamiento en políticas de filtrado URL, siendo factible sumar diferencialmente los accesos y/o denegaciones a fin de aplicar una política final de maquina o grupo de usuarios
- Que integre la capacidad para la generación de logs y sincronización de los mismos a consola corporativa, de acuerdo a cada una de las acciones tomadas en concordancia con la regla URL definida ya sea bloqueo o permisión según sea el caso; dicho log deberá contener toda la información detallada desde el URL bloqueado/permitido hasta el usuario/equipo detectado así como hora/fecha y descripción integra del evento; no debe requerir de instalación y/o módulo reflejado en componentes de programa en "Agregar quitar Programas -> Panel de Control"
- Integrar la capacidad Web Filtering sobre sitios URL que ocupen protocolo seguro (HTTPS); no debe requerir de instalación y/o módulo reflejado en componentes de programa en "Agregar quitar Programas -> Panel de Control"

CONTROL DE DISPOSITIVOS:

- Incorpore capacidades de "Device Control" administrables ya sea localmente o en forma remota desde su consola administrativa; no debe requerir de instalación y/o módulo reflejado en componentes de programa en "Agregar quitar Programas -> Panel de Control"
- Incorporar capacidades de "Device Control" avanzadas, con el fin de delimitar, denegar o permitir dispositivos portátiles y/o medios extraíbles tales como:
    - Dispositivos de almacenamiento USB

  - Dispositivos ópticos CD/DVD
  - Impresoras USB
  - Dispositivos de almacenamiento Firewire
  - Dispositivos Bluetooth
  - Tarjetas lectoras de memoria
  - Dispositivos de imagen
  - Modems
  - Puertos LPT/COM
  - Dispositivos portátiles (móviles)
- Que incorpore funciones avanzadas para el control de dispositivos siendo posible aplicar reglas con el fin de delimitar, denegar o permitir de acuerdo a las siguientes condiciones del dispositivo periférico conectado:
  - Marca
  - Modelo
  - Serie
- Incorporar funciones avanzadas para el control dispositivos siendo capaz de asignar políticas de acuerdo a grupos de trabajo local o grupos dinámicos mediante un Directorio Activo; así mismo provea extensión de operación por usuario local y/o usuarios de un Directorio Activo.
- Que incorpore funciones avanzadas para el control de dispositivos mediante grupos de "dispositivos", siendo posible asignar reglas y/o directrices mediante grupos pre-establecidos de dispositivos con el fin de facilitar administración así como el control adecuado de los dispositivos conectados a las estaciones de trabajo.

CONSOLA DE ADMINISTRACIÓN:

- Servidor de administración y consola administrativa deberá poder implementarse así como proveer soporte multiplataforma compatible con al menos los siguientes sistemas operativos:
  - Microsoft Windows Server 2012R2, 2012, 2008R2, 2008, 2003
  - Microsoft Windows Server Core 2012R2, 2012, 2008R2, 2008 Core
  - Microsoft Windows 8.1, 8, 7, Vista, XP (CAL Microsoft puede limitar el soporte extendido, más sin embargo solución administrativa deberá poder instalarse y ser compatible con sistemas indicados)
  - RedHat, Debian, Ubuntu, Suse, Fedora & Mandriva asi como la mayoría de distribuciones basadas en gestor de paquetes RPM y DEB
- Servidor de administración y consola administrativa deberá ofrecer compatibilidad para despliegue rápido mediante OVF; a fin de simplificar el despliegue de "Appliance Virtual" para el funcionamiento correcto de servidor administrativo de la solución adquirida
- Servidor de administración y consola administrativa deberá poder implementarse sobre plataforma Windows mediante un paquete todo en uno que incluya todos los elementos requeridos para instalación simplificada, así como ofrezca un fácil despliegue de solución administrativa; dicho paquete deberá incluir por defecto a los motores de base de datos así como todo lo que integralmente requiere para su correcto funcionamiento el servidor y consola de administración

- Servidor de administración y consola administrativa deberá ofrecer compatibilidad con al menos las siguientes bases de datos:
    - MySQL 5.5 o superior
    - MS SQL Server 2008 R2 o superior
- El servidor de administración y consola administrativa deberá ofrecer una consolidada y completa administración de los productos adquiridos, así como en su totalidad indicar el estado, configuraciones y políticas aplicadas de cada uno de los nodos internos ligados a dicha consola de administración
- El servidor de administración y consola administrativa deberá ofrecer posibilidad de integración con Active Directory, tanto para instalación remota de clientes así como para autenticación local de administradores y roles de acceso a la misma
- El servidor de administración y consola administrativa deberá ofrecer diversos y variados roles de acceso mediante grupos de usuarios con el fin de definir niveles de acceso a administración de los diferentes recursos que dicha consola administrativa ofrezca a los administradores TI internamente
- El servidor de administración y consola administrativa deberá provisionar acceso web mediante servidor de aplicaciones JAVA
- La consola de administración deberá operar en su totalidad en modalidad web, así como integralmente deberá estar desarrollada y compilada sobre código JAVA
- El servidor de administración y consola administrativa deberá ofrecer posibilidad de segmentación para grandes redes mediante nodos de sincronización remota; de tal forma de facilitar la administración y sincronización de los clientes remotos, dichos nodos de sincronización podrán obrar como gestores de firmas, repositorios locales de instaladores así como receptores de políticas y estados de los clientes locales
- La consola de administración deberá ser totalmente web, así como funcionalmente deberá ser compatible con cualquier navegador web tanto en sistemas operativos Microsoft, GNU/Linux, Mac OS y/o cualquier otro que a conveniencia pueda ocuparse para el acceso a dicha consola de administración
- La consola de administración web deberá garantizarse para al menos los siguientes navegadores en las versiones indicadas o superiores, sin requerir la instalación de algún plugin y/o complemento adicional del lado del cliente final:
    - Firefox 20+
    - Internet Explorer 10+
    - Chrome 23+
    - Safari 6+
    - Opera 12+
- La consola de administración web deberá ofrecer por completo administración para todos los productos ofertados independientemente del sistema operativo donde corre cliente o servidor, de forma tal que en su totalidad y absolutamente todos los productos sean administrados desde una sola interfaz web
- La consola de administración debe incorporar Dashboard accesibles desde cualquier navegador web y desde cualquier punto dentro o fuera de la red

local; no debe requerir para dicha operación el uso de IIS o motor diferente al integrado nativamente por la solución

- La consola de Administración no deberá requerir de la existencia de un Dominio de Autenticación de Usuarios para su buen funcionamiento o como condicionante de operación; sin embargo deberá permitir administrar clientes antivirus en distintos grupos de trabajo o multi-dominios ya existentes
- La consola de administración web no deberá requerir para su funcionamiento u operar sobre plataformas ASP, JSP o PHP
- La consola de administración deberá manejar múltiples tipos de Licencias de Software, en diferentes cantidades de equipos y fechas de expiración
- La consola de administración no deberá requerir el uso de MMC (Microsoft Management Console) para el funcionamiento de la misma o como requisito de instalación
- En términos de una correcta administración se requiere que una configuración establecida para un determinado cliente (endpoint) pueda ser exportada, tanto desde la Consola de Administración, como desde el mismo cliente, para poder ser importada en otros clientes, de ser necesario
- La consola de administración deberá facultar instalación remota desatendida ya sea ocupando autenticación local o vía un directorio de autenticación, no importando si esta se realiza en dominio o en grupos de trabajo
- La consola y servidor de administración no deben requerir System Center Configuration Manager (SCCM), CM12, CM0, ConfigMgr, Configuration Manager o similar para uso de consola administrativa y/o servidor de administración; no debe figurar en especificaciones del fabricante (web/datasheets)
- El servidor central de administración (consola/servidor) deberá ser compatible a nivel de almacenamiento de registros (logs) con base de datos MySQL y SQL Server; dicha compatibilidad deberá garantizar funcionamiento correcto con versiones "libre de pago" de dichas bases de datos (MySQL Community Edition & MS SQL Server Express)
- La consola y servidor de administración no deberán requerir Microsoft Message Queue como requisito para instalación y/o operación.
- Se debe poder instalar n cantidad de consolas administrativas y todas deben poder integrarse a la consola central
- Se debe incluir la instalación en el sitio o remotamente por parte de personal técnico de la empresa adjudicada especializado y certificado por la solución para su debida implementación.
- Soporte técnico por demanda bajo los siguientes esquemas: correo electrónico, llamada telefónica, asistencia remota y presencial; con un tiempo de respuesta máximo de 24 horas suministrado directamente de parte de la empresa adjudicada
- Deben incluir como mínimo 4 visitas programadas de revisión de consola en el sitio durante los dos años del licenciamiento, en cada visita se generará un reporte que será entregado a la Dirección de Gestión de TI.