TABLA DE CONTENIDO:

1. INFORMACIÓN GENERAL

El presente documento contiene los Términos de Referencia, elaborados por la UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS para la adquisición de los productos de software descritos en los términos técnicos del presente documento, en desarrollo de las actividades previstas en su misión.

2. OBJETO

Contratar los servicios de renovación y suministro de licencias, soporte técnico 5x8 y actualizaciones (update y upgrade) del software de seguridad para equipos servidores, PC, portátiles, escritorios y aplicaciones virtuales de la Universidad Distrital Francisco José de Caldas y beneficios en descuento para adquisición de licencias para vinculados a la Universidad, durante 3 años a partir del 28 de noviembre de 2017 según las especificaciones técnicas descritas en este documento así:

- Renovar el licenciamiento de las licencias de “Kaspersky Endpoint Security Business Select” con las que cuenta actualmente la Universidad Distrital Francisco José de Caldas.

- Adquirir licencias nuevas de “Kaspersky Endpoint Security Business Select”, a fin de ampliar la cobertura del parque informático del campus de la Universidad.

- Adquirir licencias del software “Kaspersky Security for Virtualization Server” compatible con la infraestructura de servidores virtuales administrador por la Red de Datos UDNET a fin de ampliar la cobertura a los mismos.

- Adquirir licencias del software “Kaspersky Security for Virtualization” compatible con XenApp 7.6 y XenDesktop 7.6, a fin de ampliar la cobertura a la infraestructura de escritorios y aplicaciones virtuales administrada por la Red de Datos UDNET.

3. ANTECEDENTES

La Universidad Distrital dispone de un parque informático conformado por equipos servidores, PC, portátiles, escritorios y aplicaciones virtuales que actualmente cuenta con 3395 licencias el software de seguridad Kaspersky® instalado y en funcionamiento, el cual ha protegido los dispositivos de ataques de ransomware, backdoor, rootkits, troyanos, keyloggers, spyware, virus y otros malware protegiendo la confidencialidad, disponibilidad e integridad de la información almacenada en estos.

Los equipos servidores, PC y portátiles del parque informático de la Universidad han contado con la protección del software de seguridad Kaspersky® desde el 13 de agosto de 2008, cuyo licenciamiento se ha adquirido mediante contratos trianuales. El último contrato fue realizado en noviembre de 2014 adquiriendo con este: 2600 licencias por arrendamiento del software de seguridad, el cual fue ampliado en 795 licencias en diciembre de 2016 para dar cubrimiento a los equipos adquiridos el último año incluyendo la sede Bosa Porvenir.

El software de seguridad ha permitido la detección y bloqueo de ataques de red, archivos con malware y otras amenazas durante el periodo del último contrato (noviembre de 2014 a la fecha) así:

Año	Ataques de Red Bloqueados	Archivos Malware Bloqueados
2014 (Noviembre a Diciembre)	496	2388
2015 (Enero a Diciembre)	4366	55693
2016 (Enero a Diciembre)	1105	69707
2017 (Enero a Septiembre)	448	211103

Tabla 1. Estadísticas de ataques de red y malware.

Nota: La información presentada en la tabla 1 es extraída de los informes de funcionamiento que se encuentran en el recurso compartido: \\contnet3\BK_Argos\Antivirus (Si presenta algún problema con el acceso es necesario comunicarse con la Red de Datos UDNET al correo: servidores@udistrital.edu.co).

4. JUSTIFICACIÓN

La Universidad Distrital dispone de un parque informático conformado por equipos servidores, PC, portátiles, escritorios y aplicaciones virtuales que actualmente cuenta con 3395 licencias el software de seguridad Kaspersky® instalado y en funcionamiento, lo cual permitiría la aplicación del nuevo licenciamiento de forma inmediata mitigando altamente el riesgo del cambio a otra marca de software de seguridad ya que esta migración implicaría la desinstalación del software actual a uno diferente incurriendo en tiempos altos en la instalación de las 3400 licencias (cantidad que se busca

adquirir en el presente proceso) adquiridas del software de otro fabricante, tiempo en el cual los equipos serían vulnerables a ataques de ransomware, backdoor, rootkits, troyanos, keyloggers, spyware, virus y otros malware lo que aumentaría considerablemente el riesgo en la afectación de la confidencialidad, disponibilidad e integridad de la información.

Los equipos servidores, PC, portátiles, escritorios y aplicaciones virtuales del parque informático de la Universidad requieren protección contra amenazas de malware y ataques informáticos atendiendo a la necesidad de preservar la integridad de información; para lo cual cuentan con el software de seguridad Kaspersky® que ha protegido el parque computacional de la Universidad Distrital Francisco José de Caldas, desde el 13 de agosto de 2008, contra ataques de software malicioso como: spam, spyware, adware, phising, ransomware, backdoor, riskware, rootkits, troyanos, keyloggers, virus, gusanos, dialers, hacking tolos, jokes, exploits, entre otros.

La instalación, configuración, gestión y puesta en funcionamiento de los productos de Kaspersky® ya es conocida y gestionada por el personal técnico del área de soporte de las diferentes sedes, así como la administración que se realiza desde el área de plataformas de la Red de Datos UDNET; un cambio de fabricante del software de seguridad aumentaría los riesgos en la confidencialidad, disponibilidad e integridad de la información dado que el personal ya capacitado en este producto deberá capacitarse en un nuevo producto, generando de esa manera tiempos en los cuales no se contaría con la cobertura completa.

El afinamiento que se ha venido realizando de manera continua ha permitido permanente evaluar el software en producción, concluyendo que ha protegido de manera efectiva la información de los dispositivos mencionados, esto puede evidenciarse en los informes de funcionamiento que se encuentran en el recurso compartido: \\contnet3\BK_Argos\Antivirus (Si presenta algún problema con el acceso es necesario comunicarse con la Red de Datos UDNET al correo: servidores@udistrital.edu.co).

De acuerdo a lo anterior, se requiere la renovación del licenciamiento del software de seguridad “Kaspersky Endpoint Security” dada su efectividad, bajo consumo de recursos en los equipos PC, Portátiles y Servidores, el bloqueo efectivo a los ataques antes mencionados, el soporte prestado por la casa matriz y la empresa proveedora, y por encontrarse posicionado entre los cinco (5) mejores antivirus de acuerdo a la evaluación disponible en línea en:

1. http://www.toptenreviews.com/software/security/best-antivirus-software/
2. http://www.av-comparatives.org/

5. ALCANCE

Renovación y adquisición durante 3 años a partir del 28 de noviembre de 2017 del licenciamiento del software de seguridad *Kaspersky* para equipos servidores, PC, portátiles y plataformas virtuales administradas por la Red de Datos UDNET de la Universidad Distrital Francisco José de Caldas en las siguientes cantidades:

- Renovar el licenciamiento de las 3395 licencias de "Kaspersky Endpoint Security Business Select" con las que cuenta actualmente la Universidad Distrital Francisco José de Caldas.

- Adquirir 5 licencias nuevas de "Kaspersky Endpoint Security Business Select", a fin de ampliar la cobertura del parque informático del campus de la Universidad.

- Adquirir 30 licencias del software "Kaspersky Security for Virtualization Server" compatible con la infraestructura de servidores virtuales administrador por la Red de Datos UDNET a fin de ampliar la cobertura a los mismos.

- Adquirir 200 licencias del software "Kaspersky Security for Virtualization" compatible con XenApp 7.6 y XenDesktop 7.6, a fin de ampliar la cobertura a la infraestructura de escritorios y aplicaciones virtuales administrada por la Red de Datos UDNET.

6. ANÁLISIS DE RIESGOS

Los riesgos previsibles en la ejecución del contrato, se sujetarán a los criterios definidos en este numeral, sin afectar el alcance de las obligaciones a cargo de cada una de las partes, considerando que está a cargo del proveedor la ejecución de las condiciones solicitadas en el contrato y a cargo de la Universidad el pago del valor pactado.

Los siguientes hacen parte de aquellos hechos constitutivos de riesgo, que a criterio de la Red de Datos UDNET pueden presentarse durante la ejecución del contrato:

5.1. RIESGO PREVISIBLE

Son los posibles hechos o circunstancias que, por la ejecución del contrato, es factible que sucedan.

Para los efectos del presente documento, se consideran como riesgos previsibles:

Riesgos previsibles con cargo al contratista

- Disminución de la calidad en la prestación de los servicios contratados.
- Devoluciones o cambio por incumplimiento de las especificaciones técnicas y/o calidad del servicio.
- Pérdida de la documentación de certificaciones y licenciamiento del software por hurto, atentados o deterioro, como consecuencia del transporte.
- Atrasos y/o fallas en el licenciamiento y soporte por el incumplimiento de tiempos y/o en disponibilidad de personal.
- La divulgación de información no autorizada y confidencial que se conozca en virtud del cumplimiento de obligaciones.
- La no toma de las medidas de seguridad industrial apropiadas por el proveedor, a favor de la conservación de las condiciones físicas y mentales de sus trabajadores, así como de terceras personas que activa o pasivamente tenga en alguna relación.
- Cambio en la tasa representativa del mercado.

Riesgos previsibles a cargo de la Universidad Distrital

- Incumplimiento de las obligaciones establecidas en las especificaciones técnicas.
- El no pago del contrato, en la forma establecida.
- Descripción equivocada de características para la adquisición del licenciamiento y soporte.
- La no ejecución del contrato en la forma debida y establecida en las especificaciones técnicas.
- La no comunicación permanente por parte del supervisor del contrato con el proveedor que ocasione demoras y tropiezos en el desarrollo de la ejecución del contrato.

5.2. RIESGO IMPREVISIBLE

Son aquellos hechos o circunstancias donde no es factible su previsión, es decir, el acontecimiento de su ocurrencia, tales como desastres naturales, actos terroristas, guerras, o eventos que alteren el orden público. Estos riesgos deberán estar considerados por parte de los proveedores.

Para los efectos del presente documento, se consideran como riesgos imprevisibles:

- Cambios normativos y/o tributarios.

- Atraso y sobre costos en la entrega del licenciamiento y soporte. Variación en los precios de mercado diferentes a la regulación del gobierno de los insumos, actividades, sistemas de distribución de transporte, entre otros, necesarios para cumplir con el objeto y las obligaciones pactadas.

- Circunstancias de fuerza mayor o caso fortuito.

5.3. OTROS RIESGOS

Son los posibles hechos o circunstancias que se podrían presentar por la no ejecución del contrato, la no adquisición del licenciamiento y los servicios de soporte, es factible que sucedan.

Para los efectos del presente documento, se consideran como otros riesgos:

- Incumplir con la directiva presidencial 01 de febrero de 1999 que indica textualmente" los *organismos y entidades no deberán adquirir obras literarias, artísticas, científicas, programas de computador, fonogramas y señales de televisión captadas violatorias o que se presuma violen el derecho de autor o los derechos conexos*".

- Los equipos PC, Portátiles, servidores y plataformas virtuales estarían expuestos a amenazas tales como: spam, spyware, adware, phising, ransomware, backdoor, riskware, rootkits, troyanos, keyloggers, virus, gusanos, dialers, hacking tools, jokes, exploits, entre otros., entre otros, creando vulnerabilidades informáticas y comprometiendo la confidencialidad, disponibilidad e integridad de la información de la Universidad almacenada en los mismos.

- El sistema operativo de los equipos PC, Portátiles, servidores y las plataformas virtuales de la Universidad estaría desprotegido frente a toda amenaza informática, ocasionando el posible fallo del mismo y originando contratiempos en las actividades administrativas y académicas de la institución.

6. PRESUPUESTO

El presupuesto oficial estimado para la presente invitación es hasta por la suma de XXX MILLONES DE PESOS M/CTE ($XX.000.000), incluido IVA y demás Impuestos Nacionales y Distritales, según Certificado de Disponibilidad Presupuestal Nº XXXX del XX de XXXXX con cargo al rubro de "Gastos de computador", expedido por el Jefe de la Sección de Presupuesto de la Universidad Distrital.

7. CONFIDENCIALIDAD

El proponente respetará el carácter confidencial de toda la información obtenida dentro del marco de la ejecución del contrato y no deberá divulgarla a terceros, sin acuerdo previo y por escrito de la Universidad Distrital Francisco José de Caldas.

8. ESPECIFICACIONES TÉCNICAS

Las características conocidas deben ser observadas por los oferentes en el momento de responder el pliego de condiciones que cumplan en su totalidad con los factores técnicos mínimos obligatorios. De no cumplir con estas características la propuesta no será aceptada por no permitir la escogencia objetiva del contratista.

8.3. CARACTERÍSTICAS MÍNIMAS DE CARÁCTER OBLIGATORIO

El software contratado debe corresponder a las últimas versiones funcionales liberadas en el mercado durante el tiempo de licenciamiento contratado.
Para la configuración, puesta en funcionamiento y carga de las nuevas licencias del software, el proveedor designará personal experto certificado en el software de seguridad para Endpoint (PC, Portátiles, servidores).
Los productos para Endpoint (PC, Portátiles, servidores) de los sistemas Windows deben contar con Idioma español.
Protección general en los equipos contra todo tipo de amenazas tales como: spam, spyware, adware, phising, ransomware, backdoor, riskware, rootkits, troyanos, keyloggers, virus, gusanos, dialers, hacking tolos, jokes, exploits, entre otros.
Limpieza automática de virus, spyware y demás software malicioso.
Actualización automática a través de Internet, tanto para los patrones de búsqueda como para el motor del sistema, con una periodicidad programable máxima de tres días; labor realizada en las consolas desde donde se replicará a los demás equipos a través de la red local.
Consolas centralizadas de administración que permitan: • Realizar instalación del software antivirus en los diferentes equipos. • Crear grupos y subgrupos donde se creen las políticas de protección y actualización individualmente.

• Generar como mínimo los siguientes reportes gráficos configurables para la gestión del software de seguridad y la respuesta a entes de control: Informe de bloqueos de aplicaciones, Informe de Filtrado Web, Informe de Errores, Informe de la Versión del software de seguridad, Informe de Licenciamiento del software de seguridad, Informe de Usuarios Infectados, Informe de Virus, Informe de Vulnerabilidades de software instalado en la estación de trabajo y/o servidor administrado, Informe de Actualización del software de seguridad, Informe de Software de Terceros Instalado, Inventario De Hardware completo (procesadores, memoria, adaptadores de video, discos de almacenamiento, adaptadores de audio, adaptadores de red, monitores, drives de CD/DVD), vulnerabilidades. • Detectar y reportar en qué equipo de la red se presenta el ingreso de virus. • Enviar mensajes emergentes a equipos individuales, listas de equipos, grupos o subgrupos. • Desinstalar remotamente software de terceros instalado en las máquinas clientes con sistema operativo Windows, usando elementos de remoción nativos del componente de administración Endpoint o incluyendo secuencias avanzadas de desinstalación. • Realizar instalación remota de software de terceros, a través de la plataforma de administración centralizada para que sea instalado en las estaciones de trabajo y/o servidores administrados con sistema operativo Windows. • Identificar vulnerabilidades en productos de terceros instalados en las estaciones de trabajo y/o servidores administrados con sistema operativo Windows. • Realizar inventario de hardware y de software de todas las máquinas clientes con la posibilidad de registro de dispositivos (ej.: router, switch, proyector, accesorio, etc.), informando fecha de compra, ubicación, serial, número de identificación, entre otros.
El proveedor realizará jornadas de transferencia de conocimiento al personal de soporte y plataformas de las diferentes sedes de la Universidad Distrital Francisco José de Caldas, relacionadas con la operación, manejo básico y adecuado del software de seguridad para el parque computacional. Los temas y cronograma se coordinarán con el supervisor y personal técnico de UDNET al inicio de la ejecución del contrato.
El proveedor ofrecerá a los estudiantes, docentes y administrativos de la universidad, licencias versión hogar con un descuento de al menos el 50% sobre el valor comercial durante los 3 años de duración del contrato, las cuales serán adquiridas mediante un Botón de Pago en la página WEB del proveedor.

El proveedor será el responsable de la instalación y correcto funcionamiento en un tiempo inferior a 30 días calendario de los productos adquiridos en cada uno de los equipos y plataformas virtuales del parque informático de la Universidad hasta el total cubrimiento del licenciamiento adquirido: 3400 para Endpoint (PC, Portátiles, servidores), 30 servidores virtuales y 200 XenApp 7.6 y XenDesktop 7.6.
Protección Endpoint con gestión desde la consola de administración para equipos de cómputo con sistemas operativos Windows 7, Windows 8, Windows 8.1, Windows 10 o nuevas versiones de Sistemas Operativos Microsoft® para PC y Portátiles, mínimo con los módulos: • Control de inicio de aplicaciones. • Control de actividad de aplicaciones. • Control de vulnerabilidades. • Control de dispositivos. • Control WEB. • Antivirus de Archivos. • Antivirus de correo. • Antivirus de Internet. • Antivirus para chat. • Firewall. • Prevención de intrusiones. • Guardián del sistema. • Seguridad con la ayuda de la nube. • Tareas planificadas: Actualización, Análisis completo, Análisis de áreas críticas, Análisis personalizado.
Protección Endpoint con gestión desde la consola de administración para equipos de cómputo con sistemas operativos MAC (para PC, Portátiles o Servidores), mínimo con los módulos: • Antivirus de Archivos. • Antivirus de internet. • Prevención de intrusiones. • Seguridad con la ayuda de la nube. • Tareas planificadas: Actualización, Análisis completo, Análisis personalizado.
Protección Endpoint con gestión desde la consola de administración para equipos de cómputo con sistemas operativos Linux (para PC, Portátiles o Servidores), mínimo con los módulos: • Antivirus de Archivos. • Seguridad con la ayuda de la nube. • Tareas planificadas: Actualización, Análisis completo, Análisis personalizado.
Protección File Server con gestión desde la consola de administración para equipos de cómputo con sistemas operativos tipo servidor: Windows 2008 R2, Windows 2012 R2 o cualquier otra nueva versión de Sistemas Operativos de Microsoft® para servidor, mínimo con los módulos: • Antivirus de Archivos. • Anti encriptación.

• Seguridad con la ayuda de la nube. • Tareas planificadas: Actualización, Análisis completo, Análisis personalizado.
Protección con gestión desde la consola de administración para equipos móviles con sistemas operativos Android, mínimo con los módulos: • Antivirus de Archivos. • Control de aplicaciones. • Seguridad con la ayuda de la nube. • Protección contra adware y autodialers. • Antirrobo (Localización - SIM). • Control WEB. • Control Wi-Fi - cámaras - Bluetooth. • Tareas planificadas: Actualización, Análisis.
Cualquiera de las 3400 licencias para Endpoint (PC, Portátiles, servidores) podrá ser usada para protección Endpoint para Windows, protección Endpoint para MAC, protección Endpoint para Linux, protección File Server para Windows Server o protección para equipos móviles con Android, dados los constantes cambios entre sistemas operativos que se presentan en la Universidad por sus fines académicos e investigativos.
Protección con gestión desde la consola de administración para ambientes de virtualización XenApp 7.6 y XenDesktop 7.6. La protección debe estar basada en una máquina virtual que pueda ser desplegada en cada Hypervisor (Host) y que a su vez sea la encargada de realizar todas las tareas core de actualización y análisis de manera planificada para los escritorios y aplicaciones virtuales que están alojados en cada Hypervisor. Cada sesión de XenApp y XenDesktop debe tener un agente liviano que cuente mínimo con los siguientes módulos: • Antivirus de Archivos. • Seguridad con la ayuda de la nube. • Antivirus de correo. • Antivirus de Internet. • Antivirus para chat. • Firewall. • Prevención de intrusiones.
Protección con gestión desde la consola de administración para servidores virtuales que estén alojados bajo las plataformas VMware vSphere, Citrix XenServer, Microsoft Hyper-V y KVM. La protección debe estar basada en una máquina virtual que pueda ser desplegada en cada Hypervisor (Host) y que a su vez sea la encargada de realizar todas las tareas core de actualización y análisis

de manera planificada para las máquinas virtuales que están alojadas en cada Hypervisor. Cada máquina virtual debe tener un agente liviano que cuente mínimo con los siguientes módulos: • Antivirus de Archivos. • Control de actividad de aplicaciones. • Firewall. • Seguridad con la ayuda de la nube.
En el caso en que el fabricante modifique el nombre del conjunto de software o las funcionalidades de alguno de sus componentes o el tipo o niveles de licenciamiento, el proveedor estará en la obligación de hacer la gestión necesaria con la casa matriz, sin costo adicional para la Universidad, logrando que se mantenga el nivel de funcionalidad de los aplicativos descritos anteriormente.

8.4. SOPORTE

El soporte técnico corresponde a la responsabilidad del fabricante, mediante el proveedor, de dar respuesta y solución a la aparición de un nuevo software malintencionado (virus, spyware, phishing, pharming, etc.) en un plazo inferior a 24 horas.
El soporté técnico incluirá la actualización permanente de las herramientas y elementos que componen la solución, en términos de listas y definiciones de virus, así como de la lógica (motores de revisión – engines), tecnologías y técnicas utilizadas por el fabricante de la solución en todos y cada uno de los componentes que la constituyen.
El proveedor debe otorgar el Soporte técnico, incluyendo solución a problemas con la instalación, de todos los componentes de los productos adquiridos con el licenciamiento del presente documento, durante los 3 años de licenciamiento, asegurando que este servicio se preste en sitio, remoto, telefónico o correo electrónico, con personal certificados en el software.

8.5. ACTUALIZACIONES

Las actualizaciones deben tener dos (2) componentes:

UPGRADE: Corresponden a las nuevas versiones liberadas al mercado, durante el periodo de licenciamiento.
UPDATE: Corresponden a las definiciones de nuevos virus y motor de escaneo (scan engine), que se generen durante el periodo de licenciamiento.

8.6. EXPERIENCIA TÉCNICA.

El proveedor debe presentar certificación expedida por la casa matriz donde se indica que es canal Partner GOLD (o equivalente a la marca) o superior de los productos adquiridos con el licenciamiento, teniendo en cuenta que en orden ascendente los niveles de certificación son: Silver, Gold, Platinum (o equivalente a la marca)
El proponente debe anexar mínimo dos (2) certificaciones, contratos o facturas en original o fotocopia legible, de contratos ejecutados o en ejecución en Colombia, que permitan verificar que el objeto sea similar al del presente proceso en cuanto a software de seguridad para Endpoint. - La información solicitada debe incluir: • Nombre de la entidad contratante. • Objeto del contrato. • Valor del contrato (incluyendo adiciones). • Fecha de inicio y de finalización del contrato (incluyendo prórrogas). - No se aceptan auto certificaciones o auto facturas.
El proponente debe anexar mínimo dos (2) certificaciones, contratos o facturas en original o fotocopia legible, de contratos ejecutados o en ejecución en Colombia, que permitan verificar que el objeto sea similar al del presente proceso en cuanto a software de seguridad para ambientes de virtualización. - La información solicitada debe incluir: • Nombre de la entidad contratante. • Objeto del contrato. • Valor del contrato (incluyendo adiciones). • Fecha de inicio y de finalización del contrato (incluyendo prórrogas). - No se aceptan auto certificaciones o auto facturas.

9. LICENCIAMIENTO Y SERVICIOS.

Ítem	Descripción

1	3400 Licencias durante 3 años del software de seguridad para Endpoint (Windows, MAC, Linux y Android) y File Server para Windows, incluyendo actualizaciones (update y upgrade) y soporte 5x8.
2	200 Licencias durante 3 años del software de seguridad para ambientes de virtualización XenApp 7.6 y XenDesktop 7.6, incluyendo actualizaciones (update y upgrade) y soporte 5x8.
3	30 licencias durante 3 años del software de seguridad para servidores virtuales en VMware vSphere, Citrix XenServer, Microsoft Hyper-V y KVM, incluyendo actualizaciones (update y upgrade) y soporte 5x8.
4	Instalación y correcto funcionamiento en un tiempo inferior a 30 días calendario de los productos adquiridos en cada uno de los equipos y plataformas virtuales del parque informático de la Universidad hasta el total cubrimiento del licenciamiento adquirido: 3400 para Endpoint (Windows, MAC, Linux y Android), 30 servidores virtuales y 200 XenApp 7.6 y XenDesktop 7.6.

Tabla 1. Licenciamiento y servicios.

10. DURACIÓN DEL CONTRATO

El plazo para la ejecución del contrato, consistente en la entrega del licenciamiento total a nombre de la Universidad Distrital, la carga de las licencias en los equipos servidores, PC, portátiles, escritorios y aplicaciones virtuales y la transferencia del conocimiento; tendrá una duración de 30 días calendario.

El licenciamiento del software de seguridad será durante tres (3) años a partir del 28 de noviembre de 2017, periodo durante el cual el proveedor prestará los servicios de soporte, y actualizaciones.

11. VALOR Y FORMA DE PAGO

- El valor del contrato será el adjudicado, el cual incluirá el IVA correspondiente y demás impuestos nacionales y distritales.

- La Universidad pagará al contratista el valor del contrato en un solo contado previa entrega de:

- Registro del licenciamiento expedido por la casa matriz a nombre de la Universidad Distrital Francisco José de Caldas, el cual debe indicar el tiempo de licenciamiento y la cantidad de licencias.
- Presentación de la respectiva factura.
- Certificación de cumplido por parte de la supervisión del contrato.
- Registro de transferencia de conocimiento.
- Y demás documentos exigidos por la Universidad.

12. EVALUACIÓN DE LAS PROPUESTAS

Los criterios a evaluar serán los siguientes

CRITERIOS A EVALUAR	RESULTADO	OFICINA ENCARGADA
CAPACIDAD JURÍDICA		
VERIFICACIÓN CAPACIDAD FINANCIERA		
EVALUACIÓN TÉCNICA	CUMPLE O NO CUMPLE	RED UDNET

12.3. EVALUACIÓN TÉCNICA

Se realizará a partir de los siguientes componentes:

ÍTEM	COMPONENTE	UBICACIÓN EN LA PROPUESTA (N° PÁGINA)	CUMPLE / NO CUMPLE
1	El software contratado debe corresponder a las últimas versiones funcionales liberadas en el mercado durante el tiempo de licenciamiento contratado.		
2	Para la configuración, puesta en funcionamiento y carga de las nuevas licencias del software, el proveedor designará personal experto certificado en el software de seguridad para Endpoint (PC, Portátiles, servidores).		
3	Los productos para Endpoint (PC, Portátiles, servidores) de los sistemas Windows deben contar con Idioma español.		

4	Protección general en los equipos contra todo tipo de amenazas tales como: spam, spyware, adware, phising, ransomware, backdoor, riskware, rootkits, troyanos, keyloggers, virus, gusanos, dialers, hacking tolos, jokes, exploits, entre otros.		
5	Limpieza automática de virus, spyware y demás software malicioso.		
6	Actualización automática a través de Internet, tanto para los patrones de búsqueda como para el motor del sistema, con una periodicidad programable máxima de tres días; labor realizada en las consolas desde donde se replicará a los demás equipos a través de la red local.		
7	Consolas centralizadas de administración que permitan: • Realizar instalación del software antivirus en los diferentes equipos. • Crear grupos y subgrupos donde se creen las políticas de protección y actualización individualmente. • Generar como mínimo los siguientes reportes gráficos configurables para la gestión del software de seguridad y la respuesta a entes de control: Informe de bloqueos de aplicaciones, Informe de Filtrado Web, Informe de Errores, Informe de la Versión del software de seguridad, Informe de Licenciamiento del software de seguridad, Informe de Usuarios Infectados, Informe de Virus, Informe de Vulnerabilidades de software instalado en la estación de trabajo y/o servidor administrado, Informe de Actualización del software de seguridad, Informe de Software de Terceros Instalado, Inventario De Hardware completo (procesadores, memoria, adaptadores de video, discos de almacenamiento, adaptadores de audio, adaptadores de red, monitores, drives de CD/DVD), vulnerabilidades. • Detectar y reportar en qué equipo de la red se presenta el ingreso de virus. • Enviar mensajes emergentes a equipos individuales, listas de equipos, grupos o subgrupos. • Desinstalar remotamente software de terceros instalado en las máquinas clientes con sistema operativo Windows, usando elementos de remoción nativos del componente de administración Endpoint o incluyendo secuencias avanzadas de desinstalación. • Realizar instalación remota de software de terceros, a través de la plataforma de administración centralizada para que sea instalado en las estaciones de trabajo y/o servidores administrados con sistema operativo Windows.		

	• Identificar vulnerabilidades en productos de terceros instalados en las estaciones de trabajo y/o servidores administrados con sistema operativo Windows. • Realizar inventario de hardware y de software de todas las máquinas clientes con la posibilidad de registro de dispositivos (ej.: router, switch, proyector, accesorio, etc.), informando fecha de compra, ubicación, serial, número de identificación, entre otros.		
8	El proveedor realizará jornadas de transferencia de conocimiento al personal de soporte y plataformas de las diferentes sedes de la Universidad Distrital Francisco José de Caldas, relacionadas con la operación, manejo básico y adecuado del software de seguridad para el parque computacional. Los temas y cronograma se coordinarán con el supervisor y personal técnico de UDNET al inicio de la ejecución del contrato.		
9	El proveedor ofrecerá a los estudiantes, docentes y administrativos de la universidad, licencias versión hogar con un descuento de al menos el 50% sobre el valor comercial durante los 3 años de duración del contrato, las cuales serán adquiridas mediante un Botón de Pago en la página WEB del proveedor.		
10	El proveedor será el responsable de la instalación y correcto funcionamiento en un tiempo inferior a 30 días calendario de los productos adquiridos en cada uno de los equipos y plataformas virtuales del parque informático de la Universidad hasta el total cubrimiento del licenciamiento adquirido: 3400 para Endpoint (PC, Portátiles, servidores), 30 servidores virtuales y 200 XenApp 7.6 y XenDesktop 7.6.		
11	Protección Endpoint con gestión desde la consola de administración para equipos de cómputo con sistemas operativos Windows 7, Windows 8, Windows 8.1, Windows 10 o nuevas versiones de Sistemas Operativos Microsoft® para PC y Portátiles, mínimo con los módulos: • Control de inicio de aplicaciones. • Control de actividad de aplicaciones. • Control de vulnerabilidades. • Control de dispositivos. • Control WEB. • Antivirus de Archivos. • Antivirus de correo. • Antivirus de Internet. • Antivirus para chat. • Firewall. • Prevención de intrusiones. • Guardián del sistema. • Seguridad con la ayuda de la nube. • Tareas planificadas: Actualización, Análisis completo, Análisis de áreas críticas, Análisis personalizado.		

12	Protección Endpoint con gestión desde la consola de administración para equipos de cómputo con sistemas operativos MAC (para PC, Portátiles o Servidores), mínimo con los módulos: • Antivirus de Archivos. • Antivirus de internet. • Prevención de intrusiones. • Seguridad con la ayuda de la nube. • Tareas planificadas: Actualización, Análisis completo, Análisis personalizado.		
13	Protección Endpoint con gestión desde la consola de administración para equipos de cómputo con sistemas operativos Linux (para PC, Portátiles o Servidores), mínimo con los módulos: • Antivirus de Archivos. • Seguridad con la ayuda de la nube. • Tareas planificadas: Actualización, Análisis completo, Análisis personalizado.		
14	Protección File Server con gestión desde la consola de administración para equipos de cómputo con sistemas operativos tipo servidor: Windows 2008 R2, Windows 2012 R2 o cualquier otra nueva versión de Sistemas Operativos de Microsoft® para servidor, mínimo con los módulos: • Antivirus de Archivos. • Anti encriptación. • Seguridad con la ayuda de la nube. • Tareas planificadas: Actualización, Análisis completo, Análisis personalizado.		
15	Protección con gestión desde la consola de administración para equipos móviles con sistemas operativos Android, mínimo con los módulos: • Antivirus de Archivos. • Control de aplicaciones. • Seguridad con la ayuda de la nube. • Protección contra adware y autodialers. • Antirrobo (Localización - SIM). • Control WEB. • Control Wi-Fi - cámaras - Bluetooth. • Tareas planificadas: Actualización, Análisis.		
16	Cualquiera de las 3400 licencias para Endpoint (PC, Portátiles, servidores) podrá ser usada para protección Endpoint para Windows, protección Endpoint para MAC, protección Endpoint para Linux, protección File Server para Windows Server o protección para equipos móviles con Android, dados los constantes cambios entre sistemas operativos que se presentan en la Universidad por sus fines académicos e investigativos.		
17	Protección con gestión desde la consola de administración para ambientes de virtualización XenApp 7.6 y XenDesktop 7.6. La protección debe estar basada en una máquina virtual que pueda ser desplegada en cada		

	Hypervisor (Host) y que a su vez sea la encargada de realizar todas las tareas core de actualización y análisis de manera planificada para los escritorios y aplicaciones virtuales que están alojados en cada Hypervisor. Cada sesión de XenApp y XenDesktop debe tener un agente liviano que cuente mínimo con los siguientes módulos: • Antivirus de Archivos. • Seguridad con la ayuda de la nube. • Antivirus de correo. • Antivirus de Internet. • Antivirus para chat. • Firewall. • Prevención de intrusiones.		
18	Protección con gestión desde la consola de administración para servidores virtuales que estén alojados bajo las plataformas VMware vSphere, Citrix XenServer, Microsoft Hyper-V y KVM. La protección debe estar basada en una máquina virtual que pueda ser desplegada en cada Hypervisor (Host) y que a su vez sea la encargada de realizar todas las tareas core de actualización y análisis de manera planificada para las máquinas virtuales que están alojadas en cada Hypervisor. Cada máquina virtual debe tener un agente liviano que cuente mínimo con los siguientes módulos: • Antivirus de Archivos. • Control de actividad de aplicaciones. • Firewall. • Seguridad con la ayuda de la nube.		
19	En el caso en que el fabricante modifique el nombre del conjunto de software o las funcionalidades de alguno de sus componentes o el tipo o niveles de licenciamiento, el proveedor estará en la obligación de hacer la gestión necesaria con la casa matriz, sin costo adicional para la Universidad, logrando que se mantenga el nivel de funcionalidad de los aplicativos descritos anteriormente.		
20	El soporte técnico corresponde a la responsabilidad del fabricante, mediante el proveedor, de dar respuesta y solución a la aparición de un nuevo software malintencionado (virus, spyware, phishing, pharming, etc.) en un plazo inferior a 24 horas.		
21	El soporté técnico incluirá la actualización permanente de las herramientas y elementos que componen la solución, en términos de listas y definiciones de virus, así como de la lógica (motores de revisión – engines), tecnologías y técnicas utilizadas por el fabricante de la solución en todos y cada uno de los componentes que la constituyen.		

22	El proveedor debe otorgar el Soporte técnico, incluyendo solución a problemas con la instalación, de todos los componentes de los productos adquiridos con el licenciamiento del presente documento, durante los 3 años de licenciamiento, asegurando que este servicio se preste en sitio, remoto, telefónico o correo electrónico, con personal certificados en el software.		
23	Actualizaciones UPGRADE: Corresponden a las nuevas versiones liberadas al mercado, durante el periodo de licenciamiento.		
24	Actualizaciones UPDATE: Corresponden a las definiciones de nuevos virus y motor de escaneo (scan engine), que se generen durante el periodo de licenciamiento.		
25	El proveedor debe presentar certificación expedida por la casa matriz donde se indica que es canal Partner GOLD (o equivalente a la marca) o superior de los productos adquiridos con el licenciamiento, teniendo en cuenta que en orden ascendente los niveles de certificación son: Silver, Gold, Platinum (o equivalente a la marca)		
26	El proponente debe anexar mínimo dos (2) certificaciones, contratos o facturas en original o fotocopia legible, de contratos ejecutados o en ejecución en Colombia, que permitan verificar que el objeto sea similar al del presente proceso en cuanto a software de seguridad para Endpoint. - La información solicitada debe incluir: o Nombre de la entidad contratante. o Objeto del contrato. o Valor del contrato (incluyendo adiciones). o Fecha de inicio y de finalización del contrato (incluyendo prórrogas). - No se aceptan auto certificaciones o auto facturas.		
27	El proponente debe anexar mínimo dos (2) certificaciones, contratos o facturas en original o fotocopia legible, de contratos ejecutados o en ejecución en Colombia, que permitan verificar que el objeto sea similar al del presente proceso en cuanto a software de seguridad para ambientes de virtualización. - La información solicitada debe incluir: o Nombre de la entidad contratante. o Objeto del contrato. o Valor del contrato (incluyendo adiciones). o Fecha de inicio y de finalización del contrato (incluyendo prórrogas). - No se aceptan auto certificaciones o auto facturas.		

13. OFERTA ECONÓMICA

Ítem	Productos	VALOR (SIN IVA)	% IVA	VALOR (CON IVA)
1	3400 Licencias durante 3 años del software de seguridad para Endpoint (Windows, MAC, Linux y Android) y File Server para Windows, incluyendo actualizaciones (update y upgrade) y soporte 5x8.			
2	200 Licencias durante 3 años del software de seguridad para ambientes de virtualización XenApp 7.6 y XenDesktop 7.6, incluyendo actualizaciones (update y upgrade) y soporte 5x8.			
3	30 licencias durante 3 años del software de seguridad para servidores virtuales en VMware vSphere, Citrix XenServer, Microsoft Hyper-V y KVM, incluyendo actualizaciones (update y upgrade) y soporte 5x8.			
4	Instalación y correcto funcionamiento en un tiempo inferior a 30 días calendario de los productos adquiridos en cada uno de los equipos y plataformas virtuales del parque informático de la Universidad hasta el total cubrimiento del licenciamiento adquirido: 3400 para Endpoint (Windows, MAC, Linux y Android), 30 servidores virtuales y 200 XenApp 7.6 y XenDesktop 7.6.			
			TOTAL:	

14. GLOSARIO

- Endpoint: Equipo cliente o servidor con sistema operativo conectado a la infraestructura de red de la Universidad.
- Actualizaciones update: conjunto de parches que mejoran o corrigen fallos de una versión especifica de un conjunto de software.
- Actualizaciones upgrade: versión superior y mejorada de un conjunto de software.
- Malware: conjunto de software que aprovecha las vulnerabilidades del software o sus usuarios con fines malintencionados.
- Confidencialidad: Característica de la seguridad de la información que tiene como fin dar acceso exclusivamente a los sistemas o personas que estén autorizados.

- Disponibilidad: Característica de la seguridad de la información de encontrarse a disposición en el momento que se requiera de los sistemas o personas que tienen acceso a ella.
- Integridad: Característica de la seguridad de la información que busca preservar los datos libres de modificaciones no autorizadas.
- Plataforma virtual: Conjunto de software que simula a un equipo de cómputo físico en todas sus características, con ventajas como el mayor aprovechamiento de los recursos de procesamiento y almacenamiento, una tolerancia a fallos mayor y una gestión de los recursos más sencilla.
- File server: Equipo servidor con sistema operativo que tiene como fin el almacenamiento de información corporativa.